CRISC Boot Camp (4-days)

Become a CRISC and defend, protect and future-proof your enterprise

Course objectives

Candidates should expect to gain competencies in the following areas after successful completion of the training course:

- To identify the universe of IT risk to contribute to the execution of the IT risk management strategy
- To analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.
- To determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives.
- To 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.

The course includes:

- Course reference manual containing copy of course slides, support documents, quizzes and answers
- Practice exam
- Course Certificate

Audience

This four-day training targeted towards IT professionals, Risk professionals, Control professionals, Business analysts, Project managers, Compliance professionals enables IT professionals for the unique challenges of IT and enterprise risk management, and positions them to become strategic partners to the enterprise. ISACA®'s Certified in Risk and Information Systems Control™ (CRISC™) certification instantly validates skills and expertise in risk and information systems control.

It proves ability to understand and articulate business risk, implement appropriate IS controls and develop effective plans to mitigate risk.

Prerequisite

Basic understanding of IT security or IT security management is useful.

Duration

This is **a four-day CRISC Boot Camp**. The course starts at **09:30** and runs until **16:30**.

Alternate timings can be arranged upon request. The course can be held on a **date that suits you.**

Location

Our **CRISC Boot Camp** will be **delivered Online Remotely using online training platforms**. It can also be run at **our training venue** near **Liverpool Street (London)** or any preferred location in the **UK or Europe.**

CRISC Boot Camp Course Outline

Domain 1—IT Risk Identification

Collect and review information, including existing documentation, regarding the organization's internal and external business and IT environments

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.

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.

To 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

Domain 2—IT Risk Assessment

Analyze risk scenarios based on organizational criteria

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.

Update the risk register with the results of the risk assessment.

Domain 3—Risk Response and Mitigation

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.

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.

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

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).

Review the results of control assessments to determine the effectiveness of the control environment.