ISACA CYBERSECURITY AUDIT & RISK PROGRAM

ISACA®

Amman Chapter

IT SECURITY C&T

www.itsecuirtyct.com

training@itsecurityct.com

Table of Contents

Content
About ISACA Amman Chapter
About IT Security C&T
About the Program Event
Who Should Enroll
Learning Path
Instructor Bio
Cyber Security Audit Catalogue
CISA Catalogue
CRISC Catalogue
Program Pricing

IT SECURITY C&T

ISACA Amman Chapter

ISACA
Amman Chapter

About ISACA Amman Chapter

ISACA Amman Chapter was formally established in Q4 2018. The planned strategic position for ISACA Amman Chapter to be a leading non-profit association in the Jordanian market in information assurance fields covering IS audit, information security, information systems control and Governance of Enterprise IT.

The chapter aims to deliver regular educational events/sessions and to equip the market with the needed skills in the aforementioned fields. Such umbrella would unite all related efforts, serve the Jordanian market to face the current IT challenges, and support organizational efforts in digital transformation while keeping an eye on information systems controls and governance.

IT SECURITY C&T

About IT Security C&T

IT Security C&T was incorporated with the vision to be the leading information security and technology risk management resource center in the Middle East and North African Region. We are specialized in the delivery of affordable high-end information security and technology risk management services that are hard to find within the region at the same cost.

This team is formed by leading specialists in their field, with experience track records of 10 - 20 years serving at key locations within the MENA region and around the world. The mission is to use this accumulated experience, knowledge, and skills, to develop highly trained bilingual consultants and trainers who are able to deliver world-class services to clients within the region.
Company Services: Solutions, Training and Consulting

IT SECURITY C&T

Our Services

- Cyber Security Solutions
- Strategic Security Services
- Technical Consulting Services
- Managed Security Services
- Cyber Security Academy

Cyber SECURITY SOLUTIONS

TECHNICAL CONSULTATING SERVICES

STRATEGIC SECURITY SERVICES

MANAGED SECURITY SERVICES

CYBER SECURITY ACADEMY

IT SECURITY C&T

SAMPLE CUSTOMERS

About ISACA Cybersecurity Audit and Risk Program

IT SECURITY C&T

ISACA Amman Chapter

In Cooperation between IT Security C&T and ISACA Amman Chapter

Start Date: July 23rd, 2022

End Date: August 4th, 2022

Program Hours: from 9:00 am – 5:00 pm Jordan Time.

"Full Day Training"

Attendance Options: Onsite / Online

Instructor: Tichaona Zororo

Location: Kempinski– Amman, Jordan

Coffee & Lunch Served to Attendees

Learning Path

Cybersecurity Audit

Cyber Security Audit Certificate

2 Days

From July 23rd to July 24th, 2022

CISA

Certified Information Systems Auditor (CISA)

4 Days

From July 25th to July 28th, 2022

CRISC

Certified in Risk and Information Systems Control (CRISC)

4 Days

From August 1st to August 4th, 2022

Who Should Enroll The Program

IT/IS Auditors

IT Consultants

Security and Risk Professionals

Project Managers

IT Audit Managers

Business Analysts

Program Instructor:
Tichaona Zororo

Certified in

CGEIT, CRISC, CDPSE, CRMA, CISM, CISA
and COBIT Certified Assessor

Mr. Zororo is Director, Digital Transformation & Innovation Advisory, with EGIT | Enterprise Governance of IT (Pty) Ltd., an Information & Technology [IT] Advisory firm based in South Africa, Namibia, Zambia and Zimbabwe focusing on advising Boards of Directors, Senior Business Leaders, IT Executives and Management on Modernisation, Digital Transformation and Innovation Advisory,
Cybersecurity, IT Auditing, Social Media Governance & Auditing and IT Governance.

Tichaona is credited for being the first COBIT Certified Assessor in Southern Africa, the first African and person from Africa to sit on the ISACA Board of Directors and to chair its Audit and Risk Committee and establish an internal audit function for ISACA. An accredited COBIT and ISACA Certification qualifications trainer.

Program Instructor: **Tichaona Zororo**

Tichaona is an advisor to several Boards of Directors, IT and Business Leaders on Digital and Digital Transformation, Strategy, Governance of Enterprise IT, IT, Cybersecurity, IT Risk and IT Auditing. He is a member of the Council [Board of Directors] of the Vaal University of Technology, a Member of its Audit & Risk Committee and Governance Committees.

He is a sought-after Digital Transformation & Innovation Governance Advisor, Thought Leader, Trainer, Speaker and Published Author in IT Governance, COBIT, IT Auditing, Social Media, IT Modernisation, Cloud Computing, Predictive Analytics, Artificial Intelligence and Cybersecurity and a Researcher of Digital and Digital Transformation Strategies.

Tichaona Zororo is Certified in the Governance of Enterprise IT [CGEIT], Certified in Risk and Information Systems Control [CRISC], Certified Data Privacy Solutions Engineer [CDPSE], Certified in Risk Management Assurance [CRMA], Certified Information Security Manager [CISM], Certified Internal Auditor [CIA], Certified Information Systems Auditor [CISA] and COBIT Certified Assessor. He Holds a BSc. Honours in Information Systems [MSU], A Post Graduate Diploma in Computer Auditing [Wits], an Executive Education Certificate in Digital Disruption, Digital Transformation Strategies [Judge Business School, University of Cambridge] and several certificates in business and IT.

A renowned COBIT Subject Matter Expert and Advisor, Tichaona is credited for being the first COBIT Certified Assessor in Southern Africa, the first African and person from Africa to sit on the ISACA Board of Directors [2016 - 2020] and to chair its Audit and Risk Committee [2016 – 2019] and establish aninternal audit function for ISACA. An accredited COBIT and ISACA Certification qualifications trainer, Tichaona Zororo participated in the development and review of numerous COBIT publications and ISACA research papers on Big Data, Cloud Computing, BYOD and Outsourced IT Services to mention but a few.

Cybersecurity Audit

Cyber Security Audit Certificate

From July 23rd to July 24th, 2022

Duration: 2 Days

Course Overview

The impact of cybercrime on business is enormous. Mitigating these risks and lowering their impact on business is essential.

This course provides the framework to align cybersecurity strategies with the organizational goal to protect the organization's privacy and intellectual property. The course will help delegates learn about their role and responsibilities, better understand the cybersecurity policy and standards, assess the threats with the help of vulnerability management tools and manage enterprise identity and asset and respond quickly to a security incident.

Cybersecurity Audit

Cyber Security Audit Certificate

Course Objectives

After completing this course, you will be able to:

- Identify roles and responsibilities of an auditor
- Define basic cybersecurity principles
- Gain an understanding of security frameworks to identify best practices
- Identify cyber and legal regulatory requirements to aid in compliance assessments
- Perform a risk assessment
- Define threat and vulnerability management

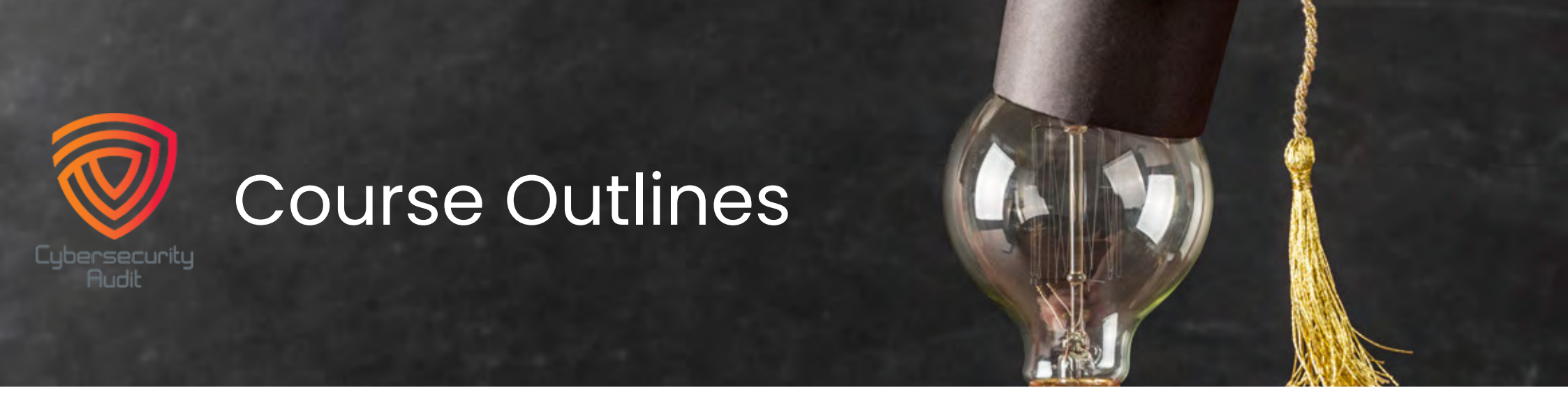
Cybersecurity Audit

Cyber Security Audit Certificate

Course Objectives

After completing this course, you will be able to:

- Enhance asset, configuration, change and patch management practices
- Assess network security from security architecture to traffic analysis to segmentation to data loss prevention
- Identify application security controls
- Distinguish between firewall and network security technologies
- Identify cloud strategies and controls
- Identify the benefits and risks of containerization



Course Outlines

Audit's Role in Cybersecurity

- Cybersecurity and cyberspace
- Overall control requirements
- Three lines of defense
- The role of audit in cybersecurity assessment

Governance

- Cybersecurity risks
- Security frameworks and standards
- Areas of cybersecurity governance control
- Threat actors and threat events
- Define key performance indicators (KPI) for measurement of operational effectiveness of cybersecurity controls

Operations

- Cybersecurity operational processes and controls.
- Security operations center (SOC), threat intelligence and ISAC.
- Cybersecurity threat actors and advanced persistent threats (APTs)
- Attack vectors
- Control requirements to mitigate threats

Technology

- Risk and controls relating to specific information technologies that can impact protection of digital assets
- Difference between firewall and network security technologies
- Security weaknesses in cloud strategies and controls
- Benefits and risks of containerization

Cybersecurity Audit

Examination

Number of Questions	75 questions
Pass Mark	65% or 49/75
Test Location	Online Testing Remotely

Exam Description

Candidates explore concepts related to evaluating cybersecurity risk and auditing the cybersecurity controls for an organization and then demonstrate their understanding of the topics by achieving a passing score on the Cybersecurity Audit Certificate exam.

Number of Questions Per Area:

- 45% or 34/75 Cybersecurity Operations
- 30% or 22/75 Cybersecurity Technology Topics
- 20% or 15/75 Cybersecurity Governance
- 05% or 4/75 Cybersecurity and Audit’s Role

Cyber Information Systems Auditor (CISA)

From July 25th to July 28th, 2022

Duration: 4 Days

Course Overview

The CISA designation is a globally recognized certification for IS audit control, assurance and security professionals. Being CISA-certified showcases your audit experience, skills and knowledge, and demonstrates you are capable to assess vulnerabilities, report on compliance and institute controls within the enterprise.
Professionals strongly suggest that if you want to get into IS auditing or advance your IS auditing career, you should obtain a CISA.

Course Description

The CISA Examination Preparation Course is an intensive course that will cover some of the more challenging topics from the CISA job practice. Drill through sample exam items and practical application, ask your most pressing questions and get the answers to build your confidence as you prepare for exam day.

Cyber Information Systems Auditor (CISA)

Course Objectives

After completing this course, you will be able to:

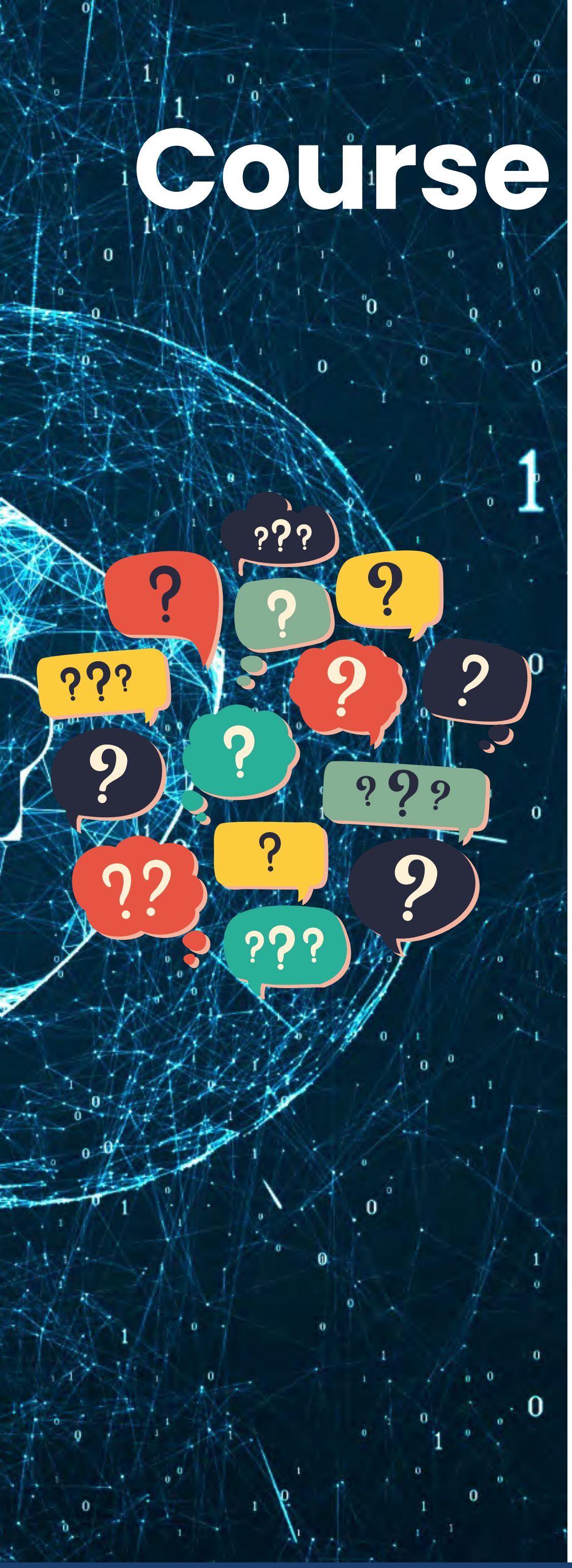
- Confirms your knowledge and experience
- Quantifies and markets your expertise
- Demonstrates that you have gained and maintained the level of knowledge required to meet the dynamic challenges of a modern enterprise
- Is globally recognized as the mark of excellence for the IS audit professional
- Combines the achievement of passing a comprehensive exam with recognition of work and educational experience, providing you with credibility in the marketplace

Cyber Information Systems Auditor (CISA)

Course Objectives

After completing this course, you will be able to:

- Increases your value to your organization
- Gives you a competitive advantage over peers when seeking job growth
- Helps you achieve a high professional standard through ISACA's requirements for continuing education and ethical conduct



Course Domains

The Process of Auditing Information Systems (21%)

Governance and Management of IT (17%)

Information Systems Acquisition, Development and Implementation (12%)

Information Systems Operations, Maintenance and Service Management (23%)

Protection of Information Assets (27%)

Certified Information Systems Auditor®
An ISACA® Certification

Course Outlines

Domain 1—The Process of Auditing Information Systems

A. Planning

- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments

B. Execution

- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques.

Course Outlines

Domain 2—Governance and Management of IT

A. IT Governance

- IT Governance and IT Strategy IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization

B. IT Management

- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT

Certified Information Systems Auditor®
An ISACA® Certification

Course Outlines

Domain 3—Information Systems Acquisition, Development, and Implementation

A. Information Systems Acquisition and Development

- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design

B. Information Systems Implementation

- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Con version
- Post-implementation Revie

Certified Information Systems Auditor®
An ISACA® Certification

Course Outlines

Domain 4—Information Systems Operations and Business Resilience

A. Information Systems Operations

- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management

B. Business Resilience

- Business Impact Analysis (BIA) System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)

Course Outlines

Domain 5—Protection of Information Assets

A. Information Systems Operations

-Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- dentity and Access Management
- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices

B. Security Event Management

- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics

Certified Information Systems Auditor®
An ISACA® Certification

Examination

Number of Questions	150 questions
Pass Mark	45% - 60% Scaled score of 450
Test Location	Testing Center

Exam Description

Candidates explore concepts related to evaluating cybersecurity risk and auditing the cybersecurity controls for an organization and then demonstrate their understanding of the topics by achieving a passing score on the Cybersecurity Audit Certificate exam.

Number of Questions Per Area:

- 21% The Process of Auditing Information Systems
- 17% Governance and Management of IT
- 12% Information Systems Acquisition, Development and Implementation
- 23% Information Systems Operations, Maintenance and Service Management
- 27% Protection of InformationAssets

Certified in Risk and Information Systems Control (CRISC)

From August 1st to August 4th, 2022

Duration: 4 Days

Course Overview

The CRISC course is an intensive, four-day review program to prepare individuals who are planning to sit for the Certified in Risk and Information System Controls (CRISC) exam. The course focuses on the key points covered in the CRISC Review Manual 6th Edition and includes class lectures, group discussions, exam practice and answer debriefs.

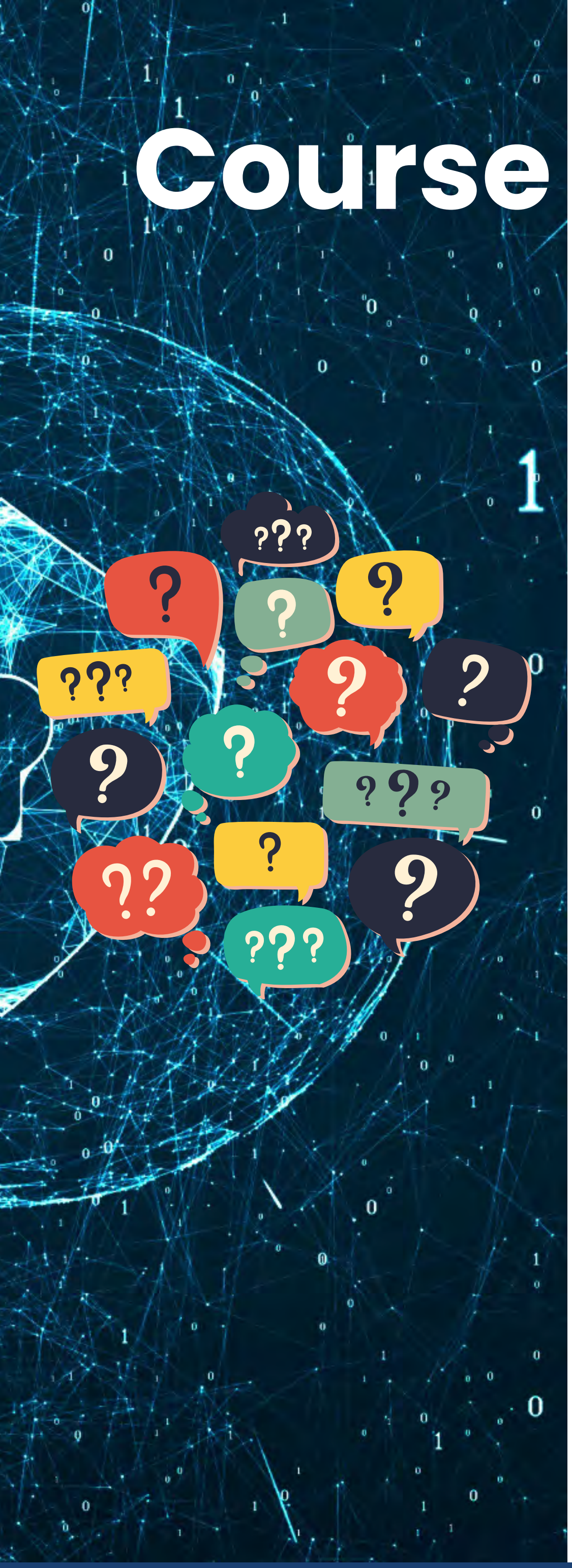
The course is intended for individuals with familiarity with and experience in IT and enterprise risk management.

Certified in Risk and Information Systems Control (CRISC)

Course Objectives

After completing this course, you will be able to:

- Identify risks
- Assess current and potential risks
- Respond and Mitigate risks
- Ensure risk and control monitoring as risk reporting
- An understanding of the format and structure of the CRISC certification exam
- A knowledge of the various topics and technical areas covered by the exam
- Practice with specific strategies, tips and techniques for taking and passing the exam



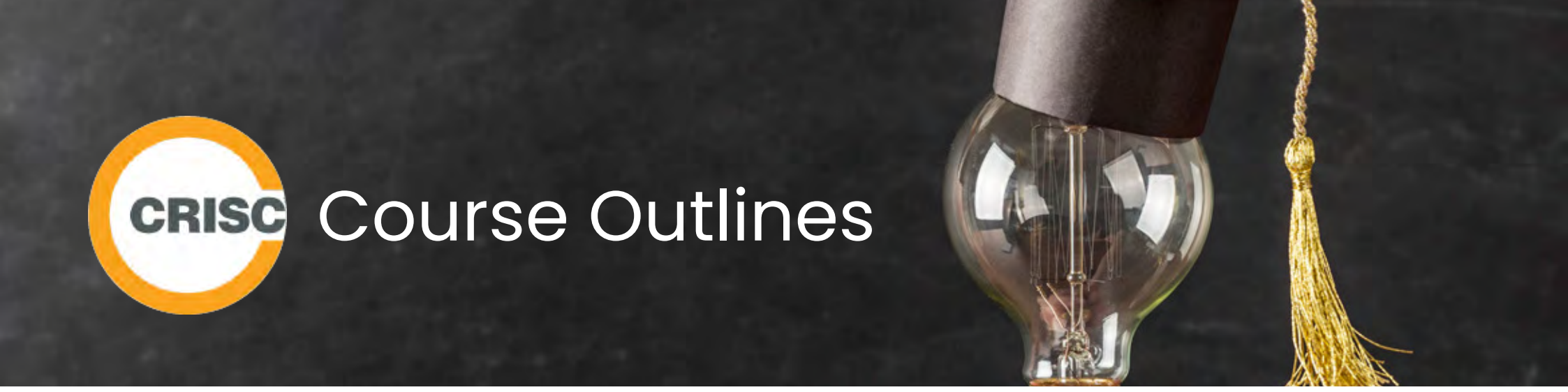
Course Domains

Governance (26%)

IT Risk Assessment (20%)

Risk Response and Mitigation (32%)

Information Technology and Security (22%)



CRISC Course Outlines

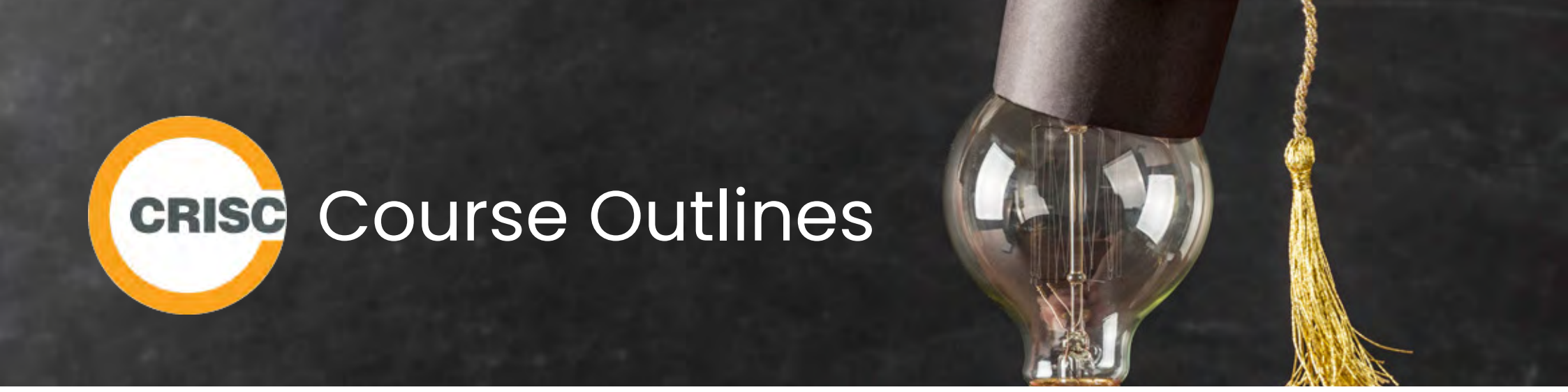
Domain 1 – Governance

A. Organizational Governance

- Organizational Strategy, Goals, and Objectives
- Organizational Structure, Roles, and Responsibilities
- Organizational Culture
- Policies and Standards
- Business Processes

B. Risk Governance

- Enterprise Risk Management and Risk Management Framework
- Three Lines of Defense
- Risk Profile
- Risk Appetite and Risk Tolerance
- Legal, Regulatory, and Contractual Requirements
- Professional Ethics of Risk Management



CRISC Course Outlines

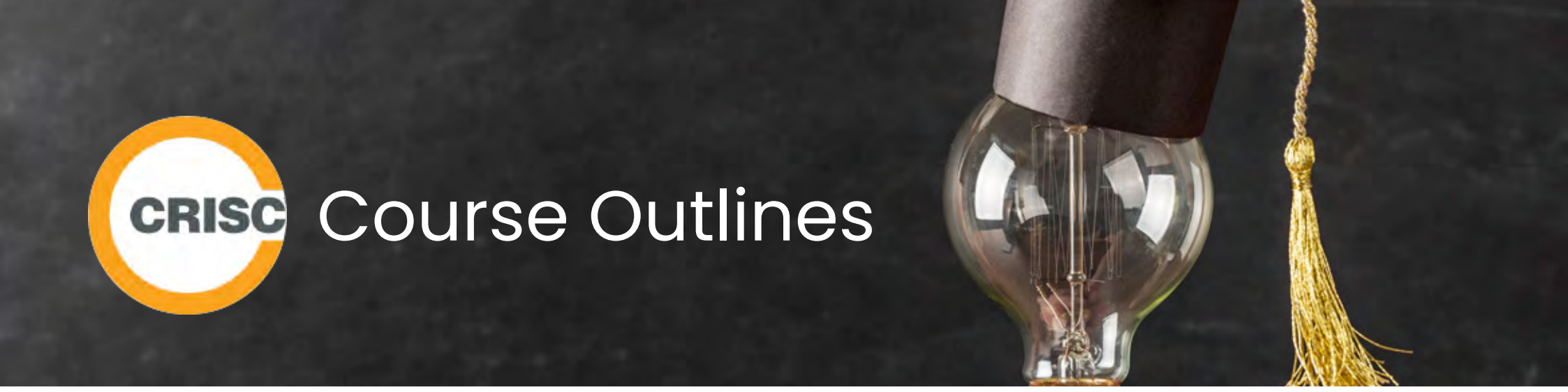
Domain 2 – IT Risk Assessment

A. IT Risk Identification

- Risk Events (e.g., contributing conditions, loss result)
- Threat Modelling and Threat Landscape
- Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
- Risk Scenario Development

B. IT Risk Analysis and Evaluation

- Risk Assessment Concepts, Standards, and Frameworks
- Risk Register
- Risk Analysis Methodologies
- Business Impact Analysis
- Inherent and Residual Risk



CRISC Course Outlines

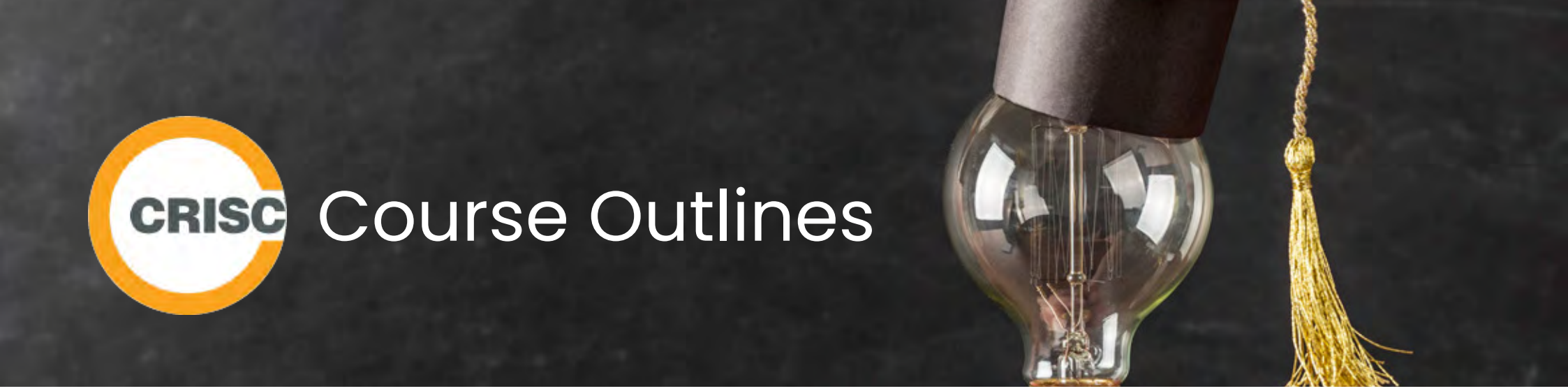
Domain 3 – Risk Response and Mitigation

A. Risk Response

- Risk Treatment / Risk Response Options
- Risk and Control Ownership
- Third-Party Risk Management
- ssue, Finding, and Exception Management
- Management of Emerging Risk

B. Control Design and Implementation

- Control Types, Standards, and Frameworks
- Control Design, Selection, and Analysis
- Control Implementation
- Control Testing and Effectiveness Evaluation



Domain 4 – Information Technology and Security

A. Information Technology Principles

- Enterprise Architecture
- IT Operations Management (e.g., change management, IT assets, problems, incidents)
- Project Management
- Disaster Recovery Management (DRM)
- Data Lifecycle Management
- System Development Life Cycle (SDLC)
- Emerging Technologies

B. Information Security Principles

- Information Security Concepts, Frameworks, and Standards
- Information Security Awareness Training
- Business Continuity Management
- Data Privacy and Data Protection Principles

CRISC

Examination

Number of Questions	150 questions
Pass Mark	200 - 800 Scaled score of 450
Test Location	Testing Center

Exam Description

Eligibility is established at the time of exam registration and is good for twelve (12) months (365 days). Exam registration and payment are required before you can schedule and take an exam. You will forfeit your fees if you do not schedule and take the exam during your 12-month eligibility period. No eligibility deferrals or extensions are allowed.

Number of Questions Per Area:

- 26% Governance
- 20% IT Risk Assessment
- 32% Risk Response and Mitigation
- 22% Information Technology and Security

PROGRAM PRICING

Course	Jordan & LAVANT Prices	
	Non-Member	ISACA Member
Full Program Price Per Attendee Course Duration: 10 Days July 23 –August 4, 2022	JOD 1,850.00	JOD 1,150.00
Cyber Security Audit Only Price Per Attendee Course Duration: 2 Days July 23 – July 24, 2022	JOD 600.00	JOD 400.00
CISA Course Only Price Per Attendee Course Duration: 4 Days July 25 – July 28, 2022	JOD 785.00	JOD 600.00
CRISC Course Only Price Per Attendee Course Duration: 4 Days August 1 – August 4, 2022	JOD 785.00	JOD 600.00

Our Presence

IT SECURITY C&T

IT Security Consulting & Training

AMMAN-JORDAN
IMex Building 37 ,Princess Rahma Bint Al Hassan ST.

+962 6 5535043

+962 79 196 3466

info@itsecurityct.com

training@Itsecurityct.com

www.itsecurityct.com