CRISC Prep Training

BILGINC IT Academy
info@bilginc.com
bilginc.com

Duration: **4 Day**

New - Prepare for the ISACA CRISC certification exam.

In this course, you'll cover all four domains of the Certified in Risk and Information Systems Control (CRISC) exam and gain the knowledge and concepts required to obtain CRISC certification. Since its inception in 2010, the CRISC certification is for IT and business professionals who identify and manage risks through the development, implementation, and maintenance of appropriate information systems (IS) controls. This credential demonstrates expertise in identifying and managing enterprise IT risk and implementing and maintaining information systems controls.

Is This The Right Course?

At least three years cumulative work experience performing tasks across at least three CRISC domains is recommended.

Who Should Attend?

IT risk management professionals with at least 3 years of relevant professional work experience in IT risk and information systems control including:

- Security Directors/Managers/Consultants
- Compliance/Risk/Privacy Directors and Managers
- IT Audit Directors/Managers/Consultants
- Compliance/Risk/Control Staff

Prerequisites

At least three years cumulative work experience performing tasks across at least three CRISC domains is recommended.

What You Will Learn

The 4 domains covered in this course are:

- IT risk identification
- IT risk assessment
- Risk response mitigation
- Risk and control monitoring and reporting

Training Outline

CRISC Prep Training

BILGINC IT Academy
info@bilginc.com
bilginc.com

Duration: **4 Day**

Domain 1: IT Risk Identification

Identify the universe of IT risk to contribute to the execution of the IT risk management strategy in support of business
objectives and in alignment with the enterprise risk management (ERM) strategy.

- Collect and review information, including existing documentation, regarding the organization's internal and
  external business and IT environments to identify potential or realized impacts of IT risk to the organization's
  business objectives and operations.
- Identify potential threats and vulnerabilities to the organization's people, processes and technology to enable IT risk
  analysis.
- Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact
  to business objectives and operations.
- Identify key stakeholders for IT risk scenarios to help establish accountability.
- Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into
  the enterprise-wide risk profile.
- Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with
  business objectives.
- Collaborate in the development of a risk awareness program, and conduct training to ensure that stakeholders
  understand risk and to promote a risk-aware culture.

Domain 2: IT Risk Assessment

Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based
decision making.

- Analyze risk scenarios based on organizational criteria (e.g., organizational structure, policies, standards,
  technology, architecture, controls) to determine the likelihood and impact of an identified risk.
- Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.
- Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk
  environment.
- Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability.
- Communicate the results of risk assessments to senior management and appropriate stakeholders to enable riskbased decision making.
- Update the risk register with the results of the risk assessment.

Domain 3: Risk Response Mitigation

Determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with
business objectives.

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions.
- Consult with, or assist, risk owners on the development of risk action plans to ensure that plans include key elements (e.g., response, cost, target date).
- Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level.
- Ensure that control ownership is assigned to establish clear lines of accountability.
- Assist control owners in developing control procedures and documentation to enable efficient and effective control execution.
- Update the risk register to reflect changes in risk and management's risk response.
- Validate that risk responses have been executed according to the risk action plans.

Domain 4: Risk and Control Monitoring and Reporting

Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.

- Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk.
- Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile.
- Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making.
- Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance.
- Monitor and analyze key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls.
- Review the results of control assessments to determine the effectiveness of the control environment.
- Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making.