Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 2 of the official CISSP study guide. Here are the top things that you need to know from this chapter on personnel security and risk management concepts.

Understand the security implications of hiring new employees. To properly plan for security, you must have standards in place for job descriptions, job classification, work tasks, job responsibilities, the prevention of collusion, candidate screening, background checks, security clearances, employment agreements and non-disclosure agreements. By deploying these mechanisms, you ensure that new hires are aware of the required security standards, protecting your organization's assets.

Understand onboarding and offboarding. Onboarding is the process of adding new employees to the organization using socialization and orientation. Offboarding is the removal of an employee's identity from the identity and access management system once that person has left the organization.

Know the principle of least privilege. The principle of least privilege states that users should be granted the minimum amount of access necessary for them to complete their required work tasks or job responsibilities. Know about employee oversight. Throughout the employment lifetime of personnel, managers should regularly review or audit the job descriptions, work tasks, privileges and responsibilities of every staff member.

Know why mandatory vacations are necessary. Mandatory vacations of one to two weeks are used to audit and verify the work tasks and privileges of employees. This often results in the easy detection of abuse, fraud or negligence. Know about UBA and UEBA. User behavior analytics UBA and user and entity behavior analytics UEBA are the concepts of analyzing the behavior of users, subjects, visitors, customers etc for some specific goal or purpose.

Understand employee transfers. Personnel transfers maybe treated as a termination and rehire rather than a personnel move. This depends on the organization's policies and the means they have determined to best manage this change. Some of the elements that go into making the decision as to which procedure to use include whether the same user account will be retained, if their clearance will be adjusted, if their new work responsibilities are similar to the previous position and if a clean slate account is required for auditing purposes in the new job position.

Be able to explain proper termination policies. A termination policy defines the procedure for terminating employees. It should include items such as always having a witness, disabling the employee's network access and performing an exit interview. A termination policy should also include escorting the terminated employee off the premises and requiring the return of security tokens and badges and other company property.

Be able to define overall risk management. The process of identifying factors that could damage or disclose data, evaluating those factors in light of data value and countermeasure cost and implementing cost-effective solutions for mitigating or reducing risk is known as risk management. By performing risk management, you lay the foundation for reducing risk overall.

Understand risk analysis and the key elements involved. Risk analysis is the process by which upper management is provided with details to make decisions about which risks are to be mitigated, which should be transferred and which should be accepted. To fully evaluate risks and subsequently take the proper precautions, you must analyze the following, assets, asset valuation, threats, vulnerabilities, exposure, risk, realized risk, safeguards, countermeasures, attacks and breaches.

Know how to evaluate threats. Threats can originate from numerous sources including IT, humans and nature. Threat assessment should be performed as a team effort to provide the widest range of

perspectives. By fully evaluating risks from all angles, you reduce your system's vulnerability.

Understand qualitative risk analysis. Qualitative risk analysis is based more on scenarios than calculations. Exact dollar figures are not assigned to possible losses. Instead, threats are ranked on a scale to evaluate their risks, costs and effects. Such an analysis assists those responsible for creating proper risk management policies.

Understand quantitative risk analysis. Quantitative risk analysis focuses on hard values and percentages. A complete quantitative analysis is not possible because of intangible aspects of risk. The process involves valuing assets and identifying threats and then determining a threat's potential frequency and the resulting damage, which leads to the risk response tasks of the cost benefit analysis of safeguards.

Know what single loss expectancy SLE is and how to calculate it. SLE is an element of quantitative risk analysis that represents the cost associated with a single realized risk against a specific asset. The formula is SLE equals asset value AV times the exposure factor EF.

Know what annualized loss expectancy, ALE is and how to calculate it. ALE is an element of quantitative risk analysis that represents the possible yearly cost of all instances of a specific realized threat against a specific asset. The formula is ALE equals single loss expectancy, SLE times annualized rate of occurrence ARO.

Know the formula for safeguard evaluation. In addition to determining the annual cost of a safeguard, you must calculate the ALE for the asset if the safeguard is implemented. Use the formula ALE before safeguard minus ALE after safeguard minus annual cost of safeguard equals the value of the safeguard to the company.

Know the options for handling risk. Reducing risk or risk mitigation is the implementation of safeguards and countermeasures. Assigning risk or transferring a risk places the cost of loss, a risk represents onto another entity or organization. Purchasing insurance is one form of assigning or transferring risk. Risk deterrence is the process of implementing deterrence to would-be violators of security and policy. Risk avoidance is the process of selecting alternate options or activities that have lower associated risk than the default, common, expedient or cheap option. Accepting risk means management has evaluated the cost benefit analysis of possible safeguards and has determined that the cost of the countermeasure greatly outweighs the possible cost of loss due to the risk. It also means that management has agreed to accept the consequences and the loss of the risk if realized.

Understand security control assessment SCA. An SCA is the formal evaluation of a security infrastructure's individual mechanisms against a baseline or reliability expectation. Understand security monitoring and measurement. Security controls should provide benefits that can be monitored and measured. If a security control's benefits cannot be quantified, evaluated or compared, then it does not actually provide any security.

Understand risk reporting. Risk reporting involves the production of a risk report and a presentation of that report to interested and relevant parties. A risk report should be accurate, timely, comprehensive of the entire organization, clear and precise to support decision making. It should be updated on a regular basis.

Understand the risk maturity model RMM. The risk maturity model is a means to assess the key indicators and activities of a mature, sustainable and repeatable risk management process. The RMM levels are Ad-Hoc, preliminary, defined, integrated and optimized.

Know about legacy system security risk. Legacy systems are often a threat, because they may not be

receiving security updates from their vendors. End of life EOL is the point at which a manufacturer no longer produces a product. End of service life EOSL or end of support EOS are those that are no longer receiving updates or support from the vendor.

Understand social engineering. Social engineering is a form of attack that exploits human nature and human behavior. The common social engineering principles are authority, intimidation, consensus, scarcity, familiarity, trust and urgency. Social engineering attacks may be used to elicit information or gain access through the use of pretexting and or prepending. Social engineering attacks include phishing, spear phishing, business email compromise, whaling smishing, vishing, spam, shoulder surfing, invoice scams, hoaxes, impersonation, masquerading, tailgating, piggybacking, baiting, dumpster diving, identity fraud, typosquatting and influence campaigns.

Know how to implement security awareness training and education. Before actual training can take place, awareness of security as a recognized entity must be created for users. Once this is accomplished, training or teaching employees to perform their work tasks and to comply with the security policy can begin. All new employees require some level of training so that they will be able to comply with all standards, guidelines and procedures mandated by the security policy. Education is a more detailed endeavor in which students and users learn much more than they actually need to know to perform their work tasks. Education is most often associated with users pursuing certification or seeking job promotion.

Know about the need for periodic content reviews and effectiveness evaluations. It's important to perform periodic content reviews of all training materials. This is to ensure that the training materials and presentations stay in line with business goals, organizational mission and security objectives. Some means of verification should be used to measure whether the training is beneficial or a waste of time and resources. Those are the study essentials that you need to know for chapter 2, personnel security and risk management concepts.

From:
http://www.trident365.com/ - **三叉戟**

Permanent link:
http://www.trident365.com/doku.php?id=projects:cissp:chapter2

Last update: **2025/05/18 17:14**