ISACA® (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Contact the ISACA Bookstore
E-mail: bookstore@isaca.org
Tel: +1.847.660.5650
Fax: +1.847.253.1443

CRISC™ Exam Prep Materials

**NEW!**

**CRISC™ Review Questions, Answers & Explanations Database—12-Month Subscription**
by ISACA

The CRISC™ Practice Question Database is a comprehensive 500-question pool of items that contains the questions from the CRISC™ Review Questions, Answers & Explanations Manual, 4th Edition. The database is available via the web, allowing CRISC candidates to log in at home, at work or anywhere they have Internet connectivity. The database is MAC and Windows compatible.

Exam candidates can take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing CRISC candidates to identify their strengths and weaknesses and focus their study efforts accordingly.

Other features provide the ability to select sample exams by specific job practice domain, view questions that were previously answered incorrectly and vary the length of study sessions, giving candidates the ability to customize their study approach to fit their needs.

After purchase, access this course by visiting your MyISACA page and clicking CRISC™ Question Database button.

Member: US $185.00
Non-member: US $225.00
Product Code: XMXCR14-12M

**NEW!**

**CRISC™ Review Questions, Answers & Explanations Database—6-Month Extension**
by ISACA

The CRISC™ Questions, Answers & Explanations Database—6-Month Extension can only be purchased as an extension to the CRISC Questions, Answers & Explanations Database—12-Month Subscription.

Member: US $85.00
Non-member: US $115.00
Product Code: XMXCR14-EXT180

**NEW!**

by ISACA

The CRISC™ Review Manual, 6th Edition is a comprehensive reference guide designed to help individuals prepare for the CRISC exam and understand IT-related business risk management roles and responsibilities. The manual has been enhanced over the past editions and represents the most current, comprehensive, peer-reviewed IT-related business risk management resource available worldwide.

The 6th edition manual is organized to assist candidates in understanding essential concepts and studying the following job practice areas:

- IT Risk Identification
- IT Risk Assessment
- Risk Response and Mitigation
- Risk and Control Monitoring and Reporting

The CRISC™ Review Manual, 6th Edition offers an easy-to-navigate format. Each of the book’s four chapters has been divided into two sections for focused study. Section one of each chapter contains:

- Definitions and objectives for the four areas
- Task and knowledge statements
- Self-assessment questions, answers and explanations
- Suggested resources for further study

Section two of each chapter consists of reference material and content that support the knowledge statements. The material enhances CRISC candidates’ knowledge and/or understanding when preparing for the CRISC certification exam. Also included are definitions of terms most commonly found on the exam.

Member: US $85.00
Non-member: US $115.00
Product Code: CRR6ED

Available in Spanish
Product Code: CRR6EDS

3701 Algonquin Road | Suite 1010
Rolling Meadows, IL 60008 | USA
P: +1.847.253.1545
F: +1.847.253.1443
E: info@isaca.org
isaca.org

Order online at isaca.org/bookstore
by ISACA

The CRISC™ Review Questions, Answers & Explanations Manual, 4th Edition is designed to familiarize candidates with the question types and topics featured in the CRISC exam.


Many questions have been revised or completely rewritten to be more representative of the CRISC exam question format, and/or to provide further clarity or explanation of the correct answer. These questions are not actual exam items, but are intended to provide CRISC candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam.

To help candidates maximize—and customize—study efforts, questions are presented in the following two ways:

• Sorted by job practice area—Questions, answers and explanations are sorted by the CRISC job practice areas. This allows the CRISC candidate to refer to questions that focus on a particular area as well as to evaluate comprehension of the topics covered within each practice area.

• Scrambled as a sample 150-question exam—The questions are arranged to represent a full-length CRISC exam, with questions chosen in the same percentages as the current CRISC job practice areas. Candidates are urged to use this sample test to simulate an actual exam, but also to determine their strengths and weaknesses in order to identify areas that require further study. Answer sheets and an answer/reference key for the sample exam are also included. All sample test questions have been cross-referenced to the questions sorted by practice area, making it convenient for the user to refer back to the explanations of the correct answers.

Member: US $60.00
Non-member: US $80.00
Product Code: CRQ4ED
Available in Spanish
Product Code: CRQ4EDS

— URMILLA PERSAD, CISA, CISM, CRISC
IT Audit Manager, First Citizens Trinidad & Tobago
Port of Spain, Trinidad & Tobago
ISACA Member Since 2004

Becoming ISACA-certified doesn’t just say you’re well read or well connected. It announces that you have the expertise and insight to speak with authority. The credibility that it adds lets you create value for your enterprise. Your ISACA certifications are more than just credentials; they are platforms that can elevate your career.

CERTIFICATION EXAMS ARE HELD IN JUNE / SEPTEMBER / DECEMBER.
To learn more or register for an upcoming exam go to: www.isaca.org/certifications
**Risk Resources**

**COBIT® 5 for Risk**
by ISACA

Effectively managing IT risk helps drive better business performance by linking information and technology risk to the achievement of strategic enterprise objectives.

Risk is generally defined as the combination of the probability and impact of an event and its consequence. COBIT® 5 for Risk defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

COBIT® 5 for Risk provides:
- Stakeholders with a better understanding of the current state and risk impact throughout the enterprise
- Guidance on how to manage the risk to levels, including an extensive set of measures
- Guidance on how to set up the appropriate risk culture for the enterprise
- Guidance on risk assessments that enable stakeholders to consider the cost of mitigation and the required resources against the loss exposure
- Opportunities to integrate IT risk management with enterprise risk
- Improved communication and understanding amongst all internal and external stakeholders

**Risk Scenarios Using COBIT® 5 for Risk**
by ISACA

Risk scenarios are recognized as powerful tools that help risk professionals to ask the right questions and prepare for the unexpected. Scenario analysis has become an important component of enterprise risk management.

COBIT® 5 for Risk Scenarios Using COBIT® 5 for Risk gives guidance on the development of IT-related risk scenarios, as well as providing guidance on how to use COBIT® 5 for Risk to solve for current business issues. The publication provides a high level overview of risk concepts, along with over 50 complete risk scenarios covering all 20 categories described in COBIT® 5 for Risk. Special guidance is given on how the COBIT® 5 enablers can help in risk management activities. The accompanying toolkit contains interactive risk scenario templates for each of the 20 categories.

**FISMA and the Risk Management Framework**
by Gantz, Philpott

If you are responsible for meeting federal information security requirements such as FISMA, this book is all you need to know to get a system authorized. Now in the first full revision of FISMA since its inception in 2002, a new wave of stronger security measures are now available through the efforts of the Department of Defense, Office of the Director of National Intelligence, Committee for National Security Systems and the National Institute of Standards and Technology.

Based on the new FISMA requirements for 2011 and beyond, this book catalogs the processes, procedures and specific security recommendations underlying the new Risk Management Framework. Written by an experienced FISMA practitioner, this book presents an effective system of information assurance, real-time risk monitoring and secure configurations for common operating systems.

**Advanced Persistent Threats: How to Manage the Risk to Your Business**
by ISACA

This book explains the nature of the security phenomenon known as the advanced persistent threat (APT). It provides helpful advice on how to assess the risk of an APT to the organization and recommends practical measures that can be taken to prevent, detect and respond to such an attack. In addition, it highlights key differences between the controls needed to counter the risk of an APT attack and those commonly used to mitigate everyday information security risk.

This book is designed primarily for security managers, IT managers, IT auditors and students studying for computer science or information security qualifications. It is written in clear, nontechnical language so it will also be of value to business managers and government officials responsible for valuable intellectual assets or critical services that might be the target of an APT attack.

**Business Continuity Management: Choosing to Survive**
by Abdullah Al Hour

Business Continuity Management: Choosing to Survive shows you how to systematically prepare your business, not only for the unthinkable, but also for smaller incidents which, if left unattended, could well lead to major disasters.

A business continuity management (BCM) program is critical for every business today, and this book will enable you to develop and implement yours to maximum effect.

An effective BCM program will have a positive impact on your business, not only enabling you to carry on ‘business as usual’ in the event of an incident, but also in its day-to-day running. You will realize:
- Improved organizational performance
- Improved stakeholder confidence (including shareholders, customers, supply chain)
- Competitive advantages
- Financial savings
- Increased profits

With specific reference to BS23201, ANSI/ASIS SPC.1-2009, ISO27031 and ISO/IEC 24762, this up-to-date, practical resource will guide you through all the elements of a BCM program, plans and implementations. It covers all the critical elements of your program, from people and premises to technology and facilities management.

**Order online at isaca.org/bookstore**
CIO Best Practices: Enabling Strategic Value with Information Technology, 2nd Edition
by Joseph F. Shanari, Gary Colvin, Karl D. Schubert, Michael H. Hugos

Anyone working in information technology today feels the opportunities for creating and enabling lasting value. The CIO helps define those opportunities and turn them into realities. Now in a second edition, CIO Best Practices is an essential guide offering real-world practices used by CIOs and other IT specialists who have successfully mastered the blend of business and IT responsibilities. For anyone who wants to achieve better returns on their IT investments, CIO Best Practices, Second Edition presents the leadership skills and competencies required of a CIO addressing comprehensive enterprise strategic frameworks to fully leverage IT resources.

This practical resource provides best practice guidance on the key responsibilities of the CIOs and their indispensable executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries. It is the most definitive and important executive leadership role in modern enterprises of all sizes and industries.

by Douglas Landoll


Trusted to assess security for leading organizations and government agencies, including the CIA, NSA, and NATO, Douglas Landoll unveils the little-known tips, tricks, and techniques used by savvy security professionals in the field. He details time-tested methods to help you:

- Better negotiate the scope and rigor of security assessments
- Effectively interface with security assessment teams
- Gain an improved understanding of final report recommendations
- Deliver insightful comments on draft reports

The book includes charts, checklists, and sample reports to help you speed up the data gathering, analysis, and document development process. Walking you through the process of conducting an effective security assessment, it provides the tools and up-to-date understanding you need to select the security measures best suited to your organization.

Fraud Prevention and Detection: Warning Signs and the Red Flag Systems
by Rodney T. Stamler, Hans J. Marschendorf, Mario Possamai

Lessons can be learned from major fraud cases. Whether the victim is a company, public agency, nonprofit, foundation, or charity, there is a high likelihood that many of these frauds could have been prevented or detected sooner if early Red Flag warning signs had been identified and acted upon. Fraud Prevention and Detection: Warning Signs and the Red Flag Systems will enable officers and directors, internal and external stakeholders, as well as outside analysts to protect themselves and their organizations against fraud by effectively detecting, analyzing, and acting on early Red Flag warning signs. Based on an empirically tested strategy, the Red Flag System reflects the authors’ more than 100 years combined experience in the investigation of fraud in high-profile, global cases in North America, Africa, Europe, and the Far East.

This book’s no-nonsense approach empowers those charged with protecting organizations to stop these frauds before the organization’s livelihood is jeopardized or to mitigate damage when fraud has occurred.

Risk Assessment and Decision Analysis with Bayesian Networks
by Norman Fenton and Martin Neil

Although many Bayesian Network (BN) applications are now in everyday use, BNs have not yet achieved mainstream penetration. Focusing on practical real-world problem solving and model building, as opposed to algorithms and theory, Risk Assessment and Decision Analysis with Bayesian Networks explains how to incorporate knowledge with data to develop and use (Bayesian) causal models of risk that provide powerful insights and better decision making.

The book first establishes the basics of probability, risk, and building and using BN models, then goes into the detailed applications. The underlying BN algorithms appear in appendices rather than the main text since there is no need to understand them to build and use BN models. Keeping the body of the text free of intimidating mathematics, the book provides pragmatic advice about model building to ensure models are built efficiently.
Information Technology Risk Management in Enterprise Environments
by Jake Kouns and Daniel Minoli

This book provides a comprehensive review of industry approaches, practices and standards on how to handle the ever-increasing risks to organizations’ business-critical assets. Through a practical approach, this book explores key topics that enable readers to uncover and remediate potential infractions. The authors present an effective risk management program by providing:

- An overview of risk assessment, mitigation and management approaches and methodologies
- Processes for developing a repeatable program for technological issues and human resources
- Definitions of key concepts and security standards in the area of risk management
- Analytical techniques for assessing the amount of risk and the benefit of risk remediation
- Information on the development and implementation of a risk management team

Member: US $104.00
Non-member: US $114.00
Product Code: 84WRM

Fraud Analysis Techniques Using ACL
by David Coderre

Fraud Analysis Techniques Using ACL offers auditors and investigators:

- Authoritative guidance on the use of computer-assisted audit tools and techniques in fraud detection
- A CD-ROM containing an educational version of ACL
- An accompanying CD-ROM containing a thorough fraud tool kit with two sets of customizable scripts to serve your specific audit needs
- Case studies and sample data files that you can use to try out the tests
- Step-by-step instructions on how to run the tests
- A self-study course on ACL script development with exercises, data files and suggested answers

The tool kit also contains 12 utility scripts and a self-study course on ACL scripting which, includes exercises, data files and proposed answers. Filled with screen shots, flow charts, example data files descriptive commentary highlighting explaining each step, and case studies offering real-world examples of how the scripts can be used to search for fraud it is the only tool kit you will need to harness the power of ACL to spot fraud.

Member: US $211.00
Non-member: US $221.00
Product Code: 82WACL

LIKE BOOKS?
Consider the real value of an ISACA membership.

Over 575 FREE e-Book downloads available for ISACA members, including:

- Advanced Persistent Threats: How to Manage the Risk to your Business
- Risk Scenarios: Using COBIT® 5 for Risk
- And hundreds MORE!

Need CPEs? For less than $200 annually*, membership also offers over 70 FREE CPE hours each year—Well more than the required 40 annual hours needed to maintain your certification at an unbeatable price.

*Contingent on regional chapter dues. More than 90% of all ISACA memberships are under $200.