# CISA Certification

1. **The Process of Auditing Information Systems**
    a. Knowledge of ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards
    b. Knowledge of the risk assessment concepts and tools and techniques used in planning, examination, reporting and follow-up
    c. Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes
    d. Knowledge of the control principles related to controls in information systems
    e. Knowledge of risk-based audit planning and audit project management techniques, including follow-up
    f. Knowledge of the applicable laws and regulations that affect the scope, evidence collection and preservation, and frequency of audits
    g. Knowledge of the evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis, forensic investigation techniques, computer-assisted audit techniques [CAATs]) used to gather, protect and preserve audit evidence
    h. Knowledge of different sampling methodologies and other substantive/data analytical procedures
    i. Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure, issue writing, management summary, result verification)
    j. Knowledge of audit quality assurance (QA) systems and frameworks
    k. Knowledge of various types of audits (e.g., internal, external, financial) and methods for assessing and placing reliance on the work of other auditors or control entities

2. **Governance and Management of IT**

. Knowledge of the purpose of IT strategy, policies, standards and procedures for an organization and the essential elements of each
    a. Knowledge of IT governance, management, security and control frameworks, and related standards, guidelines and practices
    b. Knowledge of the organizational structure, roles and responsibilities related to IT, including segregation of duties (SoD)
    c. Knowledge of the relevant laws, regulations and industry standards affecting the organization
    d. Knowledge of the organizations technology direction and IT architecture and their implications for setting long-term strategic directions
    e. Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures
    f. Knowledge of the use of capability and maturity models
    g. Knowledge of process optimization techniques
    h. Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, personnel management)
    i. Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes, including third-party outsourcing relationships
    j. Knowledge of enterprise risk management (ERM)

k. Knowledge of the practices for monitoring and reporting of controls performance (e.g., continuous monitoring, quality assurance [QA])

l. Knowledge of quality management and quality assurance (QA) systems

m. Knowledge of the practices for monitoring and reporting of IT performance (e.g., balanced scorecard [BSC], key performance indicators [KPIs])

n. Knowledge of business impact analysis (BIA)

o. Knowledge of the standards and procedures for the development, maintenance and testing of the business continuity plan (BCP)

p. Knowledge of the procedures used to invoke and execute the business continuity plan (BCP) and return to normal operations

**3. Information Systems Acquisition, Development and Implementation**

. Knowledge of benefits realization practices, (e.g., feasibility studies, business cases, total cost of ownership [TCO], return on investment [ROI])

a. Knowledge of IT acquisition and vendor management practices (e.g., evaluation and selection process, contract management, vendor risk and relationship management, escrow, software licensing), including third-party outsourcing relationships, IT suppliers and service providers.

b. Knowledge of project governance mechanisms (e.g., steering committee, project oversight board, project management office)

c. Knowledge of project management control frameworks, practices and tools

d. Knowledge of the risk management practices applied to projects

e. Knowledge of requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis, vulnerability management, security requirements)

f. Knowledge of the enterprise architecture (EA) related to data, applications and technology (e.g., web-based applications, web services, n-tier applications, cloud services, virtualization)

g. Knowledge of system development methodologies and tools, including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques, secure coding practices, system version control)

h. Knowledge of the control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data

i. Knowledge of the testing methodologies and practices related to the information system development life cycle (SDLC)

j. Knowledge of the configuration and release management relating to the development of information systems

k. Knowledge of system migration and infrastructure deployment practices and data conversion tools, techniques and procedures

l. Knowledge of project success criteria and project risk

m. Knowledge of post-implementation review objectives and practices (e.g., project closure, control implementation, benefits realization, performance measurement)

**4. Information Systems Operations, Maintenance and Support**

. Knowledge of service management frameworks

a. Knowledge of service management practices and service level management

b. Knowledge of the techniques for monitoring third-party performance and compliance with service agreements and regulatory requirements

c. Knowledge of enterprise architecture (EA)

d. Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)

e. Knowledge of system resiliency tools and techniques (e.g., fault-tolerant hardware, elimination of single point of failure, clustering)

f. Knowledge of IT asset management, software licensing, source code management and inventory practices

g. Knowledge of job scheduling practices, including exception handling

h. Knowledge of the control techniques that ensure the integrity of system interfaces

i. Knowledge of capacity planning and related monitoring tools and techniques

j. Knowledge of systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing)

k. Knowledge of data backup, storage, maintenance and restoration practices

l. Knowledge of database management and optimization practices

m. Knowledge of data quality (completeness, accuracy, integrity) and life cycle management (aging, retention)

n. Knowledge of problem and incident management practices

o. Knowledge of change management, configuration management, release management and patch management practices

p. Knowledge of the operational risk and controls related to end-user computing

q. Knowledge of the regulatory, legal, contractual and insurance issues related to disaster recovery

r. Knowledge of business impact analysis (BIA) related to disaster recovery planning

s. Knowledge of the development and maintenance of disaster recovery plans (DRPs)

t. Knowledge of the benefits and drawbacks of alternate processing sites (e.g., hot sites, warm sites, cold sites)

u. Knowledge of disaster recovery testing methods

v. Knowledge of the processes used to invoke the disaster recovery plans (DRPs)

**5. Protection of Information Assets**

. Knowledge of the generally accepted practices and applicable external requirements (e.g., laws, regulations) related to the protection of information assets

a. Knowledge of privacy principles

b. Knowledge of the techniques for the design, implementation, maintenance, monitoring and reporting of security controls

c. Knowledge of the physical and environmental controls and supporting practices related to the protection of information assets

d. Knowledge of the physical access controls for the identification, authentication and restriction of users to authorized facilities and hardware

e. Knowledge of the logical access controls for the identification, authentication and restriction of users to authorized functions and data

f. Knowledge of the security controls related to hardware, system software (e.g., applications, operating systems) and database management systems.

g. Knowledge of the risk and controls associated with virtualization of systems

h. Knowledge of the risk and controls associated with the use of mobile and wireless devices, including personally owned devices (bring your own device [BYOD])

i. Knowledge of voice communications security (e.g., PBX, Voice-over Internet Protocol [VoIP])

j. Knowledge of network and Internet security devices, protocols and techniques

k. Knowledge of the configuration, implementation, operation and maintenance of network security controls

l. Knowledge of encryption-related techniques and their uses

m. Knowledge of public key infrastructure (PKI) components and digital signature techniques

n. Knowledge of the risk and controls associated with peer-to-peer computing, instant messaging, and web-based technologies (e.g., social networking, message boards, blogs, cloud computing)

o. Knowledge of the data classification standards related to the protection of information assets

p. Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets

q. Knowledge of the risk and controls associated with data leakage

r. Knowledge of the security risk and controls related to end-user computing

s. Knowledge of methods for implementing a security awareness program

t. Knowledge of information system attack methods and techniques

u. Knowledge of prevention and detection tools and control techniques

v. Knowledge of security testing techniques (e.g., penetration testing, vulnerability scanning)

w. Knowledge of the processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)

x. Knowledge of the processes followed in forensics investigation and procedures in collection and preservation of the data and evidence (i.e., chain of custody)

y. Knowledge of the fraud risk factors related to the protection of information assets