2025/10/5 看了CyberSecurity Architect Handbook的书，作者提到CISM也是推荐架构师考的一个证书，所以我准备放到明年的目标中去。 查了一下， 受験費用 ISACA会員 $575 (非会員$760) ※4 新入会員US$175国際会費US$145東京支部US$30 合格了之后，申请认证需要50USD如果先成为会员，再报名考试，则需要750USD比非会员要便宜，而且买书也会便宜点。 公司估计愿意报销考试费，但不愿意报销会员费吧，直接760USD考，然后申请认证的50USD自己出，但认定通过后还是要交会员费和支部会员费的。 东京有好3个考场（当然线上考也可以），高田马场，新桥，秋叶原。周末没有座位，只能平日，而且一天只有上午10点和下午2点可以选。 4小时，150道题，4个Domain难度上来说小于CISSP和CCSP高于SC不知道是不是。 并且，题目不确定的可以选Flag后面再Review这一点相对来说压力就小好多了。 两本参考书Questions的就没有必要买了Review Manual可以入手一本，日亚是是3万日元。 https://www.amazon.co.jp/CISM%E3%83%AC%E3%83%93%E3%83%A5%E3%83%BC%E3%83%9E%E3%83%8B%E3%83%A5%E3%82%A2%E3%83%AB%E3%80%81%E7%AC%AC16%E7%89%88-Isaca/dp/1604209011/ 但官网电子书是139USD只要2万日元。 https://destcert.com/cism-certification-guide/

Mike Study Plan WK1:

1. Begin Reading Chapter 1 of the CISM Study Guide
2. Finish Reading Chapter1 of the CISM Study Guide
3. Watch LinkedIn CISM1 Section 1-4
4. CISM Study Guide Chapter1 Review Questions
5. Take a well-deserved break!

WK2:

1. Begin Reading Chapter 2 of the CISM Study Guide
2. Finish Reading Chapter2 of the CISM Study Guide
3. Watch LinkedIn CISM1 Section 5-9
4. CISM Study Guide Chapter2 Review Questions
5. Take a well-deserved break!

WK3:

1. Begin Reading Chapter 3 of the CISM Study Guide
2. Finish Reading Chapter 3 of the CISM Study Guide
3. Watch LinkedIn CISM2 Section 1-6
4. CISM Study Guide Chapter3 Review Questions
5. Take a well-deserved break!

WK4:

1. Begin Reading Chapter 4 of the CISM Study Guide
2. Finish Reading Chapter 4 of the CISM Study Guide
3. Watch LinkedIn CISM2 Section 7-12
4. CISM Study Guide Chapter4 Review Questions
5. Take a well-deserved break!

WK5:

1. Begin Reading Chapter 5 of the CISM Study Guide
2. Finish Reading Chapter 5 of the CISM Study Guide
3. Watch LinkedIn CISM3 Section 1-4
4. CISM Study Guide Chapter5 Review Questions
5. Take a well-deserved break!

WK6:

1. Begin Reading Chapter 6 of the CISM Study Guide
2. Finish Reading Chapter 6 of the CISM Study Guide
3. Watch LinkedIn CISM3 Section 5-9
4. CISM Study Guide Chapter6 Review Questions
5. Take a well-deserved break!

WK7:

1. Begin Reading Chapter 7 of the CISM Study Guide
2. Finish Reading Chapter 7 of the CISM Study Guide
3. Watch LinkedIn CISM3 Section 10-13
4. CISM Study Guide Chapter7 Review Questions
5. Take a well-deserved break!

WK8:

1. Begin Reading Chapter 8 of the CISM Study Guide
2. Finish Reading Chapter 8 of the CISM Study Guide
3. Watch LinkedIn CISM4 Section 1-3
4. CISM Study Guide Chapter8 Review Questions
5. Take a well-deserved break!

WK9:

1. Begin Reading Chapter 9 of the CISM Study Guide
2. Finish Reading Chapter 9 of the CISM Study Guide
3. Watch LinkedIn CISM4 Section 4-6
4. CISM Study Guide Chapter9 Review Questions
5. Take a well-deserved break!

2025/10/22 今天再次试用1个月的领英会员，然后把CISM的Mike的课程的一小部分下载好了。

其他参考书： https://leanpub.com/cismlastmile 10美元
https://www.youtube.com/playlist?list=PL7XJSuT7Dq_UffFGcmTvKL7JeHweC5HKU

WHY should you take ISACA's CISM exam after the CISSP? HOW can you do it quickly? Read on...

1 CISM is LESS TECHNICAL than CISSP It focuses much more on process and governance. Your technical depth from CISSP is more than enough!

2 CISM is MORE STRATEGIC in its focus than CISSP It provides substantial high value leadership knowledge, complementing your CISSP foundation, expanding your perspective as a security leader.

3 CISM exam is more narrow in terms of subject matter This makes preparation faster vs CISSP for most candidates.

HOW can you prepare quickly?

 CISM Exam Prep: The Complete Course 11+ hours, FREE on YouTube, https://lnkd.in/g-_NnxEP

 CISM: The Last Mile ($10 on Leanpub) Targeted coverage of every topic on the exam syllabus.

https://lnkd.in/ds2AWV2q

 CISM Questions, Answers, and Explanations (ISACA) The book version of 1000 questions is half the price of the online test bank. https://amzn.to/447IuQl

Online Practice Quizzes (PocketPrep) Affordable and effective option to augment what comes with study guides (~$21/mth). Get it at https://lnkd.in/g5nm6c4k

https://www.scworld.com/sc-awards-finalists CISM和CISA CCSP一并被列为最受欢迎的IT资格，虽然有人说ISC2的ISSMP也能代替CISM的位置，但它需要等2年才能考，所以这期间如果公司允许的话，还是考一个CISM吧。

12-12 今天收到通知说CISM要在2026年Q4改考試大纲，所以还是趁早考吧 1-20 CISM合格后，需要在5年内申请认定，共需要5年工作经验，有CISSP可以减免2年，这样只要3年。 即使Rezil找不到人证明KPMG找李桑（时长是2年9个月），然后下一家公司找老板证明也是可以的。

# Mike Chapple CISM Chapter Essentials

## Chapter1 Today's Information Security Manager

**Know the three objectives of cybersecurity.** *Confidentiality* ensures that unauthorized individuals are not able to gain access to sensitive information. *Integrity* ensures that there are no unauthorized modifications to information or systems, either intentionally or unintentionally. *Availability* ensures that information and systems are ready to meet the needs of legitimate users at the time those users request them. **Describe how information security strategies should be aligned with organizational goals and objectives.** As information security managers develop their plans, they should use reliable techniques to assess the current state of the program, such as threat research, SWOT analysis, and gap analysis. They may then identify the initiatives that will move the organization from the current state to its desired state. **Explain how security strategies are influenced by internal and external factors.** Security strategies must be aligned with the business, but they must also incorporate other influences. Information security managers must remain abreast of emerging technologies, social media, the business environment, the organization's risk tolerance, regulatory requirements, third-party considerations, and the threat landscape as they develop, monitor, and revise cybersecurity strategies. **Know why stakeholder commitment and communication are essential to success.** As information security leaders roll out new strategies, they must ensure that they have the support of senior leaders and other stakeholders. They may do this by clearly outlining how information security supports the organization's broader goals and objectives, identifying the business impact of security initiatives, and identifying clear success criteria. **Explain how security controls may be categorized based on their mechanism of action and their intent.** Controls are grouped into the categories of managerial, operational, and technical based on the way that they achieve their objectives. They are divided into the types of preventive, detective, corrective, deterrent, compensating, and physical based on their intended purpose. **Describe the diverse impacts of data breaches on organizations.** When an organization suffers a data breach, the resulting data loss often results in both direct and indirect damages. The organization suffers immediate financial repercussions due to the costs associated with the incident response, as well as long-term financial consequences due to reputational damage. This reputational damage may be difficult to quantify, but it may also have a lasting impact. In some cases, organizations may suffer operational damage if they experience availability damages, preventing them from accessing their own information. **Explain why data must be protected in transit, at rest, and in use.**Attackers may attempt to eavesdrop on network transmissions

containing sensitive information. This information is highly vulnerable when in transit unless protected by encryption technology. Attackers also might attempt to breach data stores, stealing data at rest. Encryption serves to protect stored data as well as data in transit. Data is also vulnerable while in use on a system and should be protected during data processing activities. **Know how data loss prevention (DLP) systems block data exfiltration attempts.** DLP technology enforces information handling policies to prevent data loss and theft. DLP systems may function at the host level, using software agents to search systems for the presence of sensitive information. They may also work at the network level, watching for transmissions of unencrypted sensitive information. DLP systems detect sensitive information using pattern-matching technology and/or digital watermarking. **Explain how data minimization reduces risk by reducing the amount of sensitive information that we maintain.** In cases where we cannot simply discard unnecessary information, we can protect information through de-identification and data obfuscation. The tools used to achieve these goals include hashing, tokenization, and masking of sensitive fields.

## Chapter2 Information Security Governance and Compliance

**Governance programs guide and direct security efforts.** Information security governance efforts should integrate with other corporate governance programs to support both the business's goals and its security strategy. Organizations should draw on existing governance frameworks, such as COBIT and the ISO standards, to avoid redundant effort and to align with industry best practices. **Policy frameworks consist of policies, standards, procedures,and guidelines.** Policies are high-level statements of management intent for the information security program. Standards describe the detailed implementation requirements for policies. Procedures offer step-by-step instructions for carrying out security activities. Compliance with policies, standards, and procedures is mandatory. Guidelines offer optional advice that complements other elements of the policy framework. **Organizations often adopt a set of security policies covering different areas of their security programs.** Common policies used in security programs include an information security policy, an acceptable use policy, a data ownership policy, a data retention policy,an account management policy, and a password policy. The specific policies adopted by any organization will depend on that organization's culture and business needs. **Policy documents should include exception processes.** Exception processes should outline the information required to receive an exception to security policy and the approval authority for each exception. The process should also describe the requirements for compensating controls that mitigate risks associated with approved security policy exceptions. **Organizations face a variety of security compliance requirements.** Merchants and credit card service providers must comply with the Payment Card Industry Data Security Standard (PCI DSS). Organizations handling the personal information of European Union residents must comply with the EU General Data Protection Regulation (GDPR). All organizations should be familiar with the national, territory, and state laws that affect their operations. **Standards frameworks provide an outline for structuring and evaluating cybersecurity programs.** Organizations may choose to base their security programs on a framework, such as the NIST Cybersecurity Framework (CSF) or International Organization for Standardization (ISO) standards. U.S. federal government agencies and contractors should also be familiar with the NIST Risk Management Framework (RMF). These frameworks sometimes include maturity models that allow an organization to assess its progress. Some frameworks also offer certification programs that provide independent assessments of an organization's progress toward adopting a framework. **Audits and assessments monitor compliance with requirements.** Audits are externally commissioned, formal reviews of the capability of an organization to achieve its control objectives. Assessments are less rigorous reviews of security issues, often performed or commissioned by IT staff. Organizations providing services to other entities may wish to conduct a service organization controls (SOC) audit under SSAE 18.

## Chapter3 Information Risk Management

**Know how risk identification and assessment helps organizations prioritize cybersecurity efforts.** Cybersecurity analysts try to identify all of the risks facing their organization and then conduct a business impact analysis to assess the potential degree of risk based on the probability that it will occur and the magnitude of the potential effect on the organization. This work allows security professionals to prioritize risks and communicate risk factors to othersin the organization. **Know that vendors are a source of external risk.** Organizations should conduct their own systems assessments as part of their risk assessment practices, but they should conduct supply chain assessments as well. Performing vendor due diligence reduces the likelihood that a previously unidentified risk at a vendor will negatively impact the organization. Hardware source authenticity techniques verify that hardware was not tampered with after leaving the vendor's premises. **Be familiar with the risk management strategies that organizations may adopt.** Risk avoidance strategies change business practices to eliminate a risk. Risk mitigation techniques reduce the probability or magnitude of a risk. Risk transference approaches move some of the risk to a third party. Risk acceptance acknowledges the risk and continues normal business operations despite the presence of the risk. **Understand how disaster recovery planning builds resiliency.** Disaster recovery plans activate when an organization experiences a natural or human-made disaster that disrupts normal operations. The disaster recovery plan helps the organization quickly recover its information and systems and resume normal operations. **Be familiar with the privacy controls that protect personal information.** Organizations handling sensitive personal information should develop privacy programs that protect that information from misuse and unauthorized disclosure. The plan should cover personally identifiable information (PII), protected health information (PHI), financial information, and other records maintained by the organization that might impact personal privacy.

## Chapter4 Cybersecurity Threats

**Be able to describe several key attributes in which threat actors differ.** We can classify threat actors using four major criteria. First, threat actors may be internal to the organization, or they may come from external sources. Second, threat actors differ in their level of sophistication and capability. Third, they differ in their available resources and funding. Finally, different threat actors have different motivations and levels of intent. **Know the many different sources of threat actors.** Threat actors may be very simplistic in their techniques, such as script kiddies using exploit code written by others, or quite sophisticated, such as the advanced persistent threat posed by nation-state actors and criminal syndicates. Hacktivists may seek to carry out political agendas,whereas competitors may seek financial gain. We can group hackers into white-hat, gray-hat, and black-hat categories based on their motivation and authorization. **Be able to explain how attackers exploit different vectors to gain initial access to an organization.** Attackers may attempt to gain initial access to an organization remotely over the Internet,through a wireless connection, or by attempting direct physical access. They may also approach employees over email or social media. Attackers may seek to use removable media to trick employees into unintentionally compromising their networks, or they may seek to spread exploits through cloud services. Sophisticated attackers may attempt to interfere with an organization's supply chain. **Know how threat intelligence provides organizations with valuable insight into the threat landscape.** Security teams may leverage threat intelligence from public and private sources to learn about current threats and vulnerabilities. They may seek out detailed indicators of compromise and perform predictive analytics on their own data. Threat intelligence teams often supplement open source and closed source intelligence that they obtain externally with their own research. **Be able to explain why security teams must monitor supply chain risks.** Modern enterprises depend on hardware,

software, and cloud service vendors to deliver IT services to their internal and external customers. Vendor management techniques protect the supply chain against attackers seeking to compromise these external links into an organization's network. Security professionals should pay particular attention to risks posed by outsourced code development, cloud data storage, and integration between external and internal systems.

## Chapter5 Information Security Program Development and Management

**Be able to describe the purpose of the charter.** The core of the charter is the scope statement, which defines the security objectives included in the program and the portion of the organization covered by the program. The charter should also address the business purpose of the program, a statement of authority, roles and responsibilities,governance structures, documentation, enforcement mechanisms, and processes for periodic program reviews. **Know how metrics are used to assess the efficiency and effectiveness of the information security program.** Key performance indicators (KPIs) are metrics that demonstrate the success of the security program in achieving its objectives. KPIs look at historical performance. Key goal indicators (KGIs) measure progress toward defined goals. Key risk indicators (KRIs) try to quantify the security risk facing an organization. KRIs look forward at future potential risks. **Be able to explain how security training and awareness ensures that individuals understand their responsibilities.** Security training programs impart new knowledge to employees and other stakeholders. They should be tailored to meet the specific requirements of an individual's role in the organization.Security awareness programs seek to remind users of the information they have already learned, keeping their security responsibilities top-of-mind. **Know that security managers are people managers.** Security managers lead a team of professionals and are responsible for the motivation, development, and management of those team members. This includes providing training that helps employees keep their skills current and certifications that help employees validate their skills. **Know that security managers are financial managers.** Security managers bear responsibility for managing a budget allocated to the information security program. They must understand how the fiscal year used by their organization affects funds availability and how to work within the budgeting and accounting processes used by their organization. **Be able to explain how information security must work closely with other business functions.** Security managers should cultivate relationships with other business leaders to ensure that security is well integrated with other business functions. This includes integrating with the human resources function for employee hiring,transfers, and termination. It also includes aligning with procurement and accounting functions for product and service acquisitions. Security leaders should also work carefully with other information technology leaders and the organization's auditors.

## Chapter6 Security Assessment and Testing

**Be able to list the vulnerabilities that exist in modern computing environments.** Cybersecurity professionals should remain aware of the risks posed by vulnerabilities both on-premises and in the cloud. Improper or weak patch management can be the source of many of these vulnerabilities, providing attackers with a path to exploit operating systems, applications, and firmware. Weak configuration settings that create vulnerabilities include open permissions, unsecured root accounts, errors, weak encryption settings,insecure protocol use, default settings, and open ports and services. When a scan detects a vulnerability that does not exist, the report is known as a false positive. When a scan does not detect a vulnerability that actually exists, the report is known as a false negative. **Know the purpose of threat hunting.** Threat hunting activities presume that an organization is already compromised and search for indicators of those compromises. Threat hunting

efforts include the use of advisories, bulletins, and threat intelligence feeds in an intelligence fusion program. They search for signs that attackers gained initial access to a network and then conducted maneuver activities on that network. **Know the purpose of vulnerability scans.** Vulnerability scans leverage application, network, and web application testing to check for known issues. These scans may be conducted in a credentialed or noncredentialed fashion and may be intrusive or nonintrusive,depending on the organization's needs. Analysts reviewing scans should also review logs and configurations for additional context. **Describe how penetration testing places security professionals in the role of attackers.** Penetration tests may be conducted in a manner that provides the testers with full access to information before the test (white box), no information at all (black box), or somewhere in between those two extremes (gray box). Testers conduct tests within the rules of engagement and normally begin with reconnaissance efforts, including war driving, war flying, footprinting, and open source intelligence (OSINT). They use this information to gain initial access to a system. From there, they seek to conduct privilege escalation to increase their level of access and lateral movement/pivoting to expand their access to other systems. They seek to achieve persistence to allow continued access after the vulnerability they initially exploited is patched. At the conclusion of the test, they conduct cleanup activities to restore systems to normal working order and remove traces of their activity. **Describe how bug bounty programs incentivize vulnerability reporting.** Bug bounty programs allow external security professionals to probe the security of an organization's public-facing systems. Testers who discover vulnerabilities are provided with financial rewards for their participation. This approach is a good way to motivate hackers to work for good, rather than using discovered vulnerabilities against a target. **Know how to use cybersecurity exercises to ensure that teams are prepared for security incidents.** Exercises are designed to test the skills of security professionals. Blue teams are responsible for managing the organization's defenses. Offensive hacking is used by red teams as they attempt to gain access to systems on the target network. White teams serve as the neutral moderators of the exercise. Purple teaming is conducted after an exercise to bring together the red and blue teams for knowledge sharing.

## Chapter7 Cybersecurity Technology

**Know the role of endpoint security technologies in an enterprise cybersecurity program.** Antimalware software protects endpoint devices from many different threats. Antimalware software uses signature detection and heuristic detection to prevent malware infections. Endpoint detection and response (EDR) platforms manage the detection, containment, investigation, and remediation of endpoint security incidents. Data loss prevention (DLP) systems prevent the unauthorized exfiltration of sensitive data. Change and configuration management systems maintain secure system configurations, whereas patch management ensures that security updates are consistently applied. System hardening techniques close holes that might be exploited by an attacker. **Explain the role of network segmentation.** Network segmentation techniques place systems and users of different security levels on different network segments, containing the damage caused by a potential security incident. Firewalls provide segmentation of networks into security zones, whereas VLANs group users and devices by function. **Understand the security requirements for routers, switches,and other network devices.** Routers and switches must be protected against unauthorized physical access to avoid compromise. Switch security techniques include VLAN pruning, the prevention of VLAN hopping, and port security. Router security techniques include the use of access control lists to filter traffic and quality of service controls to prioritize important network use. **Explain the three major cloud service models.** In the anything-as-a-service (XaaS) approach to computing, there are three major cloud service models. Infrastructure-as-a-service (IaaS) offerings allow customers to purchase and interact with the basic building blocks of a technology infrastructure. Software-as-a-service (SaaS) offerings provide customers with access to a fully managed application running in the cloud. Platform-as-a-service (PaaS) offerings provide a platform where customers may run

applications that they have developed themselves. **Describe the four major cloud deployment models.** Public cloud service providers deploy infrastructure and then make it accessible to any customers who wish to take advantage of it in a multitenant model. The term private cloud is used to describe any cloud infrastructure that is provisioned for use by a single customer. A community cloud service shares characteristics of both the public and private models. Community cloud services do run in a multitenant environment, but the tenants are limited to members of a specifically designed community. Hybrid cloud is a catch-all term used to describe cloud deployments that blend public, private, and/or community cloud services together. **Understand the shared responsibility model of cloud security.** Under the shared responsibility model of cloud security,cloud customers must divide responsibilities between one or more service providers and the customers' own cybersecurity teams. In an IaaS environment, the cloud provider takes on the most responsibility,providing security for everything below the operating system layer. In PaaS, the cloud provider takes over added responsibility for the security of the operating system itself. In SaaS, the cloud provider is responsible for the security of the entire environment, except for the configuration of access controls within the application and the choice of data to store in the service. **Understand secure software development concepts.** Software should be created using a standardized software development lifecycle that moves software through development, test, staging, and production environments. Developers should understand the issues associated with code reuse and software diversity. Web applications should be developed in alignment with industry-standard principles such as those developed by the Open Web Application Security Project (OWASP). **Explain secure code deployment and automation concepts.** Code repositories serve as a version control mechanism and centralized authority for the secure provisioning and deprovisioning of code. Developers and operations teams should work together on developing automated courses of action as they implement a DevOps approach to creating and deploying software. Software applications should be designed to support both scalability and elasticity. **Understand the goals of cryptography.** The four goals of cryptography are confidentiality, integrity, authentication, and nonrepudiation. Confidentiality is the use of encryption to protect sensitive information from prying eyes. Integrity is the use of cryptography to ensure that data is not maliciously or unintentionally altered. Authentication refers to the uses of encryption to validate the identity of individuals. Nonrepudiation ensures that individuals can prove to a third party that a message came from its purported sender. **Explain the differences between symmetric and asymmetric encryption.** Symmetric encryption uses the same shared secret key to encrypt and decrypt information. Users must have some mechanism to exchange these shared secret keys. Asymmetric encryption provides each user with a pair of keys: a public key, which is freely shared, and a private key, which is kept secret. Anything encrypted with one key from the pair may be decrypted with the other key from the same pair. **Explain how digital signatures provide nonrepudiation.** Digital signatures provide nonrepudiation by allowing a third party to verify the authenticity of a message. Senders create digital signatures by using a hash function to generate a message digest and then encrypting that digest with their own private key. Others may verify the digital signature by decrypting it with the sender's public key and comparing this decrypted message digest to one that they compute themselves using the hash function on the message. **Understand the purpose and use of digital certificates.** Digital certificates provide a trusted mechanism for sharing public keys with other individuals. Users and organizations obtain digital certificates from certificate authorities (CAs), who demonstrate their trust in the certificate by applying their digital signature. Recipients of the digital certificate can rely on the public key it contains if they trust the issuing CA and verify the CA's digital signature. **Explain the major components of an identity and access management program.** Identity and access management systems perform three major functions: identification, authentication, and authorization. Identification is the process of a user making a claim of identity, such as by providing a username. Authentication allows the user to prove their identity. Authentication may be done using something you know, something you have, or something you are. Multifactor authentication combines different authentication techniques to provide stronger security. Authorization ensures that authenticated

users may only perform actions necessary to carry out their assigned responsibilities.

## Chapter8 Incident Response

**Security events are occurrences that may escalate into a security incident.** An event is any observable occurrence in a system or network. A security event includes any observable occurrence that relates to a security function. A security incident is a violation or imminent threat of violation of computer security policies,acceptable use policies, or standard security practices. Every incident consists of one or more events, but every event is not an incident. **The cybersecurity incident response process has four phases.** The four phases of incident response are preparation;detection and analysis; containment, eradication, and recovery; and post-incident activities. The process is not a simple progression of steps from start to finish. Instead, it includes loops that allow responders to return to prior phases as needed during the response. **Security event indicators include alerts, logs, publicly available information, and people.** Alerts originate from intrusion detection and prevention systems, security information and event management systems, antivirus software, file integrity checking software, and third-party monitoring services. Logs are generated by operating systems, services, applications, network devices, and network flows. Publicly available information exists about new vulnerabilities and exploits detected “in the wild” or in a controlled laboratory environment. People from inside the organization or external sources report suspicious activity that may indicate that a security incident is in progress. **Policies, procedures, and playbooks guide incident response efforts.** The incident response policy serves as the cornerstone of an organization's incident response program. This policy should be written to guide efforts at a high level and provide the authority for incident response. Procedures provide the detailed, tactical information that CSIRT members need when responding to an incident. CSIRTs often develop playbooks that describe the specific procedures that they will follow in the event of a specific type of cybersecurity incident. **Incident response teams should represent diverse stakeholders.** The core incident response team normally consists of cybersecurity professionals with specific expertise in incident response. In addition to the core team members, the CSIRT may include representation from technical subject matter experts, IT support staff,legal counsel, human resources staff, and public relations and marketing teams. **Incidents may be classified according to the attack vector where they originate.** Common attack vectors for security incidents include external/removable media, attrition, the web, email,impersonation, improper usage, loss or theft of equipment, and other/unknown sources. **Response teams classify the severity of an incident.** The functional impact of an incident is the degree of impairment that it causes to the organization. The economic impact is the amount of financial loss that the organization incurs. In addition to measuring the functional and economic impact of a security incident, organizations should measure the time that services will be unavailable and the recoverability effort. Finally, the nature of the data involved in an incident also contributes to the severity of the information impact.

## Chapter9 Business Continuity and Disaster Recovery

**Understand the four steps of the business continuity planning process.** Business continuity planning involves four distinct phases: project scope and planning, business impact analysis, continuity planning, and approval and implementation. Each task contributes to the overall goal of ensuring that business operations continue uninterrupted in the face of an emergency. **Describe how to perform the business organization analysis.** In the business organization analysis, the individuals responsible for leading the BCP process determine which departments and individuals have a stake in the business continuity plan. This analysis serves as the foundation for BCP team

selection and, after validation by the BCP team, is used to guide the next stages of BCP development. **List the necessary members of the business continuity planning team.** The BCP team should contain, at a minimum,representatives from each of the operational and support departments; technical experts from the IT department; physical and IT security personnel with BCP skills; legal representatives familiar with corporate legal, regulatory, and contractual responsibilities; and representatives from senior management. Additional team members depend on the structure and nature of the organization. **Know the legal and regulatory requirements that face business continuity planners.** Business leaders must exercise due diligence to ensure that shareholders' interests are protected in the event disaster strikes. Some industries are also subject to federal, state,and local regulations that mandate specific BCP procedures. Many businesses also have contractual obligations to their clients that they must meet before, during, and after a disaster. **Explain the steps of the business impact analysis process.** The five stages of the business impact analysis process are the identification of priorities, risk identification, likelihood assessment,impact analysis, and resource prioritization. **Describe the process used to develop a continuity strategy.** During the strategy development phase, the BCP team determines which risks they will mitigate. In the provisions and processes phase, the team designs mechanisms and procedures that will mitigate identified risks. The plan must then be approved by senior management and implemented. Personnel must also receive training on their roles in the BCP process. **Explain the importance of comprehensively documenting an organization's business continuity and disaster recovery plans.** Committing the plan to writing provides the organization with a written record of the procedures to follow when disaster strikes. It prevents the “it's in my head” syndrome and ensures the orderly progress of events in an emergency. **Be familiar with the common types of recovery facilities.** The common types of recovery facilities are cold sites,warm sites, hot sites, mobile sites, and multiple sites. Be sure you understand the benefits and drawbacks for each such facility. **Understand the technologies that may assist with database backup.** Databases benefit from three backup technologies.Electronic vaulting is used to transfer database backups to a remote site as part of a bulk transfer. In remote journaling, data transfers occur on a more frequent basis. With remote mirroring technology,database transactions are mirrored at the backup site in real time. **Explain the common processes used in disaster recovery programs.** These programs should take a comprehensive approach to planning and include considerations related to the initial response effort, personnel involved, communication among the team and with internal and external entities, assessment of response efforts, and restoration of services. DR programs should also include training and awareness efforts to ensure personnel understand their responsibilities and lessons learned sessions to continuously improve the program. **Know the five types of disaster recovery plan tests and the impact each has on normal business operations.** The five types of disaster recovery plan tests are: read-through tests, structured walk-throughs, simulation tests, parallel tests, and full-interruption tests. Checklist tests are purely paperwork exercises,whereas structured walk-throughs involve a project team meeting. Neither has an impact on business operations. Simulation tests may shut down noncritical business units. Parallel tests involve relocating personnel but do not affect day-to-day operations. Full-interruption tests involve shutting down primary systems and shifting responsibility to the recovery facility.