Course Outline

CRISC-Certified in Risk and Information Systems Control exam preparation

Duration

30 hours

Target Audience:

IT professionals interested in earning Certified in Risk and Information Systems Controls (CRISC) certification. CRISC is for IT professionals, risk professionals, business analysts, project manager and/or compliance professionals, how to work towards evaluation and mitigation of risk, and who have job experience in the following areas:

* Risk identification, assessment and evaluation;
* Risk response and monitoring and
* IS control design/monitoring and implementation/maintenance.

- CRISC® Seminar-Curriculum

Our CRISC exam preparation course assists IT professionals to accomplish the following business objectives in their enterprise:

* Designing, implementing, monitoring & maintaining risk-based, effective IS controls
* Compliance with regulatory requirements

Also covered are the 5 domains as required by ISACA (described below):

1. Risk Identification Assessment and Evaluation (RI)
2. Risk Response (RR)
3. Risk Monitoring (RM)
4. IS Control Design and Implementation (CD)
5. IS Control Monitoring and Maintenance (MM)

Risk Identification Assessment and Evaluation (Domain I Content)

The Risk Identification Assessment and Evaluation domain deals with the following:

- Identify, assess and evaluate risk to enable the execution of the enterprise risk management strategy
- Identify potential threats and vulnerabilities for business processes
- Develop a risk awareness program and conduct training
- Validate risk appetite and tolerance with senior leadership
- Create and maintain a risk register to ensure that all identified risk factors are accounted for
- Assemble risk scenarios to estimate thelikelihood and impact of significant events to the organization

Risk Response (Domain II Content)

The Risk Response domain deals with developing and implementing risk responses to ensure that risk factors and events are addressed in a cost-effective manner and in line with business objectives.

- Identify and evaluate risk response options
- Review risk responses with the relevant stakeholders for validation of efficiency, effectiveness and economy
- Apply risk criteria to assist in the development of the risk profile
- Assist in the development of risk response action plans
- Assist in the development of business cases supporting the investment plan

Risk Monitoring (Domain III Content)

The Risk Monitoring domain will help the participant in monitoring risk and communicate information to the relevant stakeholders to ensure the continued effectiveness of the enterprise's risk management strategy:

- Collect and validate data that measure key risk indicators (KRIs)
- Monitor and communicate key risk indicators (KRIs)
- Facilitate independent risk assessments and risk management process reviews to ensure they are performed efficiently and effectively
- Identify and report on risk, includingcompliance, to initiate corrective action and meet business and regulatory requirements

IS Control Design and Implementation (Domain IV Content)

The IS Control Design and Implementation domain will help the participant to deal with the design and implementation ofinformation systemscontrols in alignment with the organization's risk appetite and tolerance levels to support business objectives:

- Interview process owners and review process design documentation
- Analyze and document business process objectives and design
- Design information systems controls
- Facilitate the identification of resources (e.g., people, infrastructure, information, architecture)
- Monitor the information systems control design and implementation process
- Provide progress reports on the implementation of information systems controls
- Test information systems controls to verify effectiveness and efficiency prior to implementation
- Implement information systems controls to mitigate risk

- Facilitate the identification of metrics and key performance indicators(KPIs)

IS Control Monitoring and Maintenance (Domain V Content)

The I Control Monitoring and Maintenance domain will help the participant to deal with monitoring and maintaining information systems controls to ensure they function effectively and efficiently:

- Plan, supervise and conduct testing to confirm continuous efficiency and effectiveness of information systems controls
- Collect information and review documentation to identify information systems control deficiencies
- Review information systems policies, standards and procedures
- Assess and recommend tools and techniques
- Evaluate the current state of information systems processes using a maturity model
- Determine the approach to correct information systems control deficiencies
- Provide information systems control status reporting to relevant stakeholders to enable informed decision making