ISACA CISA Bootcamp

Course Summary

Topics

- The Process of Auditing Information Systems
- Governance and Management of IT
- Information Systems Acquisition, Development and Implementation
- Information Systems Operations, Maintenance and Support
- Protection of Information Assets

Prerequisites

There are no prerequisites for this course.

Duration

Four or five days

ISACA CISA Bootcamp

Course Outline

I. The Process of Auditing Information Systems

A. Develop and implement a risk-based IT audit strategy in compliance with IT audit standards to ensure that key areas are included.
B. Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
C. Conduct audits in accordance with IT audit standards to achieve planned audit objectives.
D. Report audit findings and make recommendations to key stakeholders to communicate results and effect change when necessary.
E. Conduct follow-ups or prepare status reports to ensure that appropriate actions have been taken by management in a timely manner.

II. Governance and Management of IT

A. Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support the organization's strategies and objectives.
B. Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives.
C. Evaluate the IT strategy, including the IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the organization's strategies and objectives.
D. Evaluate the organization's IT policies, standards, and procedures, and the processes for their development, approval, implementation, maintenance, and monitoring, to determine whether they support the IT strategy and comply with regulatory and legal requirements.
E. Evaluate the adequacy of the quality management system to determine whether it supports the organization's strategies and objectives in a cost-effective manner.
F. Evaluate IT management and monitoring of controls (e.g., continuous monitoring, quality assurance [QA]) for compliance with the organization's policies, standards and procedures.
G. Evaluate IT resource investment, use and allocation practices, including prioritization criteria, for alignment with the organization's strategies and objectives.
H. Evaluate IT contracting strategies and policies, and contract management practices to determine whether they support the organization's strategies and objectives.
I. Evaluate risk management practices to determine whether the organization's IT-related risks are properly managed.
J. Evaluate monitoring and assurance practices to determine whether the board and executive management receive sufficient and timely information about IT performance.
K. Evaluate the organization's business continuity plan to determine the organization's ability to continue essential business operations during the period of an IT disruption.

III. Information Systems Acquisition, Development and Implementation

A. Evaluate the business case for proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether it meets business objectives.
B. Evaluate the project management practices nd controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization.
C. Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation and status reporting is accurate.
D. Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements.
E. Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls and the organization's requirements are met.
F. Conduct postimplementation reviews of systems to determine whether project deliverables, controls and the organization's requirements are met.

ISACA CISA Bootcamp

Course Outline (cont'd)

IV. Information Systems Operations, Maintenance and Support

A. Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives.
B. Evaluate service level management practices to determine whether the level of service from internal and external service providers is defined and managed.
C. Evaluate third-party management practices to determine whether the levels of controls expected by the organization are being adhered to by the provider.
D. Evaluate operations and end-user procedures to determine whether scheduled and nonscheduled processes are managed to completion.
E. Evaluate the process of information systems maintenance to determine whether they are controlled effectively and continue to support the organization's objectives.
F. Evaluate data administration practices to determine the integrity and optimization of databases.
G. Evaluate the use of capacity and performance monitoring tools and techniques to determine whether IT services meet the organization's objectives.
H. Evaluate problem and incident management practices to determine whether incidents, problems or errors are recorded, analyzed and resolved in a timely manner.
I. Evaluate change, configuration and release management practices to determine whether scheduled and nonscheduled changes made to the organization's production environment are adequately controlled and documented.
J. Evaluate the adequacy of backup and restore provisions to determine the availability of information required to resume processing.
K. Evaluate the organization's disaster recovery plan to determine whether it enables the recovery of IT processing capabilities in the event of a disaster.

V. Protection of Information Assets

A. Evaluate the information security policies, standards and procedures for completeness and alignment with generally accepted practices.
B. Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information.
C. Evaluate the design, implementation and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures and applicable external requirements.
D. Evaluate the design, implementation and monitoring of physical access and environmental controls to determine whether information assets are adequately safeguarded.
E. Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets (e.g., backup media, offsite storage, hard copy/print data and softcopy media) to determine whether information assets are adequately safeguarded