ISACA Certified Information Systems Auditor

Study Guide & Practice Questions

Table of Contents

The Process of Auditing Information Systems

The first domain of the CISA exam is the process of auditing information systems. It accounts for 21% of the questions on the exam and is the second largest domain on the exam. Particular attention should be paid to the process of building an audit program, the functions it supports, and the roles it plays within the organization.

For an organization, having a charter, or written purpose statement, is critical for the internal audit function. This function should have independence and top-level support from within the organization. It should also be aligned with the overall goals and objectives of the organization.

The ISACA auditing standards framework defines the mandatory audit standards and guidelines that facilitate consistent and comprehensive audits. The Information Technology Assurance Framework (ITAF) contains elements of both COBIT and ISACA auditing standards and guidelines—this framework is to be used as a comprehensive guide for instituting the assurance framework within and organization.

Risk Analysis

Risk analysis is a critical part of auditing. It should be done initially in order to help the IS auditor determine what warrants further investigation and to help them better structure an audit plan. ISACA provides the Risk IT Framework to help determine the processes of governing, evaluating, and responding to risks within an organization.

Controls within an organization come in many forms such as policies, procedures, systems, and processes that reduce risk and support business goals and objectives. Each control should have a documented objective that states the control's purpose. Controls can be either automatic or manual.

General computing controls are applied across an organization, while most systems will have additional controls in place specific to itself.

The Audit Process

An Audit is a planned evaluation of internal controls and their corresponding objectives. The primary purpose of an audit is to gather evidence supporting the operation of controls within the environment that determine its effectiveness. The evidence typically contains screenshots of the control's configuration, written notes, correspondence, process and procedure documentation, and business records.

The audit is typically guided by a methodology, which help ensure the audits are both repeatable and consistent from one organization to the next. This ensures the auditor provides the same level of value to each organization with which they work and that their goals and methods are easily identifiable. Audits come in many forms, including: operational, financial, integrated, IS, administrative, compliance, forensic, and service provider audits. Pre-audits are typically done to help facilitate planning and scope development.

Key things an auditor should attempt to gather during an audit are: policies and procedures documentation, charters, third-party contract, organizational charts, incident logs, standards and systems documentation.

Sampling is used when testing each individual component is untenable based upon size or time constraints. The method of sampling used needs to be carefully chosen to ensure a proper representation of the environment is used to support any findings. The main types of sampling are: statistical, judgmental, attribute, stop-or-go, discovery, and stratified sampling. Each type has its own use-case and benefits.

A key component to a successful audit is the interviews of key staff and stakeholders. These interviews are critical to helping the auditor understand the dynamics of the workplace, along with specific roles and responsibilities. The interviews will also afford the auditor the chance to have a back and forth to ensure a solid understanding of any particular systems or processes.

Of particular importance to the exam is understanding that in some cases, organizations will rely upon third-party audit reports. The most common example of this is the SSAE 16 audit of data center providers or other vendors that will handle some of the organization's data or access to that data. SSAE 16 is formerly known as SAS 70.

Sometimes audits are performed using automated solutions to help facilitate speed and repeatability. When these tools are used, an auditor needs to ensure they verify the findings of the tools and be sure to correspond them to any specific transactions used. This ensures the evidence is reliable, which is a key component of an audit. Another use-case for these automated tools is a continuous audit. Continuous audits are relatively new to many organizations, but provide tremendous value in that they can look at trends, provide real-time feedback, and are not confined by a specific window of time.

Risk Types and Decisions

As part of the CISA exam, a critical thing to understand is the different types of risk you will encounter within an environment. These risk types are: control, detection, inherent, audit, and sampling. The direct impact of an auditor on risk is solely confined to detection as this is the risk that an auditor will miss a risk during the course of an audit. Each risk combined is known as the audit risk.

Once Risk has been identified, the organization and focus on reduction, transfer, avoidance, or acceptance of the risk. Reduction of risk is the implementation of controls to reduce the risk. Transfer of risk is typically done by purchasing insurance against the risk. Avoidance is typically done by the organization no longer participating in the risky activity or no longer using the application with the risk. Risk acceptance is where the organization decides the risk is a cost of doing business and minimal effort is made to correct it. This is typically done when the risk is minimal or otherwise unavoidable.

The control self-assessment is a critical component to understand. It involves identifying and assessing risks, identifying and assessing controls, developing a questionnaire, analyzing completed questionnaires, control remediation, and awareness training. This process ensures that protections are not foregone for the sake of efficiency where the control is providing value.

Two key types of testing are compliance and substantive. Compliance testing determines if a control is designed and implemented appropriately while substantive testing is done to verify the integrity of business process transactions.

Governance and Management of IT

The second domain of the CISA exam is governance and management of IT. 16% of the exam will be based upon this domain. The key takeaways here are understanding the IT process, the structure of the department, and the key management practices that make up IT. Another key component is understanding the process of developing a business continuity plan. The important thing to remember is that the first step in this process is always a business impact analysis to ensure emphasis is placed on the proper components.

Proper IT governance cannot be achieved without a top-down approach. Upper management needs to be driving the governance. Typically, this is done through a steering committee comprised of top executives who set the strategic direction and policies for the organization that align with the business' goals and objectives. These policies, and associated risk appetite, are carried out through chief information officers (CIO) or chief information risk officers (CIRO).

The CIO and CIRO are responsible for many things including: developing security policies, handling incident management, vulnerability management, and identity and access management.

Risk Management and Assessments

Risk management is key to the governance and management of IT CISA domain. It refers to identifying key assets and their vulnerabilities. Once risks are identified, steps can be taken to either mitigate, transfer, avoid, or accept the risk. Risk mitigation is either completely resolving or greatly reducing the threat a risk poses to the organization. Risk transfer is the migration of the risk burden from one organization to another such as when an organization purchases insurance against a particular risk such as cyber liability insurance. Risk avoidance is simply when an organization avoids partaking in a process or application that poses the risk to the organization. Risk acceptance is the determination an organization makes that the risk does not pose a significant threat to the organization or that there is no other way around it.

Risk assessments can be qualitative or quantitative. Qualitative risk assessments are probably the most common and categorize risks in the form of high, medium, low, informational or similar. Quantitative risk assessments focus on linking risks with dollar amounts. Quantitative risk assessments are typically harder to perform accurately.

Key Management Practices

Effective operation of an IT department or organization necessitates certain key management practices such as: personnel management, sourcing, change management, financial management, quality management, portfolio management, controls management, and security management. Personnel management focuses on hiring, development and evaluation of employees, on-boarding and off-boarding, and development and maintenance of an employee

handbook and other guiding policies. Sourcing is concerned with who is in charge of the business processes and whether or not those processes are insourced or outsourced. Change management is focused on controlling the change that occurs within an environment to minimize downtime, variables, and security issues. Financial management is concerned with keeping track of the complex IT expenditure to ensure efficiency. Quality management focuses on ensuring processes are measured and managed to drive continued improvement. Portfolio management is the systematic management of IT projects, investments, and activities. Controls management ensures proper implementation and management of controls and their objectives. Security management focuses on vulnerability and risk assessments, incident management, compliance management, identity and access management, business continuity and disaster recovery management, and capacity planning and management.

Critical to the proper governance of the IT function is a formal management and reporting structure, along with documented roles, responsibilities, and job descriptions. Segregation of duties should be apparent and enforced to ensure there is no single point of failure in any critical business process.

Business Continuity and Disaster Recovery

Business continuity plans should be able to account for man-made and natural disasters allowing the organization to continue critical business functions in the event of a disaster. The process of developing a business continuity plan begins with a statement of the goals and objectives. A business impact analysis (BIA) is completed and each critical process is tied to a statement of impact. This statement can be qualitative or quantitative. The next step is a criticality analysis wherein each business process is ranked in terms of criticality. The rankings can be qualitative, quantitative, or subjective. A maximum tolerable downtime is then documented for each process. These metrics are what drive the recovery time objective and recovery point objective for each process.

Recovery time objective is the time to restoration of services while recovery point objective is the maximum data loss.

Continuity plans consist of procedures for safety, declaration of disaster, definitions of responsibilities, contact information for key individuals, procedures for recovery, continuity of operations, and restoration of assets. These plans should be tested periodically and the types of tests typically performed are: document review, walkthrough, simulation, parallel test, and cutover test. Parallel testing allows for live workloads to be replicated on DR equipment while real workloads continue on production equipment. A cutover test allows for full functionality of production data on DR equipment. This is the riskiest and most complex means of testing a BC/DR plan. It is not a requirement for organizations to perform cutover tests as they can introduce issues within the environment that are only acceptable during a true disaster. Parallel tests are often sufficient to prove the efficacy of the BC/DR plan. These plans need to be

periodically reviewed, updated, and distributed among the chosen team, but should be kept to only the chosen team and not widely distributed.

From an auditing standpoint, the auditor should review the organization's policies, processes, and records to ensure the steering committee is at work in the planning and implementation of BC/DR planning. The goal here is to ensure proper alignment of business goals and objectives with the BC/DR plan. Interviews are a critical component for auditing a business continuity plan. Another critical component of particular interest to IS auditors is documentation of past test results of BC/DR plans. This is probably the greatest indicator of proper business objective alignment.

Proper auditing of the IT governance model of an organization should include a review of processes involved with updating policies and procedures documents. This ensures that the organization is putting forth a good-faith effort to follow and maintain the policy documents.

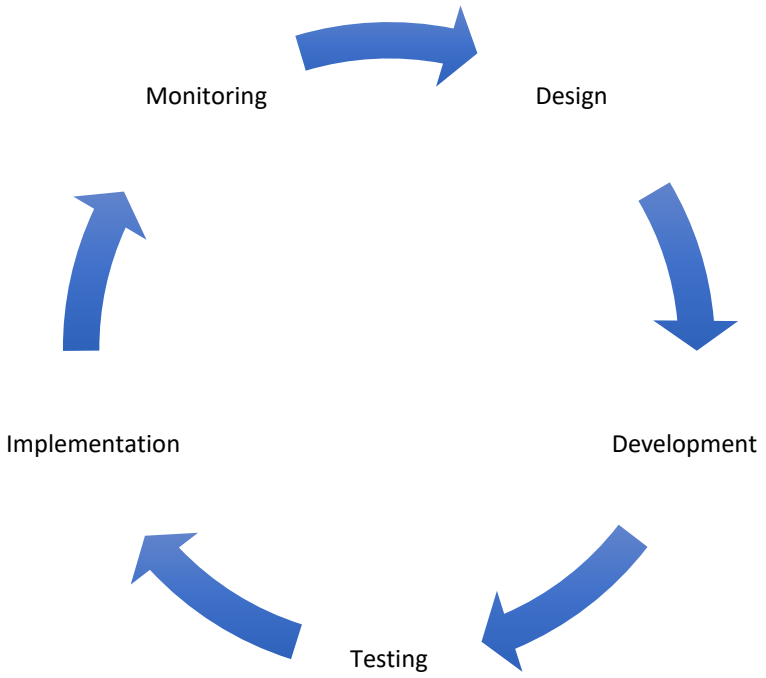
Information Systems Acquisition, Development, and Implementation

The third domain of the CISA exam is Information Systems acquisition, development, and implementation. It comprises 18% of the exam. This section is concerned with the management of the IT life cycle.

As with many other domains on the CISA exam, this section puts emphasis on the written documentation of processes and procedures. The goal of written documentation is to lay out the goals and objectives of the organization and ensure processes are both repeatable and consistent—this domain is no different.

IT Oversight and Program Management

Program management is critical to the IT life cycle and pertains to oversight of IT projects. The leader of this effort is known as a program manager and they're responsible for ensuring the project managers are on-task, budgets are adhered to, resource allocation is appropriate, and that status reports are prepared when needed for presentation to senior management.



Business Process Management Lifecycle

The key to development of a new project within IT is a business case that can be approved by management. The business case should state a business problem and how this project aims to

solve that in as many ways as possible. The business case ensures the project is not being undertaken without being properly supported and critical to the business in some aspect.

Business Cases and Project Planning

Business cases typically include: a description of the business problem, feasibility study results, high-level project plan, a budget, metrics, and risks. The business problem can be described in quantitative or qualitative terms. The high-level project plan should include the number of resources required and a basic timeline. The metrics included should be a description of how measurements will be taken to ensure business benefit, along with existing versus expected measurements after implementation. If possible, the estimates should include examples of how similar this project is to other projects that have been undertaken by the organization in the past. The risks section should include potential risks of the new application and how the organization can anticipate mitigating those risks.

Projects require formal planning as well as formal change management processes in the event a change needs to be made to scope or implementation. Another critical component to an IT project is the review done after the completion of the project. This ensures that future projects will not meet the same stumbling blocks and that improvements can constantly be made in the process.

Software Development and Acquisition Lifecycle

Software development and acquisition is typically managed through a process—the most common method is the SDLC, which is a set of activities undertaken that ensure newly implemented applications meet organizational needs.

SDLC phases are: feasibility study, requirements definition, design, development, testing, implementation, and post implementation. Each is formally documented, reviewed, and measured to ensure value to the organization and track improvement.

The testing phase of the SDLC has different types of testing, each of which should be performed. Unit testing is where each individual component of an application is tested as it is built. This ensures the unit functions correctly and does what it was designed to do. Often, the testing procedures for this phase are explicitly documented by the developers so someone can verify the unit works. System testing occurs when an application and its modules have been implemented within an environment and are tested from beginning to end. That is, each unit is tested outside of its own vacuum and verified. Functional testing ensures the developmental requirements have been met. These test results should be recorded and used as proof of compliance to project requirements. User acceptance testing is conducted to ensure an application meets the needs of the users. The testing requirements should include clearly documented tests to determine the functionality of the application meets the needs of the users. Once this phase is completed, the company often agrees to pay for the application and

delivery can be finalized. Quality assurance testing is the final phase wherein testing is conducted to ensure an application performs to system specifications and expectations. This is typically done by the IS function within an organization and not the standard user population.

Popular alternatives to SDLC are: rapid application development, object-oriented system development, agile development, and reverse engineering.

Change Management

Change management is a key component to this domain. Change management is focused on controlling the changes to an environment that ensure changes are planned, tested, reviewed, and discussed prior to implementation. Configuration management is similar, but revolves around the configuration of things in the environment like operating systems, applications, and networking equipment.

The Zachman framework is a popular framework used to provide varying degrees of detail and insight into an otherwise complex IT architecture. Data flow diagrams are also important, and they depict the various relationships of different components within IT.

	Data	**Functional (Application)**	**Network (Technology)**	**People (Organization)**	**Time**	**Strategy**
Scope	List of data sets important in the business	List of business processes	List of business locations	List of organizations	List of events	List of business goals and strategy
Enterprise Model	Conceptual data/object model	Business process model	Business logistics	Workflow	Master schedule	Business plan
Systems Model	Logical data model	System architecture	Detail system architecture	Human interface architecture	Processing structure	Business rule model
Technology Model	Physical data/class model	Technology design	Technology architecture	Presentation architecture	Control structure	Rule design
Detailed Representation	Data definition	Program	Network architecture	Security architecture	Time definition	Rule speculation
Function Enterprise	Usable data	Working function	Usable network	Functioning organization	Implemented schedule	Working strategy

Application Controls

Any application that accepts data input should ensure the integrity of that data at some level through the process. Controls for applications of this type are: input validation, processing validation, and output validation. These validation schemes check the data at various points in the process of the application. They ensure the data is normalized and of the types expected given the application. During the course of an audit, auditors should expect to receive documentation explaining the applications, charters, and records pertaining to these applications for review. This helps the auditor understand how the programs work, the process involved in obtaining new applications, and the reviews in place to ensure any acquisition is in line with business goals and objectives.

Third Party Assessments

Any third parties used by an organization should be assessed as part of a comprehensive risk assessment to ensure compliance and alignment with organizational goals and objectives.

A particular third-party relationship to pay attention to is the cloud-based infrastructure and application provider. The relationship can be broken up in to three main types: software as a service (SaaS), Infrastructure as a service (IaaS), and Platform as a service (PaaS). SaaS is when a cloud-based provider simply provides access to a software in the cloud. Users will use this service the same way they would if the application were hosted in-house. IaaS is when a cloud provider gives access to infrastructure in the cloud such as virtual machines or networking equipment. PaaS is when a cloud provider is giving access to their tools and platforms for an organization to leverage as part of their development lifecycle or a resell of services.

Information Systems Operations, Maintenance, and Support

The fourth domain of the CISA exam is Information Systems operations, maintenance, and support. It makes up 20% of the exam and is the third most focused section of the exam. The important information to understand from this domain is how day to day operations are run, how maintenance scheduled and backup retention is structured. Additionally, important is understanding the methods in which business continuity can be deployed to support the goals and objectives of the business.

In order to support the overall business goals and objectives, all operations within the IT function should be managed and monitored. This necessitates documented processes, procedures, and projects to ensure they are measurable for continued improvement and alignment with other objectives within the organization.

Service Management Frameworks

Popular and proven service management frameworks to base IT operation upon are COBIT and ITIL. These frameworks provide a good benchmark for how operations should be managed and monitored and they fit most businesses and the IT processes within them.

Hardware and Software Business Goal Support

An important part of this domain is the understanding of common IS hardware and software and how they can be configured and leveraged to support business goals and objectives. The understanding must cover a wide range from virtualization and software-defined networking to RAID levels and common operating system configurations. Auditors should also be familiar with common network monitoring tools to facilitate a more seamless audit and help in understanding utilization and potential capacity planning issues within an organization.

OSI Model

The 7-layer OSI model is made up of: physical, data link, network, transport, session, presentation, and application layers. The physical layer is about the electrical and physical devices and specifications. Typically, this refers to cabling, signaling, and wireless waves. The data link layer is concerned with the way data is transferred across the network. The data in this layer is referred to as frames and some error correction and avoidance are built into this layer such as in switches. The network layer is focused on the actual delivery of data from one side of the network to another or to entirely different networks. This is where routing happens. The transport layer is focused on the reliability of data being transferred. Here is where we discuss connection-oriented versus connectionless protocols such as TCP and UDP. TCP ensures proper delivery from one station to another, while UDP simply sends the traffic without regard for order of packets or delivery at all. The session layer is concerned with controlling sessions

such as the establishment, termination, and recovery of sessions. Common protocols in this layer are SIP, sockets, and NetBIOS. The presentation layer is used to convert data from its raw format to a presentable form. The best example is encryption/decryption. The application layer is focused on programs that interact with users, such as email clients. Common protocols in this layer are DNS, DHCP, and HTTP.

Layer	Name	Examples
1	Physical	Cabling CAT-5/Cat-6, 802.11PHY
2	Data Link	Ethernet, MAC/LLC, ARP
3	Network	IP, ICMP, IGMP
4	Transport	TCP/UDP
5	Session	SIP, sockets, named pipes
6	Presentation	Encryption/decryption, codecs
7	Application	SMTP, DNS, SNMP, SSH

RAID Configurations

RAID levels can also be important to understand for the CISA exam as they are critical to understand certain data protection schemes and configuration choices. RAID 0 is the least protective as it is striping and cannot tolerate a single drive failure, while RAID 6 can tolerate 2 drive failures. RAID 1 and RAID 5 are similar in their protection, but perform it in different ways. RAID 1 simply has 1 active drive and then a copy of it in the array, while RAID 5 distributes parity information across each drive in the array allowing for speed benefits over RAID 1.

RAID Level	Description	Fault Tolerance
0	Striping	None
1	Mirroring	1 drive
5	Parity	1 drive
6	Double parity	2 drives

Virtualization

Virtualization allows for multiple operating systems to run on a single piece of hardware. The virtual machines are abstracted from the physical server through a layer known as a hypervisor. This hypervisor relays all of the commands from each operating system on the virtual machines to the physical hardware of the server. Most commonly today these run on hardware known as blade servers, which allows for a more physical dense environment, and often saves on operating costs and rack space than traditional rack-mount servers.

Database Management

Auditors should also be familiar with database management systems and their concepts such as relational databases that store information. Relational databases refers to the concept that disparate, but related data may be located in different tables within a single database that can be retrieved together using a query language for a single, unified report or correlation of information. Security in these databases is centered on three main tenets: access controls, encryption, and audit logging.

Enterprise and Network Architecture

Enterprise architecture is based on two different sides: infrastructure and on-going activities with long-term goals in mind. The main goals commonly associated with enterprise architecture are: scalability, agility, transparency, consistency, repeatability, efficiency, and resilience. Scalability refers to the ability of an infrastructure to scale to meet the demands of an enterprise. The key here is balancing cost with effectiveness. Agility refers to the flexibility of the design to adapt to new objectives of the organization. Transparency is concerned with documentation and ease of understanding. Consistency refers to the type of components and configurations used throughout the architecture. This should speed up troubleshooting and reduce downtime in the event of a failure. Repeatability refers to how simple things are to duplicate based on the configuration. Efficiency is a metric that is directly resultant from the combination of consistency and repeatability. Any issues that arise should be much simpler to resolve because of consistency and repeatability of the infrastructure. Resilience refers to reducing single points of failure within the architecture.

Network architecture is comprised of multiple components and it means different things to different people. Typically, it is referring to one of the following: physical network architecture, logical network architecture, data flow architecture, or network standards and services. The network architecture helps build different types of networks such as: personal area network, local area network, campus area network, metropolitan area network, and wide area network.

Network Type	Distance Measurement	Usage and Technology
Personal Area Network	Feet	Personal devices, Bluetooth, NFC
Local Area Network	100's of feet	Small home office, 802.11
Campus Area Network	A few miles	Business with multiple buildings in close proximity, wireless mesh, layer 2 connections between locations

Metropolitan Area Network	Dozens of miles	Business with multiple locations within a city or area, MPLS, T1, frame relay
Wide Area Network	100's or 1000's of miles	Multiple organizations, large distances, CSU/DSU

The most common network cable types are twisted pairs and are: shielded twisted pairs, screened unshielded twisted pairs, screened shielded twisted pairs, unshielded twisted pairs. These cables come in various categories ranging from Category 3 to Category 8. The most common in use today is Category 6 or Category 7 in high-end applications where electromagnetic interference may be a concern.

Capacity Planning and Management

In order to understand capacity planning and management for networks, an auditor must understand subnetting and classless IP addressing schemes. These will tell the auditor how much available room there is on a particular subnet and help them determine if a recommendation should be made to increase or decrease the subnet scope. Subnetting will also help in ensuring security and routing between various networks within the same organization.

Disaster Recovery

Another important aspect to this domain is disaster recovery and planning. Continued operation in the event of a disaster is critical to the survivability of an organization and their overall security posture since disasters come in all shapes, sizes, and scopes. It is important to remember that disaster recovery goes beyond the technical aspects of the recovery methods and operating types of the remote sites. A proper DR plan also includes emergency communication plans and detailed steps for key personnel to perform in the event of a disaster.

Site Type	Typical RTO	Cost
Hot	0-24 hours	$$$$
Warm	24 hours – 7 days	$$$
Cold	Over 7 days	$$
Mobile	2-7 days	$$$-$$$$

Hot sites are alternate processing centers where backup equipment is already configured and running ready to take the live production load whenever necessary. This is the most expensive type of recovery site and makes recovery much easier. Warm sites are similar, but the systems often need to be powered on or have data migrated over to ensure proper functionality. Cold sites range in readiness from rented rack space that is waiting for companies to bring physical

devices from the primary datacenter or order equipment to a temporary place that will be decided at a later date.

Some organizations may opt to lever a third-party disaster recovery site. In those instances, they must ensure they take the following into consideration: definition of a disaster, equipment configuration, availability of equipment during a disaster, customer priorities, data communications, testing, right to audit, and security and environmental controls. These considerations ensure the organization gets what it is expecting from the third-party and that they are protected from all standpoints.

Replication, Backups, and Backup Rotation

An auditor must also be familiar with the concept of replication and at what levels this can occur. Replication refers to the method of copying data from a primary site to a secondary site such as a hot or warm site. Typically, there are 6 areas where replication can occur: disk storage system, operating system, database, transaction-level, application, and virtualization. Disk storage system refers to the replication that happens between SANS or other storage systems. This is probably the most common for larger organizations, although some opt for multiple levels of replication. Operating system level replication can occur as well in the form of server clusters or distributed file systems. Database-level replication refers to server clustering as well where database servers are built in a cluster and the databases are replicated on a certain schedule or ad-hoc. Transaction-level refers to the replication of individual transactions to a secondary site. This offers a great deal of protection and greatly reduces the RPO. Application-level replication is not typically used, but some applications support writing copies of data to two different application servers simultaneously. Finally, there is virtualization-level replication where full copies of virtual machines are kept between two different sites in the event of a disaster. Replication can be either synchronous or asynchronous. Synchronous replication refers to writing data both to a primary location and a secondary location at one time as part of a single operation. There are performance drawbacks to using this method. Asynchronous replication refers to the method of replication where data is written in real time locally, but replicated on some schedule to a secondary location. This incurs no performance penalty, but it does affect RPO negatively, which may be acceptable in many cases. This is the most common type used.

Data backups are another critical component to this domain. The integrity of backups is paramount as is the security of the storage, transmission, and disposal of backups. The types of backup schemes are: full backup, incremental, and differential backups. Full backups are complete copies of data. Incremental copies are copies of only changed data since the last full or incremental backup. Differential backups are copies of data that has changed since only the last full backup. Often these schemes are combined based on the criticality of the asset being protected.

Another critical component of backups is the rotation of the backup media. The common methods for doing this are first in, first out, grandfather-father-son, and towers of Hanoi. First in, first out is simple and is typically used when long-term retention of not of particular concern. This means that once the retention limit is hit, the oldest backup is overwritten or deleted. Grandfather-father-son is the most common. This method uses a scheme where full backups are performed once a week, followed by incremental or differential backups daily. They are kept until retention has been reached. The towers of Hanoi method is by far the most complex and refers to the Towers of Hanoi puzzle.

The storage of backup media should be off-site and secured. The destruction of backup media is also important. If the drives or tapes are to be discarded they should be physically destroyed to ensure the data is not recoverable. It is also critical that backups are routinely tested to ensure proper recovery is possible. The integrity of these backups is probably the most critical component.

Another important backup concept is the service level agreement. The SLA is what determines how backup rotation and schemes are selected. SLA documentation and requirements should drive the processes and procedures behind the backup implementations.

Auditing this domain centers around understanding technical complexities of hardware and software configuration and technical concepts related to the protection of data. Each component should have clear documentation for policies, procedures, and processes that the auditor can review.

Protection of Information Assets

The fifth, and most focused, domain on the CISA exam is the protection of information assets. This domain accounts for 25% of the exam. This domain is primarily about the identification and protection of assets deemed critical to the organization. As with each section, top-down support is critical.

Security Management Program Activities

The primary processes support information assets and security policy within the organization are security monitoring, auditing, security awareness training, incident response, information classification, vulnerability management, and corrective and preventative action processes.

The roles within security should be clearly developed, defined, and communicated. Each person within the security team should have a clear understanding of their roles and responsibilities for securing the organization and supporting business goals and objectives.

Access Management

The most important activity in a security management program is access management. This is what controls access to sensitive data of an organization so it is critical to get it right. The overall concept of access management consists of: user access management, network access management, and access log review.

User Access Management

User access management is concerned with managing the many facets of user access to systems. Typically, this is made up of user access provisioning, user access termination, and internal job transfers. User access provisioning is the process where access is granted for users, including creation of accounts for new users. This process should be explicitly documented to include who is authorized to make the requests, how the requests are handled, and who is allowed to approve the requests—as well as how the requests are recorded and stored. Any request that involve administrative access to the domain should go through a more rigorous process involving multiple layers of approval. The risk for this process is great and should be managed very carefully. User access termination is concerned with how removal of access is handled when an employee is terminated or moves to another company. This access includes any physical and logical access. The criticality of the information being accessed will drive the timeline for this phase, but typically 24 hours is sufficient. When accounts are locked, they should not simply have the password changed, but the account should be invalidated for both the protection of the information assets as well as the terminated employee's reputation. In some cases, additional steps should be taken such as notifying other employees of the termination and/or reviewing the employee's actions prior to and after termination. Additionally, a periodic review should be conducted to ensure proper access is enforced and to

make sure that there has been no privilege creep for some users. Finally, employee transfers should employee its own processes to ensure that the employee does not retain any unneeded access to sensitive files and data from their old department. This is easy to forget and often goes unnoticed for quite some time, but it is critical to address.

Password Management

Some common techniques for managing passwords that auditors should familiarize themselves with are: account lockouts, password lengths, password complexity, password expiration, password reuse, and password rechange. Account lockouts should typically be configured to lock a user account out after a certain number of invalid attempts. This protects against bruteforce attacks. Password length is important because it greatly shortens the amount of time a hacker needs to bruteforce or break a password. Typically, users should be taught to think of passwords as passphrases so they are more likely to have longer, easier to remember passwords that will not necessitate writing them down or falling into patterns. Password complexity refers to the distribution of characters within the password. Things like capital and lower-case letters, numbers, and symbols. Password expiration refers to the length of time a specific password is valid. This could be as often as every 30 days to as infrequent as once per year. Password reuse refers to the issue when users will use the same password to access multiple services. This is a serious security issue because the organization is not often responsible for every location where a password is used and a breach at one location may lead to a breach at another simply because of the same passwords in use. Finally, password rechange refers to the minimum amount of time users must wait between password changes. This is used to help prevent users from re-using an old password by maxing out the history quota.

A common way to augment password strength is with the requirement of a second factor. A second factor is a combination of two types of credentials from the following: something you know, something you have, or something you are. Something you know refers to a typical password. Something you have refers to something like a hardware or software token. Something you are refers to biometrics such as iris scanners or fingerprint readers.

Mobile Devices

Auditors should also be familiar with common protections for mobile devices. These protections include authentication policies, encryption, remote wipe, and download restrictions. Authentication policies refers to auto-lock and complex password requirements rather than the standard pin required on many smartphones. Encryption refers to ensuring either the entire operating system is encrypted on the mobile device or that the company data on the device is encrypted. Remote wipe allows a company to remotely wipe company data from a mobile device in the event of a stolen device or a rogue employee. Download restrictions allow an employer to ensure employees can only download approved applications.

This is critical as sometimes malicious applications make it onto the devices through various means.

Network Security Controls

Auditors should be familiar with network security controls and network-based threats. Some common network-based threats include: unauthorized access, spoofing, eavesdropping, malware, denial of service, access bypass, man-in-the-middle, and man-in-the-browser. Common network security controls to remedy these attacks are: user authentication, machine authentication, anti-malware, encryption, switched networks, intrusion detection systems, intrusion prevention systems, website filtering, data leakage prevention, application whitelisting, and netflow.

With the ever-increasing ubiquity of wireless networks, securing them continues to become a top priority. There are many ways to protect wireless networks, but a defense in depth approach should be used. Common attacks for wireless networks include: eavesdropping, war driving and war chalking, weak encryption, spoofing, and session hijacking. The best means of protecting against these attacks include using appropriate antennas, reducing transmit power, using WPA/WPA2 encryption, segregating the networks and requiring VPN, ensure appropriate patches are in place, and leveraging 2-factor or 802.1x authentication rather than a pre-shared key. If a pre-shared key must be used, it should be rotated relatively frequently.

Firewalls and DMZ Configurations

Firewalls are a critical component for securing information assets. They can easily enforce a policy and provide additional protection if used in a stateful fashion. Application firewalls can provide more granularity by watching for and protecting from some common application-layer attacks such as: SQL injection, cross-site scripting, buffer overflow, session tampering, and denial of service. These kinds of firewalls give administrators more insight into the type of traffic that is flowing through the network, not simply allowing or blocking traffic based on policies such as a screening firewall.

Another important function of a firewall in an organization is often to provide a demilitarized zone network (DMZ). A DMZ allows an organization to ensure internet-based users who need to access their systems can do so in a secure manner without potentially compromising the internal network.

Intrusion Detection and Prevention Systems

Intrusion detection systems are a detective control that passively listens for malicious traffic on the network and logs the traffic. If something suspicious happens, administrators will often get an alert and can handle per organizational policy.

Intrusion prevention systems are preventative controls that actively watch traffic flowing through the network for malicious activity. If malicious activity is found, the device has the capability to shut down the session and alert administrators.

In some instances, organizations may use honeypots or honeynets in a secured network in order to trap and prevent hackers from getting further into their network. They may also use it to keep abreast of potentially upcoming threats to their organization or as a way to know they are being targeted. Honeypots are intentionally vulnerable systems that seemingly contain sensitive company information that are left as a trap for hackers. Honeynets are the same concept, but are a network of honeypots. The two main groups of honeypots and honeynets are: high interaction and low interaction. High interaction honeypots and honeynets are systems that are typically completely, or heavily, unpatched allowing for an easy target for hackers. Low interaction honeypots and honeynets are designed to simulate production and allow IDS and IPS to alert on activity to them.

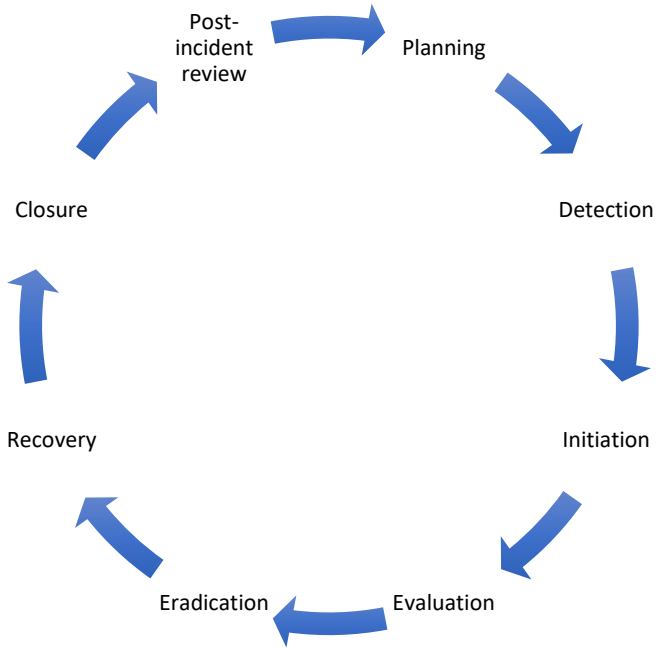
Key concepts for this domain are: change management, configuration management, incident management, threat management, and security awareness training. Change and configuration management ensure integrity throughout the environment by requiring any changes to the environment whether they be configuration changes on network equipment to allow for new access or the addition of storage to a virtualization platform be tracked and approved by a committee. This way, no one is making changes in a vacuum and all components can be accounted for when a change is proposed.

Incident and Threat Management

Incident Management

Incident management is a process containing two parts: proactive activities and responsive activities. Proactive activities refers to helping prevent incidents from ever occurring. The responsive side focuses on how to deal with incidents once they have occurred. Proactive activities can include: vulnerability and threat monitoring, situational awareness, threat hunting, vulnerability management, advanced anti-malware, system hardening, and intrusion prevention. Each of these are proactive steps that can allow an organization to stay ahead of an incident and prevent it before it occurs. Incident response is made up of 9 steps, which include: planning, detection, initiation, evaluation, eradication, recovery, closure, and post-incident review. Each of these phases are important to a comprehensive incident response procedure. Planning is critical as this is where all of the options are laid out for how a response should occur. Detection is the phase where an organization becomes aware of the incident, typically through alerts, logs, network performance impact, or IDS alerts. The next phase is initiation where the company begins their response to the intrusion. Then, the evaluation phase is where the organization reviews the data to understand the scope of the breach. The eradication phase is where responders ensure the infection or foothold is removed. This may involve firewall changes, removing malware, or locking accounts. The recovery phase is where

backups are typically restored to a pre-incident state or where equipment is replaced. The remediation phase is where changes are made that will prevent or reduce the chances of the incident recurring. Closure is the official closing of incident response actions and the incident is considered resolved. The post-incident review is where responders meet and discuss the incident in more detail such as the cause, impact, and the effectiveness of the response. This is where improvements can be made to the process and how preventative measures can become better in the future.



Incident Response Lifecycle

Threat Management

Threat management focuses on the threats posed to an organization and the process of attempting to manage these threats. That is, ensuring they pose less of a threat to the organization. This can be accomplished in many ways such as threat hunting and threat modeling. Threat hunting uses indicators of compromise (IOCs) to look for threats within the environment based on known indicators that the threat is present. An example is threat hunting for a particular strain of malware that is known to change file extensions to something with every present infection. The file extension change is an IOC for that particular malware. Commonly, this is done in two different ways internally and externally. Internal threat management uses security tools like IPSs and firewalls to look for IOCs. Externally, this is done by subscribing to feeds for publicly known threats. Threat modeling is the process of looking for potential threats.

Security Awareness Training

Security awareness training is focused on training organizational staff on how their responsibilities and tasks can help protect the organization from threats. Ensuring that each person is familiar with security concepts can help make them the first line of defense against attacks such as phishing or social engineering.

Forensic Investigations, Concepts, and Phases

Another important part of this domain is forensic investigation. During the course of a forensic investigation, determining facts is the main focus. Information is gathered, generally for the use in a legal proceeding. The chain of custody ensures that the information gathered was done so in a non-intrusive way and that the data maintains integrity. The key components for an effective chain of custody are: identification, preservation, analysis, and presentation. Identification is focused on the evidence that was found and the tools and methods used to find it. The evidence can be composed of interviews, network devices, computers, and mobile devices. Preservation is a description of the tools and methods used to retain the evidence. In particular, this focuses on detailed records of chain of custody. Analysis is a description of the findings and interpretation of the data gathered. Typically, this includes a reconstruction of events. Finally, the presentation is a formal document that puts all of the above together in a clear and concise way. This presentation includes any opinions the examiner may have of the evidence gathered and analyzed.

The most important methods to understand for forensic investigations are: data acquisition, data extraction, data protection, and analysis and transformation. Data acquisition is the process of acquiring the data. Typically, this data is pulled from a harddrive or other storage media or audit logs. The tools typically used for this are data copiers such as beyond compare or robocopy. Data extraction focuses on taking the forensic data from either a running system or a third-party system. When this is done, the analyst must be sure that the data maintains integrity and security during the transfer process. The data protection phase is concerned with integrity of the data. Computers that are used as the source for forensic data must be physically locked to ensure only authorized persons have access and that the chain of custody is clean. The machines cannot be connected to network. The analysis and transformation phase involves using automated tools to analyze the data and search for specific things. Often, data will have to be transformed to ensure a human or their tool can read it.

Access Controls

Access control is another important section for this domain. Important access control concepts to know include the subject/object relationship, fail open vs fail closed, least privilege, segregation of duties, and split custody. A subject is typically a person that wants to access an object, which is typically a resource such as a file or application. Fail open is the concept of an automatic security model failing to a state where it is open and controls are not applied. Fail closed is the concept of failing to a more secure state where less things are accessible.

Typically, we prefer fail closed, but, in some cases, fail open is required such as building security systems in the event of a fire. Least privilege refers to the concept where users should be given the access they need and nothing more. Segregation of duties is the concept that an individual should not have all access required to perform a critical function alone. As an example, this means ensuring a single user cannot perform both implementation and QA work. Split custody is the concept that means knowledge of a specific subject is split between two different people to ensure security. An example of this is splitting the password into multiple parts and giving a single part to each person and requiring that neither knows the rest of the password. This is commonly done in banks to ensure a single person does not know the entire combination to a safe.

Two access control models that are important to the CISA exam include: mandatory access control and discretionary access control. Mandatory access control is controlled centrally and users are unable to change it. It's used to control a subject's access to objects within a network. When access is attempted, the operating system determines if access should be allowed or denied based upon access properties of the subject and the object. Discretionary access control allows the owner of an object to determine which subjects have access.

Common threats to access controls are malware, eavesdropping, logic bombs, scanning attacks, race conditions, missing patches, default settings, misconfigured permissions, application vulnerabilities, and application logic.

Points of Network Entry and Internet Access

Securing points of entry into the network are critical to securing information assets. These points of entry are typically the internet and the corporate LAN. The LAN should be secured using network access controls such as 802.1X to ensure only properly authorized users and equipment should be allowed on the LAN.

Internet-based access poses another challenge for organizations. Since we are continually evolving to a decentralized workforce, remote access must be retained. The key to secure remote access is authentication and encryption. Authentication ensures the user is who they say they are. Typically, this is a username and password, but should also include a second factor where possible to ensure security. Encryption ensures the communication between the remote user and the corporate environment is secure. The data the remote user is working with may be sensitive and should be kept securely. VPNs play a huge role in this process. These would be referred to as compensating controls given that the physical controls for the environment are not enforceable for remote users.

Identification, Authentication, and Authorization

Key concepts for this domain also include identification, authentication, and authorization. Identification requires no proof and it is not relied upon for any access. Authentication is the

process of verifying identity, such as getting proof in addition to the identity like a password and a second factor. Authorization is the process of ensuring a properly authenticated user is given proper access to objects and resources within the network. Understanding the differences between each of these terms is critical to many questions on the CISA exam.

Term	Definition
Plaintext	The original, unencrypted message, file, or stream.
Ciphertext	The encrypted message, file, or stream.
Encryption	The process of transforming plaintext into ciphertext through the use of an encryption algorithm.
Hash function	A cryptographic operation on data that returns a fixed length result—used to verify integrity.
Message digest	The output of a cryptographic hash function.
Digital signature	The result of encrypting the hash of a message with the sender's private key.
Algorithm	The mathematical formula used to perform encryption, decryption, digests, or signatures.
Decryption	The process of transforming ciphertext back into plaintext through the use of a cryptographic function.
Cryptanalysis	An attack used against a cryptosystem to find the encryption key that has been used.
Encryption key	A block of characters used in an encryption algorithm to encrypt or decrypt a stream or block of data or to create and verify a digital signature.
Key encrypting key	A key used to encrypt another key.
Key length	The size of an encryption key—generally measured in bits.
Block cipher	An encryption algorithm that works on blocks of data.
Stream cipher	An encryption algorithm that works on a continuous stream of data such as video or wireless networks.
Initialization vector	A random number used to introduce additional entropy into some ciphers.
Symmetric encryption	A method of encryption that uses the same key for both encryption and decryption.

Asymmetric encryption (public key encryption)	A method of encryption, decryption, and digital signatures that uses a pair of encryption keys called a public key and a private key.
Key exchange	The process of exchanging encryption keys used in a symmetric encryption scheme.
Nonrepudiation	A digital signature property whereby a sender cannot refute the sending of a message because it was signed by their private key.

Encryption and Public Key Infrastructure

Public key infrastructure (PKI) was designed to solve the problem of secure and reliable key exchange, storage, and management. The key components of PKI are: digital certificates, certificate authority, registration authority, certificate revocation list, and certification practice statement. Digital certificates are the certificates assigned to members of the PKI and contains their public key and a block of information that identifies the owner. This typically includes information like an email address, name, organization name, and organizational unit. The certificate authority (CA) is the entity that assigns the certificates and publishes them. The CA ensures the identity of the certificate holder is who they say they are. The registration authority (RA) is typically part of the CA, but sometimes it is separate. It is responsible for ensuring the registration process goes smoothly. It verifies the information provided to it in the certificate signing request and may look at government issued ID or other information to verify identity. The certificate revocation list (CRL) is responsible for maintaining a list of certificates that have been revoked for some reason. This may be used if a private key was stolen or if a user was terminated. Other CAs and entities who trust the CA should consult with the CRL to ensure the validity of a certificate before accepting it. The certification practice statement is a published statement that describes how the CA issues and manages their digital certificates. This helps understand the strength of the certificate issued from this CA.

Threats

Malware Threats

A common threat to the security of information assets is malware. Malware comes in many forms, some of which are: viruses, worms, Trojan horses, spyware, rootkits, and bots. The threats posed by these malwares varies from general performance issues to stolen or deleted data. Malware can get into an organization in many ways. The most common way is through malicious attachments in email or through unauthorized USB devices. However, malware can also find its way in by exploiting machines with missing patches, exploiting software vulnerabilities, insecure configurations, or fault architecture. Some administrative controls to address malware are: spam policies, business-related internet access, restrict removable media,

restrict file downloads, ensure proper permissions on the workstations, and no personally-owned computers. We can also impose technical controls to limit malware within an environment by using advanced anti-malware tools that look at memory as well as on disk, ensuring wide-spread deployment of anti-malware tools on workstations and servers, enforcing a web filter, using DLP systems, reducing end-user privileges, using an IPS, blocking removable media, removing internet access on servers, booting servers from protected images, and blocking read-only objects.

Environmental Threats

It's important to remember that not only are we up against malicious actors, but also environmental variables. Some important environmental threats and vulnerabilities to be familiar with are: electric vulnerabilities like surges, spikes, inrushes, noise, dropouts, brownouts, and blackouts; and physical vulnerabilities like temperature, humidity, dust and dirt, smoke and fire, and earthquakes.

Spikes and surges are rapid increases in voltage that are short-lived, but can provide incredible damage to electrical components. Inrushes are a sudden increase in current that can lead to a voltage drop to critical components. Noise is electromagnetic interference for incoming power. Dropout is a momentary loss of power that lasts a very short time. Brownouts are a sustained drop in voltage that can last for several hours. Blackouts are a complete loss of electricity. To combat these electrical vulnerabilities, we can use UPSs, generators, and dual power feeds. This will allow us to reduce the potential for service disruption and allow us to operate during times of less than optimal electrical power.

Fire suppression is a key component to protecting information assets. There are many types of centralized fire suppression systems. The best for computer equipment is typically inert gas since it will not adversely impact the electronic components, but can still put out the fire.

Type	Description
Wet pipe	All sprinkler pipes are filled with water. Each sprinkler head has a heat-sensitive bulb which triggers when a pre-set temperature is reached, causing a water dispersal to put out the fire.
Dry pipe	Dry pipes are often used when temperatures can go below freezing for periods of time. The pipes are filled with compressed air, which temperature causes the bulbs to break, a valve lets water into the pipes to then put out the fire.
Pre-action	Commonly found in datacenters, this system is basically dry pipes until another event occurs like a smoke alarm, which then fills

	the pipes with water. If the ambient temperature is high enough to break the bulbs, the heads release water, which will put out the fire.
Deluge	This system is like the dry pipe system without the ambient temperature sensors. When an alarm is triggered, the pipes fill with water and put out the fire.
Inert gas	This is the best choice for electronic equipment because it does not impact the components, but can still put out the fire by displacing oxygen. The gas often used now is FM-200.

Physical Security

Physical security is also a concern when protecting information assets. The most common physical security threats are: theft, sabotage, espionage, covert listening devices, tailgating, propped doors, and poor visibility. Tailgating is a technique that malicious actors may use to gain physical access to a building. It involves following an employee into a building without having to show their own security badge. It's commonly referred to as piggybacking as well. Some countermeasures that can be deployed for physical security are: keycard systems requiring every user to badge-in to gain access, cipher locks requiring users to know a code to gain access to the building, fences and walls, bollards, video surveillance, visual notices, bug sweeping, security guards, and guard dogs.

Auditing of Information Asset Protection Controls

Auditing information asset protection is a critical component to passing the CISA as well. The critical components to audit are: security management, logical access controls, network access paths, access management, user access controls, password management, user access provisioning, employee terminations, access logs, investigative procedures, points of presence, network security controls, network access controls, network change management, vulnerability management, environmental controls, physical security controls, and physical access controls.

Audit target	**Process**
Policies, processes, procedures, and standards	Request and review IS policies to determine what processes are required. From there, request appropriate process and procedure documentation. Verify adequate coverage for each topic as compared to an industry standard like ISO 27001.

Records	For any security management process with record keeping, the business records should be examined to determine adherence to the processes.
Security Awareness Training Program	Examine training materials, procedures, and records to determine effectiveness. During interviews, questions should be asked to verify that SAT has been done and that it has been effectively retained.
Data ownership and management	Ask about the methodology used to ascertain ownership and management of data. Determine whether there are any company-wide policies for data management or if it is unstructured.
Data custodians	If custodians are used, the auditor should determine if the custodian discharges the wishes of the owner or if they decide on their own.
Security administrators	If IT staff is responsible for this, the auditor should determine if the IT staff are knowledgeable and qualified to handle this responsibility.
New and existing employees	Determine if any policies and security awareness training exists to ensure individuals are aware of their role in securing company data and not misusing it.

Auditing network paths is import as it ensures there are undocumented paths of access for users that are not taken into account in the security policies. This would include ensuring that all WiFi is accounted for and controlled.

Auditing user access controls should include a focus on authentication, authentication bypass, access violations, user account lockouts, IDS/IPS, dormant accounts, shared accounts, system accounts, and any jump servers.

Auditing password management should draw your attention towards: password standards/policies, minimum length of the passwords, complexity requirements, expiration, history enforcement, minimum time between changes, display configuration, transmission, storage, account lockouts, access to encrypted passwords, and password vaulting.

Auditing user access provisioning should include a focus on: access request processes, access approvals, new employee provisioning (onboarding), segregation of duties, and access reviews.

Auditing employee termination processes should include: the termination process itself, timeliness of completed requests, access reviews to ensure proper adherence, and contractor access and terminations. If the termination processes do not account for each of the above, it should be considered deficient and recommendations be made to ensure all are accounted for.

Access Logs and Investigative Procedures

In order to make use of access logs, they should be audited. They do not provide much benefit if they are not reviewed and actionable. The auditor should determine which events are recorded and what information is included in those. The auditor should also understand the technical aspects of the system enough to know what should be logged to make effective recommendations. A note should be made noting whether the logs are decentralized or aggregated and centralized. The auditor should also ensure the access logs are protected from alteration and destruction. Policies should ensure access logs are reviewed routinely and the auditor should determine if that is adhered to. The auditor should also ensure retention of logs in accordance with policy, industry standard, and compliance. Additionally, the auditor should determine whether or not the organization is alerted to log events.

Investigative procedures for the organization should also be audited as part of this domain. The key things to review are: investigation policies and procedures, computer crime investigations, and computer forensics. First, the auditor should determine if there are any policies for investigations. If there are, the auditor needs to ensure this includes information on who is responsible for investigating, where information about investigations is stored, and where they're reported. It should also be determined if there are policies and procedures related to computer crime investigations. Part of this processes is the auditor understanding how to relay the results of internal investigations to law enforcement. Finally, the auditor should determine if there are any policies and procedures related to computer forensic investigations. The tools that are used and techniques should be noted. Also, the auditor should determine the level of qualifications of any trained investigators.

Internet points of presence should be reviewed as well such as search engines, social networking sites, online sales sites, and domain names to determine the spread of organizational information. Search engines may contain valuable company information that may need to be eradicated. Social networking sites may contain unauthorized disclosing of information that should be investigated. Online sales sites may contain company information or hardware for sale that the company should be aware of and notify law enforcement about. Domain names should also be investigated to ensure contact information is verified.

Network security controls should be audited to ensure proper protection of information assets. Typically, this is done by performing an architecture review, which should include a review of architecture documents, ensure support of business objectives, compliance with security policy, comparisons of documented versus actual architecture, and the change and review processes.

Network access controls should be audited as well. Particular attention should be paid to user authentication, firewalls, IDS/IPS, web filtering, cloud access security broker, DLP systems, remote access configurations, jump servers, dial-up modems, and wi-fi access points. Proper configuration and adherence to both company policy and industry standards should be ensured through this review.

Network change management should be audited as well to determine the effectiveness of any policies and procedures in place. This audit should include a review of the change control policy, change logs, change control procedures, emergency changes, any rolled-back change policies, documentation updates, and any links to a development lifecycle.

Vulnerability management should be audited to ensure a company is doing what they can to be proactive in their approach to securing information assets. This audit should review alert management to determine responsiveness, infrastructure penetration testing, application penetration testing, and patch management procedures.

Auditing of environmental controls is very important as well. This should include noting and reviewing any power conditioning equipment such as line conditioners or UPS. This should also include backup power, HVAC systems, water detection, fire detection and suppression, and cleanliness of the datacenter.

Physical security controls should be audited. As part of this audit, the auditor should determine and note the proximity to hazards such as dams, rivers/lakes, fault lines, volcanoes, airports, and freeways. The auditor should also look for any external marking on the building indicating what's inside.

Finally, physical access controls should be audited and tested. These controls include physical barriers, surveillance, guards and guard dogs, and keycard systems. Auditing these systems, the auditor should make sure they understand how each layer works together to provide comprehensive security and how they may be improved to better achieve organizational objectives and goals.

Exam Practice Questions

1. Why would an IS auditor want to review the organizational chart during the course of an audit?
    a. To increase efficiency in each business unit
    b. To gain an understanding of the workflow
    c. To understand the separation of duties in the IS department
    d. To understand responsibilities and authority of every person in the organization

Correct Answer is D – Understanding the organizational chart of an organization can give an auditor a quick view into the structure of the organization, which may allow them to find easy recommendations in the event of single points of failure or continuity.

2. What is audit risk?
    a. Detection risk
    b. Inherent risk
    c. Control risk
    d. All of the above

Correct Answer is D – Audit risk is the combination of control risk, detection risk, and inherent risk. Control risk is the risk that a material error exists that is undetectable by the control framework in use by the organization. Detection risk is the risk that an auditor may inadvertently overlook errors in the course of an audit. Inherent risk is risk that errors are inherent in the business processes and compensating controls do not exist to resolve.

3. Which concern is paramount for an IS auditor while he performs a forensic investigation?
    a. Preservation of data
    b. State of host operating system
    c. Disclosing hidden code found in the analyzed data
    d. Hash totals

Correct Answer is A – The primary concern of a forensic auditor should be the preservation of data. If the data is not preserved correctly, it may be inadmissible in court and/or invalidate all findings of analysis.

4. Which audit technique will provide the auditor with the best evidence of segregation of duties?
    a. Reviewing the structure of the organizational chart
    b. Interviewing upper management
    c. Informally talking with middle management and end-users
    d. Observation and interview results

Correct Answer is D – The best way for an auditor to determine the implementation of segregation of duties is through interviews and observation. This allows the auditor to ask

questions that will lead him to the answer rather than simply relying upon documentation that may be dated or loosely followed internally.

5. Which of the following application risks is the greatest danger to an organization?
    a. Keylogging
    b. Payload stager
    c. File inventorying
    d. Unwanted outbound connections

Correct Answer is D – Unwanted outbound connections are far and away the largest risk listed. This risk would allow a machine to be a staging ground for further attacks or allow information to be siphoned off unknown to the organization. This would also allow an attacker to attack other machines internally from a "trusted" machine on the network.

6. A critical function of a firewall is:
    a. Traffic routing
    b. Traffic filtering
    c. Traffic logging
    d. Traffic decryption

Correct Answer is B – While a firewall can perform many functions, it's primary role is as that of a traffic filter. This allows an organization to implement a policy in accordance with internal policy documentation that enforces the agreed-upon rules of the organization. More advanced firewalls will also allow the organization to perform more in-depth analysis of traffic and make baselining risk and detection capabilities more robust.

7. Which RAID level provides the greatest level of redundancy?
    a. RAID 6
    b. RAID 0
    c. RAID 1
    d. RAID 5

Correct Answer is A – RAID 6 can withstand the failure of two disks within an array due to the fact that there are two parity blocks used instead of one. RAID 5 can withstand one drive failure; RAID 0 is a stripped volume so it cannot withstand any failures; RAID 1 can withstand a single disk failure.

8. What is recovery point objective?
    a. The amount of time it takes to recover in the event of a disaster
    b. The period for which recent data will be lost in a disaster
    c. The number of point-in-time backups retained for a disaster
    d. The point at which a disaster necessitates a recovery

Correct Answer is B – Recovery point objective is the period for which data will be lost in a disaster. It's typically measured in hours or days. So, an RPO of 4 hours means a company will

lose 4 hours of data in the event of a disaster. Likewise, RTO is the time it takes for recovery to occur.

9. What is the primary responsibility of the data administrator?
    a. Developing data dictionary system software
    b. Developing physical database structures
    c. Maintaining database system software
    d. Defining data elements, data names, and their relationships

Correct Answer is D – The primary responsibility of a data administrator is to define data attributes like names, elements, and their relationships to one another.

10. Which of the following tools is best for testing software modules?
    a. Desk checking
    b. Documented process walkthrough
    c. Blackbox testing
    d. Developer interviews

Correct Answer is C – Blackbox testing is the best way to test an application or modules of an application because it looks at it the same way a hacker would, which is the most accurate way to calculate the risks associated with it.

11. While reviewing the IT infrastructure, an IS auditor notices that storage resources are continuously being added. The IS auditor should:
    a. Recommend disk mirroring or RAID 1
    b. Recommend implementation of a change control process
    c. Review the capacity management process
    d. Recommend a compression algorithm

Correct Answer is C – If storage is constantly needing to be adjusted, it is indicative of a shortcoming in the capacity planning process. This shortcoming could result in downtime if proper utilization is not accounted for at the worst. The best case scenario is that a lot of man-hours are lost on the inefficiency associated with constantly having to be reactive rather than proactive.

12. Which control is the best method to ensure that data in a file has not been changed during transmission?
    a. Hash values
    b. Check digits
    c. Parity bits
    d. Reasonableness check

Correct Answer is A – Hash values are the best way to verify file integrity since they take into account the contents of the file and are hard to duplicate with strong algorithms such as SHA256 or SHA512.

13. Which of the following is the most effective technical control for enforcing an internal acceptable use policy?
    a. Routing inbound internet traffic through a reverse proxy server
    b. Implementing a basic firewall with appropriate access rules
    c. Routing outbound traffic through a content-filtering proxy server
    d. Requiring users to sign an agreement

Correct Answer is C – The best way to enforce an acceptable use policy with a technical control is ensuring outbound internet traffic flows through a content filter. This ensures that policies are set on the content filter and are enforced equally for all users.

14. At which layer of the OSI model do confidentiality, authentication, and data integrity services for transmissions operate?
    a. Presentation layer
    b. Session layer
    c. Network layer
    d. Physical layer

Correct Answer is C – Most confidentiality, authentication, and data integrity controls operate at the network layer. Some of these controls can operate at higher layers when focused on files and not the transmission of data.

15. The Annual Loss Expectancy of a risk without compensating or mitigating controls is expected to be $100,000. You recommend a control that will save 60% of the loss at an annual cost of $30,000 over the life of the process. Is this a justifiable expenditure?
    a. No. ALE is not a reliable metric to use for justifying a control
    b. No. The savings of implementing the control is insufficient to justify the expenditure
    c. Maybe, but it depends on the risk appetite of the organization
    d. Yes, the new cost of the risk is lower than the cost of the control

Correct Answer is D – The answer is yes because the total cost of an uncompensated or unmitigated risk in this instance is $100,000. Mitigating the risk to 60%, the total cost comes to $40,000. Comparing the new cost of the risk to the cost of the control ($30,000), we see that this is an easily justifiable spend of security budget.

16. Which of the following is most true regarding manual controls versus automated controls?
    a. Manual controls require human interaction while automated controls do not, but the difference is inconsequential in an audit

b. Manual controls only require human interaction in the early stages, while automated controls are fully independent
c. Automated controls are not susceptible to human error while manual controls are, which should be taken into account during an audit
d. There is no difference

Correct Answer is C – Automated controls are setup once and run independently without human intervention. Manual controls require a human to follow documentation to produce the desired outcome. This leaves manual controls susceptible to human error, which should be taken into account in audits. Documentation should be clear, thorough, and revisited often when updates or changes should occur. Multiple people should be trained to use the documentation as well.

17. If an environment is properly segmented and separation of duties is adhered to, which role is incompatible with that of the Quality Assurance group?
    a. Computer operator
    b. Security administrator
    c. Database administrator
    d. Systems analyst

Correct Answer is D – In a properly segmented environment, the role of systems analyst does not exist under the group of quality assurance. This role is part of software development and entails the design of applications, technical requirements, and development of test plans. The quality assurance group should be the group responsible for checking behind the systems analyst to ensure documentation is sufficient for checking the quality of software.

18. To whom should an internal IS auditor report?
    a. IS management / director
    b. Business unit management
    c. Senior management
    d. Shareholders

Correct Answer is C – An internal IS auditor needs independence. They need enough authority that their recommendations carry weight. They should be able to make recommendations freely without fear of reprisal or castigation from within the business units. As such, they are typically found outside of the normal chain of command.

19. What is the difference between compliance testing and substantive testing?
    a. Compliance testing determines if controls have been properly designed and implemented, and functioning correctly. Substantive testing determines the integrity and accuracy of transactions that flow through processes and IS
    b. Compliance testing is only concerned with ensuring adherence to compliancy regulations while substantive testing is concerned with ensuring adherence to industry-wide standards.

c. Compliance testing focuses on the processes of the business, while substantive testing focuses on IS processes.
d. Substantive testing is a part of compliance testing.

Correct Answer is A – Compliance testing attempts to ensure that control procedures have been properly designed and implemented. It is also concerned with whether or not the control is functioning as it should. It often examines things such as change and configuration management processes. Substantive testing attempts to ensure the accuracy and integrity of information flow. An example would be test transactions that are followed and tested at each phase of the process.

20. What is/are the primary measurements used to determine the effectiveness of a biometric system?
    a. False reject rate
    b. False accept rate
    c. Crossover error rate
    d. All of the above

Correct Answer is D – Biometric systems are judged by three main metrics: false reject rate, false accept rate, and crossover error. False reject rate is when valid users are rejected erroneously—margin of error is too small. False accept rate is when unauthorized users are accepted in error—margin of error is too large. Crossover error rate is the point where the false reject rate is equal to the false accept rate—this is the balance you want to strike for biometric systems.

21. What is the difference between reduced sign-on and single sign-on?
    a. Reduced sign-on is the consolidation of credentials needed for users to access services, while single sign-on is the reduction in the number of times a user must login
    b. They are interchangeable terms
    c. Reduced sign-on is the limitation placed on user accounts such that they can only login at certain times of the day, while single sign-on is a method in which the user only has to login once to access all services
    d. Both a and b

Correct Answer is A – Reduced sign-on is where authentication repositories are consolidated such that individual applications all use a single source of authentication. This ensures users do not have to remember many different credentials for different applications. Single sign-on is an environment where many applications in an environment are aware of the authentication status for a user such that the user does not have to login again with the same credentials.

22. What is the strongest measure an auditor can recommend for an organization to secure their Wi-Fi network?
    a. Disable SSID broadcast
    b. Implement MAC address filtering

c. Use a 12-character or longer pre-shared key
d. Implement 802.1x certificate-based authentication

Correct Answer is D – The strongest form of wireless authentication is to use 802.1x with a requirement for a PKI-issued certificate combined with user login. Often this is tied to RADIUS or Active Directory. Disabling SSID broadcast should not be considered a strong control as a malicious actor will be able to easily see the network regardless. Security through obscurity is rarely an effective technique, but can be used as part of a defense-in-depth strategy. MAC address filtering is a step up, but is still relatively easily bypassed by hackers who can manually change their MAC addresses to match those they see actively connected to the network. Using a long, complex pre-shared key is a good option, but it must be rotated manually and often to ensure security. This introduces complexity and the chance for human error. It must also be combined with strong encryption greater than RC4.

23. Which of the following is an example of asymmetric, or public key, cryptography?
    a. AES
    b. ECC
    c. DES
    d. Blowfish

Correct Answer is B – Elliptic curve cryptography is an example of asymmetric encryption. Asymmetric encryption refers to two different keys being used for different reasons. The private key is used to decrypt content that has been encrypted with the public key. This ensures only the intended recipient can read the content. Signing the content with the private key then means others can be sure the content came from the proper sender. The other options listed are examples of symmetric encryption where only a single key is used for encryption and decryption. These types of applications typically combine a password as a point of entropy and security for the key. These are best used in one-way communications between a small number of users and require the password or entropy key to be sent in an out of band method.

24. What constitutes a tier 4 data center reliability rating?
    a. Single-path cooling and power distribution
    b. Multi-path, single-active cooling and power distribution without a raised floor
    c. Multi-path, dual-active cooling and power distribution with a raised floor
    d. Multi-path, single-active cooling and power distribution with a raised floor

Correct Answer is C – Tier 4 is the highest rated datacenter. It is fully redundant in every aspect (UPS, generator, and cooling distribution) and has a raised floor. Tier 1 contains a single-path power and cooling. A UPS, generator, and a raised floor are not requirements. Tier 2 may have redundant components for cooling, but power is single-path. Maintenance typically requires downtime in Tier 2 datacenters. Tier 3 datacenters include multi-path, single active cooling and power with a raised floor, UPS, and generator.

25. During the course of an audit, an IS auditor discovered a network switch plugged in at a user's desk. What action should the auditor take?
    a. Include the finding in the report
    b. Ask the employee to remove the switch when they are finished
    c. Include a review of the switch in the scope of the audit
    d. Report the finding immediately as high-risk

Correct Answer is D – This finding is high-risk and should be reported directly to management to ensure timely corrective action. A rogue switch can allow unsecured access to the network to a physically-present malicious actor. It can also pose risk to network reliability.