CISSP Domain 1

SECURITY AND RISK MANAGEMENT

Domain Objectives

After completing this domain, the participant will be able to:

1. Explain the concepts of confidentiality, integrity, and availability.
2. Differentiate between confidentiality, integrity, and availability.
3. Recognize security governance principles.
4. Describe how the security function of an organization aligns to that organization’s business strategy, goals, mission, and objectives.
5. Describe various typical roles and responsibilities related to security within organizations.

Domain Objectives (continued)

6. Identify governance processes within organizations, and explain how those may affect security.
7. Identify specific security control frameworks based on a brief description or list of framework attributes.
8. Discern between the concepts and meaning of “due care” and “due diligence.”
9. Describe common practices used for asset valuation and the challenges/benefits associated with each.
10. Distinguish between threats and vulnerabilities.

Domain Objectives (continued)

11. Identify common practices of risk assessment and analysis.
12. Know the four common methods of risk management.
13. Know how to choose from the four common methods of risk management.
14. Recognize common practices for selecting security controls.
15. List the various types, classes, and categories of security controls.
16. Describe the importance of monitoring and measuring the security program and controls and why this is performed on a continuous basis.

Domain Objectives (continued)

17. Recognize common risk frameworks.
18. Apply risk-based management concepts to the supply chain and the use of third parties for risk assessment and monitoring.
19. Recognize standard threat modeling concepts.
20. Apply threat modeling methodologies.
21. Recognize common threats and risks.
22. Recognize the purpose of the service level agreement, how it augments the contract, and which items should be contained in each.

Domain Objectives (continued)

23. Determine and document minimum security requirements.
24. Recognize the various forms of compliance requirements (laws/regulations, standards, and contracts).
25. Understand the concept of regulatory compliance, especially in the context of modern privacy requirements, and identify typical regulations encountered in practice.
26. Recognize the role of digital rights management (DRM) solutions in protecting intellectual property.
27. Recognize modern international legal restrictions on import/export of data and IT tools.

Domain Objectives (continued)

28. Identify common privacy terms used in current personal data protection laws worldwide.
29. Describe the hierarchy of written governance (policies, standards, guidelines, and processes).
30. Identify the various means to support personnel security goals, including common policies and procedures.
31. Explain how modern legal frameworks affect international data flow and how the information security industry is responsible for many compliance requirements.

Domain Objectives (continued)

32. Describe the importance of security training, education, and awareness and how to differentiate between those elements.
33. Describe the necessity of business continuity and disaster recovery (BCDR) functions, and recognize basic foundational concepts.
34. Explain the ethical standards to which a professional security practitioner will be expected to uphold, as well as the standards of behavior and performance expected of (ISC)^2 members.

DOMAIN AGENDA

Concepts of Confidentiality, Integrity, and Availability

Organizational/Corporate Governance

Risk Management Concepts

Compliance Requirements

Legal and Regulatory Issues that Pertain to Information Security in a Global Context

DOMAIN AGENDA (CONTINUED)

- Security Policy, Standards, Procedures, and Guidelines
- Personnel Security Policies and Procedures
- Security Awareness, Education, and Training Program
- Business Continuity Requirements
- Professional Ethics
- Domain Review

Module 1

CONCEPTS OF CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

MODULE OBJECTIVES

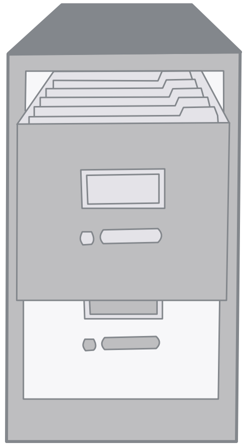
1. Explain the concepts of confidentiality, integrity, and availability.
2. Differentiate between confidentiality, integrity, and availability.

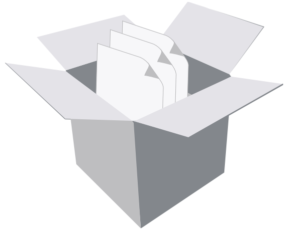
THE CIA TRIAD

- **Confidentiality**: only authorized entities have access to the data
- **Integrity**: there are no unauthorized modifications of the data
- **Availability**: authorized entities can access the data when and how they are permitted to do so

CIA TRIAD EXAMPLES

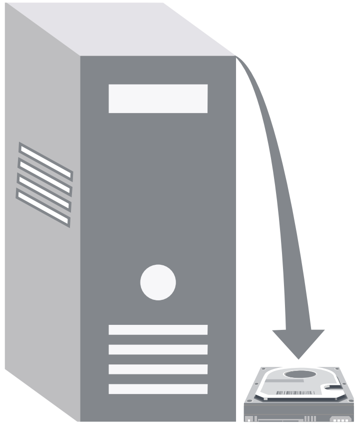
A lock on a safe provides **confidentiality**





Version control provides **integrity**

Backups provide **availability**



Module 2

ORGANIZATIONAL/CORPORATE GOVERNANCE

MODULE OBJECTIVES

1. Recognize security governance principles.
2. Describe how the security function of an organization aligns to that organization’s business strategy, goals, mission, and objectives.
3. Describe various typical roles and responsibilities related to security within organizations.
4. Identify governance processes within organizations and how those may affect security.
5. Identify specific security control frameworks based on a brief description or list of framework attributes.
6. Discern between the concepts and meaning of “due care” and “due diligence.”

SECURITY GOVERNANCE PRINCIPLES

Governance: the process of how an organization is managed. This includes all aspects of how decisions are made for that organization and can (and usually does) include the policy, roles, and procedures the organization uses to make those decisions.

Security governance: the entirety of the policies, roles, and processes the organization uses to make security decisions. Just as each organization has its own unique governance structure, it will also have security governance specific to its purposes and objectives.

ALIGNING THE SECURITY FUNCTION TO THE ORGANIZATION’S BUSINESS STRATEGY, GOALS, MISSION, AND OBJECTIVES

- Security is a support function (with exceptions for security companies).
- The security practitioner must understand how the organization functions, *then* determine how the security department can help the organization meet its goals.
- Bad security practices can negatively impact the organization as much as (or more than) the attacks they’re intended to prevent.

ORGANIZATIONAL PROCESSES

- Each organization will determine its own decision-making process. Some organizations use a governance committee.
- Some business decisions can affect security:
  - Acquisitions
  - Mergers
  - Divestitures

ORGANIZATIONAL ROLES AND RESPONSIBILITIES

Sample security roles:

- Senior management (CEO/COO/CIO/CSO/CTO/CFO, etc.)
- Security manager/officer/director
- Security personnel
- Administrators/technicians
- Users

SECURITY CONTROL FRAMEWORKS

- ISO 27001/27002 – A list of controls and control objectives to support infosec.
- COBIT
- ITIL – effective IT operations mgt.
- RMF – Risk Mgt Framework – NIST /BSI / SON / GSA
- CSA STAR - Cloud Security Alliance

DUE CARE/DUE DILIGENCE

Due care: what the organization owes its customers

Due diligence: any activity used to demonstrate or provide due care

Module 3

RISK MANAGEMENT CONCEPTS

MODULE OBJECTIVES

1. Describe common practices used for asset valuation and the challenges/benefits associated with each.
2. Distinguish between threats and vulnerabilities.
3. Identify common practices of risk assessment and analysis.
4. Know the four common methods of risk management.
5. Know how to choose from the four common methods of risk management.
6. Recognize common practices for selecting security controls.
7. List the various types, classes, and categories of security controls.

MODULE OBJECTIVES (CONTINUED)

8. Describe the importance of monitoring and measuring the security program and controls and why this is performed on a continuous basis.
9. Recognize common risk frameworks.
10. Apply risk-based management concepts to the supply chain and the use of third parties for risk assessment and monitoring.
11. Recognize standard threat modeling concepts.
12. Apply threat modeling methodologies.
13. Recognize common threats and risks.

MODULE OBJECTIVES (CONTINUED)

14. Recognize the purpose of the service level agreement, how it augments the contract, and which items should be contained in each.
15. Determine and document minimum security requirements.

RISK MANAGEMENT CONCEPTS

Risk: the possibility of damage or harm and the likelihood that damage or harm will be realized.

Acceptable risk: the level of risk (and if a particular risk) is suitable relative to the rewards offered by conducting operations.

ASSET VALUATION

Determining the value of the organization's assets

- Assets:
  - Tangible (things)
  - Intangible (intellectual property), Reputation, goodwill
  - People
  - Liquid (cash/negotiable items)
- Value metrics:
  - Monetary
  - Relative

ASSET VALUATION (CONTINUED)

- Business Impact Analysis (BIA)
  - Measures the value of an asset, the threats and risks posed to/by the asset, and the impact to the organization if the asset were affected.
  - Used in other aspects of security, as well.

IDENTIFY THREATS AND VULNERABILITIES

- **Threats:** any aspects that create a risk to the organization, its function, and its assets, e.g.:
  - Natural
  - Criminal
  - User error
- **Vulnerabilities:** any aspects of the organization’s operation that could enhance a risk or the possibility of a risk being realized, e.g.:
  - Software
  - Physical
  - Personnel – unskilled workers.

RISK ASSESSMENT/ANALYSIS

- Risk is often rated according to three factors:
  - Impact
  - Likelihood
  - Exposure
- Two common methods:
  - Qualitative – uses rankings to measure risk e.g. low, medium and high. It is subjective
  - Quantitative – uses monetary values to arrive at a value for risk. It is objective.

RISK RESPONSE

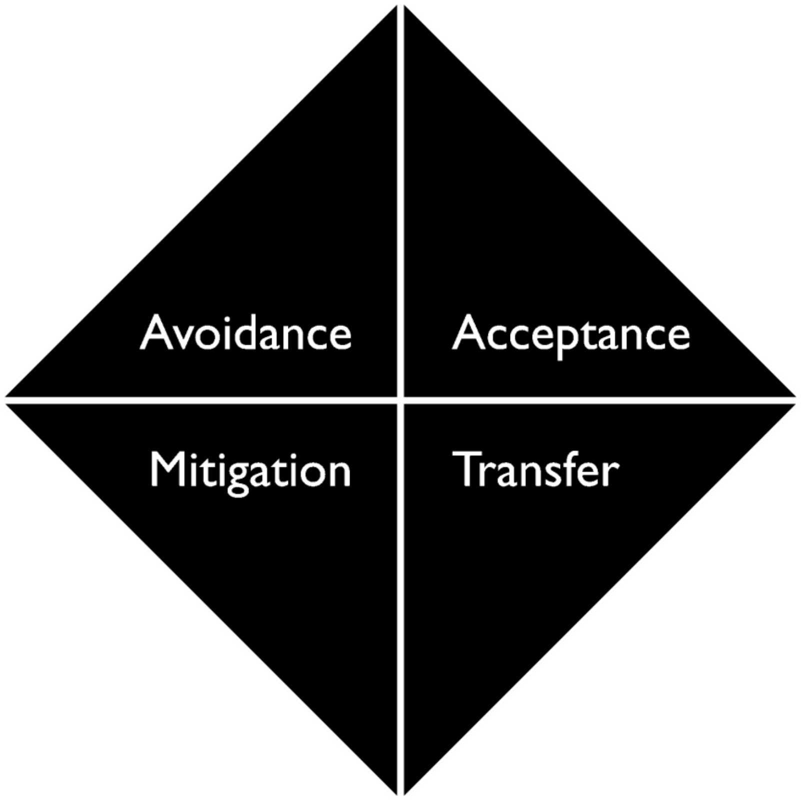


Figure 1.1: General Risk Management Options

RISK RESPONSE (CONTINUED)

Residual risk: risk that remains after the security controls are put into place

ACTIVITY: SWIMMING WITH SHARKS

INSTRUCTIONS
You are the security manager for a commercial fishing operation. Your company is considering adding a new line of business to the organization, in the form of ecotourism, where paying customers join your crews at work sites, and are lowered into the water in steel cages, in order to observe and photograph sharks.

How would this organization engage in:

- Risk acceptance?
- Risk avoidance?
- Risk mitigation?
- Risk transference?

SECURITY CONTROLS

- **Security controls:** methods, tools, mechanisms, and processes used in risk mitigation:
  - Safeguards (before risk is realized)
  - Countermeasures (after)
- All security controls have a detrimental impact on operations; control selection must entail a cost/benefit analysis.

Security Control Selection: A Traditional Model

- **Single loss expectancy (SLE):** the expected negative impact related to a particular risk (the risk being assessed)
- **Annual rate of occurrence (ARO):** the number of times per year a given impact is expected, expressed as a number
- **Annual loss expectancy (ALE):** the SLE multiplied by the ARO, which gives us the estimated annual cost related to a particular risk
- ALE = SLE x ARO

APPLICABLE TYPES OF CONTROLS

- **Technical/logical:** implemented with or by automated or electronic systems
- **Physical:** implemented through a tangible mechanism
- **Administrative:** implemented through policy and procedure

SECURITY CONTROL CATEGORIES

- **Directive:** Controls that impose mandates or requirements.
- **Deterrent:** Controls that reduce the likelihood someone will choose to perform a certain activity.
- **Preventative:** Controls that prohibit a certain activity.
- **Compensating:** Controls that mitigate the effects or risks of the loss of primary controls.
- **Detective:** Controls that recognize hostile or anomalous activity.
- **Corrective:** Controls that react to a situation in order to perform remediation or restoration.

SECURITY CONTROL CATEGORIES (CONTINUED)

- **Recovery:** Controls designed to restore operations to a known good condition following a security incident.
- Optimal control implementation requires **defense in depth** (also referred to as “layered defense”)
- A single type/category of control increases risk in the event of failure
- Multiple types/categories of controls increases the difficulty of attack

MONITORING AND MEASUREMENT

- After control selection, monitoring and enforcement is necessary
- Ongoing/continuous
- May involve a security control assessment (SCA)
- Reporting (to: management, regulators; from: internal monitoring, auditors, third-party monitoring)
- Should include continuous improvement efforts

MONITORING AND MEASUREMENT (CONTINUED)

- Vulnerability assessments
- Penetration testing

RISK FRAMEWORKS

- ISO
- COSO
- ISACA
- NIST

APPLY RISK-BASED MANAGEMENT CONCEPTS TO THE SUPPLY CHAIN

- Every organization has security dependencies with external entities (vendors, suppliers, customers, contractors)
- Risk management methodologies should be applied to all of these entities, possibly including:
  - Governance review
  - Site security review
  - Formal security audit
  - Penetration testing

APPLY RISK-BASED MANAGEMENT CONCEPTS TO THE SUPPLY CHAIN (CONTINUED)

When direct review of external entities is not viable, third party assessment and monitoring can be used

- ISO-certified audits
- CSA STAR evaluation
- AICPA SSAE 16 SOC reports

UNDERSTAND AND APPLY THREAT MODELING CONCEPTS AND METHODOLOGIES

- **Threat modeling:** looking at an environment, system, or application from an attacker's viewpoint and trying to determine vulnerabilities the attacker would exploit
- Popular model: STRIDE
  - **S**poofing
  - **T**ampering
  - **R**epudiation
  - **I**nformation disclosure
  - **D**OS
  - **E**levation of privilege
- Other models: OCTAVE, Trike

RISKS ASSOCIATED WITH HARDWARE, SOFTWARE, AND SERVICES

Hardware:

- Theft
- Natural disaster
- Fire

Software:

- Defects
- Lack of security
- Malware

Services:

- DoS/DDOS
- "Man-in-the-middle"
- Social engineering

MINIMUM SECURITY REQUIREMENTS

- Involve stakeholders in the development/acquisition/planning process as soon as possible (close to the start of the endeavor).
- Ensure that requirements are specific, realistic, and measurable.
- Record and document all elements of the discussion and outcome.
- Restate your understanding of customer requests back to them to confirm what they intended to say and what you comprehend.
- Don’t choose tools or solutions until the requirements are understood.
- If possible, create diagrams, models, and prototypes to solidify mutual understanding of the requirements before commencing full-scale development and production.

SERVICE LEVEL REQUIREMENTS

Service-level agreement (SLA): defines the minimum requirements of a business arrangement and codifies their provision

- Every element of the SLA should include a discrete, objective, numeric metric with which to judge success or failure
- Often used as a payment discriminator
- Best serve recurring, continual requirements not singular or infrequent events

ACTIVITY: SLA OR NOT?

You are the security manager for a chain of retail stores. Your company recently entered into negotiation with an external provider of data archiving services who will securely store your nonproduction data for long-term purposes. You are asked by senior management to review the contract terms and SLA. Select whether each of the following is BEST addressed through an SLA, a contract, or neither?

a) The amount of data the customer can move to the archive daily.

b) The format in which the data will stored.

c) The media that will be used to store the data.

ACTIVITY: SLA OR NOT? (CONTINUED)

d) Security methods used to routinely protect the data in storage.

e) Volume of storage made available to the customer.

f) Results of routine data integrity checks.

ACTIVITY: SLA OR NOT? – ANSWERS

a) SLA
b) Contract
c) Contract
d) Neither
e) Contract
f) SLA

Module 4

COMPLIANCE REQUIREMENTS

MODULE OBJECTIVES

1. Recognize the various forms of compliance requirements (laws/regulations, standards, and contracts).
2. Understand the concept of regulatory compliance, especially in the context of modern privacy requirements, and identify typical regulations encountered in practice.
3. Identify common privacy terms used in current personal data protection laws worldwide.

CONTRACTUAL, LEGAL, INDUSTRY STANDARDS, AND REGULATORY REQUIREMENTS

- **Compliance:** adherence to an external mandate

- **Privacy:** the right of a human being to control the manner and extent to which information about him or her is distributed

- **Audits/auditing:** the tools, processes, and activities used to perform compliance reviews

CONTRACTUAL MANDATES

Payment Card Industry Data Security Standard (PCI DSS)

- Voluntary
- Comprehensive and well-designed
- Consequences enforced by the PCI Council
- Multiple merchant levels
- Requirements for protecting cardholder data, not saving the CVV

LEGAL STANDARDS

Case law sets precedents used in future cases; these can become legal standards the courts use to determine expectations such as due care.

INDUSTRY STANDARDS

- Set by industry participants and concerned entities
- Can eventually evolve into a legal standard
- May be accepted by regulators
- Standards you should be familiar with:
  - ISO
  - CSA STAR
  - Uptime Institute

REGULATORY STANDARDS

Standards set by government bodies

Regulations you should know:

- GDPR
- The Privacy Act (Australia)
- HIPAA
- APPI (Japan)
- Personal Data Protection Law (Argentina)
- Personal Data Protection Law (Singapore)
- GLBA
- PIPEDA
- SOX
- FISMA

COMMON PRIVACY LAW TENETS

- Notification
- Participation
- Scope
- Limitation
- Accuracy
- Retention
- Security
- Dissemination

Module 5

LEGAL AND REGULATORY ISSUES THAT PERTAIN TO INFORMATION SECURITY IN A GLOBAL CONTEXT

MODULE OBJECTIVES

1. Recognize the role of digital rights management (DRM) solutions in protecting intellectual property.
2. Recognize modern international legal restrictions on import/export of data and IT tools.
3. Explain how modern legal frameworks affect international data flow and how the information security industry is responsible for many compliance requirements.

CYBER CRIMES AND DATA BREACHES

Sample crimes:

- Malware
- Unauthorized access
- Ransomware
- Theft
- Illegal use of resources
- Fraud

Specific area of law that you should be familiar with: **data breach notification**

LICENSING AND INTELLECTUAL PROPERTY REQUIREMENTS

- **Intellectual property:** intangible assets
- Use of someone else’s intellectual property (including software) often requires licensing. Some forms of licensing:
  - Site
  - Per-seat
  - Shareware
  - Public domain (not a license type, but a property type)

DIGITAL RIGHTS MANAGEMENT (DRM)

- **DRM:** create an additional layer of access control within the organization for those files/data sets that contain proprietary material
- DRM solution traits:
  - Persistency
  - Continuous audit trail
  - Dynamic policy control
  - Interoperability
  - Automatic expiration
- DRM solutions often require the use of a local agent installed on endpoint devices.

IMPORT/EXPORT CONTROLS

- Some countries limit import of security tools, particularly encryption solutions (Russia, Brunei, Mongolia)
- International legal restrictions (Wassenaar Agreement)
- Some countries limit export (United States)

TRANS-BORDER DATA FLOW

- International movement of data has become technically easier and faster, but more complicated legally
- The General Data Protection Regulation (GDPR) prevents any EU citizen’s privacy data from going to any country that does not have equivalent privacy law

GDPR COMPLIANCE

Countries that have EU-style privacy laws:

- All EU countries
- Andorra
- Singapore
- Switzerland
- Japan
- Israel
- Australia
- Argentina
- Uruguay
- Canada

GDPR COMPLIANCE (CONTINUED)

Countries that don’t:

- The United States (*unless* the entity subscribes to the Privacy Shield program)
- Everywhere else

Compliance exception: an organization may use standard contractual clauses and internal policy to stipulate GDPR compliance

PRIVACY TERMS

- **Personally identifiable information (PII):** any data about a human being that could be used to identify that person
- Examples (from various jurisdictions/statutes):
  - Name
  - Tax identification number/Social Security number
  - Home address
  - Mobile telephone number
  - Specific computer data (MAC address, IP address of the user’s machine)

PRIVACY TERMS (CONTINUED)

- Credit card number
- Bank account number
- Facial photograph
- Data subject
- Data owner/data controller
- Data processor
- Data custodian

Module 6

SECURITY POLICY, STANDARDS, PROCEDURES, AND GUIDELINES

MODULE OBJECTIVES

1. Describe the hierarchy of written governance (policies, standards, guidelines, and processes).

POLICY/STANDARDS/PROCEDURES/GUIDELINES

- **Policy:** the written aspect of governance (including security governance)
- **Standards:** specific mandates explicitly stating expectations of performance or conformance
- **Procedures:** explicit, repeatable activities to accomplish a specific task
- **Guidelines:** similar to standards in that they describe practices and expectations of activity to best accomplish tasks and attain goals; however, unlike standards, guidelines are not mandates but rather recommendations and suggestions

Module 7

PERSONNEL SECURITY POLICIES AND PROCEDURES

MODULE OBJECTIVES

1. Identify the various means to support personnel security goals, including common policies and procedures.

CANDIDATE SCREENING AND HIRING

- Detailed job descriptions
- Checking references
- Employment history
- Background check
- Financial profile

EMPLOYMENT AGREEMENTS AND POLICIES

- Employee handbook
- Employment contract
- Nondisclosure agreement (NDA)

ONBOARDING AND TERMINATION PROCESS

Onboarding

- Review of the contract terms and job description
- Formal initial training to familiarize the new employee with the organization’s security policies and procedures
- Signing NDA
- Secure process for issuing the employee any access information or tools

Termination

- Lock user account
- Recover property
- Exit interview
- Review NDA

VENDOR, CONSULTANT, AND CONTRACTOR AGREEMENTS AND CONTROLS

- Additional contractual protections
- Distinct accounts
- Escort requirements
- Distinguishing identification
- NDA

COMPLIANCE POLICY REQUIREMENTS

- Acceptable use policies (AUPs)
- Common facets:
  - Data access
  - System access
  - Data disclosure
  - Passwords
  - Data retention
  - Internet usage
- Surveillance, within restraints of applicable law

PRIVACY POLICY REQUIREMENTS

Document organization’s privacy requirements, within constraint of applicable laws

- Available to employees/staff
- Available to customers

Module 8

SECURITY AWARENESS, EDUCATION, AND TRAINING PROGRAMS

MODULE OBJECTIVES

1. Describe the importance of security training, education, and awareness and how to differentiate between those elements.

FORMS OF INSTRUCTION

- **Education**: Formal classes, usually in an accredited academic institution outside the organization of employment, often with a degree program or professional certification.
- **Training**: Semi-formal, usually offered by the organization itself (or by vendors), presented by subject matter experts (typically security practitioners).
- **Awareness**: Informal and often unscheduled and not mandatory, awareness elements typically are used to remind and encourage employees about operating in a secure manner.

METHODS AND TECHNIQUES TO PRESENT AWARENESS AND TRAINING

- Computer-based training
- Live instruction
- Reward mechanisms
- Regular communications

PERIODIC CONTENT REVIEWS

Any instruction must be kept current; the instructor should review the following on a regular basis:

- Applicable laws
- Security tools
- Organizational security policy
- Recent widespread attack styles and methodology

PROGRAM EFFECTIVENESS EVALUATION

- Participant testing
- Penetration testing
- Log reviews

Module 9

BUSINESS CONTINUITY REQUIREMENTS

MODULE OBJECTIVES

1. Describe the necessity of business continuity and disaster recovery (BCDR) functions, and recognize basic foundational concepts.

BUSINESS CONTINUITY REQUIREMENTS

- **Business continuity (BC):** actions, processes, and tools for ensuring an organization can continue critical operations during a contingency
- **Disaster recovery (DR):** tasks and activities required to bring an organization back from contingency operations and reinstate regular operations
- Often referred to jointly as “BCDR”

DEVELOP AND DOCUMENT SCOPE AND PLAN

- **Maximum allowable downtime (MAD):** measure of how long an organization can survive an interruption of critical functions (also referred to as maximum tolerable downtime (MTD))
- **Recovery time objective (RTO):** the target time set for recovering from any interruption
- **Recovery point objective (RPO):** measure of how much data the organization can lose before the organization is no longer viable

BUSINESS IMPACT ANALYSIS (BIA)

BIA: the effort to determine the value of each asset belonging to the organization, as well as the potential risk of losing assets, the threats likely to affect the organization, and the potential for common threats to be realized

Methods:

- Survey
- Financial audit
- Customer response

BUSINESS IMPACT ANALYSIS (BIA) (CONTINUED)

The organization (and the BIA in particular) benefits from information about potential threats and attacks.

- External business/security intelligence vendors
- Open sources
- Malware management firms
- Government and industry feeds

Module 10

PROFESSIONAL ETHICS

MODULE OBJECTIVES

1. Explain the ethical standards to which a professional security practitioner will be expected to uphold, as well as the standards of behavior and performance expected of $(ISC)^2$ members.

(ISC)^2 ® CODE OF ETHICS

Preamble:

- The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.
- https://www.isc2.org/Ethics

(ISC)^2 ® CODE OF ETHICS (CONTINUED)

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principles.
- Advance and protect the profession.

Member can lose certification for noncompliance.

ORGANIZATIONAL CODE OF ETHICS

- An organization can create internal guidance, as well, reflecting applicable law, social norms, and cultural mores.

- EXAMPLE (from the guide):
  - Is the admin’s report acceptable and valid?
  - What should be done with/to the employee?
  - What should be done with/to the admin?

Module 11

DOMAIN REVIEW

DOMAIN SUMMARY

Many of the concepts introduced in this domain will serve as the foundation for discussion throughout the rest of this guide; be sure you have an understanding of the ideas so you can grasp the rest of the material.

DOMAIN REVIEW QUESTIONS

1. Alice has some data that is extremely valuable. She backs it up from her computer to a flash stick, and she puts the flash stick in a safe deposit box. Which two principles of the CIA triad does this address?

A. Confidentiality and integrity

B. Confidentiality and availability

C. Integrity and availability

D. Availability and nonrepudiation

ANSWER

The correct answer is B.

Alice is ensuring a form of availability by having a backup; if her laptop is lost, stolen, or malfunctions, she does not also lose the data—she can restore the saved data to another machine. She is also providing a form of confidentiality by locking up the flash stick; this practice deters the ability of others to access the flash stick. (Note: this ONLY provides confidentiality for the flash stick; we have no idea if she is also providing confidentiality to the data while it is live on her laptop.) The question does not describe any practice that could constitute integrity protection, and the CIA triad does not deal with nonrepudiation.

DOMAIN REVIEW QUESTIONS

2. An organization’s recovery time objective (RTO) must always be less than:

A. 12 hours

B. The time it takes to alert the public

C. The maximum allowable downtime (MAD)

D. The duration allowed by regulators

ANSWER

The correct answer is C.

The organization will cease to be viable once the MAD is reached (this is the definition of MAD); therefore, the critical path must be recovered in less time than that (which is the definition of the RTO). No arbitrary time duration (such as answer A) is suitable for all organizations; every organization will determine its own MAD and RTO. Likewise, regulators do not typically dictate RTO/MAD (exception: critical infrastructure industries, such as power generation, may be subject to downtime stipulations). Public notification has no bearing on RTO.

DOMAIN REVIEW QUESTIONS

3. A security practitioner holding an (ISC)^2 certification is expected to *first* serve:

A. The client

B. The industry

C. (ISC)^2

D. Humanity

ANSWER

The correct answer is D.

Human beings as individuals, and, on a larger scale, as a species, are the paramount concern of security practitioners. All the other answers should receive lesser importance.

DOMAIN REVIEW QUESTIONS

4. Bob is the security manager for an online retailer. To protect the customer data they are entrusted with, Bob requires all personnel to attend security training sessions regularly. Bob documents and tracks which personnel have attended training, and he suspends account access for those personnel who have missed training. Which of the following answers does this *best* typify?

A. Due care

B. Due diligence

C. Legal duty

D. Reasonable expectation

ANSWER

The correct answer is B.

The evidence of providing due care is due diligence; the documentation of who attends training is evidentiary support. Due care is the legal duty owed to the customers; in this scenario that would be “don’t allow unauthorized disclosures of customer privacy data.” Due diligence is any action that supports this duty, so answer B is preferable to answers A and C. Reasonable expectation is what the customer should have when they take part in the transaction; in this situation that would be, “my personal information will be protected,” so answer D is not optimum.

DOMAIN REVIEW QUESTIONS

5. Whenever an organization chooses to perform risk mitigation to address a particular risk, what other form of risk management will also be included?

A. Risk transference

B. Risk avoidance

C. Risk capture

D. Risk acceptance

ANSWER

The correct answer is D.

Risk mitigation always leaves some residual risk; the purpose of risk mitigation is to get risk down to an acceptable level.

DOMAIN REVIEW QUESTIONS

6. In order to comply with the Payment Card Industry Data Security Standard (PCI DSS), what data element must not be stored for any length of time beyond the transaction?

A. cardholder’s name

B. Social Security number

C. IP address

D. Card verification value (CVV)

ANSWER

The correct answer is D.

PCI DSS prohibits storage of the CVV for any time beyond the transaction.

DOMAIN REVIEW QUESTIONS

7. Which of the following security tools would probably best help an organization protect its proprietary software?

A. Intrusion prevention system (IPS)

B. Antimalware suite

C. Digital rights management solution (DRM)

D. Web application firewall (WAF)

ANSWER

The correct answer is C.

DRM solutions are designed to protect intellectual property.

DOMAIN REVIEW QUESTIONS

8. Which of the following is usually perceived as having the highest level of precedence for an organization?

A. Policy

B. Guidelines

C. Procedures

D. Standards

ANSWER

The correct answer is A.

Policy is the written form of governance, and is promulgated by senior management of the organization, as a way of describing the organization’s strategic vision and goals.

DOMAIN REVIEW QUESTIONS

9. Which of the following describes a personnel security tool that should not require the employee's signature?

A. Nondisclosure agreement (NDA)

B. Personnel security policy

C. Acceptable use policy (AUP)

D. Contract

ANSWER

The correct answer is B.

The organization’s security policy is promulgated by senior management, and all personnel must comply with it; the employee does not need to sign it. All the other answers are tools which should include the employee’s signature.

DOMAIN REVIEW QUESTIONS

10. Which of the following is not a recommended method for delivering security instruction?

A. Computer-based training

B. Rote memorization

C. Live training

D. Reward mechanisms

ANSWER

The correct answer is B.

Rote memorization of security material is not a common method for delivering instruction. All the other answers are recommended methods for delivering security instruction.