INFOSECTRAIN

CISM

Certified Information Security Manager

KEY FEATURES

- ISACA Premium Training Partner
- Access to the recorded sessions
- Certified & Experienced Trainers

ISACA ACCREDITED PARTNER CISA

Overview

The uniquely management-focused CISM certification promotes international security practices and recognizes the individual who manages designs, and oversees and assesses an enterprise's information security.The demand for skilled information security management professionals is on the rise, and the CISM certification is the globally accepted standard of achievement in this area.

Target Audience

- Security consultants and managers
- IT directors and managers
- Security auditors and architects
- Security systems engineers
- Chief Information Security Officers (CISOs)
- Information security managers
- IS/IT consultants
- Chief Compliance/Privacy/Risk Officers

Pre-Requisite

Submit verified evidence of a minimum of five years of information security work experience, with a minimum of three years of work experience in three or more job practice analysis areas of information security management. The work experience must be gained within the 10 years preceding the application date for certification or within 5 years from the exam's passing date.

The following security-related certifications and information systems management experience can be used to substitute the indicated amount of information security work experience.

TWO YEARS

- Certified Information Systems Auditor (CISA) in good standing
- Certified Information Systems Security Professional (CISSP) in good standing
- Post-graduate degree in information security or a related field (e.g., business administration, information systems, information assurance)

ONE YEAR

- One full year of information systems management experience
- One full year of general security management experience
- Skill-based security certifications (e.g., SANS Global Information Assurance Certification (GIAC), Microsoft Certified Systems Engineer (MCSE), CompTIA Security +, Disaster Recovery Institute Certified Business
- Continuity Professional (CBCP), ESL IT Security Manager)

Completion of an information security management program at an institution aligned with the Model Curriculum

Exam Information

Duration	4 hours
Number of Questions	150
Question format	Multiple Choice
Passing grade	450 out of 800
Languages available	English, Japanese, Korean, Spanish

Why Infosec Train?

- Certified & Experienced Instructor
- Flexible Schedule
- Access to the recorded sessions
- Post Training Support
- Tailor Made Training
- Telegram Discussion Group

Our Expert Instructors

"

Certified Security specialist having several years of experience in Information Security across all domains including application security, vulnerability assessment, ethical hacking, pen testing and IT risk and compliance and more

PRABH NAIR

CISSP I CCSP I CSSLP I CRISC I CISM I CISA I CGEIT

"

Rahul have 19+ years of experience in Information Technology industry with specialization in Information Security. Worked with 100+ clients across 25+ countries through various short-term and long-term assignments. Certified as CISSP, CISM and 10+ more certification

RAHUL

CISSP I CISM I CITP I CMGR I MCMI I MIET I MBCS

"

An IT leader with almost 2 decades of experience in multiple industries, I have conducted over 500 training sessions to over 10000+ Some of the courses that I have taught over the years: CISSP, CCSP, CISM, CISA, CGEIT, CCSK, CompTIA securitY+, cysA+

S. RAI

CISSP I CISM I CCSP I CISA I CASP I MCA I CGEIT I PMP

HAPPY LEARNERS FROM THE WORLD

Puneet Sharma

CISM | India

Trainer explained the key concepts and practiced sample questions as well which would really help us to complete our exam successfully. Important topics were discussed in detail.

Yaqoob Kath

CISM | Canada

The trainer covered many concepts apart from exam perspective which helped in gaining much knowledge.

Shefali Shetty

CISM | India

It was a great learning experience. Instructor is highly knowledgeable and connects well with class citing real life examples. The full team is very helpful and flexible. I recommend Infosectrain for anyone looking forward to take on CISM.

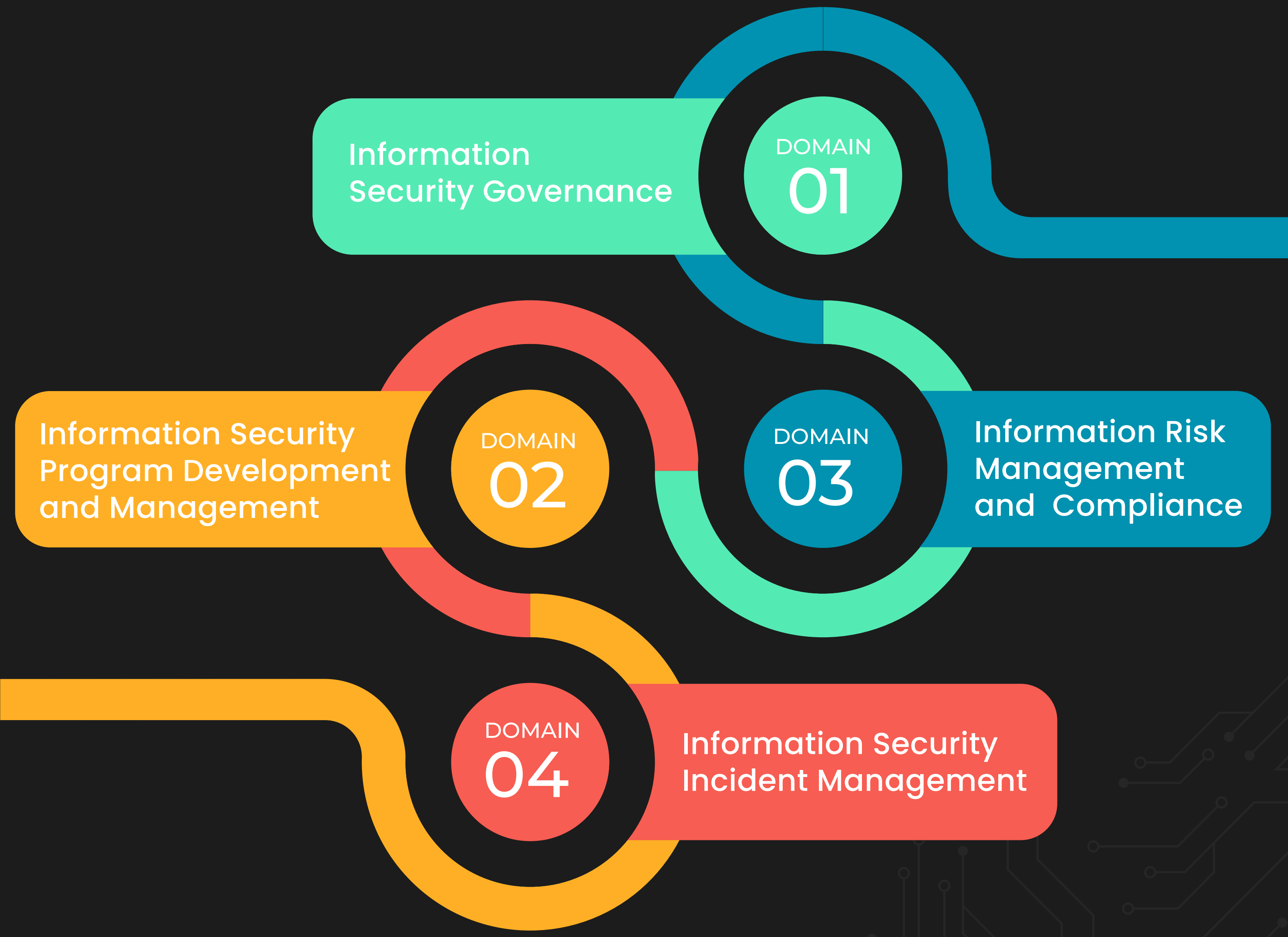
Ravi Prakash Basavaraja

CISM | India

The trainer was excellent in teaching the necessary concepts in the right way. The training will will give anyone a clear picture on the subject, as well as the tips required to face the certification exam.

CISM Course Outline

The four domains in CISM include



DOMAIN 01
Information Security Governance

DOMAIN 02
Information Security Program Development and Management

DOMAIN 03
Information Risk Management and Compliance

DOMAIN 04
Information Security Incident Management

Domain 1: Information Security Governance

TASK STATEMENTS

1.1 Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program.

1.2 Establish and/or maintain an information security governance framework to guide activities that support the information security strategy.

1.3 Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.

1.4 Establish and maintain information security policies to guide the development of standards, procedures and guidelines in alignment with enterprise goals and objectives.

1.5 Develop business cases to support investments in information security.

1.6 Identify internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) to ensure that these factors are continually addressed by the information security strategy.

1.7 Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.

1.8 Define, communicate, and monitor information security responsibilities throughout the organization (e.g., data owners, data custodians, end users, privileged or high-risk users) and lines of authority.

1.9 Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy.

KNOWLEDGE STATEMENTS

k1.1 Knowledge of techniques used to develop an information security strategy (e.g., SWOT [strengths, weaknesses, opportunities, threats] analysis, gap analysis, threat research)

k1.2 Knowledge of the relationship of information security to business goals, objectives, functions, processes and practices

k1.3 Knowledge of available information security governance frameworks

k1.4 Knowledge of globally recognized standards, frameworks and industry best practices related to information security governance and strategy development

k1.5 Knowledge of the fundamental concepts of governance and how they relate to information security

k1.6 Knowledge of methods to assess, plan, design and implement an information security governance framework

k1.7 Knowledge of methods to integrate information security governance into corporate governance

k1.8 Knowledge of contributing factors and parameters (e.g., organizational structure and culture, tone at the top, regulations) for information security policy development

k1.9 Knowledge of content in, and techniques to develop, business cases

k1.10 Knowledge of strategic budgetary planning and reporting methods

k1.11 Knowledge of the internal and external influences to the organization (e.g., emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) and how they impact the information security strategy

k1.12 Knowledge of key information needed to obtain commitment from senior leadership and support from other stakeholders (e.g., how information security supports organizational goals and objectives, criteria for determining successful implementation, business impact)

k1.13 Knowledge of methods and considerations for communicating with senior leadership and other stakeholders (e.g., organizational culture, channels of communication, highlighting essential aspects of information security) k1.14 Knowledge of roles and responsibilities of the information security manager

k1.15 Knowledge of organizational structures, lines of authority and escalation points

k1.16 Knowledge of information security responsibilities of staff across the organization (e.g., data owners, end users, privileged or high-risk users)

k1.17 Knowledge of processes to monitor performance of information security responsibilities

k1.18 Knowledge of methods to establish new, or utilize existing, reporting and communication channels throughout an organization

k1.19 Knowledge of methods to select, implement and interpret key information security metrics (e.g., key performance indicators [KPIs] or key risk indicators [KRIs])

Domain 2: Information Risk Management

TASK STATEMENTS

2.1 Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.

2.2 Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.

2.3 Ensure that risk assessments, vulnerability assessments and threat analyses are conducted consistently, at appropriate times, and to identify and assess risk to the organization's information.

2.4 Identify, recommend or implement appropriate risk treatment/response options to manage risk to acceptable levels based on organizational risk appetite.

2.5 Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.

2.6 Facilitate the integration of information risk management into business and IT processes (e.g., systems development, procurement, project management) to enable a consistent and comprehensive information risk management program across the organization.

2.7 Monitor for internal and external factors (e.g., key risk indicators [KRIs], threat landscape, geopolitical, regulatory change) that may require reassessment of risk to ensure that changes to existing, or new, risk scenarios are identified and managed appropriately.

2.8 Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.

2.9 Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives.

KNOWLEDGE STATEMENTS

k2.1 Knowledge of methods to establish an information asset classification model consistent with business objectives

k2.2 Knowledge of considerations for assigning ownership of information assets and risk

k2.3 Knowledge of methods to identify and evaluate the impact of internal or external events on information assets and the business

k2.4 Knowledge of methods used to monitor internal or external risk factors

k2.5 Knowledge of information asset valuation methodologies

k2.6 Knowledge of legal, regulatory, organizational and other requirements related to information security

k2.7 Knowledge of reputable, reliable and timely sources of information regarding emerging information security threats and vulnerabilities

k2.8 Knowledge of events that may require risk reassessments and changes to information security program elements

k2.9 Knowledge of information threats, vulnerabilities and exposures and their evolving nature

k2.10 Knowledge of risk assessment and analysis methodologies

k2.11 Knowledge of methods used to prioritize risk scenarios and risk treatment/ response options

k2.12 Knowledge of risk reporting requirements (e.g., frequency, audience, content)

k2.13 Knowledge of risk treatment/response options (avoid, mitigate, accept or transfer) and methods to apply them

k2.14 Knowledge of control baselines and standards and their relationships to risk assessments

k2.15 Knowledge of information security controls and the methods to analyze their effectiveness

k2.16 Knowledge of gap analysis techniques as related to information security k2.17 Knowledge of techniques for integrating information security risk management into business and IT processes

k2.18 Knowledge of compliance reporting requirements and processes

k2.19 Knowledge of cost/benefit analysis to assess risk treatment options

Domain 3: Information Security Program Development and Management

TASK STATEMENTS

3.1 Establish and/or maintain the information security program in alignment with the information security strategy.

3.2 Align the information security program with the operational objectives of other business functions (e.g., human resources [HR], accounting, procurement and IT) to ensure that the information security program adds value to and protects the business.

3.3 Identify, acquire and manage requirements for internal and external resources to execute the information security program.

3.4 Establish and maintain information security processes and resources (including people and technologies) to execute the information security program in alignment with the organization's business goals.

3.5 Establish, communicate and maintain organizational information security standards, guidelines, procedures and other documentation to guide and enforce compliance with information security policies.

3.6 Establish, promote and maintain a program for information security awareness and training to foster an effective security culture.

3.7 Integrate information security requirements into organizational processes (e.g., change control, mergers and acquisitions, system development, business continuity, disaster recovery) to maintain the organization's security strategy.

3.8 Integrate information security requirements into contracts and activities of third parties (e.g., joint ventures, outsourced providers, business partners, customers) and monitor adherence to established requirements in order to maintain the organization's security strategy.

3.9 Establish, monitor and analyze program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

3.10 Compile and present reports to key stakeholders on the activities, trends and overall effectiveness of the IS program and the underlying business processes in order to communicate security performance.

KNOWLEDGE STATEMENTS

k3.1 Knowledge of methods to align information security program requirements with those of other business functions

k3.2 Knowledge of methods to identify, acquire, manage and define requirements for internal and external resources

k3.3 Knowledge of current and emerging information security technologies and underlying concepts

k3.4 Knowledge of methods to design and implement information security controls

k3.5 Knowledge of information security processes and resources (including people and technologies) in alignment with the organization's business goals and methods to apply them

k3.6 Knowledge of methods to develop information security standards, procedures and guidelines

k3.7 Knowledge of internationally recognized regulations, standards, frameworks and best practices related to information security program development and management

k3.8 Knowledge of methods to implement and communicate information security policies, standards, procedures and guidelines

k3.9 Knowledge of training, certifications and skill set development for information security personnel

k3.10 Knowledge of methods to establish and maintain effective information security awareness and training programs

k3.11 Knowledge of methods to integrate information security requirements into organizational processes (e.g., access management, change management, audit processes) k3.12 Knowledge of methods to incorporate information security requirements into contracts, agreements and third-party management processes

k3.13 Knowledge of methods to monitor and review contracts and agreements with third parties and associated change processes as required

k3.14 Knowledge of methods to design, implement and report operational information security metrics

k3.15 Knowledge of methods for testing the effectiveness and efficiency of information security controls

k3.16 Knowledge of techniques to communicate information security program status to key stakeholders

Domain 4: Information Security Incident Management

TASK STATEMENTS

4.1 Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate classification and categorization of and response to incidents.

4.2 Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.

4.3 Develop and implement processes to ensure the timely identification of information security incidents that could impact the business.

4.4 Establish and maintain processes to investigate and document information security incidents in order to determine the appropriate response and cause while adhering to legal, regulatory and organizational requirements.

4.5 Establish and maintain incident notification and escalation processes to ensure that the appropriate stakeholders are involved in incident response management.

4.6 Organize, train and equip incident response teams to respond to information security incidents in an effective and timely manner.

4.7 Test, review and revise (as applicable) the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities.

4.8 Establish and maintain communication plans and processes to manage communication with internal and external entities.

4.9 Conduct postincident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.

4.10 Establish and maintain integration among the incident response plan, business continuity plan and disaster recovery plan.

KNOWLEDGE STATEMENTS

k4.1 Knowledge of incident management concepts and practices

k4.2 Knowledge of the components of an incident response plan

k4.3 Knowledge of business continuity planning (BCP) and disaster recovery planning (DRP) and their relationship to the incident response plan

k4.4 Knowledge of incident classification/categorization methods

k4.5 Knowledge of incident containment methods to minimize adverse operational impact

k4.6 Knowledge of notification and escalation processes

k4.7 Knowledge of the roles and responsibilities in identifying and managing information security incidents

k4.8 Knowledge of the types and sources of training, tools and equipment required to adequately equip incident response teams

k4.9 Knowledge of forensic requirements and capabilities for collecting, preserving and presenting evidence (e.g., admissibility, quality and completeness of evidence, chain of custody)

k4.10 Knowledge of internal and external incident reporting requirements and procedures

k4.11 Knowledge of postincident review practices and investigative methods to identify root causes and determine corrective actions

k4.12 Knowledge of techniques to quantify damages, costs and other business impacts arising from information security incidents

k4.13 Knowledge of technologies and processes to detect, log, analyze and document information security events

k4.14 Knowledge of internal and external resources available to investigate information security incidents

k4.15 Knowledge of methods to identify and quantify the potential impact of changes made to the operating environment during the incident response process

k4.16 Knowledge of techniques to test the incident response plan

k4.17 Knowledge of applicable regulatory, legal and organization requirements

k4.18 Knowledge of key indicators/metrics to evaluate the effectiveness of the incident response plan

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com