ExamLabs

Certified in Risk and Information Systems Control

Study Guide

Exam CRISC

CONTENTS

Chapter 1 Risk Concepts

- Basic Security Concepts
  - Goals of Information Security
  - Supporting Security Goals
- Risk Management Concepts
  - Risk Terms and Definitions
  - Standards, Frameworks, and Best Practices
- Business Perspective of IT Risk Management
  - Business Goals and Objectives
  - Business Information Criteria
  - Organizational Structures
  - Information Systems Architecture
- Managing Risk Ownership
  - Risk Ownership
  - Risk Awareness
  - Legal and Governance
- Chapter Review
  - Review Questions
  - Answers

Chapter 2 Threats and Vulnerabilities in the Enterprise

- Threats and Vulnerabilities
  - Identifying Threats and Vulnerabilities in the Enterprise
- Business Processes and Initiatives

Environmental Risk Factors
Threats
Vulnerabilities
Project and Program Management
Third-Party Management
Systems Development Life Cycle
Emerging Technologies
Management of IT Operations
Data Management
Business Continuity and Disaster Recovery Management
Chapter Review
Review Questions
Answers

Chapter 3 Identifying and Managing Risk Scenarios

Developing and Managing Risk Scenarios
Risk Identification and Classification
Risk Scenarios
Developing Risk Scenarios
Analyzing Risk Scenarios
Risk Register
Chapter Review
Review Questions
Answers

Chapter 4 Risk Assessment and Analysis

Risk Assessment Processes
NIST RMF
OCTAVE Methodology
ISO/IEC Standards
ISACA's Risk IT Framework
Performing a Risk Assessment
Quantitative and Qualitative Techniques
Quantitative

Qualitative
Combining Quantitative and Qualitative Techniques
Other Analysis Techniques
Risk Analysis
Control Analysis
Reporting Risk Assessment Results
Chapter Review
Review Questions
Answers

Chapter 5 Risk Response and Mitigation

Risk Response
Risk Response Standards and Frameworks
Understanding Risk Response Options
Evaluating Risk Response Options
Selecting Risk Response
Prioritizing Risk Responses
Risk Mitigation
Risk Response Action Plans
Control Development
System Development Life Cycle
Project Management
Project Management Frameworks
Chapter Review
Review Questions
Answers

Chapter 6 Control and Risk Monitoring

Control Monitoring
Control Testing and Assessment
Indicators
Chapter Review
Review Questions
Answers

Chapter 7 Information Systems Control Concepts

Information Security Control Concepts
- Control Classification
- Control Selection

Control Frameworks
- NIST
- COBIT
- Val IT
- PCI-DSS
- Other Control Frameworks

Chapter Review
- Review Questions
- Answers

Chapter 8 Designing and Implementing Controls

Business Perspectives of Controls
- Business Cases for Controls
- Regulatory Guidance and Controls
- Business Functions and Controls
- Information System Security Engineering
- Design Considerations
- Control Selection
- Implementing Controls

Chapter Review
- Review Questions
- Answers

Chapter 9 Measuring Risk and Control Effectiveness

Applying Key Performance Indicators
- Key Performance Indicator Review
- Key Performance Indicator Development

Chapter Review
- Review Questions
- Answers

Appendix A The NIST Risk Management Framework

- Overview
  - Tiered Approach
  - Applicability
  - Publications
- RMF Steps
  - Step 1: Categorize Information Systems
  - Step 2: Select Security Controls
  - Step 3: Implement Security Controls
  - Step 4: Assess Security Controls
  - Step 5: Authorize Information Systems
  - Step 6: Monitor Security Controls

Appendix B ISACA's Risk IT Framework

- Overview
  - Applicability
  - Publications
- Framework Focus Areas
- Risk Governance
  - RG1: Establish and Maintain a Common Risk View
  - RG2: Integrate with ERM
  - RG3: Make Risk-Aware Business Decisions
- Risk Evaluation
  - RE1: Collect Data
  - RE2: Analyze Risk
  - RE3: Maintain Risk Profile
- Risk Response
  - RR1: Articulate Risk
  - RR2: Manage Risk
  - RR3: React to Events

CHAPTER 1

Risk Concepts

In this chapter, you will:

- Review basic security concepts
- Learn about standards, frameworks, and best practices related to risk identification, assessment, and evaluation
- Learn to describe how business goals, information criteria, and organizational structures affect risk
- Determine how information systems architecture presents risk to the organization
- Learn about risk ownership and awareness
- Recognize legal, regulatory, and contractual requirements for risk management within the organization

This chapter will review a large portion of Certified in Risk and Information Systems Control (CRISC) Domain 1: Risk Identification with coverage of fundamental information security and risk management concepts. We'll cover a good deal of the terminology associated with risk management and many of the core concepts you'll need to be familiar with for the exam, but we will go into more depth on many of these concepts in later chapters.

The CRISC exam topics that we cover in this chapter are as follows and include the following domain objectives and knowledge statements:

- 1.6 Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives
- 1.7 Collaborate in the development of a risk awareness program, and

conduct training to ensure that stakeholders understand risk and to promote a risk-aware culture

---

NOTE Throughout the book, the task and knowledge statements are listed in the order they are described in the CRISC Job Practice areas, not necessarily how they are presented in the chapter.

Basic Security Concepts

To successfully sit for the CRISC exam, you should be familiar with some basic security concepts. You can't be expected to know how to manage risk in a security environment if you don't understand the basics of security. We'll assume you have some level of experience already as a security professional since risk management is a significant portion of (and a logical career progression from) the information security profession. You may also have had some level of experience in specific risk management processes during your career. As such, we won't go into detail on the basic security concepts in the upcoming sections; this chapter will just serve as a quick refresher to remind you of certain security concepts.

The CRISC exam is not a technical exam; it is more of a process- and management-oriented exam, so we won't delve into firewall configuration rules, protocol filtering, encryption, or any of the other fun stuff that security professionals do. We will, however, discuss a couple of other security concepts that are important to know for the exam since risk affects all of these concepts in different ways.

Goals of Information Security

Traditional security doctrine, as well as fundamental security knowledge you may learn from various training courses and on-the-job experience over the years, teaches that there are three fundamental security goals. These goals are what we're striving for as security professionals; they are *confidentiality*, *integrity*, and *availability*. You'll sometimes see these three terms strung together as an acronym, such as the CIA triad or, occasionally, as the AIC triad, depending upon the different security literature you read. In any event,

these three goals are what you want to achieve for all of your information systems and data. They are also characteristics that you want all of your systems, processes, procedures, methods, and technologies to have. We will discuss these three items in the next few sections and why they are important to the security profession. We'll also briefly describe some of the risks associated with these three goals.

Confidentiality

The goal of confidentiality is to keep information systems and data from being accessed by people who do not have the authorization, need-to-know, or security clearance to access that information. In other words, confidentiality means that only authorized individuals and entities should be able to access information and systems. Confidentiality can be achieved through a number of security protection mechanisms, such as rights, privileges, permissions, encryption, authentication, and other access controls. If the confidentiality of data or information systems is breached, you get the opposite of confidentiality, which is unauthorized disclosure. Unauthorized disclosure is a risk to data and information systems and one that we as security professionals struggle hard to protect against.

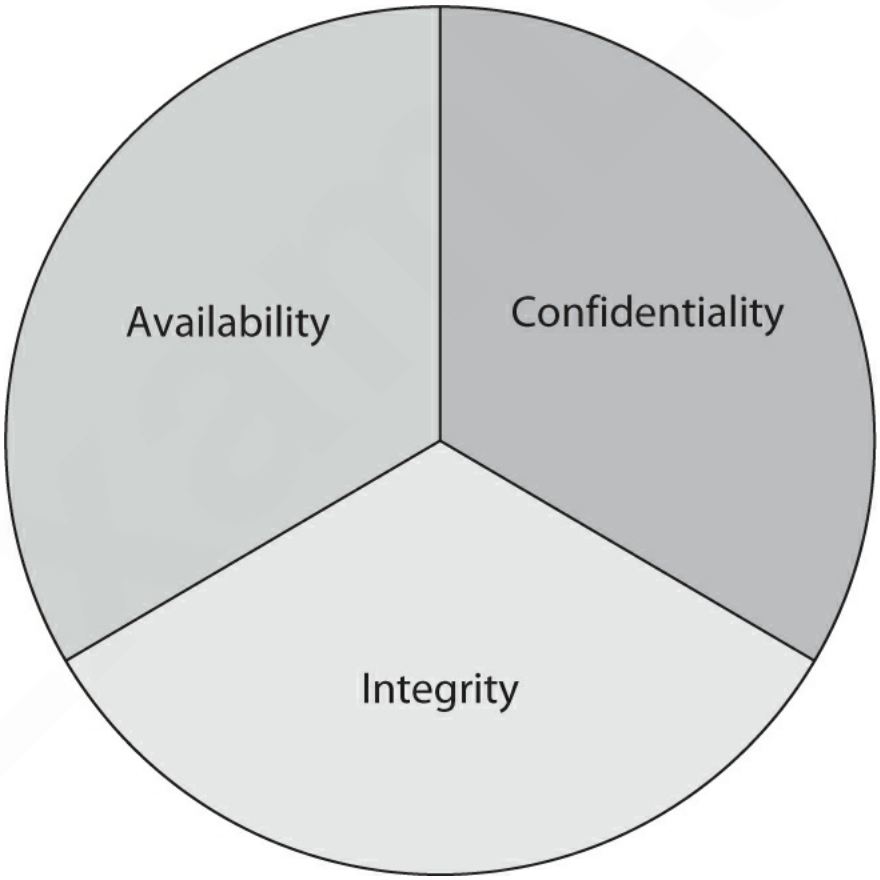
Integrity

Integrity is the characteristic of data that means the data has not been subject to unauthorized modification or alteration. In other words, it means data is left in the same state as it was when it was stored or transmitted. So, when it is accessed again or received, it should be identical to the data that was originally stored or transmitted. Integrity is achieved in several ways, by using checksums, message digests, and other verification methods. Data alteration is the opposite of integrity, particularly when the modification has not been authorized by the data owner. Data modification or alteration can happen accidentally, such as when it may be inadvertently changed because of human error or faulty transmission media. It can also happen intentionally (which is usually malicious in nature when this modification is unauthorized) by direct interaction with data during storage or transmission, such as during an attack, for example. This risk to data affects whether the data can be trusted as authentic or true, whether it can be read as intended, and whether it is corrupt.

Availability

Availability is when data and systems are accessible to authorized users at any time or under any circumstances. Even if data is kept confidential and its integrity remains intact, that does you no good if you can't access it when you need it to perform critical business functions. Availability ensures you have this data (and the information systems that process it) at your fingertips. Just as confidentiality and integrity have their opposites, data destruction or denial of service is the opposite of availability. This risk to your information systems could prevent authorized consumers of that data or users of that information system from performing their jobs, thus severely impacting your business operations. Figure 1-1 shows the relationships of the three information security goals to one another.

Figure 1-1 The three goals of information security



EXAM TIP You will need to understand the definitions of the goals of information security well for the exam. Almost everything in information risk management supports these three goals, either directly or indirectly.

Supporting Security Goals

Popular security theory sets forth the three overarching security goals but also provides for auxiliary elements that support these goals in various ways. These are concepts that, both individually and combined, help you as a security professional to maintain data confidentiality, integrity, and availability, as well as protect your systems from unauthorized use or misuse. We'll discuss these different security elements and other concepts, as well as how they support the three primary goals of security, in the next few sections.

Access Control

As a security professional, you probably already know that a *security control* is a security measure or protection applied to data, systems, people, facilities, and other resources to protect them from adverse events. Security controls can be broken down and categorized in several ways. *Access controls* directly support the confidentiality and integrity goals of security and indirectly support the goal of availability. An access control essentially means that you will proactively ensure that only authorized personnel are able to access data or the information systems that process that data. Access controls ensure that only authorized personnel can read, write to, modify, add to, or delete data. They also ensure that only the same authorized personnel can access the different information systems and equipment used to store, process, transmit, and receive sensitive data.

There are several different types of access controls, including identification and authentication methods, encryption, object permissions, and so on. Remember that access controls can be administrative, technical, or physical in nature. Administrative controls are those that are implemented as policies, procedures, rules and regulations, and other types of directives or governance. For example, personnel policies are usually administrative access controls. Technical controls are those that are most often associated with security professionals, such as firewalls, proxy servers, virtual private

network (VPN) concentrators, encryption techniques, file and folder permissions, and so on. Physical controls are those used to protect people, equipment, and facilities. Examples of physical controls include fences, closed-circuit television cameras, guards, gates, and restricted areas.

In addition to classifying controls in terms of administrative, technical, and physical, you can also classify access controls in terms of their functions. These functions include preventative controls, detective controls, corrective or remedial controls, deterrent controls, and compensating controls. All of the different controls can be classified as one or more of these different types of functions, depending upon the context and the circumstances in which they are being used.

Data Sensitivity and Classification

Asset is a general, all-encompassing term that could include anything of value to an organization. The term *asset* can be applied to data, systems, capabilities, people, equipment, facilities, processes, proprietary methods, and so on; it is anything the organization values and desires to protect. Organizations normally determine how important their assets are to them and how much protection should be afforded to those assets. For example, intellectual property is an extremely valuable asset to the organization and is normally well protected. This is really the basic fundamental concept of risk management—how much security or protection a particular system or piece of data requires, based upon how likely it is that something bad will happen to it, balanced with what the organization can really afford to spend on the protection for that asset. To make reasonable decisions on how much security an asset needs, the organization has to decide how much the asset is worth to it. We'll discuss worth in terms of dollars a bit later in the chapter, but for now let's look at it from a perspective of asset sensitivity. In terms of sensitivity, you'll usually see the term *data sensitivity* in particular, but you could also broadly consider sensitivity for any asset in an organization.

Data (or other asset) sensitivity refers to how much protection the organization feels a particular system or piece of data requires, based upon its value to the organization and the impact if it were lost, stolen, or destroyed. For example, information published on the organization's public website or in the company newsletter is public knowledge and is usually easily retrievable if, for some reason, the hard disk containing that data fails or is erased. Since the data is public, you may not consider that data to be very

sensitive in nature and require little protection for it. On the other hand, customer order data is extremely important to the organization simply because its business operations depend upon that data in order to function and turn a profit. So, it makes reasonable sense that the organization would spend a little bit more time, money, and effort in protecting that particular data. Therefore, its sensitivity, or *classification level*, would be considered somewhat higher than public data. Generally, the higher the sensitivity of the data, the more protection it is given.

In basic security classes, you typically learn about the different classifications of data found in both commercial organizations and government ones. In commercial organizations, typical data sensitivity labels include Private, Company Sensitive, Proprietary, and so on. In the U.S. government, data sensitivity levels include Confidential, Secret, and Top Secret, and they are classified based upon the level of damage to the security of the United States that could be incurred if data at these various classification levels were disclosed or lost. Remember that data sensitivity is driven by the value of the data to the organization and by the impact if it is lost, stolen, or destroyed, and it is balanced by the commitment of resources the organization is willing to provide to protect that data. Data sensitivity and classification policies specify the different formal levels of sensitivity in the organization and what those levels require in terms of protection.

Identification and Authentication

Identification and authentication are often misunderstood terms. They are related, to be sure, but they are not the same thing and really shouldn’t be used interchangeably by a knowledgeable security professional. Identification refers to the act of an individual or entity presenting valid credentials to a security system in order to assert that they are a specific entity. When you enter a username or password into a system, for example, or insert a debit card into an automated teller machine and enter a personal identification number (PIN), you are identifying yourself. Authentication is the second part of that process, where your identity is verified with a centralized database containing your authentication credentials. If the credentials you have presented match those in the authentication database, you are authenticated and allowed access to the network or resource. If they do not match, you are not authenticated and are denied access.

There are several methods of identification and authentication, including

single factor (such as username and password, for example) and multifactor, which consists of two or more of the following: something you *know* (knowledge factor), something you *have* (possession factor), or something you *are* (biometric or inherence factor). Authentication also uses a wide variety of methods and technologies, such as Kerberos and 802.1X, for example.

Authorization

Authentication to a resource doesn't automatically guarantee you have full, unrestricted access to a resource. Once you are authenticated, the system or resource defines what actions you are authorized to take on a resource and how you are allowed to interact with that resource. *Authorization* is what happens once you've successfully identified yourself and been authenticated to the network. Authorization dictates what you can or can't do on the network, in a system, or with a resource. This is usually where permissions, rights, and privileges come in. In keeping with the concept of *least privilege*, users should be authorized to perform only the minimum actions they need in order to fulfill their position responsibilities. Authorization has a few different components. First, there is *need to know*. This means there must be a valid reason or need for an individual to access a resource, and only to a certain degree. Second, an individual may have to be trusted, or *cleared*, to access a resource. This may be accomplished through a security clearance process or nondisclosure agreement, for example.

EXAM TIP Understand the differences between identification, authentication, and authorization. Remember that identification is simply presenting credentials, while authentication is verifying them. Authorization dictates what actions an individual can take on a system.

Accountability

Accountability means that a person is going to be held responsible for their actions on a system or with regard to their interaction with data. Accountability is essentially the traceability of a particular action to a particular user. Users must be held responsible for their actions, and there are different ways to do this; it is usually assured through *auditing*. First, there

must be a unique identifier that is tied only to a particular user. This way, the identity of the user who performs an action or accesses a resource can be positively established. Second, auditing must be properly configured and implemented on the system or resource. What you are auditing is a user's actions on a system or interactions with a resource. For example, if a user named Sam deletes a file on a network share, you want to be able to positively identify which user performed that action, as well as the circumstances surrounding the action (such as the time, date, from which workstation, and so on). This can be accomplished only if you have auditing configured correctly and you take the time to review the audit logs to establish accountability.

NOTE Although related, accountability is not the same thing as auditing. Accountability uses auditing as just one method to ensure that the actions of users can be traced to them and that they are held responsible for those actions. Other methods, such as nonrepudiation, are used as well.

Nonrepudiation

Nonrepudiation is closely related to accountability. Nonrepudiation ensures that the user cannot deny that they took an action simply because the system is set up such that no one else could have performed the action. The classic example of nonrepudiation is given as the proper use of public key cryptography. If a user sends an e-mail that is digitally signed using their private key, then they cannot later deny that they sent the e-mail, since only they are supposed to have access to the private key. In this case, the user can be held accountable for sending the e-mail, and nonrepudiation is assured.

Figure 1-2 summarizes the relationships between access controls, the supporting elements of information security, and the three information security goals. Note that there is no hard-and-fast rule about mapping security elements and access controls to security goals; all of these elements and controls can support any one or even more than one goal at a time. For example, encryption, a technical access control, can support both confidentiality and data integrity at the same time.

Figure 1-2 How access controls support security elements and information security goals