

PREPARE FOR THE ISACA CERTIFIED INFORMATION SECURITY MANAGER EXAM

CISM Review Manual

Gwen Bettwy, Mark Williams, Mike Beevers

Copyright © 2021 Tactical Security Inc.

All rights reserved

The characters and events portrayed in this book are fictitious. Any similarity to real persons, living or dead, is coincidental and not intended by the author.

No part of this book may be reproduced, or stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission of the publisher.

ISBN: 9798715814234

Cover design by: Art Painter
Printed in the United States of America

Prepare for the
ISACA
Certified Information
Security Manager Exam
CISM Review Manual

GWEN BETTWY
MARK WILLIAMS
MIKE BEEVERS

CONTENTS

The Exam	1
----------	---

Introduction 7

1	Information Security Governance	9
2	Information Risk Management and Compliance	55
3	Information Security Program Development and Management	105
4	Information Security Incident Management	159

The exam

ISACA offers the CISM exam around the world in specific locations. The exam is given as a four-hour computer-based exam, available at over 1,300 locations worldwide. The exam itself includes 150 multiple-choice questions. Some of the 150 questions are used for research and analysis purposes only and are not scored. As a test taker you will not know which questions fall into this category. ISACA has a scaled scoring process. A passing score is 450 points of a possible 800 points. The lowest possible score you can achieve is 200 points.

You will be notified of your results the day of the examination on your computer screen when you complete the exam.

ISACA has experience requirements to obtain CISM. The requirements involve a total of five years of information security experience. A minimum of three years Information Security Management experience in three or more of the practice areas is required and may not be substituted with other experience. You may substitute two years of the total five-year requirement with CISA, CISSP or if you have a postgraduate degree in Information Security. If you do not have any of those three things you can substitute one year with MCSE, Sec+, Certified BCP or another skill-based certification. All this experience must be within the 10 years prior to application for CISM.

Once you become certified, the journey does not end. You are required to maintain your certification through continuing education, paying the annual maintenance fee, and abiding by the ISACA code of ethics. The CISM credential is a three-year certification. To keep your certification beyond the initial three years the information security manager must collect continuing education credits known as CPE's. A total of 120 CPE credits must be obtained during the three-year certification period. There is a requirement that 20 CPEs must be obtained each year. If ISACA performs an audit on your CPEs you must be able to prove you did the work required to obtain those credits. Maintenance of a physical or logical file folder with

certificates from classes taken or any other proof of your CPE work should be maintained. There is also an annual maintenance fee required.

ISACA sets forth the following Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including audit, control, security, and risk management.
2. Perform their duties with objectivity, due diligence, and professional care, in accordance with professional standards.
3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association
4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge, and competence.
6. Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including audit, control, security, and risk management.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measure.

How to take the Exam

By this point, you likely have already realized that there is a ton of information out there relating to the CISM certification. Many people feel overwhelmed by the amount of information available, and the wide range of resources available for studying. Regardless of where or what you chose to study, you still have a need to apply your knowledge in a way that will get you a passing exam score. This chapter is all about that.

There are a few time-tested techniques that you will want to know. We have listed them below. Trust us on this. The authors of this book have taken over 30 IT/Security exams and trained over 20,000 students (about the seating capacity of Madison Square Garden) over the years. Look at the list below and learn how to apply them to your exam.

1. It is all about the money. (Cost Benefit Analysis)
2. Pick Policy. Policies are critical to all security programs.
3. Policy requires training. Everyone needs to understand their responsibilities.
4. Life Safety is your most important issue at all times.
5. Management buy-in is critical.
6. Everyone is responsible for security.
7. Needs of the business must be met.
8. Identify then manage (Identify is step 1).
9. Pick the generic answer over the technology specific.

1. It is all about the money.

Businesses are in business to make money. Security must support this goal. If it is more expensive to solve the problem than the problem unsolved will cost, then do not solve it. This implies a cost benefit analysis. Ensure that the cost of the security solution is less than the potential loss would be if it were realized.

2. Pick Policy

Policy is a written statement of management's goals and objectives. CISM is a Management exam. Keep this in mind. How does management confer their goals and objectives to their employees? Policy is the answer. Are the statements "Follow local policy" or "in accordance with local policy" ever going to be wrong? When should you NOT follow policy? Never. Pick policy when you see it in an answer.

3. Policy requires training.

As stated earlier, policy is management's goals and objectives. It is imperative that these goals and objective be passed onto the employees who will be required to follow the policies and procedures. This is often called awareness training. Always keep in mind that the CISM exam is a MANAGEMENT exam. Technology will not be as important as people. Policy changes the way people behave, but only if they are aware of what is expected of them. Policy is useless without training. Training is essential.

4. Life safety is your most important issue.

Can you imagine a security exam that indicated the requirement to cause bodily harm to others to ensure your information security? Your physical and logical security solutions must always ensure life safety. Locking the doors and preventing people from entering and exiting a building would be a huge problem in a fire situation. This should be an obvious example of a life safety issue. Do not hurt anyone during your exam.

5. Management buy-in is critical.

Management support is extremely critical. Without that support security will not happen. Management must support the creation of policies, the security team, audit, penetration tests and so on. Without management support budget is never allocated, people are never trained, and security will fail.

6. Everyone is responsible for security.

Everyone in the business has a security responsibility. The responsibility may only be locking the doors when you leave the building,

but there is a responsibility, and we need to make sure that everyone understands that responsibility.

7. Needs of the business must be met.

Security must further the business, not stop it. Security, if implemented improperly, will prevent the business/users from getting their job done. The security architecture and program need to be designed in a way to enable the business.

8. Identify then manage (Identify is step 1)

To manage an event or an incident it is necessary to first identify that something has happened. If you can identify then you can manage it. If not properly identified the damage might be extremely detrimental to our business.

9. Pick the generic answer over the technology specific

When selecting answers in an exam like CISM it is usually best to take the all-encompassing answer versus a technology specific answer. The other way you could say it is to take the politically correct answer. The answer that the politician's give that does not really answer the question specifically.

introduction

The Certified Information Security Manager (CISM) exam is divided into 4 domains. The domains are not treated equally on the exam. Some domains will have more questions than others. Below is a list of the four domains along with the percentages showing the relative level of importance for each domain.

1. Information Security Governance (24%)
2. Information Risk Management & Compliance (30%)
3. Information Security Program Development & Management (27%)
4. Information Security Incident Management (19%)

The basic strategy to the four domains is as follows.

1. Information Security Governance entails the planning of information security strategy within your business.
2. Information Risk Management & Compliance is all about discovering the level of risk within the business.
3. Once you understand your risk level you can move into Information Security Program Development & Management, which is the creation and implementation of your security plan based on the organizational business strategy and risk analysis.
4. Once the program has been implemented, the organization must prepare for things to go wrong. The Information Security Incident Management domain covers how an organization monitors and reports security events. Incident Response, Business Continuity and Disaster Recovery are some of the focal points of this domain.

chapter 1

domain 1

information security governance

24% of the Exam

According to ISACA, in this domain, you will:

Establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately, and program resources are managed responsibly.

A CISM candidate must be able to perform the following nine task statements:

- 1.1 Establish and maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and ongoing management of the information security program.
- 1.2 Establish and maintain an information security governance framework to guide activities that support the information security strategy.
- 1.3 Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.
- 1.4 Establish and maintain information security policies to communicate management's directives and guide the development of standards, procedures, and guidelines.
- 1.5 Develop business cases to support investments in information security.
- 1.6 Identify internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy.

- 1.7 Obtain commitment from senior management and support from other stakeholders to maximize the probability of successful implementation of the information security strategy.
- 1.8 Define and communicate the roles and responsibilities of information security throughout the organization to establish clear accountabilities and lines of authority.
- 1.9 Establish, monitor, evaluate and report metrics (for example, key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of the information security strategy.

A solid understanding of the following 15 knowledge statements should be attained by a CISM candidate:

- k1.1 Knowledge of methods to develop an information security strategy
- k1.2 Knowledge of the relationship among information security and business goals, objectives, functions, processes, and practices
- k1.3 Knowledge of methods to implement an information security governance framework
- k1.4 Knowledge of the fundamental concepts of governance and how they relate to information security
- k1.5 Knowledge of methods to integrate information security governance into corporate governance
- k1.6 Knowledge of internationally recognized standards, frameworks and best practices related to information security governance and strategy development
- k1.7 Knowledge of methods to develop information security policies
- k1.8 Knowledge of methods to develop business cases
- k1.9 Knowledge of strategic budgetary planning and reporting methods
- k1.10 Knowledge of the internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) and how they impact the information security strategy

- k1.11 Knowledge of methods to obtain commitment from senior management and support from other stakeholders for information security
- k1.12 Knowledge of information security management roles and responsibilities
- k1.13 Knowledge of organizational structures and lines of authority
- k1.14 Knowledge of methods to establish new, or utilize existing, reporting and communication channels throughout an organization
- k1.15 Knowledge of methods to select, implement and interpret metrics (for example, key goal indicators [KGIs], key performance indicators [KPIs], key risk indicators [KRIs])

Information is likely the most valuable resource that companies today possess. Therefore, the organization must identify the information, understand its value, figure out how to protect it appropriately, and then actually protect the information successfully. This is a tall order to fulfill as we can see by paying attention to the news on any given day. Continuously we are bombarded with reports of breaches. One company has had millions of credit card data stolen while another company has had sensitive corporate emails compromised. In other news personally identifiable information (PII), protected health information (PHI) and intellectual property (IP) are leaking into the public domain at an alarming rate. These breaches are occurring as a result of scary sounding things such as trojan horses, cross site scripting, ransomware and whaling attacks. Successful attacks are often the result of weak, unprotected applications being installed in critical infrastructure.

Websites like www.PrivacyRights.org and the Health and Human Services (HHS) wall of shame at

www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html report on known breaches, yet many other breaches do not make it into the news. Companies are hacked. Data is stolen. Users send data to their private email accounts so that they can work from home. Laptops are stolen from locked cars. Networks crash. Database administrators mistakenly delete databases. Network administrators delete

domain controllers by accident. The list of how things can go bad goes on and on.

The challenge we are faced with today is how do we create a security program that works and provides value to our business. If we create a program that enables and grows the business in a secure fashion, we will have the support of senior management that is so greatly desired.

The challenge is complicated by the fact that we must protect ALL our information and the systems that house the information whether it is in a database, spreadsheet, word document, paper files, or an employee's speech. How do we balance the need to protect information without trampling on someone's right to free speech? How can we secure it? That is not a new question. Many older naval facilities still have posters on the wall that say, "Loose lips sink ships." The point is that we need to find all of our information so that we may secure it. Clearly this is not just an IT problem.

We need to create a security program that is not just a silo. We need to merge the physical and information security worlds. Most critically we need to merge the security department into our core businesses. It needs to become part of our culture. It needs to be part of everyone's thinking. Every single person in the business has some kind of responsibility for securing information, from the CEO and board of directors to the janitors and warehouse workers.

Laws and Regulations

The security environment continues to change. One element driving some of these changes is the legal landscape. As a business it is imperative to understand what laws and regulations apply to the organization, we must secure the information in a way that meets both the business requirements as well as keeps us in compliance with those laws and regulations. New legislation is created daily and it is part of the information security manager's job to be aware of these new laws and updates to existing laws and to continue to work to ensure the organization is properly in compliance. These laws include the Health Insurance Portability and Accountability Act (HIPAA) for protecting health information, and Sarbanes-Oxley (SOX) for protecting financial information. There is also

the Federal Information Security Management Act of 2002 (FISMA) that was created to ensure that national security information is protected.

Laws and Regulations: HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 contains two rules: the privacy rule and the security rule. The privacy rule requires safeguards to protect privacy of Personal Health Information (PHI). The security rule contains administrative, technical, and physical safeguards to protect confidentiality, integrity, and security of electronic protected health information (PHI). (Yes, it says Confidentiality, Integrity and Security.) HIPAA applies to health care providers (if they transmit information in an electronic form), health plans and health care clearinghouses.

Laws and Regulations: SOX

The Sarbanes Oxley Act (SOX) of 2002 is a federal law that protects shareholders and general public from accounting errors and fraudulent practices. SOX is also known as "Public Company Accounting Reform and Investor Protection Act" in the Senate and "Corporate and Auditing Accountability and Responsibility Act" in the House. SOX was created as a result of companies like Enron that fraudulently reported their financial reports. SOX applies to publicly traded companies and their wholly owned subsidiaries. Any IT systems that affect financials are within the scope of what must be protected. SOX requires the Securities and Exchange Commission (SEC) to implement any rulings based on failures to fulfill on the SOX requirements.

Laws and Regulations: FISMA

The E-Government Act is a federal law in the United States passed in 2002. This act recognizes the importance of information security to the security and economic interests of the US. Title III of the E-Government Act, entitled Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to develop, document and implement security programs to protect information and the systems that house the

information. (Though FISMA is a US law, many other countries have adopted similar legislation.) **Laws and Regulations: PCI-DSS**

Payment Card Industry-Data Security Standard (PCI-DSS) was “developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally” according to PCI-DSS v3 Nov 2013. PCI-DSS applies to everyone involved in processing payment cards. PCI-DSS defines Cardholder Data and Sensitive Authentication Data.

- Cardholder Data:
 - Primary Account Number (PAN)
 - Cardholder name
 - Expiration date
 - Service Code
- Sensitive Authentication Data
 - Full track data (mag strip or equivalent on chip)
 - CAV2/CVC2/CVV2/CID
- PINs/PIN blocks

PCI-DSS defines 12 specific requirements. Each of these requirements are detailed at a deeper level with many more specific requirements. The 12 requirements are as follows:

1. Install & maintain a firewall configuration to protect cardholder data
2. Do not use vendor supplied defaults for system passwords and other security parameters
3. Protect cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

What is critical to know here for the exam, is the flavor of the laws / regulations, the intention of the laws / regulations, and how these laws / regulations could impact a multinational company. Not the details of each of every law / regulation.

Information Security Governance

In today's complex corporate environment where customers expect privacy and protection from identity theft, business partners require access to sensitive corporate information and intellectual property, regulators demand compliance and everyone is entitled to protection from the on-line predators, how does an organization begin to meet these basic albeit very complicated requirements?

According to the Merriam-Webster dictionary, the term 'govern' means to officially control and lead (a group of people). The term security as defined by Merriam-Webster, is the state of being protected or safe from harm. Therefore, we can extrapolate security governance the things management does to control or lead the company into a state of safety and protection from harm. To accomplish this, the organization must put a system of practices, processes, and policies in place by which the company's activities are directed and controlled. This is called governance.

The goal of information security is to protect our critical information within our business while allowing our business to accomplish its mission, meet its goals and objectives and to grow and expand. There are six critical outcomes of a company's information security governance:

1. Strategic Alignment

Information Security will be aligned with the goals of the business, allowing the business to grow and expand securely.

2. Risk Appropriately Managed

Risks will be identified, analyzed, and prioritized periodically and the appropriate controls put in place to effectively minimize those risks.

3. Value Delivery

Security decisions will be cost-justified. Money will be spent appropriately (within budget) on tools that help to secure and grow the business.

4. Optimized Resources

The tools and resources available to the security department will be used properly and effectively to secure and grow the business.

5. Performance measurement

Metrics will be put in place and exercised to provide specific measurable information to management regarding the success level of securing the business.

6. Assurance Integration

Security will be integrated with all assurance functions within the business.

**Information Security Governance
is Senior Management's direction
for the security of their business.**

Gone are the days when security is driven from the bottom up. History has shown that business activities that are driven from the bottom are doomed to failure. Likewise, “bolted-on security” or security as an afterthought is an idea that has run its course as well.

It is critical that organizations have strong leadership from executive management, as they are the ones who must be the champions for information security. It is the responsibility of the board of directors and executive management to provide direction and oversight to security activities. They must display their commitment to security by ensuring security governance is integrated into the overall corporate governance and that information security strategies are aligned with and integrated with business strategies.

The Information Security Framework provides guidance through the development and management of a comprehensive information security program. The security program is the entirety of the efforts a company expends in order to identify and protect information assets. Information, and the protection it requires, extends beyond simple IT technology solutions, and extends into policies, procedures, and controls in addition to implemented technology.

- Policy - Overall intention and direction as formally expressed by management.
- Standard - A mandatory requirement, code of practice or specification approved by a recognized external standardization organization, such

- as International Organization for Standardization (ISO).
- **Baseline** - The minimum-security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection.
 - **Procedure** - A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards.
 - **Guideline** - A description of a particular way of accomplishing something that is less prescriptive than a procedure.

~ As defined by ISACA

Exam Hint:
Have a good understanding of
the key terms: Policy,
Standard, Baseline,
Procedure, and Guideline

Roles and Responsibilities

In order to create a security structure within a business, it is first necessary to look at who is responsible for these activities. Actual titles can vary from one organization to another, but the responsibilities must be assigned. Below are a few generic roles and their responsibilities.

- **Board of Directors** - The board provides the high-level vision and strategy of the organization as well as governance and oversight to ensure the organization is working to fulfill the vision and strategies. The board is responsible to act in good faith to serve the organization for the best interest of the stakeholders. Members of the board will be held accountable for this. To ensure proper

oversight, the board must be aware of any applicable laws and regulations.

- Chief Executive Officer - The Chief Executive Officer has the responsibility of running the business and carrying out the day-to-day decisions necessary to effectively achieve the goals and objectives of the company.
- Chief Risk Officer - Some organizations wrestle with the question of 'should there be one individual or a group of people responsible for managing the risk of the organization?' When one person is responsible, he or she is often given the title of Chief Risk Officer. When several people share the load, they are referred to as a risk committee. No matter the choice, this role owns the risk management process. This person or committee needs to ensure that risk management strategies align to business strategies. The CRO must also effectively communicate risks to senior executives, the board of directors and other stakeholders.
- Chief Information Officer - The CIO is responsible for planning and overseeing Information Technology (IT) strategies. An integral part of IT is the implementation of security devices such as a firewall or IDS.
- Information Security Manager - Information Security Managers are responsible for implementing the organization's security program. They play a key role in the identification, analysis, and mitigation of risks that could impact the organizations mission. (The entire CISM certification focuses on the duties of the ISM.)
- Owners - Owners can be broken into two categories: data owners and system owners. The data owners must ensure the necessary controls are in place to protect the confidentiality, integrity and availability of the information and system owners do the same for the system(s) for which they are responsible for.
- Others - A host of other job roles may be defined by the organization based on specific needs. Examples might include business unit and functional managers, security practitioners, and trainers. Security responsibilities should be assigned based on organizational policy and operational needs.

**The Chief Risk Officer or Risk
Committee OWNS corporate risk.**

The most important task of everyone listed (and even those not listed here) is to ensure that a business can grow and expand successfully, that can only be done by incorporating security functions and concepts into everyday activities. It is critical that things come together in a logical and carefully planned process. Governance, Risk Management and Compliance (GRC) are the fundamental ingredients of information security management.

Governance is the responsibility of the board and executive management. Governance provides the structure necessary to ensure that there are processes and policies in place and that everyone within the business is following the processes and policies.

ISACA defines Information Security Governance as the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that the enterprise's resources are used responsibly.

Risk Management combines the functions of risk assessments and risk handling. The risk assessment allows the organization to understand what potential harm could come from business activities while risk handling ensures that the proper controls are put in place to minimize the harm and maximize the reward. (Risk management is explored in depth in Chapter two.) Compliance is when the organization is aware of the applicable laws and regulations and they are taking steps to ensure those requirements are satisfied. For the organization to display compliance, they must monitor and record the current status of the security controls. This can be done through

audits, assessments, penetration testing to name a few methods. Once the organization is aware of their current level of compliance, appropriate actions can be taken to close the gap between that level and desired level according to corporate policies. The term compliance can be used in reference either to internal policies or external legal requirements (such as SOX).

Business Model for Information Security

The Marshall School of Business at the University of Southern California created the Business Model for Information Security (BMIS). ISACA is developing the Systemic Security Management Model (SSMM) from the BMIS. The BMIS also has provided context for another ISACA creation - COBIT® formerly known as Control Objective for Information and Related Technology.

The BMIS takes the approach of systems theory. This is the idea that a system needs to be viewed holistically as a complete functioning unit. This leads to systems thinking that allows us to view the whole, not just the individual parts or individual systems.

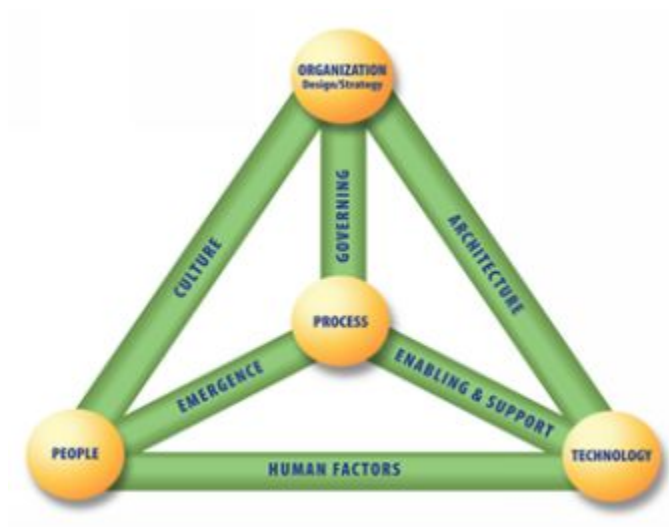


Diagram 1
BMIS

Image sourced from: <http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx>

As you can see from the BMIS information security is not just technology. Security is a combination of People, Processes and Technology. This approach allows for a much more effective security program.

The four elements to BMIS are:

1. Organization Design and Strategy

Organization's strategy that is defined in their policies, standards, procedures, and guidelines.

2. People

All the employees and contractors of a business have a job and a responsibility to the security of the company.

3. Process

Process can be formal or informal, simple, or complex, but they are the mechanisms to get things done, especially the security of information.

4. Technology

These are all the tools and applications to secure the business. This is only a single element, not security as a whole.

The dynamic interconnections are:

- Governance
 - This is how an enterprise is directed by senior management.
- Culture
 - The patterns and behavior of employees.
- Enablement and Support
 - Technology and process must be connected. Technology cannot stand on its own.
- Emergence

- The developing, often without intention, patterns of how people and processes interact within a business.
- Human Factors
 - The link between people and technology. People must understand how to use the technology they are given and its limitations.
- Architecture
 - The design of the organization's security plan and the technology selected to implement it correctly.

Strategy

How does an organization create an information security strategy? How is a security plan created in a logical fashion? How does the organization ensure that the created plan will meet the needs of the business? The regulatory and legal needs? There are many different methodologies and frameworks available. Which of these chosen really depends on the understanding of the business and its needs. We could even use a combination of different tools at different points in the process.

Exam Hint:

For the CISM exam it is only critical that we understand these options exist and where each tool is best used. More details than necessary for the exam are included below. Sometimes it is necessary to take a slightly deeper look at something in order to have a basic idea as to where it is best used.

Below are brief descriptions of some of the tools available to use in the process of strategizing Enterprise Security:

- COBIT 2019 - A framework for developing, implementing, monitoring, and improving IT governance and management practice.
- CMMI® - A process improvement framework.
- Balanced Scorecard - A [strategic planning and management system](#) that is used to align business activities to the vision and strategy of the organization.
- TOGAF - A set of tools and methodologies to developing an enterprise architecture.
- Zachman Framework - A methodology to develop a complex idea within an enterprise using simple questions to gain an understanding of the requirement.
- SABSA® - A methodology for developing business-driven, risk and opportunity focused security architectures.
- ISO 27002 - Contains best practices to be used as a reference for selecting controls to be used within an Information Security Management System.
- FISMA - Federal government requirement for federal agencies to create an information security program.
- ITIL® - A comprehensive set of best practices for IT services management.
- ISO 20000 - This is a support document for implementing ITIL.
- NIST SP 800-53 - This is the Security and Privacy Controls for Federal Information Systems and Organizations.

Strategy Methodologies: COBIT 2019

COBIT 2019 is a framework for developing, implementing, monitoring & improving information technology governance and management practices. It was originally developed by ISACA in 1996 and is now up to COBIT 2019, published in 2019.

COBIT has 5 key principles, they are:

1. Meeting stakeholder needs
 1. COBIT can be used by a business, in a customizable manner, to ensure that IT fulfills the needs of a business while managing risk appropriately.

2. Covering the enterprise end to end
 1. COBIT does not just cover the “IT function,” it integrates nicely into all aspects of enterprise governance.
3. Applying a single integrated framework
 1. COBIT aligns well with other frameworks so it can be used as the high-level holistic connector framework.
4. Enabling a holistic approach
 1. COBIT defines a set of enablers that supports a holistic approach to IT and enterprise governance within a business. Those enablers are:
 1. Principles, Policies and Frameworks
 2. Processes
 3. Organizational Structures
 4. Culture, Ethics, and Behavior
 5. Information
 6. Services, Infrastructure and Applications
 7. People, Skills and Competencies
5. Separating governance from management
 1. Governance ensures that stakeholders needs are met, direction is set, and monitoring performance is agreed upon.
 2. Management plans, builds, and runs what governance decided upon.

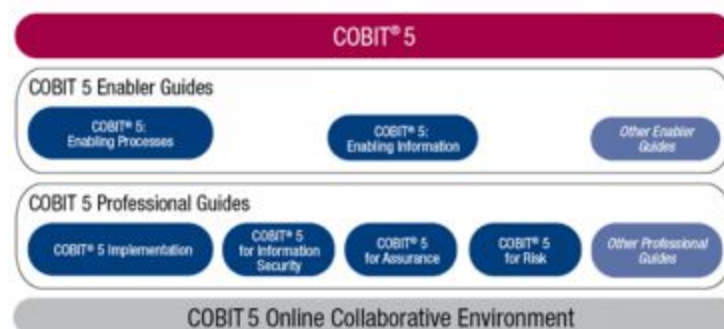


Diagram 2
COBIT 5 Collaborative Environment

~ From <https://COBITonline.isaca.org/l3-main?book=framework#framework-preface02>

Strategy Methodologies: CMMI

Capability Maturity Model Integration (CMMI) is from the CMMI Institute which is a part of Carnegie Mellon. CMMI is a model that helps to improve a process by comparing your existing processes with proven best practices. The original creation by the Software Engineering Institute at Carnegie Mellon was the Capability Maturity Model (CMM®). CMM was created specifically for the software development process. Because CMM proved to be extremely useful at improving the performance of software development processes, it was adopted for use within other business processes. A challenge with CMM was trying to integrate it into an enterprise with everything else. As a result, CMM was modified to CMMI.

CMMI has collections of:

- Effective practices
- Process improvement goals

When an organization knows which processes, they want to improve, they can then select the best solution to follow in order to improve business processes. The solutions include:

- CMMI for Acquisition (CMMI-ACQ)
- CMMI for Development (CMMI-DEV)
- CMMI for Services (CMMI-SVC)
- People CMM
- Data Maturity Model (DMM)

Strategy Methodologies: Balanced Scorecard

Dr. Robert Kaplan of the Harvard Business School and Dr. David Norton invented Balance Scorecard to provide a way to add a non-financial set of performance measurements to traditional financial performance measurements in order to provide a more balanced view of an enterprise's

performance. Balanced scorecard is a management system, not just a form of measurement that allows management to take their visions and turn them into actions.

When analyzing an enterprise, Kaplan and Norton say to look from four different perspectives:

- Financial Performance
- Satisfaction
- Efficiency
- Knowledge and Innovation

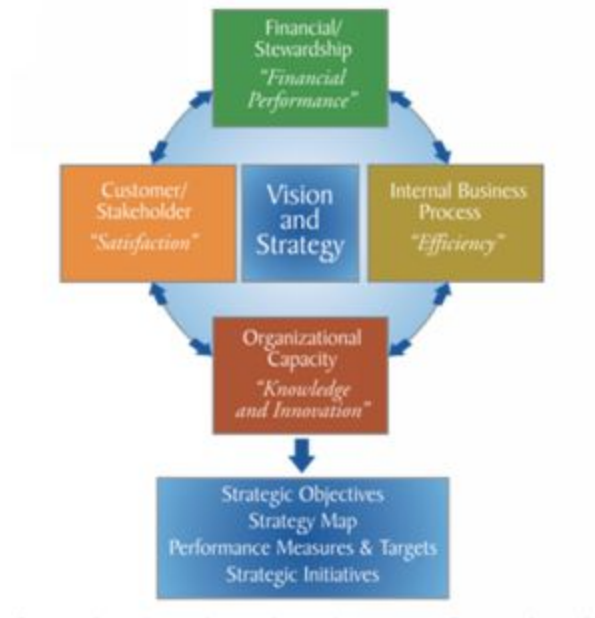


Diagram 3

Balanced Scorecard

Pulled from <http://balancedscorecard.org/Resources/About-the-Balanced-Scorecard>.

The main purpose of the balanced scorecard is to improve knowledge and therefore performance, which can be seen from the bottom of the following chart upward. The chart also shows a cause-and-effect relationship between strategy objectives.

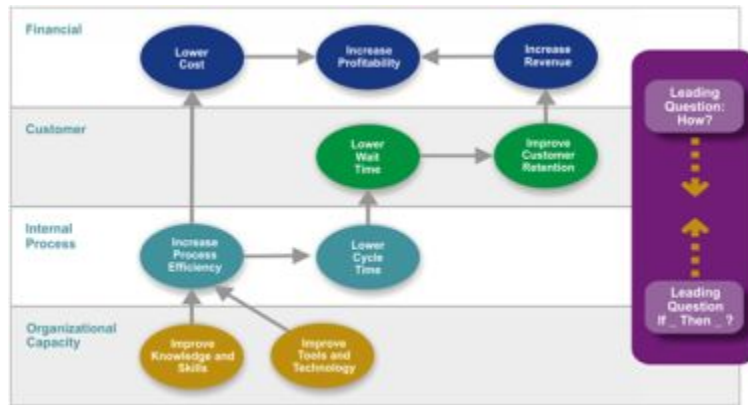


Diagram 4
Balanced Scorecard 2

Pulled from <http://balancedscorecard.org/Resources/About-the-Balanced-Scorecard>

More information can be found at <http://balancedscorecard.org>.

Strategy Methodologies: TOGAF

The Open Group Architecture Forum (TOGAF) was developed based on the US DoD Technical Architecture Framework of Information Management (TAFIM). TOGAF was developed for the purpose of providing tools and methodologies used in developing an Enterprise Architecture (EA). It is designed as a guide to get through the development process effectively and develop an architecture designed specifically for your business.

TOGAF is broken down into seven parts:

- Part 1 – Introduction
- Part 2 – Architecture Development Methodology
 - Step-by-step approach for developing an Architecture Development Method (ADM)
- Part 3 – ADM Guidelines / Technique
 - Collection of guidelines and techniques for use in TOGAF
- Part 4 – Architecture Content Framework
 - Describes the use of reusable architectural building blocks

- Part 5 – Enterprise Continuum & Tools
 - Tools to categorize and store architectural activities
- Part 6 – TOGAF Reference Models
 - Technical Reference Model (TRM) – universally applicable services useful for developing ANY system architecture
- Part 7 – Architecture Capability Framework
 - Discusses organization, processes, skills, roles & responsibilities needed to establish and operate an EA.

Strategy Methodologies: Zachman Framework

John Zachman is the man behind this framework. The Zachman framework is a combination of two basic ideas. The first is the ability to describe complex ideas and the second is the ability to turn the abstract idea into a reality.

The ability to describe a complex idea is based in a set of primitive interrogatives (aka: questions) we have all known most of our lives. Who? What? Where? When? Why? and How? Using these six basic questions we have the access to uncover the words we need to describe any complex idea. The questions are to be asked from a variety of different views that can be seen within the 6x6 grid commonly seen in discussions of this framework.

	DATA What	FUNCTION How	NETWORK Where	PEOPLE Who	TIME When	MOTIVATION Why
Objective/Scope (contextual) Role: Planner	List of things important in the business	List of Business Processes	List of Business Locations	List of important Organizations	List of Events	List of Business Goal & Strategies
Enterprise Model (conceptual) Role: Owner	Conceptual Data/ Object Model	Business Process Model	Business Logistics System	Work Flow Model	Master Schedule	Business Plan
System Model (logical) Role: Designer	Logical Data Model	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Technology Model (physical) Role: Builder	Physical Data/Class Model	Technology Design Model	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Detailed Representation (out of context) Role: Programmer	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Speculation
Functioning Enterprise Role: User	Usable Data	Working Function	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy

Diagram 5
Zachman Framework
~ From

http://www.mel.nist.gov/msid/SSP/standard_landscape/Zachman.html

Utilizing six common questions, the second part of the Zachman Framework is the transformation from an abstract idea into an actual representation of that idea through Identification, Definition, Representation, Specification, Configuration, and Instantiation.

The critical part to know about Zachman is that it is an ontology - a study of the nature of the existence of something within an enterprise. It is the ability to question and understand something, anything, within an enterprise. If you understand something, you can then begin to address its change... or its security.

A great resource to learn more about this framework is
<https://www.zachman.com/about-the-zachman-framework>.

Strategy Methodologies: SABSA

Sherwood Applied Business Security Architecture (SABSA) is “A proven framework and methodology used to meet a wide variety of Enterprise needs” -SABSA.

“A proven methodology for developing business-driven, risk and opportunity focused Security Architectures at both enterprise and solutions level that traceably support business objectives” – SABSA



Diagram 6
SABSA Lifecycle

SABSA provides assistance through the logic of the lifecycle of planning.

You must plan (Strategy & Planning) before you can build anything. If you do not plan first, you never know what you are going to get but it is likely that you will not get something that truly helps. Planning never absolutely assures that things will go well, but statistically, planning makes success much more likely.

Once we have a basic plan in place, we can Design the actual security structures that we will put into place. We need to know the controls that will solve our problems such as IDS, IPS, Firewalls, and crypto for example. We must also figure out where things will be implemented. For example: will we put a firewall in front of our data center servers? What kind of firewall? How many firewalls? What will the configuration be in each firewall?

Once the design is finalized and goes through proper reviews (e.g., peer reviews) then we can Implement our Design. We must go purchase the appropriate products. Test the products appropriately in our lab environment and, once we are sure they work properly, install them into the production environment.

Just because we have planned carefully, thoughtfully designed and tested before we installed it does not mean that things will work properly, or continue to work properly, or continue to be the best installation options. We must Manage and Measure regularly to ensure that things are working as we need them to in order to protect the data and enable the critical functions of the business.

Strategy Methodologies: ISO 27002

The International Organization for Standardization - International Electrotechnical Committee (ISO/IEC) develops international standards for just about everything. However, they do not usually create standards from nothing. Rather, the ISO takes already existing standards and modifies them to have an international spin. ISO-27002 and ISO-27001 were developed from British Standard (BS) 7799. BS-7799 was a two-part document. The first part contains recommendations and best practices for Information Security Management. The second part is used to provide assurance regarding the implementation of those best practices within a specific organization through an audit.

In a strange twist of numbers BS-7799 part 1 originally became ISO-17799 and then ISO 27002. Where BS-7799 part 2 became ISO 27001. The latest version of both ISO-27001 and 27002 are dated 2013.

From ISO.org: ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

It is designed to be used by organizations that intend to:

1. Select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001.
2. Implement commonly accepted information security controls.
3. Develop their own information security management guidelines.

Strategy Methodologies: FISMA

The Federal Information Security Management Act (FISMA) is Title III of the E-Government Act of December 2002. A risk based, cost effective security strategy is the emphasis of FISMA.

From FISMA:

Our Vision

To promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act including:

- Standards for categorizing information and information systems by mission impact
- Standards for minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems
- Guidance for assessing security controls in information systems and determining security control effectiveness
- Guidance for the security authorization of information systems

- Guidance for monitoring the security controls and the security authorization of information systems

-From

<http://csrc.nist.gov/groups/SMA/fisma/index.html>

Strategy Methodologies: ITIL

ITIL, formerly known as Information Technology Infrastructure Library, is a comprehensive set of best practices for IT management. ITIL is owned by AXELOS, which was a joint venture company between the UK Cabinet and Capita. It is believed that IT should be well planned, designed, managed, and delivered with the goal of getting the most out of our investment is critical to the successful management of IT.

For deeper research check out <http://www.itil-officialsite.com/>.

Strategy Methodologies: ISO 20000

ISO 20000 was based on BS 15000 for the purpose of IT service management. It was designed to support the best practices found within ITIL. It has expanded to now support other documents such as COBIT.

ISO 20000 has five parts to it:

- ISO 20000-1 - involves "the design, transition, delivery and improvement of services that fulfill service requirements and provide value for both the customer and the service provider".
- ISO 20000-2 - Guidance for the application for the Service Management System (SMS).
- ISO 20000-3 - Guidance for service providers that are implementing ISO 20000-1.
- ISO 20000-4 - Facilitates the development of a process assessment model.
- ISO 20000-5 - An implementation plan for service providers that are implementing ISO 20000-1

Strategy Methodologies: NIST SP 800-53

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 is the Security and Privacy Controls for Federal Information Systems and Organizations.

FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems is a challenge for federal agencies to meet. This document, NIST SP 800-53 is intended to give guidance to those agencies for specifying and selecting security controls.

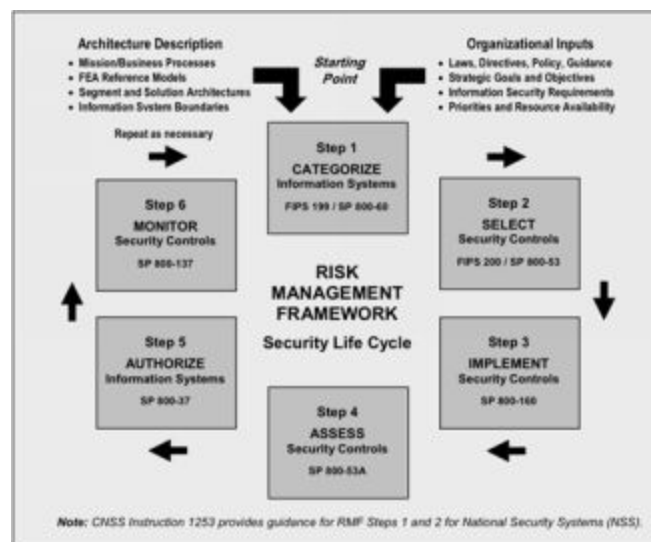


Diagram 7
NIST SP 800-53 SLC
~ From NIST SP 800-53

If you look within the 6 steps identified by the above picture you will see that NIST SP 800-53 is in Step 2 - Selecting controls.

Controls

In the previous section, we looked at different conventions that discuss Governance, Framework, Strategy and Risk Analysis. They are all designed to lead us to the selection and implementation of controls that are both effective and fiscally responsible. That is a mouth full. Let us begin by defining what controls are and then we will delve into different types of controls in order to understand our options.

Controls are those actions or technologies we utilize to restrict or influence behavior to provide a set of checks and balances on organizational activities.

Security controls can be divided into the three distinct types: Physical, Technical/Logical and Procedural/Administrative. Physical controls are the easiest to explain. They involve all the things that you can touch such as fences, dogs, and locks. The technical (a.k.a. logical) controls include things such as anti-virus software, network, or host-based intrusion detection systems (IDS), or cryptography. Procedural (a.k.a. administrative) controls include policies, procedures, and baselines.

Controls can also be divided into several distinct categories. The categories include preventive (preventative), detective, directive, corrective, and recovery. The difficulty with categories is that a single control can cross the category boundary very easily. The idea of what each category is designed to accomplish is the greater concern, not memorizing which category a single control does fit into.

- Preventive controls are designed to stop something from happening. This is probably the most difficult of categories to understand, as everything that fits in here will not work perfectly all the time. Preventative controls will not absolutely prevent something from happening, but that is their goal. A simple example of a preventative control is an Intrusion Prevention System (IPS) that attempts to block (prevent) bad things from happening, however an IPS is not 100% effective.
- Detective controls are designed to inform us that something is happening or has happened. A simple example is an Intrusion Detection System (IDS). Log files are possibly the most prevalent detective control.
- Directive controls are management statements that if not followed, have a very specific consequence. A well-written policy should include the specific consequences someone might have to face if they violate the policy as in 'anything up to and including termination of employment.' A policy with consequences constitutes a directive control.

- Corrective controls will take something that is not working and return it to a functional level. A great example of a corrective control is an Uninterruptible Power Supply (UPS) or a diesel generator, which can keep equipment running when there is a power outage. It is not ideal, but things can continue to operate.
- Recovery controls take something from a non-working or mostly non-working status to a normal condition. When a primary router has failed and the proper procedure was followed to fully restore the router to complete functionality, the procedure itself is the recovery control.

When selecting controls that satisfy our security goals the best design choice is usually to implement defense in depth. Defense in depth provides multiple levels of controls between the attacker and the sensitive information systems. These multiple levels will give the security staff and/or the incident response team the ability to detect the attack and then take the appropriate actions to defend and repair any damages.

There is yet another distinction in the way controls are divided. Controls can be divided into countermeasures and safeguards. The most common use of these terms is probably the following:

- Controls - This is the generic term that covers all safeguards and countermeasures.
- Safeguards - Safeguards are best thought of as preventive controls. Their purpose is to help prevent or reduce the chance of some bad thing from happening.
- Countermeasures - Countermeasures are best thought of as controls that are needed after something bad happens to a business.
 - For example: If I am worried that my laptop could be stolen then it is best to put in place controls (safeguards) to reduce the chance of the theft. I could use something like a cable lock when I must step away from my laptop, or place it in a locked cabinet, or better yet always keep it with myself. Should my safeguards fail then the controls (countermeasures) that need to

have been previously installed include the encryption of my sensitive data, insurance, and data backups in order to restore onto another system.

Security Program

With knowledge of laws and regulations, a security management structure within the business, and a strategy devised, we can now create our security program. The security program is effectively our actual security structure. This is where we begin to define, implement, monitor and update the policies, standards, procedures, baselines, and guidelines.

Assurance

Management needs to understand the security threat, the solutions, and have a way to understand if the solutions that have been implemented are effective and doing what they were implemented to do. In other words, management needs assurance, and in order to have assurance there needs to be a way to measure what is happening within the organization. Information security is not just about networks, it is all encompassing, so assurance needs to be all encompassing as well.

ISO 27001 addresses the need for assurance in Section nine - Performance Evaluation. The first thing that needs to be understood, is “What needs to be monitored?” followed by “How does this get monitored?” In addition to discussing how to answer those questions, ISO 27002 goes on to discuss the requirement for internal audit. The requirements for the audit should be incorporated within the Information Security Management System (ISMS). Management shall periodically review the overall corporate security posture and make changes/improvements as required.

Security Metrics

Security metrics are the tools that are used to determine if we have achieved that which we set out to achieve. Simply stated, they are a way to measure goals and the successful attainment of those goals.

ISACA primarily discusses two specific metrics Key Goal Indicators (KGI) and Key Performance indicators (KPI).

Key Goal Indicators are used to define what we are looking to accomplish. They are the targets that we are aiming for. It has been said that ‘if you aim at nothing, you will hit it every time.’ It is very difficult if not impossible to manage those things that are not identified and defined, for example when organizations attempt to embark on a project that does not have a clearly defined scope. KGIs help managers define what it is that they are trying to accomplish.

Key Performance Indicators are then used to determine if the goals have been met, and if so, how well. Given two (or more) choices, there needs to be some indicator of which choice is better or worse than the other. Without objective measurement capabilities, it is very difficult to make that determination. KPIs give that capability.

KGIs are considered “lead” indicators (Where are we trying to go?), while KPIs are considered lag indicators (Did we make it?). Together they can be used to paint a complete picture of where we are.

If Key Goal Indicators define the target and Key performance indicators measure how close we are to hitting our target, then Critical Success Factors (CSF) define the necessary resources or actions that absolutely “must happen” if we hope to get anywhere close to hitting the target.

A Balanced Scorecard (introduced earlier) functions as a dashboard of gauges to measure various performance metrics including KGIs, KPIs, and Critical Success Factors (CSF).

COBIT 2019 utilizes all three of these metrics (KGI, KPI, and CSF), and incorporates them as part of their enabling processes.

Exam Hint:

Key Goal Indicators (KGI) identify what we are trying to do. **Critical Success Factors (CSF)** are the things that must be accomplished to achieve our goal. **Key Performance Indicators (KPI)** indicate how well we are doing at continuing to achieve our goals.

Awareness, Training, and Education

Security is achieved when knowledgeable, skilled people follow tried and proven processes and procedures. A good security plan is useless when the knowledge is not extended to everyone that needs to know about it. There are three ways to spread the word: Awareness, Training and Education.

- Awareness is defined within NIST SP 800-50 as an activity that seeks to focus an individual's attention on an issue or set of issues.
- Training is defined within NIST SP 800-50 as something that strives to produce relevant and needed security skills and competencies.
- Education is defined within NIST SP 800-50 as something that integrates all the security skills and competencies of the various functional specialties into a common body of knowledge ... and strives to produce IT security specialists and professionals capable of vision and proactive response.

Combinations of all three are needed throughout a business. Training, awareness, and education allow people to properly implement security

tools, behave in a manner consistent with security policies, and understand and follow procedures.

Looking back through this chapter, we introduced and discussed a long laundry list of security related topics. We started by identifying security requirements, then aligning those requirements to business requirements and then creating and implementing a security program that addresses those requirements. We finished by discussing how the program can be measured as well as communicated to the necessary people.

During requirements definition we identified requirements as both internal, possibly from stakeholders, as well as external, possibly derived from applicable laws and regulations. We then dove into frameworks covering not only how to identify requirements, but also how to fulfill those requirements. We looked at controls that allow us to protect our assets and metrics to ascertain how well we are doing at defining our goals, getting to our goals, and maintaining our goals. Finally, we need to take this abstract strategy and turn it into a plan of action.

COBIT 2019 aligns closely with the Project Management Body of Knowledge (PMBOK). PMBOK is useful for developing and managing project plans. Expanding on PMBOK, COBIT 2019 has seven enablers that create a mesh of security projects. One of the enablers is called “Processes.” Within each project will be numerous processes, which if carefully designed to follow COBIT 2019, will ensure that each project will be aligned with other security efforts within the organization. Additionally, the project itself may be the installation of security processes into the Information Security Management System (ISMS).

A “Gap Analysis” is performed to identify the current status relative to where they “should” be or where they plan to be. Completing a gap analysis at the beginning of a project helps to create a business case for the project while conducting a gap analysis periodically during the project helps to determine if the project is on track.

Each project should have defined Critical Success Factors (CSF) used to delineate minimal requirement for successful project completion. CSFs are used to identify and document what must be done during the project.

Summary

As a business, it is critical that management first understands the need for security planning and the controls required to implement that plan. Once management understands and commits to the need for security, there needs to be a security infrastructure built into the organization - security positions need to be established, roles and responsibilities need to be defined and delegated, frameworks need to be developed, and an implementation plan created.

The business needs include fulfilling legal and regulatory requirements, so a function must be established to understand what legal obligations exist and to monitor compliance to those requirements. Further needs include the desire to keep our own data safe, and the requirement of senior management to satisfy shareholder and customer demands. Once we understand the requirements involved in securing the business, it is time to strategize. There are several tools/frameworks that can be utilized in the strategy process such as COBIT, Zachman and SABSA. Some of these tools can also help with the process of choosing and implementing security solutions.

When faced with deciding which security tool best meets our requirements, we need to keep in mind that there are different categories and types of controls. Some controls are preventative in nature and need to be used prior to a security incident, while other controls are detective or corrective in nature and are not used until after an incident. There are also administrative, technical, and physical controls. A variety of each type of control will ensure that an organization has the required defense in depth.

Controls by themselves are fine, but measurements need to be put into place to give management the assurance that the controls are meeting the needs of the business. This is the job of a KPI. A KGI and a CSF are used to develop requirements for the security development process. Finally training (awareness, training, and education) are needed to ensure that all employees have the proper skills and understanding to perform their job tasks.

All these ideas are small parts of the security program that must be developed. The security program is what will guide all decisions and

purchases that are made to secure the people, the business, and the data. A gap analysis will frequently be performed to determine if where we are aligns with where we want to be.

Chapter 1 Questions

1. Information security governance is most effective when it is:
 - a. The CIO reports directly to the board of directors
 - b. Strategically aligned with business requirements
 - c. Policies are aligned with the law only, e.g., SOX or GLBA.
 - d. Implemented in a cost-effective manner
2. Ensuring that funds are spent appropriately, and the security decisions are cost justified is an example of what critical outcome of security governance?
 - a. Risk assessment
 - b. Return on investment
 - c. Value delivery
 - d. Job security
3. The overall intention and direction of security as formally expressed by management is defined as:
 - a. Policy
 - b. Guideline
 - c. Standard
 - d. Procedure
4. Ensuring the security of information assets is the responsibility of:
 - a. Only the CEO.
 - b. Everyone in the organization plays a role in security information assets.
 - c. Only people with computer access.
 - d. Everyone in the business with security in their job description.
5. The four elements of the Business Model for Information Security (BMIS) are:
 - a. People, Mission, Technology & Guidelines
 - b. Process, Organization, Technology & Guidelines
 - c. Mission, Technology, Laws & People
 - d. People, Process, Organization & Technology

6. The Business Model for Information Security has defined several dynamic interconnections between the four elements. How is the architecture element defined?
 - a. The design of the organizations security plan and the technology selected to implement it correctly.
 - b. The developing, often without intention, patterns of how people and processes interact within a business.
 - c. The link between people and technology. People must understand how to use the technology they are given and its limitations.
 - d. The patterns and behavior of employees as a whole.
7. Which of the following frameworks focuses on process improvement?
 - a. Sherwood Applied Business Security Architecture (SABSA)
 - b. Zachman Architecture Framework
 - c. The Open Group Architectural Forum (TOGAF)
 - d. Capability Maturity Model Integration (CMMI)
8. The ability to describe complex ideas using a set of primitive interrogatives; who, what, when, where, why and how is the foundation of which architectural framework?
 - a. Sherwood Applied Business Security Architecture (SABSA)
 - b. Capability Maturity Model Integration (CMMI)
 - c. Zachman Architectural Framework
 - d. The Open Group Architectural Forum (TOGAF)
9. ISO-27002 was originally:
 - a. ISO 9000
 - b. ISO 17799
 - c. ISO 9001
 - d. BS 27002
10. What are the three types of security controls?
 - a. Physical, logical/technical, practical
 - b. Physical, practical, procedural
 - c. Logical/technical, administrative, managerial
 - d. Physical, technical/logical & administrative/procedural

11. Controls designed to return a non-functioning system to a normal status or called:
- a. Corrective
 - b. Directive
 - c. Preventive
 - d. Detective
12. An intrusion prevention system is an example of what type of control?
- a. Countermeasure
 - b. Directive
 - c. Safeguard
 - d. Physical
13. Security metrics designed to identify those things an organization intends to accomplish are known as:
- a. Key Performance Indicators (KPI)
 - b. Positive Feedback Ratio (PFR)
 - c. Maximum Tolerable Downtime (MTD)
 - d. Key Goal Indicators (KGI)
14. Security metrics designed to measure progress towards meeting an identified goal are known as:
- a. Maximum Tolerable Downtime (MTD)
 - b. Key Performance Indicators (KPI)
 - c. Key Goal Indicator (KGI)
 - d. Job Task Analysis (JTA)
15. The most important role the CEO has to fulfill on within their business is
- a. approving and supporting policies and supporting documents
 - b. putting on a good show of support for the security department
 - c. ensuring that all security professionals are performing all of the tasks in their job descriptions
 - d. approving all security device purchases

16. Critical Success Factors (CSF) defines:
- a. A lagging indicator of those items that are successfully measured
 - b. A leading indicator of those items that are successfully identified
 - c. Those actions that "must happen" for an organization to be able to reach the defined goal(s).
 - d. A dashboard of key Performance Indicators (KPI's) and Key Goal Indicators (KGI's)
17. The goal of security _____ is to "focus attention on an issue or set of issues".
- a. Training
 - b. Nagging
 - c. Education
 - d. Awareness
18. Privacy regulations are primarily focused on
- a. Identity theft
 - b. Personally identifiable information
 - c. Protecting financial information from fraud
 - d. Protecting health information
19. A tool designed to produce relevant and needed security skills is called:
- a. Security Training
 - b. Security Awareness
 - c. Education
 - d. Key Performance Indicator (KPI)
20. Imparting knowledge is the fundamental goal of:
- a. Awareness
 - b. Unilateralism
 - c. Training
 - d. Education
21. Information security frameworks are designed to provide
- a. a control list
 - b. detailed instructions
 - c. guidance

d. absolute rules

22. The most effective way for a company to ensure that employees will follow the corporate password policy is

- a. penalties for non-compliance
- b. Periodic password audits
- c. awareness training
- d. A Kerberos single sign on system

23. When creating an information security plan, it would be best to make sure that you have included

- a. Current and desired future state
- b. Budget
- c. Job descriptions
- d. Corporate mission statements

24. If a quarterly report is being written for delivery to executive management, it is important that you consider the following element

- a. Executive managements intelligence level
- b. Information security metrics
- c. Establish connections to business objectives
- d. Metric to baseline links

25. Which of the following characteristics is most important for a Chief Information Security Officer to have?

- a. Ability to map business needs to security technology solutions
- b. Ability to understand all laws potentially applicable to the business
- c. Ability to comprehend the cost of not understanding the business needs
- d. Ability to map technologies to security tools

26. The responsibility for legal and regulatory liabilities falls upon the

- a. board and senior management.
- b. chief counsel.
- c. chief risk officer.
- d. senior security manager.

27. When looking at an information security standard the MOST important field to analyze would be the

- a. initial approval date
- b. Author name
- c. Last review date
- d. Creation date

28. If a security manager is working for an international company that is governed by different laws in different jurisdictions it is best to

- a. establish standards that meet the minimum level of conformance with ALL jurisdictions
- b. develop minimum required standards with supplemental standards as needed
- c. ensure that all locations are in conformance with the laws of ALL jurisdictions
- d. select the law of one jurisdiction to follow

29. Clearly defined roles and responsibilities provides the immediate benefit for the information security manager of

- a. Separation of duties
- b. Policy compliance
- c. Proper audits
- d. Accountability

Chapter 1 Questions with Answers and Explanations

1. Information security governance is most effective when it is:
 - a. The CIO reports directly to the board of directors
 - b. Strategically aligned with business requirements**
 - c. Policies are aligned with the law only, e.g., SOX or GLBA.
 - d. Implemented in a cost-effective manner

Explanation:

Answer B: If information security governance does not support the business it will work counter to it at some point. That will only receive push back, lack of funding, discontent, etc. If it is in alignment with the business, then it can be cost effective. Policies should align with laws but not ONLY. The CIO could report to the board, but it is a business decision where they report.

2. Ensuring that funds are spent appropriately, and the security decisions are cost justified is an example of what critical outcome of security governance?
 - a. Risk assessment
 - b. Return on investment
 - c. Value delivery**
 - d. Job security

Explanation:

Answer C: Value delivery is to make cost justified security decisions. The other three - job security, return on investment, risk assessments are not goals of information security governance.

3. The overall intention and direction of security as formally expressed by management is defined as:
 - a. Policy**
 - b. Guideline
 - c. Standard

d. Procedure

Explanation:

Answer A: Policies should show managements security intentions and directions. Standards are the mandatory requirements; baselines are minimum-security controls and guidelines are good suggestions.

4. Ensuring the security of information assets is the responsibility of:

- a. Only the CEO.
- b. Everyone in the organization plays a role in security information assets.
- c. Only people with computer access.
- d. Everyone in the business with security in their job description.

Explanation:

Answer B: Everyone has a security responsibility such as not propping the wrong doors open, not letting people tailgate in, discarding trash properly, etc.

5. The four elements of the Business Model for Information Security (BMIS) are:

- a. People, Mission, Technology & Guidelines
- b. Process, Organization, Technology & Guidelines
- c. Mission, Technology, Laws & People
- d. People, Process, Organization & Technology**

Explanation

Answer D: BMIS is made up of people, processes, organization and technology.

6. The Business Model for Information Security has defined several dynamic interconnections between the four elements. How is the architecture element defined?

- a. The design of the organizations security plan and the technology selected to implement it correctly.**
- b. The developing, often without intention, patterns of how people and processes interact within a business.

- c. The link between people and technology. People must understand how to use the technology they are given and its limitations.
- d. The patterns and behavior of employees as a whole.

Explanation

Answer A: The architecture element is the design of the organizations security plan and the technology selected to implement it correctly. Everything should be with intention

7. Which of the following frameworks focuses on process improvement?
- a. Sherwood Applied Business Security Architecture (SABSA)
 - b. Zachman Architecture Framework
 - c. The Open Group Architectural Forum (TOGAF)
 - d. Capability Maturity Model Integratio (CMMI)**

Explanation

Answer D: CMMI is focused on process improvement where SABSA and TOGAF are both used to developing security architectures. Zachman allows requirements to be uncovered by providing a way to develop a complex idea.

8. The ability to describe complex ideas using a set of primitive interrogatives; who, what, when, where, why and how is the foundation of which architectural framework?
- a. Sherwood Applied Business Security Architecture (SABSA)
 - b. Capability Maturity Model Integration (CMMI)
 - c. Zachman Architectural Framework**
 - d. The Open Group Architectural Forum (TOGAF)

Explanation

Answer C: Zachman allows requirements to be uncovered by providing a way to develop a complex idea. CMMI is focused on process improvement where SABSA and TOGAF are both used to developing security architects.

9. ISO-27002 was originally:
- a. ISO 9000

- b. **ISO 17799**
- c. ISO 9001
- d. BS 27002

Explanation

Answer B: ISO 27002 was previously ISO 17799 and was sourced from BS 7799. There is no BS 27002. ISO 9000/9001 is TQM specific, a different topic.

10. What are the three types of security controls?

- a. Physical, logical/technical, practical
- b. Physical, practical, procedural
- c. Logical/technical, administrative, managerial
- d. **Physical, technical/logical & administrative/procedural**

Explanation

Answer D: Practical and Managerial are not types of security controls. They better describe activities.

11. Controls designed to return a non-functioning system to a normal status are called:

- a. **Corrective**
- b. Directive
- c. Preventive
- d. Detective

Explanation

Answer A: Corrective controls return us to a normal condition. Directive controls have a specific consequence. Preventive controls try to stop bad things from ever happening and detective controls tell us when it happens.

12. An intrusion prevention system is an example of what type of control?

- a. Countermeasure
- b. Directive

- c. **Safeguard**
- d. Physical

Explanation

Answer C: An IPS tries to protect us from an attack ever reaching us thereby safeguarding. A countermeasure assists after the threat is realized. Directive controls have a specific consequence, which an IPS does not have. Physical controls are more like locks are dogs.

13. Security metrics designed to identify those things an organization intends to accomplish are known as:
- a. Key Performance Indicators (KPI)
 - b. Positive Feedback Ratio (PFR)
 - c. Maximum Tolerable Downtime (MTD)
 - d. Key Goal Indicators (KGI)**

Explanation

Answer D: KGIs are our goals, KPIs show progress toward goals, MTD is the maximum time we can be without our business and PFR is not real.

14. Security metrics designed to measure progress towards meeting an identified goal are known as:
- a. Maximum Tolerable Downtime (MTD)
 - b. Key Performance Indicators (KPI)**
 - c. Key Goal Indicator (KGI)
 - d. Job Task Analysis (JTA)

Explanation

Answer B: KPI shows our progress towards our goals, KGI is the goal, MTD is maximum time we can be without our service, JTA is an analysis of the tasks that must be performed within a job.

15. The most important role the CEO has to fulfill on within their business is
- a. Approving and supporting policies and supporting documents**
 - b. Putting on a good show of support for the security department

- c. Ensuring that all security professionals are performing all of the tasks in their job descriptions
- d. Approving all security device purchases

Explanation

Answer A: The CEO must approve and support policies as they show senior management's goals and objectives. Approving purchases and ensuring tasks are performed is detailed work that is best performed at lower levels of business. Supporting the security department is good, but all security activities are sourced from policy.

16. Critical Success Factors (CSF) defines:

- a. A lagging indicator of those items that are successfully measured
- b. A leading indicator of those items that are successfully identified
- c. Those actions that "must happen" for an organization to be able to reach the defined goal(s).**
- d. A dashboard of key Performance Indicators (KPI's) and Key Goal Indicators (KGI's)

Explanation

Answer C: Critical success factors are just that. Critical. They MUST happen to be able to say you have been successful. They are not lagging or leading indicators they are the moment of success. It is not a dashboard of KPIs or KGIs it is the point of success.

17. The goal of security _____ is to "focus attention on an issue or set of issues".

- a. Training
- b. Nagging
- c. Education
- d. Awareness**

Explanation

Answer D: Awareness focuses attention, training is classroom-based skill set based and education is classroom-based knowledge. Nagging is never useful.

18. Privacy regulations are primarily focused on

a. Identity theft

b. Personally identifiable information

c. Protecting financial information from fraud

d. Protecting health information

Explanation

Answer B: Privacy regulations are primarily focused on personally identifiable information, some focus more specifically on health information. They do not focus on fraud or identity theft.

19. A tool designed to produce relevant and needed security skills is called:

a. Security Training

b. Security Awareness

c. Education

d. Key Performance Indicator (KPI)

Explanation

Answer A: Training provides and enhances skills; awareness only focuses attention and education is knowledge based. KPIs are metrics used to measure progress.

20. Imparting knowledge is the fundamental goal of:

a. Awareness

b. Unilateralism

c. Training

d. Education

Explanation

Answer D: Education is all about knowledge. Awareness focuses attention. Training is skill set based. Unilateralism is just a ridiculous

answer.

21. Information security frameworks are designed to provide

- a. a control list
- b. detailed instructions
- c. guidance**
- d. absolute rules

Explanation

Answer C: A framework is for guidance to guide decision makers through control selection. It is not the absolute rules or detailed instructions although the framework can help define those if they are needed at some point.

22. The most effective way for a company to ensure that employees will follow the corporate password policy is

- a. penalties for non-compliance
- b. periodic password audits
- c. awareness training**
- d. a Kerberos single sign on system

Explanation

Answer C: User are most likely to comply with policies if properly made aware and trained. Penalties are usually not a good motivator for compliance with policies. Password audits only tell you that people are in compliance or not and a single sign on system mean one password, not that the user will comply with the password policy.

23. When creating an information security plan, it would be best to make sure that you have included

- a. Current and desired future state**
- b. Budget
- c. Job descriptions
- d. Corporate mission statements

Explanation

Answer A: The plan should provide information on the desired future state allowing a road map to be created to get from where the

business is to that desired state. That will allow for security job descriptions to be defined and for the budget to be created. The Corporate mission statement should have been considered and built into the security mission statement.

24. If a quarterly report is being written for delivery to executive management, it is important that you consider the following element

a. Executive managements intelligence level

b. Information security metrics

c. Establish connections to business objectives

d. Metric to baseline links

Explanation

Answer B: Security metrics are specific and measurable giving management detailed information that they can work with. The intelligence is not the concern when writing a report. It is also not the main concern to connect elements of the report to business objectives or baselines. Those connections come later.

25. Which of the following characteristics is most important for a Chief Information Security Officer to have?

a. Ability to map business needs to security technology solutions

b. Ability to understand all laws potentially applicable to the business

c. Ability to comprehend the cost of not understanding the business needs

d. Ability to map technologies to security tools

Explanation

Answer A: CIOs need to be able at a level of executive management to be able to connect business needs to security solutions. Understanding the laws is useful as well as mapping technology to tools. It would be good to also comprehend the cost of not being able to understand business needs, but we need the CIO to understand and connect those needs to security solutions.

26. The responsibility for legal and regulatory liabilities falls upon the
- a. board and senior management.
 - b. chief counsel.
 - c. chief risk officer.
 - d. **senior security manager.**

Explanation

Answer A: Senior management and the board of directors are ultimately responsible for all that happens within a business.

27. When looking at an information security standard the MOST important field to analyze would be the
- a. initial approval date
 - b. Author name
 - c. **Last review date**
 - d. Creation date

Explanation

Answer C: When and who created the standard is not near as interesting or important as the last review date to ensure that the standard that you are looking at is still current.

28. If a security manager is working for an international company that is governed by different laws in different jurisdictions it is best to
- a. establish standards that meet the minimum level of conformance with ALL jurisdictions
 - b. **develop minimum required standards with supplemental standards as needed**
 - c. ensure that all locations are in conformance with the laws of ALL jurisdictions
 - d. select the law of one jurisdiction to follow

Explanation

Answer B: Deciding to use the lowest common set of compliance or selecting one law could cause audit failures. Forcing everyone to follow all laws may be too costly. Setting a minimum for all with

additional standards for each location based on local laws give the best chance for every site to be in regulatory compliance.

29. Clearly defined roles and responsibilities provides the immediate benefit for the information security manager of

- a. Separation of duties
- b. Policy compliance
- c. Proper audits
- d. **Accountability**

Explanation

Answer D: If people have a clear understanding of their roles and responsibilities then it is possible to figure out if someone is doing what they should or not and therefore they can be held accountable.

chapter 2

domain 2

Information risk management and compliance

30% of the Exam

According to ISACA, in this domain, you will:

Manage information risk to an acceptable level to meet the business and compliance requirements of the organization.

A CISM candidate must be able to perform the following nine task statements:

- 2.1, Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.
- 2.2, Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.
- 2.3, Ensure that risk assessments, vulnerability assessments and threat analyses are conducted consistently, at appropriate times, and to identify and assess risk to the organization's information.
- 2.4, Identify, recommend or implement appropriate risk treatment/response options to manage risk to acceptable levels based on organizational risk appetite.
- 2.5, Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.
- 2.6, Facilitate the integration of information risk management into business and IT processes (e.g., systems development, procurement, project management) to enable a consistent and comprehensive information risk management program across the organization.
- 2.7, Monitor for internal and external factors (e.g., key risk indicators [KRIs], threat landscape, geopolitical, regulatory change) that may require reassessment of risk to ensure that changes to

existing, or new, risk scenarios are identified and managed appropriately.

2.8, Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.

2.9, Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives.

A solid understanding of the following 19 knowledge statements should be attained by a CISM candidate:

k2.1, Knowledge of methods to establish an information asset classification model consistent with business objectives.

k2.2, Knowledge of considerations for assigning ownership of information assets and risk.

k2.3, Knowledge of methods to identify and evaluate the impact of internal or external events on information assets and the business.

k2.4, Knowledge of methods used to monitor internal or external risk factors.

k2.5, Knowledge of information asset valuation methodologies.

k2.6, Knowledge of legal, regulatory, organizational and other requirements related to information security.

k2.7, Knowledge of reputable, reliable and timely sources of information regarding emerging information security threats and vulnerabilities.

k2.8, Knowledge of events that may require risk reassessments and changes to information security program elements.

k2.9, Knowledge of information threats, vulnerabilities and exposures and their evolving nature.

k2.10, Knowledge of risk assessment and analysis methodologies.

k2.11, Knowledge of methods used to prioritize risk scenarios and risk treatment/response options.

k2.12, Knowledge of risk reporting requirements (e.g., frequency, audience, content).

k2.13, Knowledge of risk treatment/response options (avoid, mitigate, accept or transfer) and methods to apply them.

- k2.14, Knowledge of control baselines and standards and their relationships to risk assessments.
- k2.15, Knowledge of information security controls and the methods to analyze their effectiveness.
- k2.16, Knowledge of gap analysis techniques as related to information security.
- k2.17, Knowledge of techniques for integrating information security risk management into business and IT processes.
- k2.18, Knowledge of compliance reporting requirements and processes.
- k2.19, Knowledge of cost/benefit analysis to assess risk treatment options.

Overview

Risk management is a business process designed to identify and evaluate potential risks to business activities and to implement strategies to reduce those risks to a manageable level. When done properly, risk management should identify organizational assets, the weaknesses those assets possess as well as the many things that could cause harm to the assets. Further, risk management should attempt to forecast the chances that a risk will be realized as well as the resulting harm that will arise as a result of that risk. Finally, based upon the information learned, risk management activities should provide tools for the organization to employ to address the identified risks; to reduce or transfer the risks to an acceptable level. The level of acceptable risk is based upon the organization's tolerance or appetite for risk. Therefore, risk management should also provide a means for the organization to identify what their risk appetite is.

Simply stated, it is good business practice for an organization to put a risk management program in place to formally tackle the challenges of identifying and handling risks in all facets of the business on an ongoing basis. Organizations that fail to develop and implement risk management programs are inviting trouble upon themselves including simple outages, disasters and even complete failure. If the argument that risk management is simply good business practice does not convince you then maybe the fact that many laws and regulations require organizations to engage in risk

management activities will. Failure to do so could result in hefty fines and penalties.

Management of corporate risk, including risk to information, requires the organization to determine what the acceptable levels of risk are that will meet the business and compliance requirements of the organization.

Risk assessments should be conducted at various organizational levels. The executive management team and the board of directors should conduct top-down assessments to get a holistic perspective on the corporate risk while individual business units should conduct bottom-up assessments to gain a more granular understanding of the specific risk environment those business units operate within. Additionally, there are many different types of assessments that should work together as part of an Enterprise Risk Management (ERM) program. These include financial risk assessments, Information Technology (IT) risk assessments, strategic risk assessments, compliance risk assessments and operational risk assessments to name a few.

Risk Management Process

Most business operations are ongoing functions of the business. They happen day in and day out on a continuing basis, risk management is one of those functions. RM is an ongoing cyclic process that follows the traditional Plan-Do-Check-Act (PDCA) model. The specific steps of risk management

can be broken down into four basic elements; Identify-Assess-Mitigate-



Monitor

Diagram 8
Risk Management Process

Types of Risk Assessments

Several different type of risk assessments may be conducted by an enterprise including strategic, operational, compliance, security, IT risk and others.

- Strategic - a strategic risk assessment is looking at the big picture asking questions such as ‘what can impact the mission or strategic objectives?.’
- Operational - Operational risk assessments are more focused on those things they could result in an operational impact. Those things that could interfere with the organizations ability to deliver the products, goods and services to its customers and users. This assessment identifies risks that exist because of poor processes, poorly trained or insufficient people, faulty systems, etc.?
- Compliance - Do we know the laws & regulations, policies and procedures, contractual obligations, etc. and are we meeting the requirements? What risk exists if we fail here?
- Security - What impact would an actual breach have?
- IT risk - What happens when IT systems fail? What if the IT systems are not kept current?

- Others - Financial risk, fraud risk, market risk, credit risk, customer risk, supply chain risk, product risk, others

Integrating Risk Management

Too many times, risk management is perceived to be one of life's "necessary evils." As such it is seen only as a red line on the organizational budget and something that we are compelled to do by laws and regulations rather than a task of any real value. Additionally, the controls that are put in place because of the information learned during the risk assessment are seen as stumbling blocks that serve only to hinder productivity. Therefore, risk management activities are often placed in the periphery of the business only to be looked at when forced to by the laws and regulations.

Risk management should not be a silo program separated from other business functions. Rather, risk management functions should be integrated into all facets of the business (processes, business units, daily decision making) and supported by all members at every level. Integrating risk management activities into the entire organization requires a change in the culture of the organization. Risk management should be woven into the corporate fabric rather than an afterthought.

Risks should be documented and mapped to organizational business objectives.

Risk Management Roles & Responsibilities

Many of the roles and responsibilities pertaining to security have been discussed and defined previously in chapter one. In this section we will take a more focused look at specific roles and responsibilities as they pertain directly to enterprise risk management. A list of some of the various organizational roles follows. It is important to note that these terms are generic in nature and the actual terminology used by your organization may vary.

- Board of Directors - A part of the governance that the board of directors needs to provide is to assign ownership of risk to the

appropriate stakeholders within the organization and hold those stakeholders accountable for the decisions they make.

- Chief Executive Officer - The CEO must actively incorporate risk management into that decision making process.
- Chief Risk Officer - Some organizations wrestle with the question of 'should there be one individual or a group of people responsible for managing the risk of the organization.' When one person is responsible, he or she is often given the title of Chief Risk Officer. When several people share the load, they are referred to as a risk committee. No matter the choice, this role owns the risk management process. This person or committee needs to ensure that risk management strategies align to business strategies. The CRO must also effectively communicate risks to senior executives, the board of directors and other stakeholders.
- Chief Information Officer - Good lines of communication between the CRO and the CIO are imperative to ensure security decisions are made based upon the organizations risk management strategies.
- Information Security Manager - They play a key role in the identification, analysis and mitigation of risks that could impact the organizations mission. (The entire CISM certification focuses on the duties of the ISM.)
- Owners - Proper risk-based decisions must be made when modifying the operating environment in order to ensure the necessary controls are in place to protect the confidentiality, integrity and availability of the information or systems they own.
- Others - A host of other job roles may be defined by the organization based upon specific needs. Examples might include business unit and functional managers, security practitioners, and trainers. Security responsibilities should be assigned based upon organizational policy and operational needs.

Risk Management Terminology

An information security manager will use the following terminology every day during the course of executing his duties. A keen understanding of these terms is imperative for the purposes of doing the job as well as

passing the CISM examination. While most security managers are already familiar with these concepts, it is useful to cover them for the sake of clarity and uniformity. We will utilize these terms as we go through this chapter.

- Asset - Something that is owned by the organization and has value. Something that can be converted into cash. Assets could be tangible or intangible:
 - Tangible assets have an easy to identify real or actual value. For example, it is easy to calculate the cost of a server.
 - Intangible assets are not as clear or defined and the value may be difficult to identify because intangible value is usually connected to something else. For example, a formula used to create a product may have an actual tangible value (in this example based upon the cost to create the formula) of say \$5000. However, that formula is the foundation for our business and the intangible value may be exponentially greater than the tangible.
- Threat - Anything that has the potential to cause harm.
- Vulnerability - An exploitable weakness or a flaw.
 - Threats and vulnerabilities must relate to an asset. If there are threats without vulnerabilities to take advantage of or vulnerabilities without threats to exploit them or if the threats and vulnerabilities are not associated with an asset, then there is no risk. For example: When General Motors issues a recall on its Suburban and Tahoe vehicles due to a defect in the EPS module, that is NOT a risk to me because I do not own either of those assets.
- Likelihood -The probability or chance of something to happen. In this case, the probability that a threat will exercise a vulnerability. The frequency of a threat occurring.
- Risk -The chance that a threat can exploit a vulnerability and the resulting impact that has to the asset.
 - $\text{Threats} \times \text{Vulnerabilities} \times \text{Asset Value} = \text{Total Risk}$

- Risk - Control = Residual Risk
- Severity - The intensity of the pain that will be experienced as a result of the vulnerability.
- Impact - The probable magnitude of the loss or the resulting effect, positive or negative, of a vulnerability being exploited by a particular threat, usually thought to be negative.
- Exposure - The portion of the asset open to attack or damage from the threat.
- Exploit - The act of making use of, to take advantage of. Threats exploit vulnerabilities.
- Control - Something designed to regulate or constrain; actions to modify risk. Controls break into two categories: safeguards and countermeasures.
 - Safeguard - To guard or protect from harm. A type of control that is proactive in nature designed to address the risk before it happens. (preventative)
 - Countermeasure - Actions to oppose, neutralize or offset a threat. A type of control that is reactive in nature designed to effectively mitigate or negate the ability to exercise a vulnerability. (corrective)
- Critical
- Sensitive information



Risk Management Processes / Frameworks

Risk Management processes are never ending cyclic processes. As with most ongoing processes within a company, risk management follows the PDCA model. PDCA is also known as the Deming cycle or wheel and it was developed in the 1950's by Dr. W. Edwards Deming as a method for continuous improvement of business processes.

Plan-Do-Check-Act has been used as the cornerstone building block for many modern process improvement strategies such as Total Quality Management (TQM), Six Sigma and others. The International Organization for Standardization has utilized or adapted PDCA for several of its international standards including ISO 27001. PDCA provides the structure for all Information Security Management System (ISMS) processes. ISO 27000 takes inputs in the form of business requirements and expectations, feeds them through the PDCA cycle and produces managed information security as the output.

- Plan (Establish an ISMS) - Establish ISMS policy, objectives, processes, and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
- Do (Implement and operate an ISMS) - Implement and operate the ISMS policy, controls, processes, and procedures.
- Check (Review and monitor the ISMS) - Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
- Act (Maintain and improve the ISMS) - Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

~From ISO 27001:2005

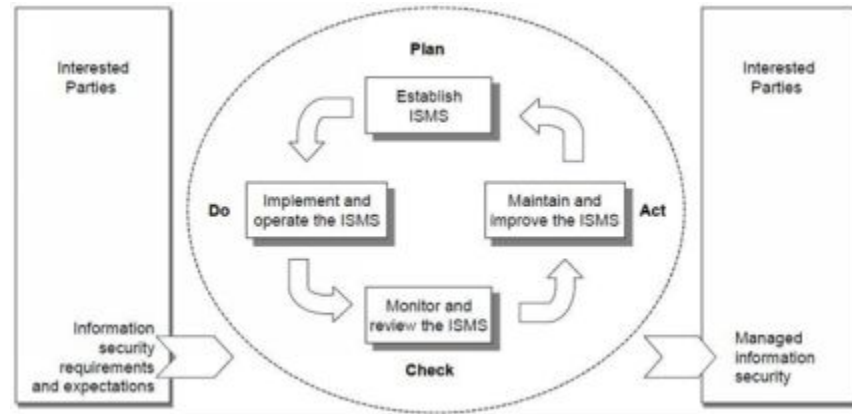


Diagram 9
Plan Do Check Act Cycle from ISO 27001

Risk Assessment / Analysis Tools

There is a smorgasbord of frameworks available to help organizations conduct risk assessments and implement a risk management program. Many of these frameworks provide the same suggestions; they just differ in their specific approach. Oftentimes companies treat these frameworks like a buffet style meal. They will find elements from one framework that they like and work well in the organization and elements from other frameworks that work well so they produce custom solutions that make use of the good pieces from each framework and leave the not so useful pieces behind.

The following frameworks will be discussed:

- COBIT 2019
- Risk IT
- NIST SP 800-30
- ISO 31000

- ANZ 4360
- ISO 27005
- Others

Frameworks: COBIT 2019

As discussed in chapter one, COBIT 2019 has matured into a framework of frameworks including the Value IT (Val IT), Risk IT and COBIT 4.1 frameworks for developing, implementing, monitoring & improving information technology governance and management practices. A portion of COBIT 2019 controls focus specifically on the management of IT risks.

The COBIT 2019 processes are divided into five categories. Each category has three or more processes. Those categories are:

- Evaluate, Direct and Monitor
- Align, Plan and Organize
- Build, Acquire and Implement
- Deliver, Service and Support
- Monitor, Evaluate and Assess

A few control examples focusing on risk are EDM03 - Ensure Risk Optimization and APO12 - Manage Risk

- EDM03 titled Ensure Risk Optimization's stated purpose is to "Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimized."
- APO12 titled Manage Risk is designed to "Integrate the management of IT-related enterprise risk with overall ERM and balance the costs and benefits of managing IT-related enterprise risk."

Frameworks: Risk IT

Also defined by ISACA, Risk IT is a framework for enterprises to identify, govern and manage IT risks. The Risk IT framework is fully covered within the COBIT framework but can be pulled out and used as a stand-alone piece.

The Risk IT principles are:

- Always connect to business objectives.
- Aligns the management of IT-related business risk to overall enterprise risk management (ERM).
- Balances the costs and benefits of managing IT risk.
- Promotes fair and open communication of IT risk.
- Establishes the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels.
- Is a continuous process and part of daily activities.

Frameworks: NIST SP 800-30

The Risk Management Guide for Information Technology Systems states that “the objective of performing risk management is to enable the organization to accomplish its mission(s)

1. by better securing the IT systems that store, process, or transmit organizational information;
2. by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and
3. by assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.”

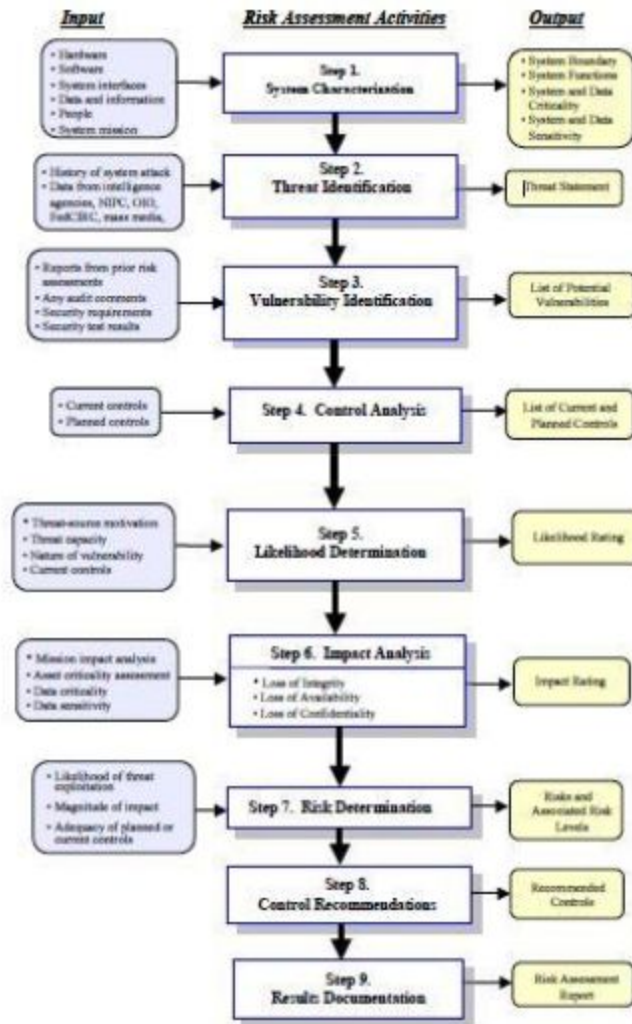


Diagram 10
NIST SP 800-30

To achieve these objectives, NIST has broken the risk management process into the following 9 steps. (Duplicate chart from SP 800-30, page 9)

1. **System characterization** - System characterization involves defining the scope of the system. During this step, the information security manager will identify what resources are required for the system to function including hardware, software, interfaces, personnel, data, etc. Additionally, this step will define what does the system do for the organization; what does it contribute to the

mission and is it or any part of it sensitive or critical to that mission.

2. Threat identification - Discovering the potential for a threat source to successfully exercise a particular vulnerability. During this step, the security manager will identify all of the potential threat sources that are applicable to the IT system.
3. Vulnerability identification - Develop a list of system vulnerabilities (flaws or weaknesses) that can be exploited by a potential threat source.

Threats without a vulnerability to exercise or vulnerabilities without a threat to take advantage of them do NOT pose any risk.

4. Control analysis - Control analysis is the process of determining what controls are currently in place or planned that can minimize or eliminate the likelihood of a threat exercising vulnerability against this system? These controls could be either technical or non-technical. Technical controls are in the form of hardware or software while the non-technical controls are management or operational such as policies and procedures.

Threat identification, vulnerability identification and controls analysis steps can be conducted in parallel with one another.

5. Likelihood determination - What are the chances that a particular identified threat will exercise a particular identified vulnerability? Some of the factors that will affect the likelihood of an attack are the motivation and capability of the threat source, the nature of the vulnerability and the existence and effectiveness of current controls. From this step a likelihood rating of high, medium, or low will result.
6. Impact analysis - What will be the effect of a threat source successfully exercising vulnerability? The information security manager must consider the following:
 7. How does this system contribute to the organizational mission?
 8. Is this system or the data contained within critical to the mission?
 9. Does the system contain any sensitive data?
 10. If the system or data are compromised, how are the core tenets of security affected?
 11. Measured as high, medium, and low as well.
12. Risk determination - Risk determination is a combination of all the above. During this step, a risk level matrix combining the high, medium, low values of likelihood and impact are created providing a picture of what risks are the most severe and which are less harmful.
13. Control recommendations - At this point, the organization should have a good picture of what controls are sufficient and where there are deficiencies. This step makes recommendations for controls to eliminate or reduce the identified risk. Some factors to consider are:
 14. How effective are the current controls and what additional value changing the controls will provide?
 15. What are the legal/regulatory requirements?
 16. Organization policy
 17. What effects will the new controls have on operations and usability?
 18. Are there any safety & reliability concerns?

19. Results documentation - The final step and possibly the most important one is to document the results of the assessment. Create an official report documenting the corporate assets, the vulnerabilities those assets possess as well as the threat-sources that could exercise the vulnerabilities. Additionally, document the controls that are recommended to protect the assets. This is a step that often gets overlooked. The unfortunate part about that is that “if it is not documented, it never happened.”

Frameworks: ISO 31000

ISO 31000:2018 - Risk management – Principles and guidelines provides principles, framework, and a process for managing risk. It can be used by any organization regardless of its size, activity, or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment. However, ISO 31000 cannot be used for certification purposes, but does provide guidance for internal or external audit programs. Organizations using it can compare their risk management practices with an internationally recognized benchmark, providing sound principles for effective management and corporate governance.

ISO 31010 compliments ISO 31000 by focusing on the risk assessment aspect of ERM.

Frameworks: ISO 27005

The International Organization for Standardization has dedicated an entire numbered series to information security. As discussed previously, ISO 27002 is a guidance document that sits at the 30,000-foot level while ISO 27001 is more of a checklist for certification. There needs to be a middle ground. That is where many of the other ISO 2700X documents fit in. ISO 27005 provides a guidance for conducting Information Security Risk Management (ISRM) within the scope of an Information Security Management System (ISMS).

The risk management process can be an iterative process of assessing and handling risk. This iterative approach allows organization to go as deep as they want to to provide a good balance to ensure risks are appropriately addressed without spending too much time and money to get there.

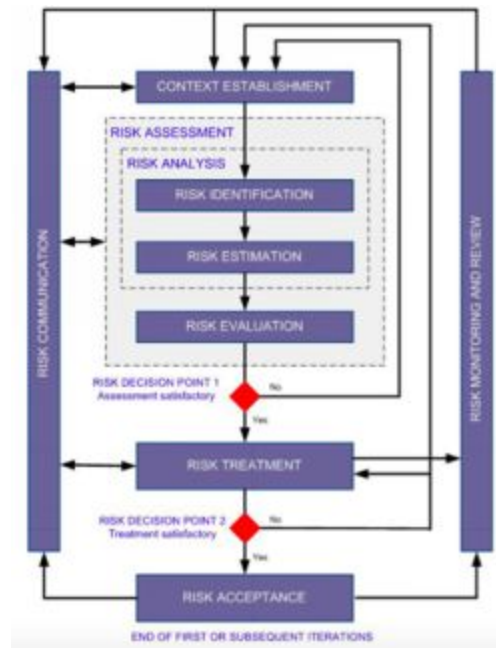


Diagram 11
ISO 27005 Risk Management Process

FAIR - Factor Analysis of Information Risk

One common problem we face when trying to address risk is that there are many different interpretations and understanding of what risk is and what the factors are that contribute to risk as well as how those factors relate to each other. Another issue is that there are many different approaches to conducting risk assessments, which in and of itself is not bad however these differing approaches may serve to compound the issue of loosely understanding the factors of risk. Finally, communicating risk to decision makers and providing a useful analysis of the risk, as a basis to form their decision is often a large challenge.

Factor Analysis of Information Risk (FAIR) has been created to help address some of these concerns. FAIR was not designed to compete with or replace other risk assessment frameworks, rather it is a tool designed to

complement those other frameworks. The Open Group discusses the use of the FAIR approach to risk as a complementary tool for the OCTAVE framework in its Risk Taxonomy Technical Standard. Additionally FAIR is utilized within ISACA's Risk IT framework.

Often, risk is discussed in qualitative terms where numerous assumptions are made. FAIR seeks to provide a framework for conducting a more quantitative analysis of the risk. (Qualitative vs quantitative risk assessment is discussed later in this study guide.) Additional information can be found at http://www.riskmanagementinsight.com/media/docs/FAIR_brag.pdf.

10 Steps broken into 4 stages:

Stage 1- Identify Scenario components

Stage 2 - Evaluate Loss Event Frequency (LEF)

Stage 3 - Evaluate Probable Loss Magnitude (PLM)

Stage 4 - Derive & Articulate Risk



Diagram 12

FAIR

~From

http://www.riskmanagementinsight.com/media/docs/FAIR_brag.pdf

RFA - Risk Factor Analysis

Other risk assessment tools exist that are not particular to information risk. One such tool is Risk Factor Analysis (RFA). Developed at Los Alamos National Laboratories, RFA is a systematic qualitative risk analysis technique for estimating project risk. While this framework was developed in a specific environment, the concepts could be used in other environments.

RFA divides risk factors into 4 risk categories. They are:

1. Budgetary - Factors that affect funding. Not having the capital at the right time to conduct the task. This could cause scheduling issues as well as technical and cost issues.
2. Schedule - Deals with those factors that affect the delivery of the project.
3. Technical - Those factors that could affect the actual performance versus the performance that was defined in the project requirements document.
4. Cost - Those factors that could impact the life cycle costs of the project. They include design/construction costs as well as operational costs.

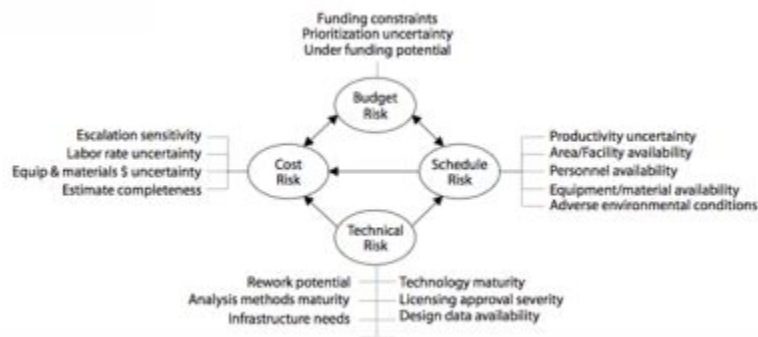


Diagram 13

RFA 1

~From <https://www.lanl.gov/orgs/d/d5/documents/risk-fact.pdf>

Risk Factor	Risk Category		
	Non/Low (0/1)	Medium (2)	High (3)
Technology Maturity	Facilities & equipment involve only proven technology or new technology for a non-critical activity.	Facilities or equipment require the adaptation of new technology from other applications to critical construction or operating functions for this project.	Facilities & equipment require the development of new technology for critical construction or operating functions for this project.
Productivity Uncertainty	The planned rate of progress needed to reach completion as planned is conservative and well within benchmarks observed for similar tasks.	The planned rate of progress needed to reach completion as planned is aggressive but still within benchmarks observed for similar tasks.	The planned rate of progress needed to reach completion as planned is extremely aggressive or no benchmark experience is available to judge the reasonableness of the planned progress rate.
Equipment/ Material Cost Uncertainty	Equipment/Material costs are well established and regulated by contracts or competitive market forces.	Equipment/Material costs are not well established but should be regulated by competitive market forces.	Equipment/ Material costs are not well established and not subject to competitive market forces.

Diagram 14
RFA 2

~From <https://www.lanl.gov/orgs/d/d5/documents/risk-fact.pdf>

Risk Assessment Methodologies

In the previous section we discussed several specific risk assessment frameworks. Each of those frameworks will take either a qualitative approach to assessing risk or it will take a quantitative approach. In some instances, a hybrid assessment is conducted. In this section, we will discuss the strengths and weaknesses of qualitative and quantitative.

Qualitative risk assessments are based upon descriptive scenarios and the output is in the form of an opinion based upon assumptions made during the scenario. Because of these assumptions, the qualitative assessment is inaccurate and very subjective. However, the major benefit to qualitative assessments is their ease of use. It takes very little time and effort to conduct a qualitative assessment.

Quantitative assessments are based upon numbers and data that can be measured. Numeric values are more precise and can be measured making quantitative assessments objective. The objective nature makes this assessment more reliable as it is based upon facts / numbers. Numbers are difficult to dispute. The problem with numbers is that they are hard to come by. It may take considerable amount of time and effort to quantify a particular value.

With quantitative assessments, the numbers are often based upon money such as the dollar amount one spends to purchase a vehicle. Other factors are not monetary in nature but can often be linked back to a dollar value. For example, how many times a year is a system likely to fail? This numeric value will be the number of instances, not the amount of money. However, we can calculate how much money it cost each time the system fails.

There is a tradeoff for this level of accuracy; it takes a considerable amount more time and skill to conduct quantitative assessments.

Quantitative assessments are based upon numerical values. These numbers should represent the loss in financial terms such as Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE).

SLE is the product of the Asset Value (AV) multiplied by the exposure factor (EF): $SLE = AV \times EF$. Exposure factor represents the magnitude of the loss. In simple terms when something bad happens a portion of the asset will be affected. That portion is represented by the exposure factor. Example: If a fire starts in a home that has four equal size rooms and the fire damages only one room, the exposure factor is 25%.

As the name implies, single loss expectancy is looking at a one-time event and the harm that results from that event. However, it is likely that an event will occur more than one time. Therefore, annualized loss expectancy seeks to quantify the loss from multiple occurrences of the same type of event. Annualized Loss Expectancy is the product of the Annual Rate of Occurrence (ARO) multiplied by SLE: $ALE = ARO \times SLE$. The ARO is the number of times a given event might happen in a 1-year time frame. Once the ALE is known, the decision makers can use this value as a reference for making risk-based decisions.

For example: Statistics indicate that Illinois will have 5 severe snowstorms each year between November and April. The ARO then is 5.

For example: statistics reveal that there have been 8 earthquakes in a 13-year period which gives us an ARO of .67 (slightly less than 1 a year)

Do not spend more on protecting the asset than it is worth.

In most situations we are not left with an “either / or” choice for conducting a risk assessment. Usually, organizations will choose the method based upon the situation at hand. For example, if emergency services are dispatched to the scene of a vehicle accident, initially all that is known is that car accidents have the potential to be “very bad;” a qualitative assessment is done. Again, qualitative assessments are fast and easy. If we have more time, we may be able to gain more facts (numbers) about the situation. For example, there are 3 cars involved in the accident and the accident occurred on a major interstate. (Now we know that interstate highway speeds are north of 55 MPH.) What is happening now is that the assessment is evolving into a hybrid assessment.

Hybrid assessments combine qualitative and quantitative assessment methodologies. Additionally, within these methodologies there are several “techniques” that can be employed such as Fault Tree Analysis and Failure Mode and Effect Analysis.

Fault Tree Analysis (FTA) is looking at the combinations of factors could come together to cause a failure and what would be the resulting impact of the failure? Using basic Boolean logic, “AND’s” and “OR’s” are used to evolve the scenario. In the above scenario about the car accident, we began to utilize this technique when we said that it was a three-car accident AND that the accident occurred on the interstate.

Failure Mode & Effect Analysis (FMEA) is a technique that divides a system into subsystems then further divides the subsystems into components. Then we ask, ‘if a particular component of a subsystem fails, what effect does it have on the subsystem and ultimately on the system?’ A good example is an automobile. Cars are comprised of several subsystems that all must work together for the car to do its job. One of the subsystems of the car is the electrical subsystem. What would happen if a taillight were to fail? This would have a minimal impact on the electrical subsystem and minimal impact on the cars ability to perform. We may receive a ticket for faulty equipment if we are spotted by a police officer, but the car still runs. On the other hand, if the battery were to fail, this has a major impact as the car will not start and thus the car cannot do what it is designed to do. At this point, there are many assumptions being made with respect to the above scenario (qualitative). If we were to include a little fault tree analysis, we could say that the battery failed, but the car has a manual transmission so we could possibly push the car and pop the clutch to start it. Problem solved. In this more evolved scenario, the failed battery is not as big a problem.

So, a hybrid risk assessment incorporates several methodologies and techniques to identify risks and to evaluate the severity of those risks. We can represent the risk with a visualization by creating a chart to assign probability and impact.

As discussed, risk is a value derived from the probability of a threat exercising a vulnerability and the impact this will have on the asset. Sample likelihood ratings might be unlikely, likely, and certain while sample impact ratings might be minimal, moderate, and severe. If more granularity is desired, the chart below could be used. No matter the choice about how

many levels of likelihood and impact the company chooses, the results would be a meaningful indicator of risk.

Based on the information learned, the organization can begin to prioritize the risks. Prioritization is required to ensure that corporate resources are utilized to maximum efficiency.

		Business impact				
		Extreme	Major	Moderate	Minor	Insignificant
		Complete operational failure, "out of the park" impact, unacceptable	Severe loss of operational capability, highly damaging and extremely costly but survivable	Substantial operational impact, very costly	Noticeable but limited operational impact, some costly	Minimal if any operational impact, negligible costs
		100%	80%	60%	20%	5%
Probability	(Almost) certain We are bound to experience further incidents of this nature – in fact they are probably occurring right now!	100%	80%	60%	25%	10%
	Probable We are likely to experience incidents of this nature before long	80%	64%	50%	20%	10%
	Possible It is distinctly possible that we will experience incidents of this nature	60%	50%	38%	16%	10%
	Unlikely Incidents of this nature are uncommon but there is a genuine chance that we may experience them at some future point	25%	20%	16%	6%	10%
	Rare Although they are conceivable, we will probably never experience incidents of this nature	5%	10%	10%	6%	10%

Note: the colors are generated automatically using Excel's conditional formatting. The values assigned to each category are arbitrary so don't obsess about them; concentrate the need to mitigate those unacceptable risk/reward ratios.

Diagram 15
Risk Assessment

~ From www.iso27001security.com/ISO27k_Risk_Register_v2.xlsm

Risk Handling

Once risk has been identified and the severity has been evaluated, the organization must decide about how to handle the risks. There are four choices available to address identified risks.

- Risk Acceptance occurs when the owner is aware of the risk has decided to bear the full burden if the event were to occur.
- Risk Mitigation involves activities designed to reduce the risk to an acceptable level.
- Risk Transference/Risk Sharing involves a third party or parties choosing to absorb some of the risk. Transferring risk may be through the purchase of insurance or through a waiver process. (Example: Companies that run dangerous sporting activities like scuba diving will require their customers to sign a waiver

accepting the risk of doing the activity. This waiver transfers the risk from the company to the client.)

- Risk Avoidance - When risk cannot be adjusted to an acceptable level through a combination of mitigation and transference, then only one choice remains: Risk Avoidance. Avoiding risk is choosing NOT to engage in the activity.

Risk cannot be transferred to an unwilling participant. The third party MUST be willing to accept that portion of risk that is being transferred.

Hopefully, through a combination of transference and mitigation, the risk can be brought to an acceptable level. If not, the organization has no other recourse than to avoid the risk.

One other risk handling option is sometimes mentioned; ignore risk. However, ignoring risk is not a good idea. It is ultimately accepting the risk without proper knowledge or understanding. It is the “head in the sand approach” and it should be avoided.

Reporting risk

When risks are identified, there may be requirements to report those risks to various principals and stakeholders. These requirements for reporting and communicating risk are based upon business drivers, local policy, laws & regulations. Factors to be considered include:

- Who to report to
- How often to report
- What information must be shared
- How to safeguard the reports

Even the reporting of risk itself involves risk. In essence, we may be required to share information about organizational threats and vulnerabilities as well as the risk handling activities or lack thereof. This information in the wrong hands can be very dangerous therefore controls need to be put in place to protect the organization from unauthorized disclosure.

Monitoring Risk

“The only constant in life is change” - Unknown.

When an organization conducts a risk assessment one time, the organization is said to be exercising “due care.” However, the environment around us is in constant change. New vulnerabilities are discovered every day. New threat sources arise, and the value of assets fluctuates. Thus, risk is a moving target that must be continually acquired and analyzed.

Organizations cannot address risk once and expect it to be adequate for the new environment. Ongoing risk assessment is mandatory to be ever aware of the current environment. To conduct continued and ongoing risk assessment and handling is to exercise “due diligence.”

Due care is to DO the same things that another person of similar capabilities would do in a similar situation.

Due diligence is an ongoing display of due care.

Security Control

According to ISO 27000:2018, a control is a “measure that is modifying risk.” Controls may include any process, policy, practice, device, or other action that modifies risk (ISO 27001). To put it another way, controls are the management, operational and technical safeguards and countermeasures put in place to protect the confidentiality, integrity and availability of information and systems within the organization.

Controls fit into two broad categories: safeguards and countermeasures.

Safeguards are controls put in place to proactively protect against the risk (ex. a wearing a seatbelt while in a moving vehicle).

Countermeasures are controls that activate in response to a risk activity (ex. airbags deploying during an auto accident).

Control baselining is a process employed by the security manager to analyze effectiveness and efficiency of selected controls.

Control Baseline Modeling

The process of creating a security baseline will create a set of minimum-security settings and

configurations for systems, processes, people, and activities within the organization. A simple definition of a baseline is “a minimum or starting point used for comparison.” Therefore, security control baselines are a basis for comparing security functions to determine if they have achieved at least that lowest level of protection. The determination of where to set the baseline needs to be based upon the acceptable level of risk and thus different baselines will be created based upon the classification level assigned. Higher classification requires stronger or more secure controls. It is likely that fewer and weaker controls will be used for lower classifications.

One nice benefit of creating baselines is that they provide consistency. Once a baseline is set, it becomes a measuring stick to evaluate security against.

As an example, let us say the organization has decided to implement a network-based intrusion detection system (IDS). The organization has

evaluated the different brands of IDS on the market, and they have chosen XYZ brand. This process has created an entry on the approved product list.

The next step is to determine the baseline for this IDS control. Baselineing an IDS involves watching and observing. Watching what network communication passes by the IDS and observing which of that communication is flagged by the IDS as possibly bad. If some legitimate communication is flagged as bad, then the IDS should be adjusted to NOT alert on those things in the future. Likewise, when known bad traffic is NOT flagged then the IDS should be adjusted again to alert when that traffic is seen in the future. This process creates a baseline of minimum settings and configurations. This baseline can be applied to all of the other intrusion detection systems in the organization. When this happens, the organization will have a consistent minimum level of security for IDS's, no matter where they are deployed.

The baseline must be kept current. As discussed, several times, the environment changes so the information security controls and baselines need to keep up. Continuous monitoring of the IDS may identify when these changes are occurring and that the control baseline needs to be updated. Thus, the IDS should provide monthly, weekly, or daily reports (frequency and type of reports provided by controls should be based upon the potential value and use of those reports.) about what the IDS is seeing. Those reports should quantify the amount of legitimate traffic compared to the amount of potentially harmful traffic that passes by. Based upon information provided by the control, the security manager may need to tune the IDS to alert on any new threat scenarios.

Control Selection

“The selection and implementation of appropriate security controls for an information system or a system-of-systems are important tasks that can have major implications on the operations and assets of an organization as well as the welfare of individuals and the Nation.” - NIST SP 800-53

Controls are the protection mechanisms and choosing correctly is imperative. So, what are the considerations when selecting the proper

controls? The starting point (aka - “first step”) for choosing controls is to analyze the risk that the control addresses. The next step might be to conduct a Cost Benefit Analysis (CBA). A CBA provides a methodical process of quantifying the pros and cons as well as the costs associated of using the controls. It becomes the basis for the decision. It is never a good idea to spend more on the control than the asset it is protecting is worth. However, cost is not the only selection criteria to consider. Some others are:

- What impact, either positive or negative, will the control have?
- Does the control have any side effects? Analyze the risk of the side effects to see the complete picture.
- Is the control dependent upon something else to function properly? If so, what happens when the other element malfunctions? What effects will that have on the control?
- Is the control going to be a single point of failure? If so, how can it be complimented and integrated into a defense in depth strategy?
- What is the total cost of ownership (TCO) of the control? Things to consider include not just the cost to acquire the control, but how much time or any special skills required to operate the control.
- Etc.

Gap Analysis

One of the outputs from information security governance is a set of control objectives. Control objectives state the purpose or desired outcome for a particular set of controls. What we expect the control to do for the organization. Once control objectives are established, controls are put in place to achieve those objectives. The destination should be a measurable quantity and the progress towards the destination should be measurable as well. The delta between the controls current capability and the objective is the control gap.

Even when the control is meeting the objective, it is still necessary to continue to conduct gap analysis. The reason being that the objectives change as a result of organizational strategy adjustments and business

objectives changing, likewise, the risk environment changes. A control may have been sufficient at one time, but because the threat has changed, that control may no longer meet the need. Again, ongoing, cyclical activities are a theme in security.

Compliance

Business drivers are the main catalyst for engaging in risk assessment and management activities. Some of those business drivers are the relevant laws and regulations that organizations are required to abide by, which we talked about in Chapter 1. Organizations must first evaluate which laws and regulations apply. Next, an evaluation must occur to determine whether the company is already in compliance and if not, then what changes need to be made. When the organization is not compliant, a risk assessment should be conducted to determine what risk this poses. Often it is not an all or none proposition. There may be levels of compliance. The organization could be non-compliant, partially compliant, or fully compliant depending upon the number of controls implemented. Each level may result in different levels of acceptable risk. The level to which a company decides to comply is a management decision. This may not be a popular statement, but it is factual. The fact is that companies may choose NOT to comply with certain laws and regulations. If that is the choice they make, then the company must be willing to pay the price for such non-compliance. (Note: Sometimes the cost of compliance outweighs the penalties for non-compliance.) An example might be when a delivery company in a major metropolitan city decides to allocate budget for parking fines. The company knows that their delivery vans will double park and it is cheaper to pay the fine (if it occurs) than it is to search for and park in a legal space.

Beyond the obvious benefit of not being hammered with large penalties and fines, compliance has several other benefits as well. Some direct benefits of compliance include:

1. A higher level of security. This reduces the chance that breaches will occur and if a breach were to occur, being compliant usually reduces the severity of the breach.

2. A Higher level of security translates to greater trust and confidence from customers and stakeholders.
3. Easier to maintain. Once compliance is achieved, it becomes a simple on-going maintenance task to keep up with regulatory changes.

Some of the indirect benefits of compliance include:

1. Plurality. When an organization takes steps to comply with one law or regulation, that work can be useful to help the organization comply with other such laws and regulations. For example, if one becomes PCI-DSS compliant, those efforts also help the organization move towards HIPAA or Sarbanes-Oxley compliance.
2. Compliance requirements provide a basis for corporate security strategies.
3. Compliance is likely to provide productivity increases.

Risk Monitoring

One aspect of enterprise risk management is to monitor the effectiveness of the risk handling activities as they are compared to the current risk landscape. This monitoring is conducted both by internal resources as well as external entities. Internal monitoring is like conducting a self-assessment. Based upon our self-assessment, we can determine if changes need to occur. The benefit is this self-assessment can happen continuously and at a low cost. External monitoring serves as a second opinion. This second look will hopefully provide an objective unbiased assessment of the organizational risk activities.

Monitoring is not enough. The information learned while monitoring must be effectively communicated. This information must be communicated internally to management and other stakeholders so that they can use the information to make risk-based decisions. Sometimes external communication may be necessary such as when the laws and regulations that we must comply with require us to do so. However, it is not good enough to say, “yes we are complying.” The fact is that no one would trust us anyhow. Therefore, many organizations are required to have trusted third

parties evaluate the risk management activities and to provide an opinion attesting to the effectiveness of those actions.

Reassessing Risk

Risk is a moving target. If we hope to have any chance to hit that target, our risk management practices must be updated. Therefore, we conduct risk assessments as cyclic processes. This does not mean that each time a risk assessment is conducted that the company will have to start completely over. Rather, the information that was utilized during the previous assessments can be recycled and updated, as necessary. But how often should a risk assessment be conducted? In general, organizations should update their assessments on a continually, recurring basis and when there are significant changes to the risk environment. It should be defined in our policy as to how often and why we start this process again. Reasons for beginning the process again include:

- Regularly scheduled basis
- Major changes have occurred to our environment
- A business unit has been sold
- Another business has been bought and we are merging the two

Information Classification

Information classification is a process of assigning information to different protection schemes based upon the value of the information. The simple fact is that information is not equal and therefore it should not be protected equally. Without an information classification program (aka - data protection plan) all information would be protected at the same level meaning that some data is protected to the appropriate level while most data is either over or under protected. The problem of over protection is the excessive, unwarranted cost for protection while the danger of under protection is the compromise of confidentiality, integrity, or availability of that information.

When conducting information classification, a business impact analysis (BIA) should be used as the basis for classification. The BIA will determine what systems and data are critical to operations and which systems contain

sensitive information to be protected. Further, the BIA reveals just how important the systems and data are to the mission.

Information Classification Program

We must define what types of data must be protected, e.g., Personally Identifiable Information (PII) or Payment Card Information (PCI) or protected health information (PHI). Within that program we need to determine how many levels of classification we will have in our scheme, e.g., Public, Secret, Top Secret, and what data fits into each level. The names of the level must also be carefully selected so that they are understandable by everyone within the business that will encounter these labels.

The responsibility for placing each piece of information into its proper classification level and then labeling the data falls on the owner. Who has access to specific levels of data should be determined by the clearance level that we give to each user. The clearance level combined with a need to know determines actual access.

When the user accesses specific information it is very necessary that they understand the information classification policy, so they understand how to handle and treat the data that they now have access to.

Summary

Developing a strong security strategy and program (Domain 1) is critical for the success of the security program within a business. That strategy and program needs to be specifically tailored to the security needs of our business. Once we have determined what a business is attempting to accomplish, we need to understand and deal with (manage) the things that impede the goals of the organization. This is risk management.

Risk management is broken into four distinct, but interrelated pieces - Identify, Assess, Mitigate, and Monitor. Keep in mind, that even though the third piece is “mitigate,” not all risks will be mitigated. It is more important that risk is properly managed rather than mitigated. Sometimes it may be most cost beneficial to accept a risk rather than to mitigating that risk.

The risk management process needs to be completely integrated into all aspects of the organization. This is done through management's commitment to security (management needs to understand that it is more cost effective to manage risk, than to ignore risk) and the proper assignment of roles and responsibilities to all members of the organization.

COBIT 2019, NIST SP 800-35, and ISO 27005 (among others) provide frameworks and methodologies to identify risk. Each method offers various strengths and weaknesses and should be chosen partially based on how well they line up with the organization's other management strategies.

Once identified, risk needs to be prioritized based on the level of threat it poses to the sustainability of the organization. This process is called risk assessment. Quantitative and Qualitative are two primary means of assessing risk. Quantitative risk analysis can be very difficult to perform and attempts to quantify or assign an exact dollar value to each risk. Qualitative risk analysis compares risks based on High, Medium, and Low in order to prioritize the risks.

After risks have been prioritized, they must be addressed or handled. The risk management process assigns the term "mitigation" to this process, but there are four options available to deal with risk. The options are accept, mitigate, transfer, and avoid. Which option you choose will be based on a cost benefit analysis of the cost of the security solution compared to the amount of potential loss if nothing is done.

Beyond choosing a general category of solution (for example "mitigate"), specific controls need to be chosen to address the need. We may choose to mitigate a risk, but we also need to determine if it is most effective to mitigate via a firewall or via an IPS. Each potential security solution has differing reporting and monitoring capabilities, which could influence our selection.

The fourth step in risk management is to continually monitor risk. Threats are not static, nor is your business, therefore risk management is an iterative process where we need to constantly monitor ourselves to understand where we are in relation to where we wanted (past tense) to be, in additions to wondering where we want (future tense) to go. Living with

and meeting past goals is not going to be good enough. Risk management should be forward thinking.

Chapter 2 Questions

1. The four main steps of a risk management process are:
 - a. Identify risks, assess risks, mitigate, and manage risks, monitor for effectiveness
 - b. Identify risks, control risks, monitor risks, analyze risks
 - c. Plan, Do, Act, Update
 - d. Identify risk, eliminate risk, monitor risk
2. Conducting a risk assessment to identify those things that could interfere with the company's ability to deliver products, goods and services to customers is known as:
 - a. A product assessment
 - b. A compliance assessment
 - c. An operational assessment
 - d. A strategic assessment
3. What is necessary to ensure security decisions are made based upon the organizations risk management strategies?
 - a. Implementation of the most recent technical controls
 - b. A security action plan
 - c. Conducting a risk assessment at least annually
 - d. Good lines of communication between the Chief Risk Officer and the Chief Information Officer
4. Asset valuation is critical to conducting a successful risk assessment. What type of assets are not clearly defined and whose value may not be easily identified?
 - a. Information assets
 - b. Intangible Assets
 - c. Intellectual property
 - d. Real property
5. The probability or chance of something occurring is known as:
 - a. Vulnerability
 - b. Likelihood

- c. Expectation
- d. Possibility

6. The product of vulnerabilities, threats and asset value is:

- a. Enterprise Risk Management
- b. Exposure
- c. Operational risk
- d. Total risk

7. As part of an enterprise risk assessment, the organization has determined that a malware outbreak is likely to infect 65% of its corporate servers. This is an example of which risk assessment variable?

- a. Exposure factor
- b. Annual Rate of Occurrence (ARO)
- c. Vulnerability
- d. Threat factor

8. Which of the following is least likely to be changed on a regular basis?

- a. Procedures for hardening a database server
- b. Current patch level of existing firewall
- c. Information security governance policy
- d. Information security baseline

9. Security controls that are reactive in nature and designed to neutralize a threat are:

- a. Corrective
- b. Preventive
- c. Countermeasure
- d. Safeguard

10. The first step to building an Information Security Management System (ISMS) is to establish ISMS policy, objectives, processes, and procedures relevant to managing risk and improving

information security to deliver results in accordance with overall policies and objectives. This is an example of which step of the Deming wheel?

- a. Plan
- b. Do
- c. Check
- d. Act

11. What type of risk assessment uses descriptive assessments to form an opinion of the risk based upon the scenario?

- a. Failure Mode and Effect Analysis
- b. Qualitative
- c. Risk Factor Analysis
- d. Quantitative

12. What type of risk assessment is based on objective facts such as monetary values?

- a. Risk Factor Analysis
- b. Failure Mode and Effect Analysis
- c. Qualitative
- d. Quantitative

13. When conducting a risk assessment what element identifies the frequency of an event?

- a. Single Loss Expectancy (SLE)
- b. Annual Rate of Occurrence (ARO)
- c. Exposure Factor (EF)
- d. Asset Value (AV)

14. In a quantitative risk assessment, the magnitude of loss is represented by:

- a. Exposure Factor (EF)
- b. Single Loss Expectancy (SLE)
- c. Asset Value (AV)
- d. Annual Rate of Occurrence (ARO)

15. What type of risk assessment uses logical “AND’s” and "OR's" to look at factors that combine together to create risk?

- a. Failure Mode and Effect Analysis (FMEA)
- b. Qualitative analysis
- c. Quantitative analysis
- d. Fault Tree Analysis (FTA)

16. A risk assessment that analyzes the effects of component failure and how that failure impacts a sub-system, and the overall system is known as:

- a. Quantitative Analysis
- b. Exposure Factor (EF)
- c. Failure Mode and Effect Analysis (FMEA)
- d. Fault Tree Analysis (FTA)

17. The four main ways to handle risk are:

- a. Accept, Mitigate, Transfer, Avoid
- b. Accept, Transfer, Mitigate, Ignore
- c. Deny, Blame, Resign, Accept
- d. Accept, Mitigate, Avoid, Ignore

18. Risk Transference must be accompanied by:

- a. Risk avoidance
- b. Risk acceptance
- c. A letter of Understanding (LOU)
- d. A Service Level Agreement (SLA)

19. Exercising the same level of care as another person of similar capabilities in a similar situation is known as:

- a. Average Care
- b. Standard Care
- c. Due Diligence
- d. Due Care

20. A measure to modify risk is known as a:

- a. Control
- b. Constraint
- c. Derivative

d. Behavior modifier

21. What type of control proactively protects against risk?

- a. Intrusion Detection System (IDS)
- b. Safeguard
- c. Firewall
- d. Countermeasure

22. When developing a timeline for the implementation of a strategic security plan the timeline should be:

- a. Based on relevant laws
- b. Aligned with business strategy
- c. 4-5 years long
- d. Based on Moore's law

23. Information security managers are responsible for analyzing the effectiveness and efficiency of security controls. What is this called?

- a. Constraint Baseline
- b. Control Baseline
- c. Control Benefit Analysis
- d. Threat Modeling

24. What technique can be utilized by an information security manager to methodically quantify the pros and cons associated with using a control as well as the costs for using the control?

- a. Compliance Assessment
- b. Threat Modeling
- c. Control Baseline
- d. Cost Benefit Analysis (CBA)

25. What is the purpose of a control objective?

- a. To define the purpose or desired outcome for a particular set of controls.

- b. To provide a basis of comparison of control systems
- c. To establish a baseline for conducting a control cost benefit analysis
- d. To deliver a set of controls that are without flaw

26. Information security managers must identify situations where the current controls are not meeting the control objectives. What is the name of the process to identify these shortfalls?

- a. Gap Analysis
- b. Least Privilege
- c. Cost Benefit Analysis
- d. Control baselining

27. Conducting a risk assessment to determine if the organization is following the applicable laws and regulations is known as:

- a. A Strategic assessment
- b. An operational assessment
- c. A security assessment
- d. A compliance assessment

28. Effective communication of risk to senior executives, the board of directors and stakeholders is the responsibility of the:

- a. Chief Executive Officer (CEO)
- b. Chief Risk Officer (CRO)
- c. Chief Compliance Officer (CCO)
- d. Chief Operations Officer (COO)

29. In order to purchase information security software a business case can best be assisted by

- a. a projection of the annual number of incidents
- b. a projected comparison against other companies spending
- c. a projection of return on investments (ROI)
- d. a projection of the cost of the failure of the control

Chapter 2 Questions with Answers and Explanations

1. The four main steps of a risk management process are:
 - a. **Identify risks, assess risks, mitigate and manage risks, monitor for effectiveness**
 - b. Identify risks, control risks, monitor risks, analyze risks
 - c. Plan, Do, Act, Update
 - d. Identify risk, eliminate risk, monitor risk

Explanation

Answer A: Risk must be assessed before it can be controlled, and it can never be fully eliminated. PDCA is a logical process flow for creating a security plan, or nearly anything else.

2. Conducting a risk assessment to identify those things that could interfere with the company's ability to deliver products, goods and services to customers is known as:
 - a. A product assessment
 - b. A compliance assessment
 - c. **An operational assessment**
 - d. A strategic assessment

Explanation

Answer C: Determining what would interfere in delivery of products would be the operations or an operational assessment. Not planning (strategic) or regulatory (compliance). A product assessment would be product specific, not delivery of said product.

3. What is necessary to ensure security decisions are made based upon the organizations risk management strategies?
 - a. Implementation of the most recent technical controls
 - b. A security action plan
 - c. Conducting a risk assessment at least annually

d. Good lines of communication between the Chief Risk Officer and the Chief Information Officer

Explanation

Answer D: For purchase decisions to be responsibly made based on risk it is necessary for the two parties responsible for those two pieces to be in good communication. A risk assessment does have to be done, but the plan or the action plan cannot be created without that knowledge. That plan might involve the latest technology but that comes later.

4. Asset valuation is critical to conducting a successful risk assessment. What type of assets is not clearly defined and whose value may not be easily identified?

a. Information assets

b. Intangible Assets

c. Intellectual property

d. Real property

Explanation

Answer B: Information assets may involve tangible or intangible styles. Intellectual property is one form of intangible. Real is usually tangible property. Intangible is the hardest to determine its value as you cannot see or touch this type of property.

5. The probability or chance of something occurring is known as:

a. Vulnerability

b. Likelihood

c. Expectation

d. Possibility

Explanation

Answer B: Likelihood is probability. You could say possibility is similar, but it is not a common term used in risk assessments. Vulnerability is a weakness or a flaw. Expectation is also not a term used in risk assessments.

6. The product of vulnerabilities, threats and asset value is:

- a. Enterprise Risk Management
- b. Exposure
- c. Operational risk
- d. Total risk**

Explanation

Answer D: Total risk is defined as a combination of asset value, threats, and vulnerabilities.

7. As part of an enterprise risk assessment, the organization has determined that a malware outbreak is likely to infect 65% of its corporate servers. This is an example of which risk assessment variable?

- a. Exposure factor**
- b. Annual Rate of Occurrence (ARO)
- c. Vulnerability
- d. Threat factor

Explanation

Answer A: Exposure factor is a percentage of loss or a percentage of impact so that a percentage of the assets value can be determined at risk.

8. Which of the following is least likely to be changed on a regular basis?
- a. Procedures for hardening a database server
 - b. Current patch level of existing firewall
 - c. Information security governance policy**
 - d. Information security baseline

Explanation

Answer C: The governance policy should not change with any kind of frequency. It should be planned with a long-range view. Patch levels and hardening procedures will change when vendors update their products, which is oh so frequent.

9. Security controls that are reactive in nature and designed to neutralize a threat are:

- a. Corrective
- b. Preventive
- c. Countermeasure**
- d. Safeguard

Explanation

Answer C: Countermeasures are reactive; they counter the effect of the threat being realized. Corrective is one way to react to a threat being realized and its damage. Safeguards try to prevent or stop the threat from ever being realized.

10. The first step to building an Information Security Management System (ISMS) is to establish ISMS policy, objectives, processes, and procedures relevant to managing risk and improving information security to deliver results in accordance with overall policies and objectives. This is an example of which step of the Deming wheel?

- a. Plan**
- b. Do
- c. Check
- d. Act

Explanation

Answer A: The Deming wheel goes in the order of Plan-Do-Check-Act. Plan is the first step.

11. What type of risk assessment uses descriptive assessments to form an opinion of the risk based upon the scenario?

- a. Failure Mode and Effect Analysis
- b. Qualitative**
- c. Risk Factor Analysis
- d. Quantitative

Explanation

Answer B: Qualitative is descriptive where Quantitative is numerical. FMEA is a combination of the two. Risk factor analysis is not real.

12. What type of risk assessment is based on objective facts such as monetary values?

- a. Risk Factor Analysis
- b. Failure Mode and Effect Analysis
- c. Qualitative
- d. Quantitative**

Explanation

Answer D: Qualitative is descriptive where Quantitative is numerical. FMEA is a combination of the two. Risk factor analysis is not real.

13. When conducting a risk assessment what element identifies the frequency of an event?

- a. Single Loss Expectancy (SLE)
- b. Annual Rate of Occurrence (ARO)**
- c. Exposure Factor (EF)
- d. Asset Value (AV)

Explanation

Answer B: Frequency is defined by ARO. EF is the percentage of loss. AV is the actual value of the asset. SLE is the cost of a single event.

14. In a quantitative risk assessment, the magnitude of loss is represented by:

- a. Exposure Factor (EF)**
- b. Single Loss Expectancy (SLE)
- c. Asset Value (AV)
- d. Annual Rate of Occurrence (ARO)

Explanation

Answer A: EF is the percentage of loss or magnitude of loss. Frequency is defined by ARO. AV is the actual value of the asset. SLE is the cost of a single event.

15. What type of risk assessment uses logical “AND’s” and "OR's" to look at factors that combine together to create risk?

- a. Failure Mode and Effect Analysis (FMEA)
- b. Qualitative analysis
- c. Quantitative analysis
- d. Fault Tree Analysis (FTA)**

Explanation

Answer D: Fault tree analysis looks at combinations of factors and analyzes the resulting effects. FTA could be used as part of either a qualitative or quantitative assessment. Failure Mode and Effect Analysis looks at systems, subsystems and components and analyzes the effects of failure.

16. A risk assessment that analyzes the effects of component failure and how that failure impacts a sub-system and the overall system is known as:
- a. Quantitative Analysis
 - b. Exposure Factor (EF)
 - c. Failure Mode and Effect Analysis (FMEA)**
 - d. Fault Tree Analysis (FTA)

Explanation

Answer C: Failure Mode and Effect Analysis looks at systems, subsystems and components and analyzes the effects of failure. Fault tree analysis looks at combinations of factors and analyzes the resulting effects. FTA could be used as part of either a qualitative or quantitative assessment.

17. The four main ways to handle risk are:
- a. Accept, Mitigate, Transfer, Avoid**
 - b. Accept, Transfer, Mitigate, Ignore
 - c. Deny, Blame, Resign, Accept
 - d. Accept, Mitigate, Avoid, Ignore

Explanation

Answer A: Ignorance and blame are never acceptable ways to handle risk. The four ways are accept, avoid, mitigate/reduce or transfer.

18. Risk Transference must be accompanied by:

- a. Risk avoidance
- b. Risk acceptance**
- c. A letter of Understanding (LOU)
- d. A Service Level Agreement (SLA)

Explanation

Answer B: When risk is transferred it does not eliminate risk for you. There is always a risk that the party that has accepted that part of the risk may not fulfill on their job (insurance companies may not pay) so that risk must also be accepted.

19. Exercising the same level of care as another person of similar capabilities in a similar situation is known as:

- a. Average Care
- b. Standard Care
- c. Due Diligence
- d. Due Care**

Explanation

Answer D: The legal system defines due care as exercising the same level of care as another person of similar capabilities in a similar situation. This is also described with the term prudent person rule.

20. A measure to modify risk is known as a:

- a. Control**
- b. Constraint
- c. Derivative
- d. Behavior modifier

Explanation

Answer A: Controls modify risk. Constraint and behavior modifier might sound good, but they are not the normal terms used in risk management. Derivative just does not make sense here since it is something based on something else.

21. What type of control proactively protects against risk?

- a. Intrusion Detection System (IDS)

- b. Safeguard**
- c. Firewall
- d. Countermeasure

Explanation

Answer B: Safeguards protect against risk or try to prevent it. Countermeasures handle things once the threat is realized. A firewall and IDS could both be considered safeguards, but they are too specific when safeguard is one of the possible answers here.

22. When developing a timeline for the implementation of a strategic security plan the timeline should be:
- a. Based on relevant laws
 - b. Aligned with business strategy**
 - c. 4-5 years long
 - d. Based on Moore's law

Explanation

Answer B: Implementation timelines need to be aligned with the business strategy in order to support business and not get in its way.

23. Information security managers are responsible for analyzing the effectiveness and efficiency of security controls. What is this called?
- a. Constraint Baselineing
 - b. Control Baselineing**
 - c. Control Benefit Analysis
 - d. Threat Modeling

Explanation

Answer B: Knowing how well your controls are working is critical. Threat modeling is about the possible attacks. Control benefit analysis is a little off, the real term would be cost benefit analysis. Same with constraint baselineing, the term is control baselineing. Knowing how things are working gets you to baselines.

24. What technique can be utilized by an information security manager to methodically quantify the pros and cons associated with using a

control as well as the costs for using the control?

- a. Compliance Assessment
- b. Threat Modeling
- c. Control Baseline
- d. Cost Benefit Analysis (CBA)

Explanation

Answer D: CBA is an analysis of the benefits of the control vs. the cost. Baselines, threat modeling and compliance assessments do not involve balancing anything against costs.

25. What is the purpose of a control objective?

- a. To define the purpose or desired outcome for a particular set of controls.**
- b. To provide a basis of comparison of control systems
- c. To establish a baseline for conducting a control cost benefit analysis
- d. To deliver a set of controls that are without flaw

Explanation

Answer A: The control objective should define the purpose of the controls. It does not establish a baseline for cost benefit analysis, nor should it show how to compare controls. Controls will be flawed; we need to watch for those weaknesses and put in appropriate controls around those if appropriate.

26. Information security managers must identify situations where the current controls are not meeting the control objectives. What is the name of the process to identify these shortfalls?

- a. Gap Analysis**
- b. Least Privilege
- c. Cost Benefit Analysis
- d. Control baselining

Explanation

Answer A: A gap analysis has the point of finding the gap between current and desired states. A cost benefit analysis is useful when trying to figure out if you should buy a control and the baseline is the

configuration minimum. Least privilege would be a desired state and must be configured in the control.

27. Conducting a risk assessment to determine if the organization is following the applicable laws and regulations is known as:

- a. A Strategic assessment
- b. An operational assessment
- c. A security assessment
- d. A compliance assessment**

Explanation

Answer D: A risk assessment done in relationship to laws and regulations would show compliance or what is lacking in order to be in compliance. It is not for planning (strategic) or operational purposes. Any assessment could be called a security assessment making it too nebulous to be a good answer.

28. Effective communication of risk to senior executives, the board of directors and stakeholders is the responsibility of the:

- a. Chief Executive Officer (CEO)
- b. Chief Risk Officer (CRO)**
- c. Chief Compliance Officer (CCO)
- d. Chief Operations Officer (COO)

Explanation

Answer B: The CRO is responsible for risk and as they are senior management, they would be the one responsible for communicating that to the rest of the senior executives (CCO, COO, CEO) and the board.

29. In order to purchase information security software a business case can best be assisted by

- a. a projection of the annual number of incidents
- b. a projected comparison against other companies spending
- c. a projection of return on investments (ROI)**

d. a projection of the cost of the failure of the control

Explanation

Answer C: The ROI calculation can most closely assist with aligning security purchases with the businesses bottom line. Frequency and cost of incidents can help with understanding the need for the control but not the money expenditure directly. Another company may not have similar goals or concerns, so it is the most irrelevant here.

chapter 3

Domain 3

Information security program development and management 27% of the Exam

According to ISACA, in this domain, you will:

Establish and manage the information security program in alignment with the information security strategy.

A CISM candidate must be able to perform the following 10 task statements:

3.1, Establish and/or maintain the information security program in alignment with the information security strategy.

3.2, Align the information security program with the operational objectives of other business functions (e.g., human resources [HR], accounting, procurement and IT) to ensure that the information security program adds value to and protects the business.

3.3, Identify, acquire and manage requirements for internal and external resources to execute the information security program.

3.4, Establish and maintain information security processes and resources (including people and technologies) to execute the information security program in alignment with the organization's business goals.

3.5, Establish, communicate and maintain organizational information security standards, guidelines, procedures and other documentation to guide and enforce compliance with information security policies.

3.6, Establish, promote and maintain a program for information security awareness and training to foster an effective security culture.

3.7, Integrate information security requirements into organizational processes (e.g., change control, mergers and acquisitions, system development, business continuity, disaster recovery) to maintain the organization's security strategy.

3.8, Integrate information security requirements into contracts and activities of third parties (e.g., joint ventures, outsourced providers,

business partners, customers) and monitor adherence to established requirements in order to maintain the organization's security strategy.

3.9, Establish, monitor and analyze program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

3.10, Compile and present reports to key stakeholders on the activities, trends and overall effectiveness of the IS program and the underlying business processes in order to communicate security performance.

A solid understanding of the following 16 knowledge statements should be attained by a CISM candidate:

- k3.1, Knowledge of methods to align information security program requirements with those of other business functions
- k3.2, Knowledge of methods to identify, acquire, manage and define requirements for internal and external resources
- k3.3, Knowledge of current and emerging information security technologies and underlying concepts
- k3.4, Knowledge of methods to design and implement information security controls
- k3.5, Knowledge of information security processes and resources (including people and technologies) in alignment with the organization's business goals and methods to apply them
- k3.6, Knowledge of methods to develop information security standards, procedures and guidelines
- k3.7, Knowledge of internationally recognized regulations, standards, frameworks and best practices related to information security program development and management
- k3.8, Knowledge of methods to implement and communicate information security policies, standards, procedures and guidelines
- k3.9, Knowledge of training, certifications and skill set development for information security personnel
- k3.10, Knowledge of methods to establish and maintain effective information security awareness and training programs

- k3.11, Knowledge of methods to integrate information security requirements into organizational processes (e.g., access management, change management, audit processes)
- k3.12, Knowledge of methods to incorporate information security requirements into contracts, agreements and third-party management processes
- k3.13, Knowledge of methods to monitor and review contracts and agreements with third parties and associated change processes as required
- k3.14, Knowledge of methods to design, implement and report operational information security metrics
- k3.15, Knowledge of methods for testing the effectiveness and efficiency of information security controls
- k3.16, Knowledge of techniques to communicate information security program status to key stakeholders

Introduction

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

1. Information security policy, objectives, and activities that reflect business objectives;
2. An approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;
3. Visible support and commitment from all levels of management;
4. A good understanding of the information security requirements, risk assessment, and risk management;
5. Effective marketing of information security to all managers, employees, and other parties to achieve awareness;
6. Distribution of guidance on information security policy and standards to all managers, employees and other parties
7. Provision to fund information security management activities;
8. Providing appropriate awareness, training, and education;
9. Establishing an effective information security incident management process;
10. Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement.

~From ISO 17799

This section will discuss many of these critical success factors and how to achieve them.

Information Security Reflects Business Objectives

Security is of no use, if it does not enable a corporation to accomplish its business objectives. In order to meet objectives, those objectives must first be identified and defined as we began in chapter one. Only then can

security be properly applied. Senior management must create the business objectives and ensure they are effectively communicated to all the appropriate parties; both internal and external.

It is the duty of the security department to develop security criteria to ensure those objectives are met, then to raise upper management's understanding of the security objectives. Management needs to be informed not only of the requirements for security but also of the business case behind those requirements. The security department cannot expect management to approve expenditures unless there is a clear business case created showing the cost benefit analysis of the security expense.

Security management's responsibility is to ensure that a business case can be created for major security expenses.

One of the greatest obstacles to achieving this goal is a disconnect between security and business. Too often security is not seen as a catalyst to push the company towards success, but rather it is viewed as a stumbling block to productivity and a red line on the corporate budget. To begin to address this issue, consider what the organizational chart looks like. How is security represented within the company?

Sometimes security is a distributed function disbursed throughout the organization. In this configuration there is a lack of central coordination. Another approach is to have security as its own stand-alone department. This overcomes the lack of central coordination that is present in a distributed system, however now there is the possibility of the security department becoming isolated and out of touch with the needs of the rest of the business. A good compromise is for the security department to have a central nucleus with satellite entities distributed to the other business units.

This approach provides a blend of central coordination while allowing security to become familiar with the needs of the business.

There is no single approach that is correct. Each organization must decide which organizational structure fits best into its corporate culture. Which approach best provides a conduit between security and business?

The basic process of creating and maintaining an information security program involves:

1. Identifying requirements
2. Create architectures
 1. People
 2. Process
 3. Technology
3. Creation of Policy, Procedures, Standards and Guidelines
 1. Methods to develop / implement & communicate
1. Policies
2. Standards
3. Procedures
4. Guidelines
4. Awareness & Training
 1. Methods to establish
 2. Methods to maintain

5. Branch out - integrate security into business processes

1. Change control

2. Procurements

3. Mergers / acquisitions

4. BCP

5. Methods to incorporate security requirements

1. Contracts

2. 3rd party management processes

6. Create and manage metrics

1. Design

2. Implement

3. Report

7. Test Security

1. Effectiveness

2. Applicability

8. Monitor Security

9. Report

Identify Security Requirements

Security requirements can be either internal or external and they can be divided into three basic categories: Confidentiality, Integrity and Availability. Internal security requirements deal with the ways in which data


and systems are protected within the organization. Much of the focus of security controls is on the internal requirements. External requirements deal with how data will be protected as it traverses into and out of our organization.

While the Information Security Manager (ISM) might know, at a high level, what types of things need to be filed into these categories, the ISM does not know the specifics. For example, the ISM knows that customer information such as credit card data or health data must be kept confidential, but they may not know where within the organization these items exist, if they exist at all. Therefore, a concerted effort must be made to identify:

- What data and systems require protection
- Who are the owners of those resources
- How valuable are those resources to the mission and
- Finally, what types of protections are appropriate.

In order to identify requirements, the security manager must have access to the stakeholders in the company who can help identify the systems and data that require protection. These stakeholders will also have insights about the level of protection that is warranted.

Surveys, questionnaires, focus groups and observation are a few of the tools the security manager can use to gather information to develop security requirements.



**Senior management must be
the champions of security for
it to be effective.**

Once the requirements have been identified they can be used to develop and implement the security program that will address the needs.

Security Architectures

Chapter one introduced some of the frameworks one could use to help create an enterprise architecture such as Zachman, SABSA, TOGAF and others. While the specific details of these frameworks differ, at their core there is a lot of commonality.

The strength of creating an architecture is the benefit that comes from the thoughtfulness and planning. Architecture requires organizations to plan, anticipate how systems and components are going to work together in an efficient, secure way to maximize productivity. The alternative to creating an architecture is that the architecture will just haphazardly evolve into something that is not manageable and does not effectively or efficiently meet the needs of the organization.

Enterprise security architecture is a high-level design that leverages the strengths of the individual components while minimizing the weaknesses they possess.

Creation of Policy, Procedures, Standards and Guidelines

From NIST SP 800-14 - Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities.

Policies, procedures, standards, baselines, and guidelines have been defined and discussed in chapter 1. In this section we will look at the mechanics of creating, communicating, and updating these most fundamental tools of the information security manager's trade.

Policies are brief, high level statements from management stating the general dos and don'ts of the organization. They serve to inform everybody what is acceptable and what is not. Organizational security policy should address three main areas: business requirements, the legal and regulatory requirements, and the threat environment.

Policy should address business needs, laws & regulations and the threat environment.

The organization should create a top-level policy that is supported by multiple functional policies. Policies should be universally applicable. However, policies should also have a mechanism for evaluating and granting exceptions. Exceptions to policy should be few. If the policy has numerous exceptions, this might indicate that the policy is too specific.

A few examples of functional policies are:

- Access control
- Acceptable use
- Information classification
- Cryptography

Policies should have a defined owner approved by management. The owner is responsible for developing, disseminating, and updating the policies. Policies should be effectively communicated to relevant employees and external parties. To be effectively communicated policies should not be written in legal jargon, rather they should be clear and easy to understand.

Procedures and standards are tools to support security policy. Procedures are step-by-step instructions for accomplishing a task while standards are the solutions that have been approved for use within the organization. Standards and procedures should be separate documents, not embedded within the policy itself. These tools provide consistent security across the organization. For example, if the organization has a procedure for material destruction, if everybody follows the procedure then the

organization knows that all material will be destroyed to an appropriate level. The same holds true for standards, they provide consistency.



Diagram 16
Document Structure

Awareness & Training

**Everyone in the organization
should receive security awareness
training at least annually.**

Training and awareness are two sides of the same coin as was introduced in Chapter 1. Training provides the necessary information and skills for users to accomplish their tasks while awareness is an ongoing reminder of what they learned. Training is a bit more detailed and comprehensive while awareness is simple and concise. Training should be provided to employees, contractors, customers, and other types of people who interact with information systems. The training should occur at least annually; more frequently as the local business needs may dictate. The level and extent of training should be commensurate with the level of access granted. To achieve the best results from the training and awareness activities, the target audience should be identified and only the relevant information should be presented.

In addition to the people receiving regular updates, the training and awareness materials should be kept current as well. As the policy, procedures and standards change or as the organizational environment changes, the educational tools must be updated.

Branch out - integrate security into business processes

Information security should be a part of project management. All projects, regardless of type will have some security elements that need addressed. It is the information security managers responsibility to ensure security requirements are defined within the projects and that security is addressed at all stages of the project.

In order to maximize the effectiveness of enterprise security efforts, it is recommended that security be well integrated into other business processes such as change control, procurement, mergers and acquisitions, business continuity planning. The list goes on and on. All these business processes should have an element of security represented within. For every step within each of these processes, there are many ways security can offer value.

The term “baked in” comes to mind. Historically, security has been an afterthought. As such, it has also been a stumbling block to productivity. If, however, security is an ongoing participant in these processes, the security function should serve to be a catalyst to deliver a better, more secure, product from the beginning.

The CISO should ensure that business decisions are risk-based decisions. This happens by engaging security in the business processes from the beginning and keeping them engaged throughout the process.

Create and Manage Metrics

The term metric essentially means “measurement.”

“Measurement is the first step that leads to control and eventually to improvement. If you can’t measure something, you can’t understand it. If

you can't understand it, you can't control it. If you can't control it, you can't improve it."

— [H. James Harrington](#)

This is true for security as well. However, too often security managers focus on metrics that may not be as useful as they think. For example, when a security tool tells us that it has identified 4652 security violations, the number is astonishing, and it seems extremely bad. But what does that mean? Does it mean the company is in grave danger and is about to experience corporate Armageddon or does it simply mean an employee has been downloading music? What is the true risk to the company? Downloading music may get the company into hot water IF the employee is pirating the music, but this probably will not be a high priority topic at the next board meeting.

Metrics need to be useful for risk management, the metrics should in some way tie back to the ROI. Good security metrics should be:

- Quantitative: a measurement of time, money, or a derivative of these and should be expressed as a number or percentage. Qualitative metrics such as those expressed as high, medium, and low do not work. The metrics must be quantitative and should be an indication of value delivered.
- Well understood across the company and industry. They should be clear and unambiguous.
- Easy. The data used to derive the metric should be easy to gather and the calculations should be easily and consistently calculated. Additionally, they should be easy to understand in relation to the value they offer the business.

Literally hundreds of metrics can be defined and measured. Most importantly, organizations must create a customized set of metrics that are helpful to the organization. The metrics can be divided into various categories such as network perimeter, applications, or reliability. An example of some metrics that may fit into each of the proposed categories follows:

- Network Perimeter:

- Number of firewall rule changes
 - Number of sites with open wireless access points
 - Number of remote connections not protected by a firewall
- Application:
 - Number of vulnerabilities per application
 - KLOC (thousand of lines of code)
 - Number of defects per KLOC
- Reliability:
 - Host up time
 - Unplanned downtime
 - Mean Time to Recover (MTTR)

The above examples have three things in common; they are quantifiable, they are easy to understand, and they provide insight about the effectiveness of the security function.

Balanced Scorecard

Once metrics have been defined and management of the metrics has begun, the organization can move on to create a balanced scorecard, which we introduced to you in Chapter 1. The balanced scorecard has been adapted for different uses over the years. The IT balanced scorecard allows the organization to set, track and achieve its business strategy and objectives by measuring aspects of the business from four basic perspectives:

- Corporate contribution - Evaluates IT performance from the perspective of executive management and board of directors; factors such as value of IT investments and management of IT investments (budgeted vs. actual) are measured.
- Customer orientation - Evaluates IT performance from a customer, user, or business unit's standpoint; factors such as business partnership and service level performance are measured.
- Operational excellence - Evaluates IT performance from the IT management standpoint as well as audit and regulatory

standpoints; factors such as process maturity, backlog and internal costs are measured.

- Future orientation - Evaluates IT performance for the perspective of the IT staff; factors such as architecture evolution, emerging technologies and service delivery are measured.

The seven-step process for creating a balanced scorecard:

Step 1: Identify the current set of BSC goals. This activity is carried out at the highest levels of the organization. The Chief Information Officer (CIO) must keep abreast of the goals and must ensure that any noticeable shift in priorities is (implicitly or explicitly) detected and expeditiously translated into an IT risk management plan.

Step 2: Map the current set of BSC goals to actionable technology objectives and establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include the objective of the assessment to a BSC goal, including delineating the context of each risk assessment against the business criteria sought to be achieved.

Step 3: Develop a risk identification system based mainly on the objectives determined in step 2. The main activities to be carried out at this stage are the profiling of specific threats and vulnerabilities to the attainment of the objectives.

Step 4: Carry out a risk assessment, considering the probability of occurrence, business impact (of the occurrence of vulnerability) and prioritization as per the standard methodology. Information security and compliance are not the only issues here. Threats to competitive advantage, reputation, furthering the mission, etc., must be considered. Only by a holistic consideration of the entire spectrum of an organization's activities and due prioritization is a technology risk assessment finalized.

Step 5: Determine the specific risk control strategy as a combination of one or more of the following, in respect to each risk being assessed (as discussed in Chapter 2):

- Risk avoidance
- Risk transfer

- Risk mitigation
- Risk acceptance

Step 6: Implement the system as per the System Development Life Cycle (SDLC) methodology, with the enumerated strategy as an integral part of the requirement and analysis phases. This is the stage at which a risk response process should be developed and maintained. It should be designed to ensure that cost-effective controls align themselves with the specific risk control strategy chosen on a continual basis. Provisions for making allowance for risk management due to compliance and regulatory guidelines would be in addition to the risk management efforts deduced from the BSC.

Step 7: Periodically review whether the technique is proving effective. The associated metrics will have to be identified at the initial stages. The final assessment must also be modulated by the subjectivity inherent in all risk-related activities. Some suggested metrics are:

- The percentage of risk management effort that is earmarked, as a result of BSC priorities, as a part of the overall risk management effort. It is suggested that this should not be less than 60 percent.
- The percentage of actual critical events that have impacted business as a part of those envisaged during the risk assessment stage.
- Number of significant incidents caused by risks not identified in the risk management process, as well as their respective business impact.
- Frequency of review of the technology risk management process
- Cost-benefit analysis of the implementation of the controls

~From <http://www.isaca.org/Journal/Past-Issues/2010/Volume-5/Pages/Use-of-the-Balanced-Scorecard-for-IT-Risk-Management.aspx>

Change and Configuration Management

Change management and configuration management are opposite sides of the same coin. Change management focuses on making sure that changes that are requested are properly evaluated, authorized, implemented, and

documented. Configuration management focuses on capturing and preserving a stable state.

Change management

Over time things change and this fact cannot be avoided. Through the normal course of business, changes are introduced to the environment around us, and we may be forced to react to those changes. Likewise, we may have a need to institute changes on our own to create a more desirable environment, an environment that has additional features and functionality or an environment free of flaws and weaknesses. When these changes happen, they can be uncontrolled and haphazard, or they can change in a controlled and documented way. Haphazard or uncontrolled changes increase organizational risk because the organization may not know the change is even occurring and the outcome of the change is unpredictable. If possible, we would like to avoid uncontrolled changes. We do this by introducing a change management program. Change management is a controlled approach to ensure that the transition results in a new stable state with the desired outcomes.

Roles of change management:

- Owners - Owners are responsible for making the final decisions about what changes to make. If a change is made and it causes further problems for the organization, the owner is the one to be held accountable. Thus, it is in the owner's best interest to ensure the changes are completed within the bounds of the change control process.
- Change control board - Because changes often impact more than one system or more than one owner, a change control board will be utilized. The change control board is a group of people charged with evaluating change requests and making decisions that are deemed to be in the best interest of the organization and the respective owners and stakeholders.
- Requestor - The individual or group that has asked for a change to occur.

Steps of change management

1. Request a change
2. Evaluate
 1. Compliance evaluation
 2. Conduct risk assessment
3. Pre-approval
4. Implementation
5. Testing
6. Final approval
7. Review to assure the change was made as documented

In the end, the change control process is designed to ensure that the changes that were requested and approved is the change that happened. No more. No less.

Configuration Management

The primary reason we make intentional changes is to make some type of improvement; to add a desired feature or to fix some undesirable behavior. We do not usually make changes with the intent of making things worse. However, despite our best attempts, sometimes changes happen that do cause more problems than we started with. Configuration management is designed to address this issue.

Configuration management is the process of preserving a known good stable state. If we have a known good configuration saved, then when a change occurs and it causes problems, we can roll back to the known good configuration.

Summary: Change management is designed to ensure that changes occur only in a controlled manner while configuration management is designed to ensure that known good conditions are preserved and documented.

Patch management

Software patches are updates, provided by the software manufacturer, to fix problems contained within the application or to add features and functionality.

Incorporating patches into an organization's environment should not happen without proper oversight, planning and controls. Applying patches in an uncontrolled manner will introduce unacceptable risks.

Patch management is a set of strategies and processes designed to control how software patches are incorporated into the organization. Patch management provides methods to identify, evaluate, implement, and verify patches.

- Identify - When the manufacturer releases a patch, organizations must be aware of the existence of the patch. Software manufacturers notify customers of the patch release using several different mechanisms including, newsletters, e-mail notifications, public announcements, and patch management tools to name a few.
- Evaluate - Once a patch becomes available, the organization must analyze the patch to determine what it does. What features does it add? What flaws does it fix? How does it change the risk equation? Based on this evaluation, decisions about how and when to implement the patch can be made.
- Implement - Implementation requires a documented plan for deploying the patch, including a schedule, devices to be patched and a rollback plan.
- Verify - Finally, after a patch has been deployed, the organization must verify that the patch was successful and provide proper documentation pertaining to the patch.

Test Security

Vulnerability assessments, penetration testing, and audits provide the organization with an ongoing evaluation of their security status. It is not good enough to put a control in place and just expect that it will work properly. Controls need to be tested to provide feedback and confidence in the ability of the control. It is not a matter of “will the control fail”, it stands to reason that all things will fail eventually. Testing provides feedback to the organization about what events could cause a failure and what will the result of the failure be. For example, will the firewall fail in a way that

continues to enforce the security policy (fail secure) or will it fail in a way that allow the policy to be circumvented (fail open)?

Test Security: Vulnerability Assessment

A vulnerability assessment is a type of security test designed to identify potential weaknesses within the system and categorize the severity of those weaknesses. A vulnerability assessment by itself does not verify the weakness. It simply identifies the potential for harm. The output from a vulnerability assessment is a long laundry list of potential problems. Potential is the operative word here. There will be false positives in the list and the potential problems must now be validated by the business. Once the confirmation is done then a decision must be made as to how to handle these issues.

Test Security: Penetration Test

A penetration test is designed to mimic the actions of the bad guys attempting to own the system. In essence, a pen testers job is to think like the bad guys and then act like the bad guys to attempt to gain access, escalate privilege and expand influence. Penetration testing is much more thorough than a vulnerability assessment in that it seeks to identify and then attempt to exploit those vulnerabilities. If a vulnerability can be exploited, then the penetration test attempts to use that as a steppingstone to further the attack. What new information is available to the tester? What additional systems can the tester see? Is there anything new that can now be seen that is potentially useful to increase the depth of penetration? In essence a penetration test goes much deeper than a vulnerability assessment will.

**Vulnerability assessments identify potential weaknesses.
Penetration testing verifies those weaknesses and
attempts to validate the severity of the weakness.**

Vulnerability assessments and penetration testing are potentially harmful to the organization. Be sure to get proper authorization before conducting these tests.

Test Security: Audit

While vulnerability assessments and penetration tests are of a technical nature, a security audit is more of an administrative tool. A security audit is a systematic analysis of the organizations policies, practices and procedures and measuring them against a set of industry accepted standards of behavior. The auditor will provide an opinion as to whether the company activities are at the acceptable level based upon the standard or they are below the standard. It is up to management to then decide upon and take appropriate steps to remedy any deficiencies discovered.

Test Security: Internal vs. External Audit

Resources within the organization or its designated contractors conduct internal audits as a self-assessment to determine the current level of compliance. This self-awareness allows the organization to quickly identify the early warning signs of a possible problem and take remedial actions before the issue becomes severe. This is analogous to people monitoring their own health. Internal audits are a cost-effective way of gauging the organizational behavior compared to the industry standard.

Unfortunately, outsiders are likely to be a little skeptical when the organization says, “We are in compliance. Trust us. We had our best internal people verify.” Therefore, to provide an unbiased objective opinion, third parties are called in to do the assessment. The main advantage of an external audit is the element of objectivity. The opinion of an outside

organization tends to hold more water than the self-proclaimed attestation from the company.

An external audit also has other advantages and some disadvantages as well. External auditors tend to be very expensive, but they should be unbiased in their assessments. There needs to be a level of trust to bring someone in and allow an outsider to view how things are or are not working within your business. Once they leave with that information there may be a leak that occurs accidentally, or possibly intentionally regarding a business's lack of security. The advantage is that when their findings are made public there is usually a level of trust in that information that you do not find when a business proclaims their own security status.

Internal Audit	External Audit
Conducted by internal resources Less Expensive Can happen more frequently Trusted by management Problems can be corrected before becoming public knowledge	Conducted by third parties Very expensive Happens infrequently Trusted by outsiders Problems may become public before remediation

Table 1 Audits

Monitor

Computers and the operational environment are dynamic. Change is inevitable. There are changes to the system hardware, changes to software, changes to the user base and so on. All of these changes lead to new vulnerabilities, new threats and ever-changing risk. The risk landscape is in constant flux. Coupled with the fact that information security is never perfect at implementation and the information security manager is left with only one choice: continued monitoring and periodic reassessment of the security of the environment. Continued monitoring is the basis for due diligence. Due diligence is an ongoing process of evaluating risk and taking necessary steps to handle those risks.

Security

Computers and the operational environment are dynamic. Change is inevitable. There are changes to the system hardware, changes to software, changes to the user base and so on. All of these changes lead to new vulnerabilities, new threats, and ever-changing risk. The risk landscape is in constant flux. Coupled with the fact that information security is never perfect at implementation and the information security manager is left with only one choice: continued monitoring and periodic reassessment of the security of the environment. Continued monitoring is the basis for due diligence. Due diligence is an ongoing process of evaluating risk and taking necessary steps to handle those risks.

Reporting

A reporting process should be created that provides the proper information, in the form of useful metrics, to management, owners and other stakeholders to allow for effective decision making. The key to creating a useful report really is useful metrics. Many trees have been uselessly slaughtered for the sole purpose of printing reports that have zero value to the organization. As we have mentioned before, for metrics to be of any value, they must quantify something, preferably something associated with money.

Corporate policy and applicable laws and regulations drive reporting requirements. The requirements for reporting should not drive the monitoring process; however, they may have an impact on the frequency of monitoring. For example, if a law requires the number of attempted intrusions to be reported monthly, then the organization must collect metrics on access attempts at least monthly. If information is gathered only once a month the business may miss the attacks as they are happening and end up responding way too late.

The information that should be included in security or audit reports varies depending on the type of report being generated. Most reports will include the following information:

- Contact information
- Scope and period

- Key events - What is being reported e.g., type of attack, systems / data affected, damage caused, etc.
- Remediation plans
- Follow-up

Emerging trends in information security

Mobile computing/BYOD

Everyday electronic companies release new, cool, got to have gadgets designed to improve our lives and make the office a better place all at the same time. Portable devices offer increased productivity by offering e-mail, file sharing, calendar management, research, financial management, etc. anywhere or any time we want them. These gadgets come in the form of mobile smart phones, tablets, MP3 players and so on.

The primary advantage of bring your own device is a significant cost savings (although this is a hotly debated topic). Due to the perceived cost savings of BYOD, these devices are increasingly finding their way into the corporate world bringing with them added functionality as well as added risk.

Companies have a difficult time managing the risk of such devices if they do not have policies outlining their acceptable use. One approach to managing the risk is to prohibit the use of these devices altogether. Absolute prohibition usually happens in the most highly secure environments of the company. Another approach is to adopt a bring your own device (BYOD) policy. BYOD allows the company to reduce capital investments by allowing employees to utilize their own portable systems. Unfortunately, BYOD throws standards and the advantages that go along with them completely out the window. So, the company can save money in one regard by not having to purchase the equipment. However, there are often additional costs associated with ensuring that all the different devices can interoperate with the rest of the corporate infrastructure. There are also costs associated with lack of productivity when the device does not interoperate well. This failure to interoperate does not just occur when the device is first introduced into the environment, rather it can occur any time

that device has an update to its operating system, or a user decides to change to a different device or an updated app.

A few recommendations about BYOD:

1. Do not allow all devices. Create a list of those that are acceptable and supported.
2. Do not allow all apps either.
3. Create an acceptable use policy. This should state under what circumstances BYOD is acceptable as well as the boundaries for BYOD utilization e.g., not in the data center.
4. Utilize vendor security applications that create a sandboxed environment on the device for all corporate data.
5. Ensure that there is a way to remotely wipe or even brick the device when it is lost or stolen.
6. Create an employee exit strategy. It is not as easy as just having the employee return the asset.
 1. Ensure all corporate data is wiped from the device.
 2. If is a cell phone and the number has been given to customers who will keep the number at the end of the employment?

Cryptography

Much is to be said about the virtues of cryptography. Cryptography is defined as the art of writing and keeping secrets. Thus, cryptographic systems can be utilized to protect the confidentiality and integrity of data while it is at rest or in transit from one system to another. Cryptography can also be used to restrict access to data and systems as well as to prove the origin of data or even receipt.

Cryptography is divided into three broad categories: symmetric, asymmetric, and hashing.




	Symmetric	Asymmetric	Hashing
Best Use	<ul style="list-style-type: none"> •Encrypting Bulk Pieces of Data 	<ul style="list-style-type: none"> •Digital Signatures •Key Exchange •Encrypting small pieces of Data 	<ul style="list-style-type: none"> •Integrity 

Table 2
Cryptography Basics

Cryptography: Symmetric

Symmetric systems utilize the same cryptovariable (aka: key) to encrypt the data as well as to decrypt the data. Of the four goals of cryptography, confidentiality, proof of origin, integrity and non-repudiation, symmetric systems provide only confidentiality. Commonly known algorithms include DES, 3DES, AES, and Blowfish.

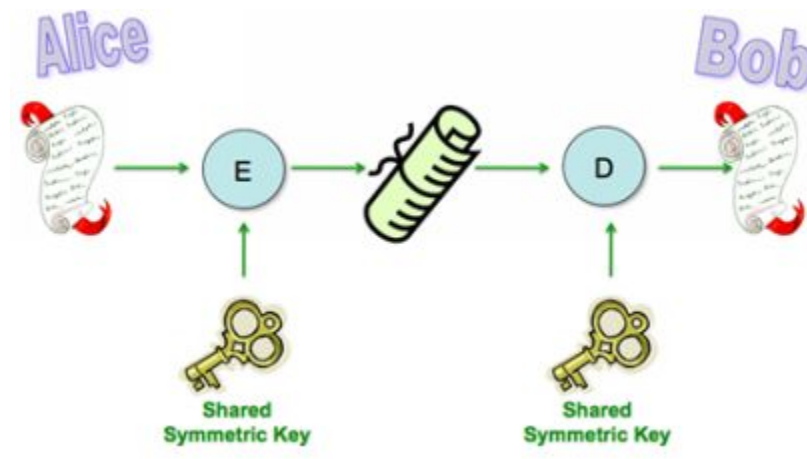


Diagram 17
Symmetric

Cryptography: Asymmetric

Asymmetric systems utilize two mathematically related keys, a private and public key pair, to meet all of the goals of cryptography. In asymmetric systems, one key is used for the encryption function and its mathematical

pair is used for the decryption function. If the private key is used to encrypt, then the associated public key is used to decrypt. The reverse holds true as well. If the private key is used to encrypt then the associated public key is used to decrypt.

If either key can be used for either function, then what determines which key to use and when? The answer is: the goal. If the goal is confidentiality, then the sender will encrypt the data with the receiver's public key. Since the receiver will be the only person with his private key, then he is the only person who can decrypt the data. Thus, the message is confidential.

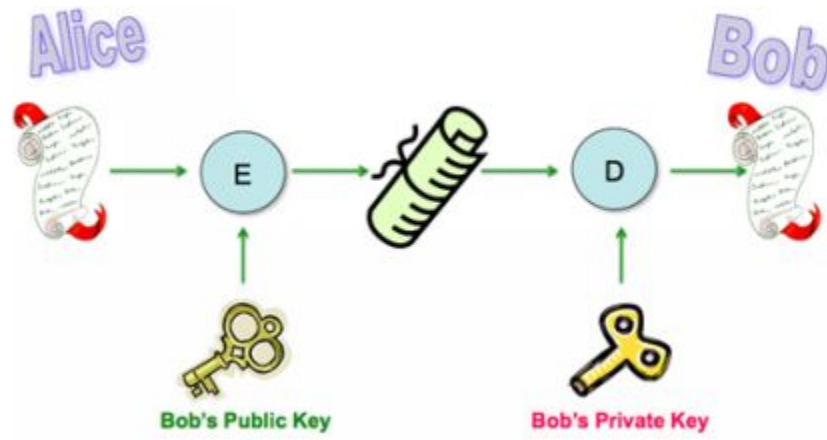


Diagram 18
Asymmetric Confidentiality

If proof of origin is the goal, then the sender will encrypt the data with the sender's private key. Again, only the sender will have this private key. The data can be decrypted by anybody with the associated public key. This method offers no confidentiality because the world has access to the public key so the world could decrypt the data. No matter who decrypts the data, he can be certain of the sender's identity. This is also known as a Digital Signature. Digital signatures, also called electronic signatures, combine asymmetric cryptographic systems with hashing functions to provide proof of origin, integrity, and non-repudiation of the data.

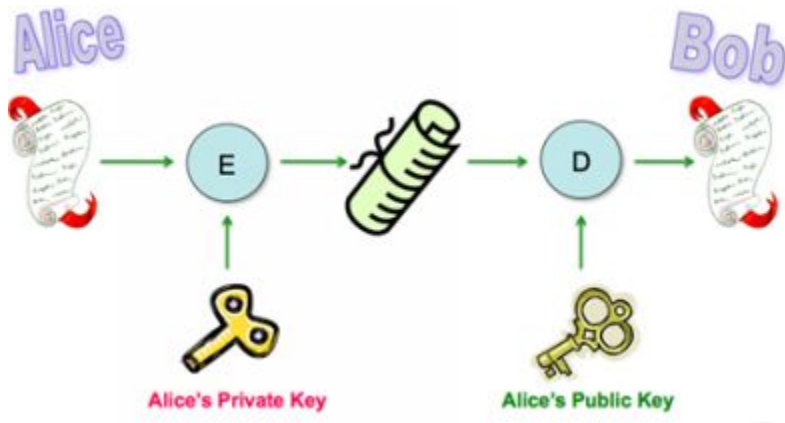


Diagram 19
Asymmetric Proof of Origin/Digital Signature

Digital signatures provide proof of origin and nonrepudiation.

One issue with public keys is how to establish trust in the public key. In other words, how do I know that the public key I have in my hand that has Bob's name on it really belongs to Bob and not some imposter? The answer is certification, which could drive us down the path to Public Key Infrastructure (PKI).

Cryptography: Digital Certificates

A trusted third-party issues digital Certificates. The third party is certifying or attesting to the fact that they have verified the identity of the individual (or organization) and that the public key that is contained within the certificate really does belong to that individual. The key word in the previous statement is "trusted." If I do not trust the third party, then how can I trust the digital certificate issued by them? Following that thought to its logical end, how do I trust the ownership of the public key? I cannot. Therefore, the Public Key Infrastructure (PKI) was created. PKI is the framework of processes and procedures dealing with public key management. PKI provides guidance for third parties pertaining to verifying

identities and issuing digital certificates. If the third party is following the guidelines, then you and I can have a high degree of confidence in the public key we possess.



Diagram 20
CA/RA

A digital certificate is a tool to verify the ownership of a public key as well as the identity of its owner.

Cryptography: Hashing

Hashing functions (not what happens at a Bob Marley concert) are mathematical tools used to protect the integrity of data. Known good data can be run through a hashing function and a hash value, or hash, that represents the known good data will be created. Because a mathematical function is used to create the hash, every time the same data is run through the same hashing function, the same result will happen.

Since the data was known good when the first hash value is created, this value can be used as a baseline. Therefore, through a process of verification, this value can help to identify if the data has been changed in any way. If the data is run through the hash function and a different value

results, then the data is no longer exactly as it was when the first baseline was calculated.

Hashing does not reveal what is different about the data only that it is not the same as when the baseline was created. If we do not know why the data has changed, then we must assume the data is no longer trustworthy and choose not to use it.

Cryptography: SSL/TLS

A very common use of cryptography today is for protecting our online shopping and banking sessions. This is accomplished by using a Virtual Private Network or VPN. A VPN is an encrypted tunnel. In essence, a VPN creates a connection between two entities over a public network, however the VPN makes it appear that the two entities are directly connected to each other on a private network. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are two of the most common VPN technologies used today. They are often used to provide secure web browsing. To initiate these secure VPN, simply type “HTTPS” into the browsers address bar followed by the URL of the site you are visiting. The “S” stands for secure and tells the browser to create an encrypted connection between the browser and the server.

Netscape invented SSL in 1995 with the “primary goal to provide privacy and reliability between two communication applications.” Since the original creation, SSL has gone through several enhancements and it serves as the basis for Transport Layer Security (TLS). Both SSL and TLS utilize a combination of symmetric and asymmetric cryptography as well as hashing.

Symmetric cryptography (e.g., AES, RC4) utilizes secret keys to provide the confidentiality that we crave to protect our sensitive information as it is being transmitted across the Internet. The symmetric key is also known as a session key.

Asymmetric cryptography (e.g., RSA, DSS) provides authentication. A digital certificate is used to verify that the server we think we are talking to really is who we believe it to be. There is a process to achieve that, but that is the first purpose. The second use of the certificate is to provide the public

key, which allows us to send a symmetric key back to the server so that our session can be encrypted.

Hashing algorithms (e.g., SHA, MD5) are used to prove the connection is reliable. A Message Authentication Code (MAC) is used to perform message integrity checks to provide this reliability.



Diagram 21
Basic SSL/TLS exchange

For the exam it is not necessary to be familiar with the intricacies of how TLS works. This is here to aide in understanding only.

Cloud Computing

The “cloud” is a very nebulous concept that is tough for us to grasp, yet we are bombarded everyday by organizations trying to get us to use the cloud. The number one benefit for using the cloud is convenience. If we store our data in the cloud, we can access it from anywhere using any device or application. A second selling feature of the cloud is that we, the users do not have to be bothered with managing and maintaining the

systems that make up the cloud. The service provider will do that for us (for a fee).

Cloud computing is basically delivering large scale computing services on demand. Service providers create large pools of services that can be used by multiple customers, then share the use of those services over a network. Those services are largely available on demand to the personal consumer or small business. Using cloud storage as an example, a consumer can use as much or as little cloud-based storage as their contract allows. If the consumer needs more storage, often a contractual change can be made over the Internet within minutes. There is also a pay as you go pricing model that allows the consumer to pay for what they use without the need for contract changes.

From the provider's perspective, the cloud infrastructure can often be setup by using common off the shelf hardware, and there is no requirement for high end equipment. Multiple low-end computers can be scaled up to achieve the required performance.

Different types of cloud computing services include communication, storage, software, and infrastructure.

- On demand
 - Communication - Original
 - Storage as a Service (SaaS)
 - Software as a Service (SaaS)
 - Platform as a Service (PaaS)
 - Infrastructure as a Service (IaaS)
- Pay as you go
- Easy to add / remove - convenient
- Controlled by others

Cloud Computing: Public Cloud

Cloud computing can be provisioned (provided) in either a public, private or combination format. An external service provider that maintains the infrastructure and sells access and service, often to the general public, offers the public cloud.

- Offered by external service provider
- To the general public
- Some services are free
- Pay for additional

Cloud Computing: Private Cloud

Larger companies may decide to install their own corporate cloud. A private cloud is then available for use by other departments. This offers many of the same benefits as the public cloud, without the worries of having an external third party having potential access to the data. Also, security and maintenance can be controlled by the parent company.

- Offered by parent company or division within the company
- Offers many of the same benefits as public cloud
- Considered a bit more secure because it is controlled by the organization

Cloud Computing: Hybrid Cloud

A hybrid cloud would be a combination of public cloud and a private. The consumer company creates their own private cloud, perhaps for corporate sensitive information, and uses a vendor provided public cloud for less or non-sensitive information. Often during times of lower processing, the private cloud can be used for both, then as requirements intensify, both clouds can be used to augment each other.

One of the major concerns with migrating to a public cloud-based solution hinges on security. Simply put, when a third-party handles data, you lose control. Many of these concerns can be addressed via Service Level Agreements (SLAs), contract clauses, or the use of a private cloud, which maintains the administration of the computers to the local company.

As an example of a security concern, US laws such as HIPAA require Personal Health Information (PHI) to be physically maintained within the US borders.

When making the transition to a cloud-based solution, some of the contractual and service level agreement terms to be worked out are:

- Actual location of the data
- Trans-border issues
- Outsourcing
- Performance
- Reliability
- Compliance
- CIA
- Forensics
- Etc.

Control Selection

Only a few controls have been mentioned here. It is necessary to research all or most controls in order to make a proper selection based on our security program and our risk assessment in order to determine the appropriate controls that we should add to our business.

With some security controls it is necessary to create a contract with a service provider. To ensure that the contract is complete it is a good idea to ensure that we employ the correct type of lawyers to review these contracts. What more than likely needs to be in the contract is a SLA for the specific service that the provider offers. The security within the service providers business and specifically how they will handle our system or information needs to be clarified and later verified.

Summary

A security strategy and program (Chapter one) based on a risk assessment (Chapter two) allows us to create the actual structure of our security program by selecting and implementing the appropriate security controls (this chapter, Chapter three). Information Security Program Development and Management is about taking a high-level risk-based plan and implementing it within the organization.

Information Security Program Development begins with affirming that the program will reflect the business objectives and meet the identified

security requirements. One of the critical components to the success of the program is developing good policy with the appropriate supporting documents. People are your best tool for security information. Policy is how an organization changes the way people think and respond, which creates the culture of the organization. Policy therefore can be thought of as the basis for corporate culture, but only if there is the appropriate level of awareness and training. Organizations must recognize the importance of training and implement it as part of any security program.

Measurement leads to control and improvement. Metrics are our tool for measuring. Careful selection of what to measure, how to measure, when to measure, and who will do the measuring is critical to managing anything, including a security program. Add to that an understanding of why we measured and what to do with the results, and you are beginning to control and improve. Balanced scorecard gives us metrics beyond the common financial measures.

Periodic testing of security measures (including the people) is an essential part of a security program. Policy should be put into place covering the requirement to perform vulnerability assessments, which identify potential vulnerabilities, and penetration tests which go one step farther and attempt to exploit vulnerabilities. These tests should be done at regular intervals and the results used to modify and improve current security procedures.

Auditing can be either internal or external. Auditing is not a control, but rather a test to see if the current controls are effective and being implemented correctly. Auditing can be done either internally or externally.

There are many emerging trends that a future CISM needs to be aware of. One of the biggest today seems to be bringing your own mobile device to work or BYOD. The risk of unowned/managed devices being used to access corporate data must be weighed against the “free” assets that an employee might bring with them into the workplace. Consideration must be given to how to handle personal devices prior to allowing them to access your data. Clear policies must be in place as well.

Cryptography is becoming an essential tool for all organizations. Symmetric cryptography has one key that is shared between two (or more) parties and has the advantage of being very fast. Asymmetric cryptography has a public and a private key pair for each individual, it is normally slower than symmetric, but has the advantage of being able to create digital signatures. Digital signatures can be used to provide proof of origin and non-repudiation. With asymmetric cryptography, a digital certificate is used to validate the owner of the public key.

Hashing is considered to be a part of cryptography although it is not used to encrypt data. Instead, it is used to create a condensed representation or fingerprint of the data, which can be used to uniquely identify something. Hashing therefore can provide data integrity.

SSL/TLS is a protocol that is a good example of a hybrid cryptography solution. SSL/TLS incorporates all three tools (symmetric, asymmetric, and hashing) to protect data in transit.

Cloud computing is another emerging technology with its own set of advantages and disadvantages. One of the main advantages is that data is available wherever and whenever it is needed. This is also one of the major disadvantages of cloud computing. Controlling access to information and verifying the confidentiality, integrity, and availability of data that is no longer under your direct control requires a high level of trust backed up by contractual obligations.

Chapter 3 Questions

1. The PRIMARY benefit of compliance is:
 1. Increase in fines and penalties
 2. Data breaches will not occur
 3. A higher level of security
 4. Ease of maintenance

2. What action must occur before stakeholders can make risk-based decisions?
 1. The results of risk assessments must be communicated to the stakeholders.
 2. A risk assessment must be conducted.
 3. An information security program must be implemented.
 4. Security awareness training must be conducted on an annual basis.

3. What are the two MAIN reasons for reassessing risk?
 1. It is part of a regular schedule or there has been a significant change to the environment.
 2. It is part of a regular schedule or to meet an audit requirement.
 3. To meet audit requirements or because a change has occurred.
 4. A business unit has been added to the company or to meet a regular schedule.

4. Who in the organization PRIMARILY has the responsibility of information classification?

1. Executive management
 2. Information Owner
 3. Information Security Manager
 4. The information User
5. A security manager can justify security expenditures by creating what?
 1. An awareness program
 2. A risk assessment
 3. A business case
 4. A gap analysis
6. What is the best way to ensure security is represented throughout the organization?
 1. A centralized security department.
 2. There is no absolutely best way. Each organization must decide which approach best fits its corporate culture.
 3. A distributed security department.
 4. A hybrid security department; partly centralized and partly distributed.
7. Security managers must have access to what group of people in order to identify systems and data that require protection?
 1. Stakeholders
 2. Users
 3. Owners
 4. Executive and Board of directors
8. A high-level design that leverages the strengths of individual components while minimizing their weaknesses is known as:

1. A Security Plan
 2. A Security Blueprint
 3. An Enterprise Security Architecture
 4. A Service Oriented Architecture

9. The three main areas a security policy should address are:
 1. Business needs, audit requirements, laws, and regulations
 2. Business needs, laws & regulations, threat environment
 3. Audit requirements, laws & regulations, Information classification
 4. Business needs, information classification, threat environment

10. Who is primarily responsible for developing, disseminating and updating security policies?
 1. The information security manager
 2. The Board of directors
 3. Data owners
 4. A management approved policy owner

11. Step by step instructions for completing a task are known as what?
 1. Standards
 2. Procedures
 3. Policies
 4. Guidelines

12. Who in the organization should receive security awareness training?
 1. Everyone with access to a computer

2. Everyone with access to classified systems or data
 3. Everyone
 4. Security managers
13. In order to maximize the effectiveness of enterprise security efforts, it is recommended that security be:
 1. Made a part of business continuity management
 2. Well integrated into other business processes
 3. Outsourced to security experts
 4. Implemented within the system life cycle
14. What type of security metrics is most useful for risk management?
 1. Fact based
 2. Normative
 3. Qualitative
 4. Quantitative
15. Which of the following is an example of an application security metric?
 1. Number of defects per thousand lines of code (KLOC)
 2. Number of firewall rule changes
 3. Host up time
 4. Mean Time to Recover (MTTR)
16. What is the FIRST step in creating a Balanced Scorecard?
 1. Develop a risk identification system
 2. Determine the risk control strategy
 3. Identify the current Balanced Scorecard goals
 4. Obtain management approval

17. What tool allows the organization to set, track and achieve its information technology business strategies and objectives by using metrics to evaluate various aspects of the business?
1. Zachman Architecture Framework
 2. An IT Balanced Scorecard (BSC)
 3. Sherwood Applied Business Security Architecture (SABSA)
 4. ISO 9001
18. What are the four perspectives used to measure and evaluate IT performance within the Balanced Scorecard (BSC)?
1. Corporate contribution, Customer orientation, Operational excellence, Future orientation
 2. Corporate ethics, Customer satisfaction, IT help desk efficiency, Financial responsibility
 3. Corporate contribution, Customer satisfaction, Operational excellence, Financial responsibility
 4. Corporate contribution, Customer orientation, Fiscal responsibility, Future orientation
19. What is the main difference between vulnerability testing and penetration testing?
1. Vulnerability testing is conducted internally while penetration testing is conducted externally.
 2. Vulnerability testing is completely safe while penetration testing is potentially harmful.
 3. Vulnerability testing identifies potential weaknesses while penetration testing attempts to validate the severity of the weakness.
 4. Vulnerability testing does not require management approval while penetration testing does.

20. A systematic analysis of an organization's policies, practices and procedures and measuring them against a set of industry accepted standards is called:
1. A risk assessment
 2. A vulnerability assessment
 3. A penetration test
 4. An audit
21. What type of audit serves as a self-assessment?
1. Internal audit
 2. External audit
 3. Compliance check
 4. Wellness check
22. What is the basis of due diligence?
1. Security Awareness
 2. A security program championed by senior management
 3. Continued monitoring
 4. Knowledge of applicable laws and regulations
23. What is the key to creating useful security reports?
1. Quantifiable metrics
 2. A qualitative analysis
 3. Lots of graphs with bright colors to hold the reader's attention
 4. Detailed analysis of the risk analysis and handling activities

24. What is the primary advantage of bring your own device (BYOD)?
1. Enhanced security provide by using many different types of devices
 2. Easier configuration management
 3. Significant cost savings
 4. Increased productivity due to employees being more familiar with using a device that they own and choose
25. In what type of environment will personal devices usually be prohibited?
1. Medical environments
 2. Data centers
 3. Research and development environments
 4. Those environments that do the highest level of processing
26. What type of cryptography is best suited for creating a digital signature?
1. Symmetric
 2. Asymmetric
 3. Hashing
 4. Both symmetric and asymmetric systems can create digital signatures
27. What are the four main goals of cryptography?
1. Protect Intellectual Property (IP), Verify message source, integrity, non-repudiation
 2. Access control, confidentiality, integrity, and availability
 3. Confidentiality, proof of origin, integrity, and non-repudiation

4. Confidentiality, integrity, availability, and authentication

28. Which of the following is an example of a symmetric cryptographic algorithm?

1. Rivest, Shamir, Adelman (RSA)
2. Advanced Encryption Standard (AES)
3. Diffie-Hellman (DH)
4. FIPS-200

29. What is the result of first hashing a message and then encrypting that hash using a private key?

1. A digital signature
2. A confidential message
3. A message digest
4. A security baseline

30. Which of the following statements is MOST true about asymmetric encryption systems?

1. The sender's public key is used to encrypt the message and the sender's private key is used to decrypt the message when confidentiality is the goal.
2. The receiver's private key is used to encrypt the message and the receiver's public key is used to decrypt the message when confidentiality is the goal.
3. The receiver's public key is used to encrypt the message and the receiver's private key is used to decrypt the message when Integrity is the goal.
4. The receiver's public key is used to encrypt the message and the receiver's private key is used to decrypt the message when confidentiality is the goal.

31. When a certificate authority (CA) issues a digital certificate, what are they attesting to?
1. They are attesting to the fact that the digital signature is valid.
 2. They are attesting to the fact that the private key and public key are mathematically linked together.
 3. They are attesting to the fact that they have verified the identity of the individual and that the public key contained in the certificate does belong to that individual.
 4. They are attesting to the fact that the private key that is associated with the public key has NOT been compromised.
32. What is the framework for managing public keys?
1. Public Key Infrastructure (PKI)
 2. Certificate Practices Statement (CPS)
 3. Certificate Revocation
 4. Private Key Infrastructure
33. What organization is responsible for issuing digital certificates and maintaining a status on those certificates?
1. Internet Assigned Numbers Authority (IANA)
 2. International Organization for Standardization (ISO)
 3. Registration Authority (RA)
 4. Certification Authority (CA)
34. In a web communication, how does the user instruct the web browser to initiate a secure connection using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to the server?

1. Type SHTTP into the address bar followed by the URL of the site to connect to.
2. Select the secure option in the internet browser settings
3. Type HTTPS into the address bar followed by the URL of the site to connect to.
4. Type either ".ssl" or ".tls" at the end of the address

35. What is the primary benefit of cloud computing for the users?

1. Free applications
2. Convenience
3. Managed services
4. Security is enhanced

36. When making purchasing decisions for information security controls these investments should be based on

1. auditor recommendations
2. cost vs. benefit analysis
3. current security attackers
4. security manager recommendations

37. A well written statement regarding a company's privacy policy will include

1. what the company will specifically do with the information it collects
2. a notification regarding the companies liability on accuracy of information.
3. the information classification process a company follows.

4. a notification of how a company will encrypt sensitive information.

38. When confirming the effectiveness of information security controls, it is best to review

1. User rights
2. Returns on security investments
3. Security metrics
4. Risk policies

Chapter 3 Questions with Answers and Explanations

1. The PRIMARY benefit of compliance is:
 1. Increase in fines and penalties
 2. Data breaches will not occur
 3. **A higher level of security**
 4. Ease of maintenance

Explanation

Answer C: A higher level of security is the most likely outcome of compliance. Fines should be decreased or eliminated if compliance is achieved. Data breaches will still occur but should be less likely and less severe. Compliance does not guarantee ease of maintenance.

2. What action must occur before stakeholders can make risk-based decisions?
 1. The results of risk assessments must be communicated to the stakeholders.
 2. **A risk assessment must be conducted.**
 3. An information security program must be implemented.
 4. Security awareness training must be conducted on an annual basis.

Explanation

Answer B: As stakeholders do not do the risk assessment, although their knowledge is invaluable in the process, they cannot make decisions without the final risk assessment information. The risk assessment must be conducted for that to be able to happen. Once that happens the program can be created and implemented and then awareness training can be conducted.

3. What are the two MAIN reasons for reassessing risk?
1. **It is part of a regular schedule or there has been a significant change to the environment.**
 2. It is part of a regular schedule or to meet an audit requirement.
 3. To meet audit requirements or because a change has occurred.
 4. A business unit has been added to the company or to meet a regular schedule.

Explanation

Answer A: Reassessing risk should be done on a regularly scheduled interval as defined in policy and when significant changes have occurred. It is not normal to do an assessment because an audit is coming. A business unit being added would be a significant change.

4. Who in the organization PRIMARILY has the responsibility of information classification?
1. Executive management
 2. **Information Owner**
 3. Information Security Manager
 4. The information User

Explanation

Answer B: The information owner is responsible for the classification of the data that they own. Executive management is responsible for all security in the business, the infosec manager is responsible for getting all security done and the information user is responsible for following policy when using the data.

5. A security manager can justify security expenditures by creating what?
1. An awareness program
 2. A risk assessment
 3. **A business case**
 4. A gap analysis

Explanation

Answer C: A business case presents the risks, the cost benefit analysis, the benefits of a specific security control. An awareness program will help everyone understand security. A risk assessment needs to be done in order to build a business case. A gap analysis examines the difference between current and desired state, which could be used to help build a business case.

6. What is the best way to ensure security is represented throughout the organization?
1. A centralized security department.
 2. **There is no absolutely best way. Each organization must decide which approach best fits its corporate culture.**
 3. A distributed security department.
 4. A hybrid security department; partly centralized and partly distributed.

Explanation

Answer B: Same as all elements of business there is no right way to do it. The manner selected must match the business and its needs. Centralized, distributed and hybrid are valid options, options is the key word.

7. Security managers must have access to what group of people in order to identify systems and data that require protection?
1. **Stakeholders**
 2. Users
 3. Owners
 4. Executive and Board of directors

Explanation

Answer A: The stakeholders have knowledge and insights that is invaluable in understanding the criticality of systems and data that users, owners, the executive suite, and the board of directors may not have.

8. A high-level design that leverages the strengths of individual components while minimizing their weaknesses is known as:
1. A Security Plan
 2. A Security Blueprint
 3. **An Enterprise Security Architecture**
 4. A Service Oriented Architecture

Explanation

Answer C: To architect is to design. An architecture is a design. A security architecture is the high-level design of the security in the enterprise that allows strengths to minimize weaknesses. Service oriented architecture would perform a similar job, but it is for services specifically. The plan is the actual security to be implemented. Blueprint is another name for industry best practices such as ISO 27002.

9. The three main areas a security policy should address are:
1. Business needs, audit requirements, laws, and regulations
 2. **Business needs, laws & regulations, threat environment**
 3. Audit requirements, laws & regulations, Information classification
 4. Business needs, information classification, threat environment

Explanation

Answer B: A policy above all else needs to assist in forwarding the business by supporting the business needs. Applicable law and regulations need to be addressed from the top level of security with the policy. The threat environment must be addressed to ensure that the proper security controls are in place. Audit requirement and information classification are too detailed to be in the policy. They should be addressed in other documents.

10. Who is primarily responsible for developing, disseminating and updating security policies?
1. The information security manager
 2. The Board of directors
 3. Data owners
 4. **A management approved policy owner**

Explanation

Answer D: The information security manager is not a bad answer, but management approved policy owner is more specific. That person could be the information security manager. The board of directors does not disseminate policies and the data owner is to follow those policies.

11. Step by step instructions for completing a task are known as what?
1. Standards
 2. **Procedures**
 3. Policies
 4. Guidelines

Explanation

Answer B: Procedures are step-by-step instructions. Standards are specific solutions/controls. Policies communicate goals and objectives, and guidelines are good ideas.

12. Who in the organization should receive security awareness training?
1. Everyone with access to a computer
 2. Everyone with access to classified systems or data
 3. **Everyone**
 4. Security managers

Explanation

Answer C: Just as everyone in the company has a security responsibility, everyone needs to be aware of their security

responsibilities, at a minimum everyone needs awareness training, some require training and or education.

13. In order to maximize the effectiveness of enterprise security efforts, it is recommended that security be:
1. Made a part of business continuity management
 2. **Well integrated into other business processes**
 3. Outsourced to security experts
 4. Implemented within the system life cycle

Explanation

Answer B: If security is well integrated into other business processes it would then be implemented into the SDLC and into business continuity management. Outsourcing security is irrelevant here. Outsource if needed, do not if it is not.

14. What type of security metrics is most useful for risk management?
1. Fact based
 2. Normative
 3. Qualitative
 4. **Quantitative**

Explanation

Answer D: Metrics need to be specific and measurable. Quantitative is numeric based making it very measurable. Qualitative does not involve measurable numbers. Facts are good to always work with, but that and normative are not types of metrics.

15. Which of the following is an example of an application security metric?
1. **Number of defects per thousand lines of code (KLOC)**
 2. Number of firewall rule changes
 3. Host up time

4. Mean Time to Recover (MTTR)

Explanation

Answer A: Defects in the code is a metric specific to applications. A firewall and a host are machines, they do require software or applications, but the rules and the up time is not a measure of the application. Same for the MTTR, that speaks to the recovery of a device (maybe the software/application) but not a security metric for the software.

16. What is the FIRST step in creating a Balanced Scorecard?
1. Develop a risk identification system
 2. Determine the risk control strategy
 3. **Identify the current Balanced Scorecard goals**
 4. Obtain management approval

Explanation

Answer C: If the goals are identified then the system and strategy can be identified. With a solid plan in place management approval is possible.

17. What tool allows the organization to set, track and achieve its information technology business strategies and objectives by using metrics to evaluate various aspects of the business?
1. Zachman Architecture Framework
 2. **An IT Balanced Scorecard (BSC)**
 3. Sherwood Applied Business Security Architecture (SABSA)
 4. ISO 9001

Explanation

Answer B: The question is a good description of IT BSC. Zachman is used to be able to describe complex situations. SABSA is used to develop security architectures. ISO 9001 is for total quality management (TQM).

18. What are the four perspectives used to measure and evaluate IT performance within the Balanced Scorecard (BSC)?
1. **Corporate contribution, Customer orientation, Operational excellence, Future orientation**
 2. Corporate ethics, Customer satisfaction, IT help desk efficiency, Financial responsibility
 3. Corporate contribution, Customer satisfaction, Operational excellence, Financial responsibility
 4. Corporate contribution, Customer orientation, Fiscal responsibility, Future orientation

Explanation

Answer A: The four perspectives in IT BSC are corporate contribution, customer orientation, operational excellence, and future orientation. What is not one of those perspectives is corporate ethics, helpdesk efficiency, customer satisfaction, financial responsibility, or fiscal responsibility.

19. What is the main difference between vulnerability testing and penetration testing?
1. Vulnerability testing is conducted internally while penetration testing is conducted externally.
 2. Vulnerability testing is completely safe while penetration testing is potentially harmful.
 3. **Vulnerability testing identifies potential weaknesses while penetration testing attempts to validate the severity of the weakness.**
 4. Vulnerability testing does not require management approval while penetration testing does.

Explanation

Answer C: Vulnerability assessments do not take that last step of trying to exploit those vulnerabilities. Damage can still be caused in a vulnerability assessment so it must also have management approval. Either can be done with internal or external teams.

20. A systematic analysis of an organization's policies, practices and procedures and measuring them against a set of industry accepted standards is called:
1. A risk assessment
 2. A vulnerability assessment
 3. A penetration test
 4. **An audit**

Explanation

Answer D: The question is a good definition of an audit, where a pen test is not an analysis of policies, but rather an intrusive test of the environment. A vulnerability assessment looks for weaknesses or flaws in the environment, not policies. A risk assessment is also not a review of policies, but a deep analysis of how bad things could be when things go wrong.

21. What type of audit serves as a self-assessment?
1. **Internal audit**
 2. External audit
 3. Compliance check
 4. Wellness check

Explanation

Answer A: Self-assessment is done by your self - an internal audit, it cannot be an external audit. The question is about audits, so compliance check and wellness checks are not the best answer to an audit.

22. What is the basis of due diligence?
1. Security Awareness
 2. A security program championed by senior management
 3. **Continued monitoring**
 4. Knowledge of applicable laws and regulations

Explanation

Answer C: Diligence is careful and persistent work. Security awareness is a part of due diligence possibly. Management championing the security program is not persistent work that needs to be applied to the program. Being knowledgeable about the laws might be an activity within due diligence.

23. What is the key to creating useful security reports?
1. **Quantifiable metrics**
 2. A qualitative analysis
 3. Lots of graphs with bright colors to hold the reader's attention
 4. Detailed analysis of the risk analysis and handling activities

Explanation

Answer A: Security reports that are useful require actionable and understandable details. Metrics should be those details. Qualitative is too subjective for a security report. Lots of graphics can be good, but they should be about quantifiable metrics. This is the wrong place for risk analysis activities.

24. What is the primary advantage of bring your own device (BYOD)?
1. Enhanced security provided by using many different types of devices
 2. Easier configuration management
 3. **Significant cost savings**
 4. Increased productivity due to employees being more familiar with using a device that they own and choose

Explanation

Answer C: BYOD has the advantage of cost savings for a business since they would then not have to purchase phones, tablets, laptops, etc. What it does not provide is enhanced security or easier management. One could hope that productivity would increase, but

that is often not the case, especially when the user chooses to upgrade to a newer, better device.

25. In what type of environment will personal devices usually be permitted?
1. Medical environments
 2. Data centers
 3. Research and development environments
 4. **Business offices**

Explanation

Answer D: Personal devices are most prohibited around extremely sensitive or highly classified data. The ability to control these devices is limited today. To ensure sensitive data is not compromised it is best to prohibit personal devices. These locations could include medical environments, data centers, or R&D environments.

26. What type of cryptography is best suited for creating a digital signature?
1. Symmetric
 2. **Asymmetric**
 3. Hashing
 4. Both symmetric and asymmetric systems can create digital signatures

Explanation

Answer B: In order to create a digital signature something (typically a hash) is encrypted with someone's private key. Asymmetric is comprised of a public / private key pair. Symmetric has a single key shared between receiver and sender for confidentiality. Hashing is for integrity checks only.

27. What are the four main goals of cryptography?
1. Protect Intellectual Property (IP), Verify message source, integrity, non-repudiation

2. Access control, confidentiality, integrity, and availability
3. **Confidentiality, proof of origin, integrity, and non-repudiation**
4. Confidentiality, integrity, availability, and authentication

Explanation

Answer C: Confidentiality, proof of origin, integrity and non-repudiation are possible with cryptography. Protecting intellectual property is one of the things that can be protected by cryptography, but only one. Access control and authentication are not done by cryptography.

28. Which of the following is an example of a symmetric cryptographic algorithm?
1. Rivest, Shamir, Adelman (RSA)
 2. **Advanced Encryption Standard (AES)**
 3. Diffie-Hellman (DH)
 4. FIPS-200

Explanation

Answer B: AES is symmetric. RSA and DH are asymmetric. FIPS-200 is a US government document.

29. What is the result of first hashing a message and then encrypting that hash using a private key?
1. **A digital signature**
 2. A confidential message
 3. A message digest
 4. A security baseline

Explanation

Answer A: Digital signatures are created by hashing something and then encrypting the hash output. The hash output is also known as

a message digest. This process does not provide any confidentiality. A security baseline is a document.

30. Which of the following statements is MOST true about asymmetric encryption systems?
1. The sender's public key is used to encrypt the message and the sender's private key is used to decrypt the message when confidentiality is the goal.
 2. The receiver's private key is used to encrypt the message and the receiver's public key is used to decrypt the message when confidentiality is the goal.
 3. The receiver's public key is used to encrypt the message and the receiver's private key is used to decrypt the message when Integrity is the goal.
 4. **The receiver's public key is used to encrypt the message and the receiver's private key is used to decrypt the message when confidentiality is the goal.**

Explanation

Answer D: Encrypting with a public key of the sender does not make sense. You would use the receiver's public key. If you encrypt with the receiver's private key, there are major problems, and the keys are now compromised. If you encrypt with the receiver's public key you achieve confidentiality, not integrity. So, the only valid statement is encrypted with the receiver's public key for confidentiality.

31. When a certificate authority (CA) issues a digital certificate, what are they attesting to?
1. They are attesting to the fact that the digital signature is valid.
 2. They are attesting to the fact that the private key and public key are mathematically linked together.
 3. **They are attesting to the fact that they have verified the identity of the individual and that the public key contained in the certificate does belong to that individual.**

4. They are attesting to the fact that the private key that is associated with the public key has NOT been compromised.

Explanation

Answer C: Certificate authorities are responsible for verifying (attesting) to the owner of the certificate being the owner of the certificate. They are not promising that the private key has not been compromised. They are not attesting to the mathematical linkage of the private and public keys, as that is simply how asymmetric works. They are also not proving that digital signatures are valid, that requires work by applications or users.

32. What is the framework for managing public keys?
 1. **Public Key Infrastructure (PKI)**
 2. Certificate Practices Statement (CPS)
 3. Certificate Revocation
 4. Private Key Infrastructure

Explanation

Answer A: PKI is a framework or infrastructure for managing public keys. PKI does require CPS and certificate revocation pieces. PKI stands for Public key not Private key.

33. What organization is responsible for issuing digital certificates and maintaining a status on those certificates?
 1. Internet Assigned Numbers Authority (IANA)
 2. International Organization for Standardization (ISO)
 3. Registration Authority (RA)
 4. **Certification Authority (CA)**

Explanation

Answer D: CAs issue certificates. RAs verify identity of the owners. ISO creates international standards for oh so many things. IANA issues IP addresses.

34. In a web communication, how does the user instruct the web browser to initiate a secure connection using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to the server?
1. Type SHTTP into the address bar followed by the URL of the site to connect to.
 2. Select the secure option in the internet browser settings
 3. **Type HTTPS into the address bar followed by the URL of the site to connect to.**
 4. Type either ".ssl" or ".tls" at the end of the address

Explanation

Answer C: HTTPS is the first part to an address that indicates the use of SSL or TLS. SHTTP is not seen in an address bar. .ssl or .tls is not a proper ending to an address. A secure option will not setup SSL or TLS for a specific web session.

35. What is the primary benefit of cloud computing for the users?
1. Free applications
 2. **Convenience**
 3. Managed services
 4. Security is enhanced

Explanation

Answer B: The benefit of cloud services is convenience for the users especially if they can access the data or service from anywhere. Security is not a benefit for the user; it is a concern for InfoSec. Managed services might be a benefit to management. Free applications might be a benefit, but for the home user not a corporate user.

36. When making purchasing decisions for information security controls these investments should be based on
1. auditor recommendations
 2. **cost vs. benefit analysis**
 3. current security attackers
 4. security manager recommendations

Explanation

Answer B: Investments should always be made based on cost vs. benefit analysis. Auditors are responsible for determining the current level of security based on something like ISO 27001. Determining investments based on attackers is irresponsible since a business may already have proper controls in place. Finally, the security manager should make recommendations based on cost vs. benefit but the direct answer to the question is the cost vs. benefit.

37. A well written statement regarding a company's privacy policy will include

1. **what the company will specifically do with the information it collects**
2. a notification regarding the company's liability on accuracy of information.
3. the information classification processes a company follows.
4. a notification of how a company will encrypt sensitive information.

Explanation

Answer A: Privacy statement should communicate to their users and customers what they can expect the company will do with their data. The policy contains liability, accuracy, classification, and encryption details.

38. When confirming the effectiveness of information security controls, it is best to review

1. User rights
2. Returns on security investments
3. **Security metrics**
4. Risk policies

Explanation

Answer C: Metrics are used to show us the facts of effectiveness of controls. User rights, ROI, and policies will not show effectiveness.

Chapter 4

Domain 4 information security incident management 19% of the Exam

According to ISACA, in this domain, you will:

Plan, establish and manage the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact.

A CISM candidate must be able to perform the following ten task statements:

- 4.1, Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate classification and categorization of and response to incidents.
- 4.2, Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.
- 4.3, Develop and implement processes to ensure the timely identification of information security incidents that could impact the business.
- 4.4, Establish and maintain processes to investigate and document information security incidents in order to determine the appropriate response and cause while adhering to legal, regulatory and organizational requirements.
- 4.5, Establish and maintain incident notification and escalation processes to ensure that the appropriate stakeholders are involved in incident response management.
- 4.6, Organize, train and equip incident response teams to respond to information security incidents in an effective and timely manner.
- 4.7, Test, review and revise (as applicable) the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities.

- 4.8, Establish and maintain communication plans and processes to manage communication with internal and external entities.
- 4.9, Conduct post-incident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.
- 4.10, Establish and maintain integration among the incident response plan, business continuity plan and disaster recovery plan.

A solid understanding of the following 18 knowledge statements should be attained by a CISM candidate:

- k4.1, Knowledge of incident management concepts and practices.
- k4.2, Knowledge of the components of an incident response plan.
- k4.3, Knowledge of business continuity planning (BCP) and disaster recovery planning (DRP) and their relationship to the incident response plan.
- k4.4, Knowledge of incident classification/categorization methods.
- k4.5, Knowledge of incident containment methods to minimize adverse operational impact.
- k4.6, Knowledge of notification and escalation processes.
- k4.7, Knowledge of the roles and responsibilities in identifying and managing information security incidents.
- k4.8, Knowledge of the types and sources of training, tools and equipment required to adequately equip incident response teams.
- k4.9, Knowledge of forensic requirements and capabilities for collecting, preserving and presenting evidence (e.g., admissibility, quality and completeness of evidence, chain of custody).
- k4.10, Knowledge of internal and external incident reporting requirements and procedures.
- k4.11, Knowledge of post-incident review practices and investigative methods to identify root causes and determine corrective actions.
- k4.12, Knowledge of techniques to quantify damages, costs and other business impacts arising from information security incidents.

- k4.13, Knowledge of technologies and processes to detect, log, analyze and document information security events.
- k4.14, Knowledge of internal and external resources available to investigate information security incidents.
- k4.15, Knowledge of methods to identify and quantify the potential impact of changes made to the operating environment during the incident response process.
- k4.16, Knowledge of techniques to test the incident response plan.
- k4.17, Knowledge of applicable regulatory, legal and organization requirements.
- k4.18, Knowledge of key indicators/metrics to evaluate the effectiveness of the incident response plan.

Introduction to Information Security Incident Management

One of the most important things that we must do is to be ready to respond to problems. Things happen - laptops are stolen, servers are hacked, networks are crashed, PII is stolen, and on and on. This author considers this a fundamentally depressing domain. We must consider the worst of the worst and plan for how to respond so that we can not only survive but minimize the impact to our people and our businesses. In chapter 2 we did a lot of work looking at how to conduct a risk assessment. Risk assessments are the foundation that we will build upon to determine what are the worst problems that we need to be prepared to handle using Business Continuity Plans (BCP), Disaster Recovery Plans (DRP) and Incident Response Plans (IRP). The good news is that once we create the IR/BC/DR capabilities we can return to a less depressing level of thought so long as we watch the environment for changes and practice, practice, practice our plans so that they will work when needed.

Our first question to address is what is the difference between IRP, BCP and DRP. There are several sources that provide varying explanations as to what these plans are and how they relate to each other. We prefer the definitions provided by the National Institute of Standards and Technology. They are below: **Incident Response (IR)**

First an incident is defined as: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

-NIST SP 800-50

Another way to say this is: an event is an observable occurrence while an incident is an adverse event.

The incident response plan is the detailed operational component that specifies the actions, personnel and activities that will take place when there is an incident occurring, or when one has recently occurred.

Business Continuity Plan (BCP)

A BCP is: The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business functions will be sustained during and after a significant disruption. - *NIST SP 800-50*

A BCP is specifically designed to keep the critical business processes functioning.

Disaster Recovery Plan (DRP)

A DRP is: A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. -*NIST SP 800-50*

A quick, simple comparison: BCP pertains to business functions whereas DRP is specifically dealing with Information Technology failures.

Plan Comparison

These plans, though they are designed to address different types of problems, are fundamentally remarkably similar to each other. Likewise, they are interwoven in many respects. So, if they are similar and even interwoven together, then why are there three different plans to begin with? Why not just have one?

To answer those questions, it might help to ask yet another question. What exactly has happened? The type of adverse event, the scope of the event and the impact of the event will dictate which of these specific documents/plans should be utilized. The titles for these documents provide us with insight both to the utility of the documents as well as to the severity of the incident.

Fundamentally the process to create the documents is the same. In fact, we have discussed this process already with PDCA - Plan, Do, Check and Act. We plan carefully, create a document, implement it and check to ensure that it will actually work then take actions to fix the holes in our plan.

Example of Incidents include:	Examples of Disasters include:	Example of Business Continuity issues include:
A virus on a computer	A fire in our data center	A critical database has crashed
Employee fraud	The data center has flooded due to heavy rains	A riot has prevented all employees from entering the HQ building
A file has been accidentally deleted	A hard drive failure has caused a cascaded issue with the routers on the network	The gaming network for a large company has been shutdown due to an attack
The joke of the day server crashed	The phone lines to a call center fail due to a cable dig that forces calls to be redirected to an alternate facility	A large bank must undergo an upgrade so that they are prepared for tax season that takes online banking down
A single cash register out of 50	Complete Internet failure	A SCADA (Supervisory Control and

within a single store crashed		Data Acquisition) system has failed
An employee fails to show to work because the area that they live in is in lockdown	“Glitches” with the roll out of new e-commerce site	A nuclear reactor has an electrical issue that cause the reactor to go offline.

Table 3
IR/BC/DR Events

Organization must define exactly what constitutes an incident, an interruption, and a disaster relative to the specific business of that organization. We must also determine where the dividing lines are between incidents or disasters or business continuity issues. The severity of the event will often be the deciding factor as to which plan, or plans need to be invoked.

In a real-life situation, when an event occurs, the organization must have a capability to detect the behavior, categorize it and then to execute the correct plan. Initially, incident response may be the only plan to execute. However, the longer the incident goes on, the more likely that the business continuity and or disaster recovery plans will also need to be executed. Additionally, during an incident, many components of the organization may be involved and impacted. There must be a way to prioritize actions and responses. All these things will be pre-planned and defined in the organization's documentation.

The documents or plans are not sufficient. We must also have well trained personnel with the right tools at their disposal with proper plans for recovery in place so that they will be successful in returning us to a normal working condition.

Senior Management Commitment

The starting point with any of these plans, or for security in general as you may have noticed it mentioned before in this study guide, is that we must have senior management's commitment. If senior management does

not understand the importance of responding and responding quickly and effectively to bad things that happen to us it will not be possible to get the people, time, and budget to create these plans.

From Senior Management we will need them to create/sign off on the policy that is specific to incidents, disasters and business continuity issues. This will provide us with their goals and objectives, specify what they believe to be their most important assets and provide strategic guidance.

Personnel

Having the right people involved in creating these plans is critical. Actual title can vary a bit, especially when you compare teams that are building the different types of plans. The knowledge and skills that we need to assemble include:

- Knowledge of the business and ALL of its critical functions, processes, equipment, personnel, etc.
- Knowledge of incident response/disaster recovery/business continuity plan building
- A strong team leader to take this project to successful completion
- Knowledge of the needed technical skills
- Personnel skills from communication to team building to problems solving

An incident response team consists of several players each with specific duties assigned. Each player of the team has specific duties, and the division of responsibilities is designed to maximize the effectiveness of the team. Some of the team members you might have on your team are:

- Incident response Manager
- Deputy IR manager
- Watch commander
- Network specialists
- Windows experts
- Unix / Linux experts
- Mobile device experts
- Communications specialists

- Forensics experts
- Others

When creating an IR team(s), the team structure of the team is important as well. Some questions to answer are:

- Will we have a central IR team or a distributed IR team? The larger the business the more likely we will need a distributed team.
- Will we have people dedicated to IR or will our responders have other primary responsibilities and IR is just a collateral duty?
- Will any of our incident response be outsourced? If so, which parts? How do we activate the third-party responders?
- How will the IR activities be coordinated?

IR Objectives

Incident response is a critical function within a company. The basic objective of IR is:

- Protect - The best choice is to not have a negative event. But, despite our best efforts at prevention we must be prepared for incidents to happen, because they will.
- Prepare - Get the right training, put the right tools in place and practice response steps.
- Detect - Perhaps the most critical step. This may be the hardest part of incident response today. We must detect that something has happened within our business. This requires a combination of the right tools and the right skills. If we know that an incident of some kind is occurring or has occurred, we can take the appropriate steps.
- Triage - The first step past detection is triage. Triage is a good medical term that means that we must prioritize and categorize so that we respond properly.
 - Categorize - What type of attacks? What types of systems and information is affected? Is it a single system or multiple systems? A single location or

- multiple? does it affect business critical systems or support systems?
 - Prioritize - What should we respond to first, second, third and so on?
- Respond - The response must be carefully performed. The response must stop the incident from progressing (if necessary), find the source of the incident, identify the damage, restore everything to a normal state and make sure the same type of incident cannot occur in the future.
- Contain the damage - If the incident cannot be immediately stopped, steps should be taken to contain and minimize the damage.
- Stop the attack - Corrective actions to stop the incident from continuing.
- Determine the source of the attack - Where did the attack come from? What kind of attack was this?
- Determine the full effect of the attack - Exactly what has been compromised and how it was compromised must be determined.
- Gather evidence - This may have started at the very beginning of the response steps but if it will be necessary to explain in a court of law what has happened evidence will be needed.
- Recover - Return all systems to a normal status.

An Incident Response Plan must be created so that the IRT knows what to do, when and how to do it.

Things to make sure we include in the IRT:

- Notification Process
- Escalation Process
- Help desk process for identifying incidents
- Response Teams

Gap Analysis

A gap analysis between the existing skills and technology that we have and the skills and technologies that we need must be done. Once we have

determined what we are missing we can take the appropriate actions to close the gap.

Lessons Learned

At the end of all incidents (or disasters or business continuity issues) the team members and possibly others should sit down and review what happened. The objective is to learn from what we did well and where we can improve for the next time. Other names for this step include postmortems, debriefing, after action review.

Incident Systems and Tools

The Incident Response Team must have the appropriate tools at their disposal. Without the right tools, there is no way to achieve the IR objectives. There are several categories of tools available. Some of the tools are generic in nature providing a lot of information about a lot of events. These tools often provide the early warning of an incident. Other tools are dedicated to a specific purpose. They allow the responder to dive deep into the incident to gather the necessary information to successfully remedy the situation.

However, tools are only a part of the equation, the team must be well trained in the proper use of these tools and they must have the necessary experience and familiarization to effectively put the tool to use. One other particularly important note; they must have proper authorization to employ the tool.

Incident Systems and Tools: Intrusion Detection System (IDS)

An IDS is a passive device that has the job of detecting an attack and raising the alarm when it sees one. An IDS is typically sitting on the sideline watching and reporting the bad behavior. This is the older of the two devices (IDS vs. IPS) and you really must be careful when purchasing equipment from a vendor because it may be called an IDS and perform IPS functionality or vice versa.

Incident Systems and Tools: Intrusion Prevention System (IPS)

An IPS is an active device with the responsibility of seeing an attack/intrusion happening and take immediate action to stop the attack. An IPS is typically sitting in line with the communication. When the IPS sees an attack it prevents the attack from continuing any further.

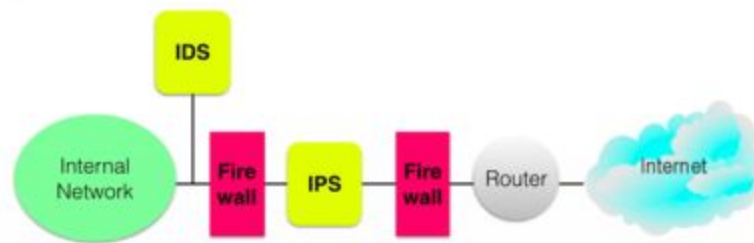


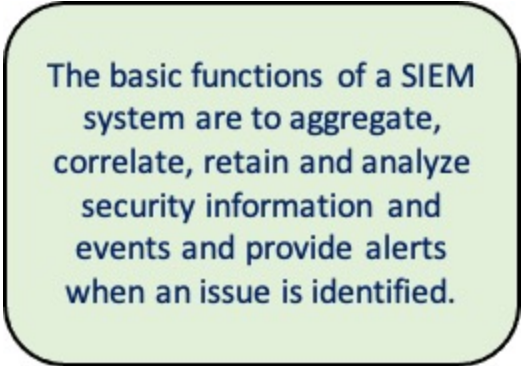
Diagram 22
IDS & IPS Differences

Incident Systems and Tools: IDS and IPS

IDS and IPS both come in network based and host-based versions. The terms are probably obvious, but just to be clear; network-based systems would be in the firewall, router, switch or sitting beside them. Host based devices are in the end device connected to the network such as a PC, server, laptop, tablet, mobile device, etc.

Both IDS and IPS devices create logs, which can be extremely important to the IRT. There is no way to respond appropriately without knowing what is happening or has happened. A log is an invaluable tool for this knowledge. The problem with these logs is twofold: 1) the log files are enormous 2) the logs must be read and analyzed. This makes it exceedingly difficult for a human to perform a manual log analysis. There was a day when that was possible because the files were small enough, but not anymore. So now we need another tool, a Security Information and Event Manager (SIEM) **Incident Systems and Tools: Security Information and Event Manager (SIEM)**

A SIEM fulfills on the need to gather log data from disparate sources as well as packet captures and provides a centralized location for storing, analyzing, and presenting the information in a uniform manner. The SIEM will then normalize the information from all these disparate sources and then it is analyzed for the purpose of identifying security incidents, monitoring user activity, or monitoring compliance. It is still especially important that the IRT is trained on how to read the output information from the SIEM. This is not an end all answer, it is a tool, it must be used properly.



The basic functions of a SIEM system are to aggregate, correlate, retain and analyze security information and events and provide alerts when an issue is identified.

Incident Systems and Tools: Protocol Analyzers

A protocol analyzer is a critical tool when analyzing network traffic, following the flow of the packets, the flow of the information and the source and destination of the traffic. It is extremely critical that the IRT is trained on network protocols to be able to utilize this tool.

These tools will allow an incident response team to “see” into the network and its devices. With that information they should be able to understand what is happening and how to respond.

A tremendous cost savings can be realized by proper implementation of these tools. The savings add up when we consider the money saved by quickly catching the attacks, reducing the downtime, and taking actions to minimize the damage as well averting potential fines and penalties that may be applicable.

IRT Training

Training of the IRT staff is one of the keys to success. There are many technical skills that they really must have in order to be effective. There have been so many things listed already for training needs through the first 3 domains, with the IRT we have at least listed the need to be trained on IDS, IPS, SIEM and protocol analyzers. Additional topics that they should really be trained on include:

- Vulnerabilities

Understanding vulnerabilities within a system or environment allows the IRT to be able to understand how an attack could be happening.

- Networking

The IRT should understand networking protocols, how they work and what specific attacks look like when they are happening.

- Operating Systems

Knowledge of MS Windows, Mac OS, RedHat, and other mobile platforms make it possible to detect and understand incidents as they occur and after.

- Malicious Software

Hackers are getting craftier with their malicious software. Understanding the difference between a cross-site scripting attack and a virus allows the IRT to understand the source and extent of the damage of a specific attack.

- Programming languages

Knowledge of the intricacies of C++ vs. JAVA (and other programming languages) enable the IRT to be able to find the weaknesses and attack points when they have been exploited.

Business Continuity and Disaster Recovery Plans

As stated, before BCP, DRP and IRP are all remarkably similar to each other. The main difference is what type of issue are we dealing with that would drive us to use a particular plan. In creating BCP/DRPs there is the standard logic of PDCA. In BCP/DRP there is a unique set of words to describe that process though. The most straightforward has the following 7 steps:

1. Policy Creation - Senior management must support the creation of a continuity plan. This support is shown through their policy at a minimum.
2. Project Management and Initiation - This step is basic project management. We must select the team and the team leader. We must know managements expected expenditure of budget and the time granted to create the plan.
3. Business Impact Assessment (BIA) - The BIA is to do a risk assessment and understand criticality of systems and allowable downtimes.
4. Recovery Strategies - Knowing the criticality of systems and allowable downtimes what will we now use to recover? A hot site? A mobile site? What agreements must be in place with what vendors?
5. Plan Development - Here is where we document. Everything understood from the first 4 steps must be put into a procedural document that outlines how to recover step by step.
6. Implementation, Testing, Updating - A document is good, but we must now create the hot site (or whatever we need to add at this time) and then test it. While testing we want to uncover the issues with the plan and update the plan. Then test again until it is at the desired level of functionality.
7. Embed the plan in the user community - A tested and proven plan is good, but now everyone in the business must know their parts of the plan. If they do not know it and know it well, they will not be able to use it when the time comes.

Business Impact Assessment (BIA)

A Business Impact Assessment (BIA) is done early in the process of building a BCP or DRP in order to determine the critical systems through a risk assessment and the specific time frames we must work within to recover before there is a critical impact on our business.

Risk assessment was covered in detail in chapter 2. As a reminder we need to do a quantitative and/or qualitative risk assessment on our assets. This will tell us both how much a loss of an asset would cost us and our prioritization of our assets. This assessment must be extended now to determine time frames required for recovery.

Our time frames to determine include:

- Maximum Tolerable Downtime (MTD)
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
- Service Delivery Objective (SDO)
- Maximum Tolerable Outage (MTO)

Time Frames: Maximum Tolerable Downtime (MTD)

The MTD is the amount of time that a system (server, service, function, etc.) can be non-functional before irreparable harm occurs. This is from the moment of failure to the point it is now functional. If the time the system is down is greater than the MTD then there will be an impact on the business that it may not be able to sustain. The damage to the business may result in the failure of the business either immediately or within the next 5 years.

Time Frames: Recovery Time Objective (RTO)

The RTO is the amount of time that we must be able to do the actual work of recovery of the failed system (server, service, function, etc.). The recommendation is to expect that we have about ½ of the MTD to do the actual recovery work. The first half of the MTD window should be allocated to: life safety issues, unexpected issues, damage assessment and finally the decision by management to go forward with the BCP or DRP.

Time Frames: Recovery Point Objective (RPO)

The RPO is effectively the point in the past where we can find our last known good backup. When we restore our backup file onto a system we will have recovered to the point in the past when that backup was made. RPO is often defined as the amount of data that we can tolerate losing, e.g., 2 minutes or 24 hours. From the RPO we can confirm that we have an appropriate backup strategy in place.

Time Frames: Service Delivery Objective (SDO)

The SDO is the desired level of service that must be provided by our recovery plan. For example, if the server that we are planning how to recover is an online banking server the question is how many simultaneous connections it must be able to handle to satisfy our business requirements.

Time Frames: Maximum Tolerable Outage (MTO)

The MTO is the maximum amount of time that the organization can tolerate operating at the reduced level at the alternate site. By the time that we reach the point of the MTO the business needs to be back at full processing capability at the home location. MTD relates to each system directly where MTO is the entire situation.

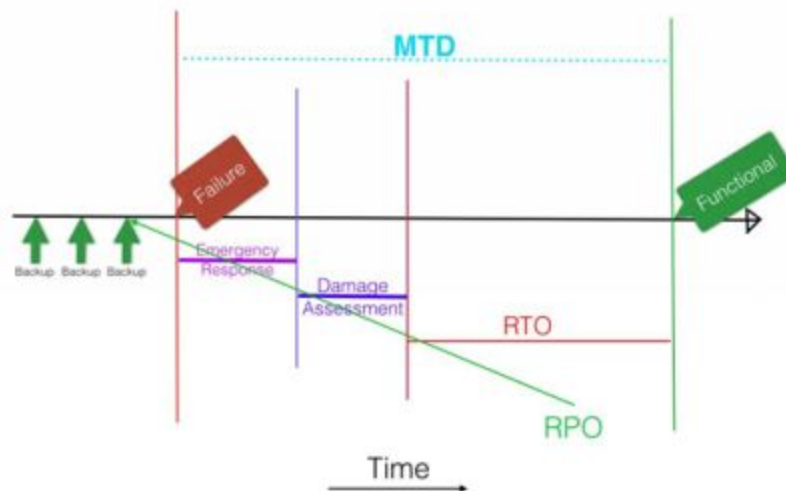


Diagram 23
BCP/DRP Time Frames

Recovery Strategies

Recovery strategies must be based on all the information gained in the BIA. Choice of the specific type of recovery site, the specific vendor agreements must all be chosen to meet the determined business needs based on the time frames determined above.

Recovery Sites: Mirrored Site

A mirrored site will have everything that is at the primary site that is necessary to the recovery of the critical systems and function. The systems and functions must be already up, working and processing data. This is going to be the most expensive option because there are two sets of employees, two rent payments, two power bills, two sets of equipment, etc., everything is duplicated at both sites (everything that is critical to the survival of the business).

Recovery Sites: Hot Site

A hot site will have nearly everything that the primary site has. It will not be up and operating, but ready to go. The most common definition of a hot site shows that the site is missing two things, people and at least some data. Once people arrive and the final bit of the data (possibly all) is loaded then the site will be up and operational.

Recovery Sites: Warm Site

A warm site is often defined as a site that has some equipment installed. Some definitions say it is the expensive equipment, some say it is the less expensive equipment, but the definitions are consistent in saying that there is only some stuff there, the rest must be added, configured, and brought online.

Recovery Sites: Cold Site

A cold site is most commonly defined as a site that is empty, think empty warehouse. There are 4 walls a roof and floor, nothing else inside. The connections from the cable company, phone company, power company or any other such company have been purchased and installed to the point of demarcation.

Recovery Sites: Mobile Site

A mobile site is defined, obviously, as something that moves. The most common is a trailer. A mobile site would most commonly be described the same way as a hot site, in other words it would be appropriate to say this is a mobile hot site. Therefore, it only needs people and some data in order to be functional.

Recovery Sites: Reciprocal Agreements

A reciprocal agreement is between two different companies, usually competing companies. These are companies that require specialty equipment or something that this other company would have access to that is critical for functionality. A simple example is a newspaper company. The printing press is very large and very expensive. If the company is not large enough to be able to afford a second site with a second press this type of agreement may be the best choice. The printing press is so expensive it is not logical to purchase one and have it sitting at a hot or warm site waiting for the day that it is needed. A service bureau agreement also does not make sense because they would not have a printing press sitting around either. A cold site is not logical as the recovery period is so long that the newspaper company would fail before the site was up and operational. So, the best choice can be to create a reciprocal agreement with another newspaper company that allows the competing company to come in and print newspapers if their site is nonfunctional. Competition is healthy. So, it does make sense to help your competing business survive through business continuity issues or disasters.

Recovery Sites: Service Bureaus

A service bureau is also known as a vendor hot site. This is a location that is owned and operated by another company. A subscription to their

service is necessary. Careful analysis of the agreement must be done as their services are usually oversold like airlines or cell phone services.

	Existing Infrastructure	Time to Recover	Cost
Mirrored Site	Fully staffed and operational now	Minutes for failover	\$\$\$\$\$\$
Hot Site	Fully equipped minus people and data	Minutes to Hours	\$\$\$\$\$
Warm Site	Some equipment	Days to Weeks	\$\$\$\$
Cold Site	An empty building with HVAC installed	Weeks to Months	\$\$\$
Mobile Site	Movable hot site	Minutes to Hours	\$\$\$\$
Reciprocal Agreement	Agreement with similar company to help each other in time of need	Days to Weeks	\$\$\$
Service Bureau	Subscription Hot Site service	Minutes to Hours	\$\$\$

Table 4
DR Sites

Recovery Sites: Site Selection

The type of site selected needs to meet the business requirement, especially tolerable time frames for outages. A business impact assessment must be done to determine the priority order of equipment and services to be recovered and the time frames it must be done inside of. Careful consideration must also be given to site location.

Site location impacts two significant issues. The first is the cause of the outage. If there is a tornado that is coming through town that has just taken out our primary location, we need to make sure that our alternate site is outside of the reach of that tornado. If it is a hurricane the reach of the hurricane is further so the site must be even further away. There is no specific number as in 100 miles or 2-hour drive. It is critical that we assess the cause of the outage and make sure that the other site is out of that area.

The second issue is the access. If we put the site a great distance from the first how are we going to get there? We must be able to get to the site within the RTO and take all restoration steps. Perhaps it will be necessary to

have personnel fly to the site in anticipation of a need to recover based on the current weather patterns, or perhaps we have personnel in the area that are effectively part-time employees. They are put to work in the event of an outage. They will be close to the site and will be able to get there quickly and begin the restoration work while everyone else is in transit to the site.

Vendor Agreements

Agreements must be planned ahead of time. These agreements include things such as:

- Delivery of a new piece of hardware within X hours.
- Redirection of phone numbers to the alternate site.
- Installation codes to be used specifically at the alternate site or on a new piece of hardware.

Plan Development

Once we have done our BIA and developed our recovery strategies it is now necessary to create a formal document with all pieces of information and steps required to be able to recover effectively. The plan must include additional items that have not been discussed so far. These items include:

- Employee Notification method.
- When something major happens to the functionality of the business how will every employee be contacted? How will you stay in contact with them? How will they communicate with you?
- Communication structure during the outage.
- If the outage is caused by a regional disaster like a hurricane, the normal phone communication systems may not be working. Will you be able to communicate by SMS or email or will you need to purchase a few satellite phones?
- General office supplies
- What supplies are needed to be able to get work done at the alternate site? Pens, paper, paper clips, stapler, staples, etc.
- Petty cash
- This is often underestimated. When food or RJ45 connectors are needed because they were forgotten or underestimated will you

have enough cash on hand? If this is a natural disaster cash may be your only option with local vendors.

- Personnel assignment during the outage.
- Some people's normal day to day jobs may not be critical enough to be needed during a major outage therefore they may be reassigned to backup or perform more critical tasks until things are returned to normal. There will also be new job assignments such as petty cash manager that will be needed during the incident and only during the incident.
- Transportation requirements to the alternate site.
- Especially in the USA there may be legal issues created if we direct our employees to get into their cars and drive to the alternate site. Our insurance plan may not cover them if they are in an accident. Beyond that we need to worry about how to get people to a site that is more than a few hours drive away. Is it best to rent a bus or buy airplane tickets?
- Succession planning
- Unfortunately, we must also plan for the loss of people If the CEO is not with us any more who will step into their place, and so on down the line?
- Level of detail included in the plan.

When writing the plan, we must decide what level of detail to include. Is the plan to be used by the person writing it, or by someone with a similar level of knowledge or by someone that happens to be available at the moment? If the plan is not detailed enough the latter may not be able to use it, but if it is too detailed in may get in the way of the former.

The list of things to include continues. The trick is to make sure all that is needed is included. The best way to do that is to perform tests.

Testing the Plan

A complete and pretty document does not mean that things are going to work. We must test. We must know what level of success management wants us to accomplish with our tests in order to consider it a successful test. Management may think they want to know without any doubt that our

plan will work, but when they find out how expensive and how dangerous that test is it is likely they will change their mind.

So, what are the goals of our test? The test should focus on

- The accuracy and currency of the plan
- Our personnel's performance and abilities
- Verifying assumptions, the plan is based on

- Testing the timing of the recovery steps
- Identifying gaps between what we can do and what we need to do

For the test to be successful the participants of the test must be determined. One particularly important role in the test is the observer(s). The observers must be very clear as to their task - observe. Our test plan must also be very clear if they are ever to break that role of observing and step in to assist, or more likely no matter how tempting to remain as observers.

The next question is who else will participate in the test? Options include those who wrote the plan, data/system owners, department managers, and general users, people with equivalent level of knowledge as those who wrote the plan as well as a few others. Part of the determination of the type of participants will be the type of test that is being performed as well as the plan assumption for participants when there is an actual business interruption.

Types of Tests

There are 5 basic levels of BCP/DRP tests:

1. Checklist - A checklist allows the participants, most likely those who created the plan, to walk through looking for missing items, completeness, and consistency. The level of assurance provided by this test is minimal, but it is the perfect place to begin testing.
2. Structured walk through - A structured walk through is like a checklist in that it happens in the safety of a conference room therefore the possibility of causing damage during the test is

greatly minimized. The participants of this test are likely to be those who created the plan although individuals from many distinct parts of the business can be included in this walk through.

3. Simulation - A simulation test leaves the safety of the conference room so it is very possible that damage can occur during this test. Since this is the first level test that is not in the conference room the simulation only pretends to act for recovery. The simplest example that everyone is familiar with is a fire drill. We do not start a fire to do a fire drill. It is a pretend situation but someone could still fall going down the stairs and break their arm so damage can occur. A similar drill can be done with equipment but the actions to recover would not actually be taken. The goal is to locate all necessary items for recovering the server without loading or activating anything. In the process of locating everything it is possible a cable is tripped on and power is lost to a server by accident.
4. Parallel - A parallel test is going to be the normal maximum level that most companies will test to. This test will bring the alternate server/service/site/etc. up to an operational level. For instance, a test where the hot site is brought to a functional level and can process data would be a parallel test so long as the main server/service/site/etc. is left in a normal operational condition. This can go wrong with a test like this, for instance traffic could get redirected to the alternate site by accident only to find it is not able to process data. Participants in this test must be carefully chosen to ensure that the proper skills according to our plan assumptions are on site.
5. Full Interruption - A full interruption test is too dangerous for most businesses. There are businesses that do go through these tests, usually due to regulatory requirements. If a business is part of the national infrastructure the legal requirements might be for them to go through tests like this on a quarterly or semi-annual basis. This is the kind of test where the data center is taken offline, and all functionality must failover to the alternate processing facility. This is extremely dangerous. Depending on how the primary site is taken offline it is possible that something may fail and not be recoverable, to add to the danger the failover

to the alternate might not work leaving a business in an actual emergency status.

	Participants	Cost	Danger Level
Checklist	Plan creators	\$	✖
Structured Walkthrough	Plan creators and business knowledgeable people	\$	✖
Simulation	Plan creators and business knowledgeable people	\$\$	✖✖
Parallel	Many skilled employees	\$\$\$\$	✖✖✖✖
Full Interruption	Everyone	\$\$\$\$\$	✖✖✖✖✖

Table 5
BC/DR Test Types

Successful Test Metrics

The test must be determined to be successful or not. During a test issues will be found. If no problems are found it is best to try the test again with a different scenario. The problems are there, and they need to be found before a real failure occurs. It is a bit of a pessimistic way to look at things, but best to test and find the problems rather than have a real failure and find the problems.

Things to measure or watch for during a test would be:

- A determination of how complete the plan is
- How well trained is the staff? Did they recover within the RTO?
- How well did internal staff work with outside vendors?
- Was all equipment that should be on site there?
- Was the equipment that needed to be located and brought in found?
- Was the data restored appropriately?
- Was data processing possible at the end?

Actual metrics can include:

- Measure of time to recover in relationship to RTO
- Percentage of recovery complete within the RTO
- Amount or percentage of data that was successfully recovered

All this information must be used to fix the plan document itself, retrain employees and then test again until it has been determined that we have performed a successful test.

Forensics

The need for forensics seems to increase on a regular basis. It is critical that a business determine their forensics needs long before anything happens to their information, infrastructure, or systems. A single misstep in the process of recovery could render what would have been good evidence into useless information.

Post incident investigations have a few basic purposes:

- Identify the cause
- Take corrective actions
- Document what happened
- Provide evidence for legal actions to be taken

The focus now is on evidence. During the planning process for IRPs, BCPs or DRPs it is necessary to determine what kind of attacks, faults, or failures demand that a corporation be able to gather forensic evidence that can be used in a court of law. The court case may be something related to:

- A failure to maintain compliance with a law that has resulted in a security breach.
- A security breach that is related to information that must be protected according to a law and a corporation needs to be able to prove they had the right defense structure in place.
- A former employee is filing an unlawful termination lawsuit and the corporation must be able to justify their termination action.
- An employee has committed fraud that results in the loss of millions for the business.

What is important when it comes to gathering forensic evidence is that we remember a few extremely critical basics.

- Forensics should only be performed by qualified individuals.
- The forensic examiner should assume that they are going to have to testify in court and take all appropriate actions based on that assumption.
- Always follow forensic best practices
- Always follow all legal procedures such as chain of custody
- Never install or run anything on the affected system.
- Gather evidence in an order of volatility. Gather the most volatile first, e.g., memory or the screen, then work on the hard drive.
- A copy of the hard drive should be made at a bit level.
- Make at least two copies of the hard drive.
- Make sure write block is on the affected drive.
- Store the original drive in a manner that protects chain of custody.
- Use forensically acceptable tools for analysis of the drive such as EnCase.
- Document, Document, Document

Summary

An incident is an occurrence that jeopardizes confidentiality, integrity or availability of a system or its information. A disaster is a hardware or software failure that causes the business to have to recover to a separate facility to sustain the business. A business continuity issue is a significant disruption to the critical processes or functions of a business.

These different events are remarkably similar to each other yet they each require their own documentation on how exactly to respond in order to save our business.

A careful process needs to be followed in order to create the capabilities to respond to incidents, disruptions and disasters in a way that minimizes the negative impact on the organization. In this process it is critical to take into consideration the level of criticality of each system/process/function within the business and the amount of time that it can be non-functional

before it becomes a serious impact on the business. A thorough understanding of the maximum tolerable downtimes for critical systems as well as the recovery time objectives and recovery point objectives is the key to successfully handling incidents.

Once all plans are created, they must be tested in a realistic manner so that all problems with the plans can be uncovered and remedied before any actual interruptions occur.

With the right tools, practice, and well-trained individuals in the proper jobs we will be able to recover our business quickly and effectively when failures occur.

Chapter 4 Questions

1. When the confidentiality, integrity or availability of an information system is jeopardized, this is referred to as a(n):
 1. Problem
 2. Incident
 3. Event
 4. Issue

2. A detailed operational component that specifies actions, personnel and activities that will take place when there is an incident occurring or when one has recently occurred is known as a:
 1. Incident Response Plan
 2. Business Continuity Plan
 3. Disaster Recovery Plan
 4. Emergency Preparedness Plan

3. What is the main difference between a business continuity plan and a disaster recovery plan?
 1. There is no difference. Business continuity plans and disaster recovery plans are the same thing with different names.
 2. A business continuity plan is related to financial activities while a disaster recovery plan is related to operations.
 3. A disaster recovery plan is a subset of a business continuity plan.
 4. A business continuity plan pertains to business functions in general while a disaster recovery plan is

specifically dealing with Information Technology (IT) failures.

4. Which of the following is the best example of a disaster?
 1. A fire in the data center
 2. A virus on a computer
 3. A server has crashed
 4. A system OS taken offline for an upgrade

5. If an information security manager is working at a global corporation it is necessary for them to ensure that the privacy policy will locally
 1. ensure compliance with the laws of the country where HQ is located.
 2. ensure compliance with the laws of the country where the data is gathered.
 3. ensure compliance with the privacy policy.
 4. ensure the privacy policy is applicable in all countries.

6. Specific duties and responsibilities should be assigned to incident response team members in a manner designed to:
 1. Minimize the stress on the team members.
 2. Maximize the effectiveness of the team.
 3. Minimize the effort required by each team member.
 4. Maximize the amount of work that can be accomplished with the least amount of team members.

7. Which of the following is a critical function of incident response?
 1. Reduce the downtime of email servers
 2. Identify laws that have been broken
 3. Prevent attacks
 4. Contain the damage

8. Following the closure of an incident, what activity should be conducted?
 1. After action review or lessons learned
 2. Create an improved notification process
 3. Purchase better incident response tools
 4. Increase incident response training

9. A passive device that observes behavior to try to detect an attack and then will raise an alarm is a:
 1. Security Information and Event Management (SIEM) system
 2. Incident Response Plan
 3. Intrusion Detection System (IDS)
 4. Intrusion Prevention System (IPS)

10. The basic functions of a Security Information and Event Management (SIEM) system are:
 1. To store and protect security information and event information.
 2. To aggregate, correlate, retain and analyze security information and events and to provide alerts to issues.
 3. Provide a secure platform to communicate security information and events to auditors.
 4. Detect and prevent security incidents and events.

11. Information security managers are part of a team that must identify critical business functions and the risks to those functions. What technique will this team utilize to identify these elements?
 1. A risk assessment
 2. A penetration test
 3. A Business Impact Analysis
 4. A vulnerability assessment

12. What metric represents the amount of time a system can be non-functional before irreparable harm occurs?
 1. Maximum Tolerable Downtime (MTD)
 2. Mean Time to Recovery (MTTR)
 3. Mean Time Between Failures (MTBF)
 4. Recovery Time Objective (RTO)

13. What metric represents the organizations tolerance for operating at a reduced level at an alternate site?
 1. Maximum Tolerable Downtime (MTD)
 2. Recovery Point Objective (RPO)
 3. Service Delivery Objective (SDO)
 4. Maximum Tolerable Outage (MTO)

14. When it is time to perform a forensic investigation, it is best to have the examination done by
 1. The first IT person on the scene
 2. Senior management
 3. A qualified professional
 4. An outside investigator

15. Any copies of the hard drive should be done
 1. At a bit level
 2. With windows copy
 3. As a ghost image
 4. By only copying suspect files

16. When an investigator is creating a proper copy of the affected hard drive the first step the investigator should take is
 1. Establish a connection to a write block device
 2. Begin a chain of custody log
 3. Create a hash value for the affected hard drive
 4. Identify the forensically acceptable tool for making the copy

17. Which recovery strategy is LEAST likely to be successful?
 1. Hot site
 2. Mirror site
 3. Reciprocal agreement
 4. Cold site

18. What metric is instrumental in determining organizational backup timeframes?
 1. Recovery Time Objective (RTO)
 2. Service Delivery Objective (SDO)
 3. Maximum Time to Recovery (MTTR)
 4. Recovery Point Objective (RPO)

19. An alternate processing site that is probably only missing the operations personnel and the latest data load is a:
1. Warm site
 2. Hot site
 3. Multiple processing site
 4. Mirror site
20. What type of recovery site usually takes days to weeks to bring on line?
1. Warm site
 2. Cold site
 3. Hot site
 4. Mobile site
21. An organization has determined that its maximum tolerable downtime is 1 hour. What is the best recovery solution to ensure the MTD is not exceeded?
1. Reciprocal Agreement
 2. Mobile site
 3. Hot site
 4. Mirrored site
22. How far should an alternate site be located from a primary site?
1. Far enough away that it will not be impacted by the same incident as the primary site.
 2. At least 60 miles from the primary site
 3. At least 300 miles from the primary site.
 4. It depends on applicable laws and regulations.
23. What type of business continuity plan / disaster recovery plan test is usually conducted in a conference room setting with test

participants stepping through the plan to identify missing elements and pitfalls?

1. A checklist
2. A full interruption
3. A simulation
4. A structured walk-through

Chapter 4 Questions with Answers and Explanations

1. When the confidentiality, integrity or availability of an information system is jeopardized, this is referred to as a(n):
 1. Problem
 2. **Incident**
 3. Event
 4. Issue

Explanation

Answer B: An incident compromises CIA. An event is simply an observable occurrence. Issues and problems are not terminology used to describe occurrences within security standards.

2. A detailed operational component that specifies actions, personnel and activities that will take place when there is an incident occurring or when one has recently occurred is known as a:
 1. **Incident Response Plan**
 2. Business Continuity Plan
 3. Disaster Recovery Plan
 4. Emergency Preparedness Plan

Explanation

Answer A: All of these plans are detailed documents with instructions on what to do in specific circumstances. The question specifically asks about an incident.

3. What is the main difference between a business continuity plan and a disaster recovery plan?

1. There is no difference. Business continuity plans and disaster recovery plans are the same thing with different names.
2. A business continuity plan is related to financial activities while a disaster recovery plan is related to operations.
3. A disaster recovery plan is a subset of a business continuity plan.
4. **A business continuity plan pertains to business functions in general while a disaster recovery plan is specifically dealing with Information Technology (IT) failures.**

Explanation

Answer D: A DR plan might be a subset of the BC plan, but DR is specific to IT and BC is the rest of the business and its functionality.

4. Which of the following is the best example of a disaster?
 1. **A fire in the data center**
 2. A virus on a computer
 3. A server has crashed
 4. A system OS taken offline for an upgrade

Explanation

Answer A: A fire in the data center is a disaster; disasters are IT related that requires moving to another locations. A server crashing, a virus or OS offline for an update do not require moving to another location such as a hot site.

5. If an information security manager is working at a global corporation it is necessary for them to ensure that the privacy policy will locally
 1. ensure compliance with the laws of the country where HQ is located.
 2. ensure compliance with the laws of the country where the data is gathered.

3. **ensure compliance with the privacy policy.**
4. ensure the privacy policy is applicable in all countries.

Explanation

Answer C: The infosec manager should ensure that policies are followed. These policies should be created based on country specific laws, not the laws of another country even if that is where HQ is located. The policy will not apply to all countries laws.

6. Specific duties and responsibilities should be assigned to incident response team members in a manner designed to:
 1. Minimize the stress on the team members.
 2. **Maximize the effectiveness of the team.**
 3. Minimize the effort required by each team member.
 4. Maximize the amount of work that can be accomplished with the least amount of team members.

Explanation

Answer B: Incidents need to be managed in the most effective way possible, if that minimized stress that is a side benefit. This optimization of the team should minimize effort and maximize the amount of work that can be accomplished.

7. Which of the following is a critical function of incident response?
 1. Reduce the downtime of email servers
 2. Identify laws that have been broken
 3. Prevent attacks
 4. **Contain the damage**

Explanation

Answer D: In an incident it is critical to contain the damage so that things do not get any worse. It is too late to prevent the attacks since this is about responding to an incident is occurring or has recently occurred. Identifying laws that have been broken might occur along the way but is not the most critical thing to do. Reducing the downtime

is great, but again we want to contain the damage so that we do not have 15 servers down instead of the original 1.

8. Following the closure of an incident, what activity should be conducted?
1. **After action review or lessons learned**
 2. Create an improved notification process
 3. Purchase better incident response tools
 4. Increase incident response training

Explanation

Answer A: At the end of the incident, it is critical to have a lessons learned meeting. This could lead to improved notifications, better tool, and better training.

9. A passive device that observes behavior to try to detect an attack and then will raise an alarm is a:
1. Security Information and Event Management (SIEM) system
 2. Incident Response Plan
 3. **Intrusion Detection System (IDS)**
 4. Intrusion Prevention System (IPS)

Explanation

Answer C: An IDS is a passive device that attempts to detect where an IPS is an active device that attempts to prevent. An Incident response plan is not a device. SIEMs work to analyze logs from many sources and correlate events to understand attacks.

10. The basic functions of a Security Information and Event Management (SIEM) system are:
1. To store and protect security information and event information.
 2. **To aggregate, correlate, retain and analyze security information and events and to provide alerts to**

issues.

3. Provide a secure platform to communicate security information and events to auditors.
4. Detect and prevent security incidents and events.

Explanation

Answer B: The basic function of a SIEM is to analyze and correlate events. It is a good thing to do but the basic function of the SIEM is not to protect that information. It is not intended for providing information to auditors. It is also not designed for preventing incidents; an IPS hopefully will do that.

11. Information security managers are part of a team that must identify critical business functions and the risks to those functions. What technique will this team utilize to identify these elements?
 1. A risk assessment
 2. A penetration test
 3. **A Business Impact Analysis**
 4. A vulnerability assessment

Explanation

Answer C: Identifying critical business functions and the risks are a business impact analysis. It is similar to a risk assessment but is designed for critical business functions. A penetration test has the purpose of finding and exploiting vulnerabilities. A vulnerability assessment is designed to identify weaknesses or flaws.

12. What metric represents the amount of time a system can be non-functional before irreparable harm occurs?
 1. **Maximum Tolerable Downtime (MTD)**
 2. Mean Time to Recovery (MTTR)
 3. Mean Time Between Failures (MTBF)
 4. Recovery Time Objective (RTO)

Explanation

Answer A: The moment when irreparable harm is cause is when a business is nonfunctional longer than the MTD. RTO is the time the teams must do the work to recover based on MTD. MTBF tells us how often we can expect these events to occur. MTTR is the average time to recover.

13. What metric represents the organizations tolerance for operating at a reduced level at an alternate site?
1. Maximum Tolerable Downtime (MTD)
 2. Recovery Point Objective (RPO)
 3. Service Delivery Objective (SDO)
 4. **Maximum Tolerable Outage (MTO)**

Explanation

Answer D: Reduced level of operation that is acceptable is the MTO. MTD is the longest amount of time that the critical systems can be down. SDO is the service level that must be provided in a minimized level of operation. RPO is the window for the work to be done to recover.

14. When it is time to perform a forensic investigation, it is best to have the examination done by
1. The first IT person on the scene
 2. Senior management
 3. **A qualified professional**
 4. An outside investigator

Explanation

Answer C: Only qualified, and possibly certified, professionals should ever do a forensic investigation. That does not have to be done by an outside investigator. It should not be senior management, even if qualified, as their job is to manage. The first IT person should secure the device according to procedures.

15. Any copies of the hard drive should be done
1. **At a bit level**

2. With windows copy
3. As a ghost image
4. By only copying suspect files

Explanation

Answer A: Bit level images are the current standard for forensic copies of hard drives. This should only be done with forensically accepted tools, not Windows copy tools or a ghost image. If only the suspect files are copied critical evidence may not be gathered because you never know where the real evidence lies until the examination is done.

16. When an investigator is creating a proper copy of the affected hard drive the first step the investigator should take is
 1. Establish a connection to a write block device
 2. **Begin a chain of custody log**
 3. Create a hash value for the affected hard drive
 4. Identify the forensically acceptable tool for making the copy

Explanation

Answer B: In forensics it is good to start with a chain of custody log. Then the right tool can be selected, the drive can be protected from changes and a hash can be created, but chain of custody first.

17. Which recovery strategy is LEAST likely to be successful?
 1. Hot site
 2. Mirror site
 3. **Reciprocal agreement**
 4. Cold site

Explanation

Answer C: Reciprocal agreements rely on a contract with a competing company. The contract needs to be extremely well written so that when there is a failure the competition will let you in. This is

exceedingly difficult to achieve. Where a hot, mirror and cold site are expected to be your own.

18. What metric is instrumental in determining organizational backup timeframes?
1. Recovery Time Objective (RTO)
 2. Service Delivery Objective (SDO)
 3. Maximum Time to Recovery (MTTR)
 4. **Recovery Point Objective (RPO)**

Explanation

Answer D: The Recovery Point Objective (RPO) determines the amount of data that can be lost. It must drive the backup timeframes. If your company has a RPO of 24 hours (no more than 24 hours of work may be lost) and they perform a full backup once a week. This company will discover that the RPO cannot be met and they may find that they have lost six-days worth of data.

19. An alternate processing site that is probably only missing the operations personnel and the latest data load is a:
1. Warm site
 2. **Hot site**
 3. Multiple processing site
 4. Mirror site

Explanation

Answer B: A Hot Site is normally missing people and data. The most common definition within the standards. A hot site can be company run or run by an external vendor. It is easy to remember that a hot site is normally missing people and data if you think about a vendor hot site. It is very unlikely that there will be employees and data at third party site.

20. What type of recovery site usually takes days to weeks to bring online?

1. **Warm site**
2. Cold site
3. Hot site
4. Mobile site

Explanation

Answer A: A warm site is missing people, data, and some major equipment. The people and the data can quickly be brought to a warm site, but the equipment may take days to a few weeks to appropriate and install.

21. An organization has determined that its maximum tolerable downtime is 1 hour. What is the best recovery solution to ensure the MTD is not exceeded?
1. Reciprocal Agreement
 2. Mobile site
 3. Hot site
 4. **Mirrored site**

Explanation

Answer D: A mirrored site can provide instant or near instant failover. Even a hot site needs people and data, which likely will not be accomplished in an hour, therefore the best solution would be a mirrored site which is often missing nothing.

22. How far should an alternate site be located from a primary site?
1. **Far enough away that it will not be impacted by the same incident as the primary site.**
 2. At least 60 miles from the primary site
 3. At least 300 miles from the primary site.
 4. It depends on applicable laws and regulations.

Explanation

Answer A: The purpose of an alternate site is to have a place to recover to. If the same event would affect both locations, then the backup site would be equally impacted as the primary site. If your

alternate site is 60 miles away and the ice storm takes out all power and makes the roads impassable across the region, then both sites could be equally affected and the alternate site would be ineffective.

23. What type of business continuity plan / disaster recovery plan test is usually conducted in a conference room setting with test participants stepping through the plan to identify missing elements and pitfalls?
1. A checklist
 2. A full interruption
 3. A simulation
 4. **A structured walk-through**

Explanation

Answer D: A structured walk-through is a tabletop event where the key players discuss the content of a plan. Often, they will verbally describe what they would do in case of an adverse event.

Glossary

2-phase commit

a distributed system's transaction control that requires updates to complete or rollback transaction controls for a database, a return to a previous state

5 rules of evidence

evidence must be admissible, authentic, complete, accurate, and convincing

acceptable use policy

defines the activities that users are allowed to do or are restricted from doing usually associated with a particular task or system e.g., internet usage or e-mail usage

access control

to control access (or mediate) between subjects and objects

access control list (ACL)

object based description of a single resource and the permission each subject

access control matrix

object based description of a system or a collection of resources

access point (AP)

the connection between a wireless and wired network

accountability

responsibility of a user to answer for the actions executed by their uniquely identified account

accreditation

the managerial approval to operate a system based upon knowledge of operational risk

accurate

details are correct, error-free

ACID test

a set of best practices for programmers to seek in all application or database design: atomicity, consistency, isolation, durability

activation

to start business continuity processes

active attack

where the attacker attempts to gain access to information and change, alter, or modify the information

active data

information residing on the hard drives or optical drives of computer systems, that is readily visible to the operating system and/or application software with which it was created and is immediately accessible to users without deletion, modification or reconstruction

administrative control

written or orally communicated controls such as a policy

administrative law

a set of laws that the organization agrees to be bound by

admissible

pertaining to law, accepted by a court

adware

malware used to advertise specific content to the user within a web browser. it usually relies on spyware for the information regarding what to advertise

aggregation

to collect many small pieces of data

agile development

software development methodology utilizing cross-functional teams

alarm filtering

the process of categorizing attack alerts produced from an ids in order to distinguish false positives from actual attacks

alert/alarm

notification of a potentially dangerous or harmful situation

algorithm

mathematical function used within cryptographic operations that performs the manipulation of the data

alternate data streams (ADS)

allows data to be concatenated to a file but not be contained within the primary data of the file. can be used as a covert storage channel

alternate site

location to perform the business function separate from the primary location. usually activated after a disaster

analysis

a review of data or a systematic assessment of threats and vulnerabilities that provides a basis for effective management of risk

annual rate of occurrence (ARO)

the number of times a specific incident occurs per year #times/year(s)

annualized loss expectancy (ALE)

the expected monetary loss of an asset due to risk over a one-year period

anomaly

aa deviation from what is considered normal

anomaly detection

the ability to identify anomalies, an unusual event

anti-virus (AV) software

software designed to detect and mitigate viruses and other malware on a system

application based intrusion detection system (IDS)

an IDS that works at the application level. usually analyzes application logs

application programming interface (API)

a library of commands maintained by a system for other programs to use, provides consistency and integrity for the programs

architecture

high level design or model with a goal of consistency across the organization

archival data

information that is not directly accessible to the user of a computer system but that the organization maintains for long-term storage and record keeping purposes

ascii (American standard code for information interchange)

ascii text does not include special formatting features and therefore can be exchanged and read by most computer systems. files that have a ".txt" extension are typical of ascii files.

attacker (black hat, hacker)

someone who wants to cause harm

assembler

converts a high-level language into machine language

asset

something of value to a business, tangible or intangible

asymmetric

encryption system using a pair of mathematically related keys, public/private key pair

atomicity

indivisible, data field must contain only one value that either all transactions take place, or none do

attack

aggressive action by an enemy intending to cause harm

attack signature

unique set of data elements that can be used to identify a specific attack

audit trail

paper or electronic data that provides a history of user/device activity

authentic

verifiable as real

authentication

a process of verification of the truth of the user's identity using something they know, have or are

authorization

decision by a system of permitting or denying access to a particular resource on the system and the specific actions that are allowed

availability

resources are accessible by the authorized user when needed

awareness

a state of being well informed

awareness training

training designed to keep people informed of policies and procedures

backup

to create a copy of data as a precaution against the loss or damage of the original data

balanced scorecard

a strategic planning and management system that is used to align business activities to the vision and strategy of the organization

baseline

a starting point to use for comparison / minimum security settings and configuration

baseline security

starting point for security settings

baselining

the act of creating a starting point to use for comparison

Bell-LaPadula (BLP) model

a lattice-based confidentiality model using stateful math to definitively prove rules that if followed will prevent all breaches of confidentiality. rules allow for writing to the same or higher level (star property), Reading at the same or lower level (simple property), and reading and writing at the same level (strong star property).

benchmarking

point of reference or comparison

best practice

a good idea that is often formalized and internationally approved, but not normally mandatory e.g., ISO 27002

Biba model

a lattice-based integrity model using stateful math to definitively prove rules that if followed will prevent integrity issues. supports the first goal of integrity only - preventing unauthorized users from making changes. the simple integrity property states that subjects may only read objects from an equal or higher level. the star integrity property states that subjects may

only write to objects at an equal or lower level. the invocation property allows subjects to only read and write (both) to their own level

binary

pertaining to a number system that has just two unique digits

birthday attack

a hash attack that looks for two different pieces of data that hash to the same value. statistical probabilities of a collision are more likely than one thinks

bit

a measurement of data. it is the smallest unit of data. a bit is either the "1" or "0" component of the binary code

blackout

prolonged loss of commercial power

blind testing

evaluation of a system without prior knowledge by the tester

blueprint

technical details of a security architecture

bollard

vehicle stopping object

boot

to load the first piece of software that starts a computer

bot

a hidden piece of malware that is installed on a host device and is then used to launch a DDoS attack

botnet

organized group of compromised computers under the command and control of another (sometimes called a bot herder, bot handler or CnC). a

network of many, perhaps thousands of bots

Brewer-Nash model

an access control model designed to prevent conflicts of interest. also called the Chinese wall model. once a subject has gained access to an object (data) that would conflict with accessing a different object, rules are put into place preventing access to the later object. e.g., access to beer is allowed, but access to a car after the beer is not allowed

bridge

a layer 2 device that used to connect two network segments and regulate traffic

brownout

reduction of voltage by the utility company for a prolonged period of time

brute force

an attack vector that tries all possible password/key combinations in an attempt to compromise a password or cryptographic key

buffer overflow

a flaw in software where the software does not validate the incoming data to ensure it will fit within the allocated buffer space. when there is too much data the software will write the extra information into the following buffer which will cause another piece of software to crash or run random code. unchecked data which spills into another location in memory

bumping

hitting a filed down key in a lock with a hammer to open

burn

slang for making (burning) a cd-rom copy of data, whether it is music, software, or other data

business case

a justification of a proposed business project

business continuity institute (BCI)

organization working with business continuity planning and management.
created the good practice guidelines

business continuity planning (BCP)

organization's prior arrangements made to maintain the functions and processes important to the existence of the organization

business continuity program

an ongoing program supported and funded by executive staff to ensure business continuity requirements are assessed, resources are allocated and, recovery and continuity strategies and procedures are completed and tested

business impact assessment (BIA)

a process to analyze business functions to determine which functions are the most critical and the impact to the business if those functions are not available

business interruption

any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at an organization location

business interruption insurance

insurance coverage for disaster related expenses that may be incurred until operations are fully recovered after a disaster

business model for information security (BMIS)

a business-oriented framework that provides a common language for managing information security

business recovery team

a group of individuals responsible for maintaining the business recovery procedures and coordinating the recovery of business functions and processes

business recovery timeline

the chronological sequence of recovery activities, or critical path, that must be followed to resume an acceptable level of operations following a business interruption. this timeline may range from minutes to weeks, depending upon the recovery requirements and methodology

business unit recovery

the component of disaster recovery which deals specifically with the relocation of a key function or department in the event of a disaster, including personnel, essential records, equipment supplies, workspace, communication facilities, workstation computer processing capability, fax, copy machines, mail services, etc.

byte

eight bits

byte level deletion

may render the data inaccessible to the application intended to be used in processing the file, but may not actually remove the data

cache

a type a computer memory that temporarily stores frequently used information for quick access

call tree

an internal list of contact information used for the communication of incident information, designed in a distributed manner so that no one person is responsible for contacting everyone

capability tables

subject based description of a system or a collection of resources

Caesar cipher

a simple substitution cipher that was used by Julius Caesar

central processing unit (CPU)

the core of a computer that calculates

centralized

concentrated into one location, controlled and managed under one authority

certificate authority

a term often used in cryptography to identify a trusted entity who issues digital certificates which are used to verify the owner of a public key. the function of creating and issuing X.509 public key certificates

certificate revocation list (CRL)

a file, often maintained by the issuing authority, that contains a list of compromised digital certificates

certification

the technical assessment of a system used to determine how well the system will function within the context of the operating environment and the associated risks. e.g., will it work for me in my environment

certification practice statement (CPS)

a declaration from the certificate authority of the actions they have taken to securely issue and manage digital certificates

chain of custody

maintaining positive control of evidence recording every aspect of its handling from the beginning of the evidence lifecycle through final disposition. the lifecycle of the evidence

change control

a process used to ensure that changes happen in a controlled, documented, and approved manner

change management

the business functions that ensure that the change control process happens

checklist test

a test to verify the completeness and availability of documentation e.g., business continuity plans or disaster recovery plans

checkpoint

part of a transaction control for a database which informs the database of the last recorded transaction

checksum

a mathematical tool for verifying no unintentional changes have been made

chosen ciphertext attack

a cryptography attack where the attacker has access to the cryptosystem and proceeds to decrypt letters and words to view the resulting plaintext in an attempt to uncover the algorithm and key that was used

chosen plaintext attack

a cryptography attack where the attacker has access to the cryptosystem and proceeds to encrypt letters and words to view the resulting ciphertext in an attempt to uncover the algorithm and key that was used

cipher block chaining (CBC)

a block cipher mode

cipher feedback (CFB)

a block cipher mode

ciphertext

the output of an encryption system, scrambled form of the message or data

ciphertext only attack

a cryptography attack where the attacker only has the ciphertext and attempts to uncover the plaintext, algorithm and key used in the encryption process

civil law

see tort law or napoleonic code

Clark and Wilson model

an integrity model designed to maintain all three goals of integrity. 1. prevent unauthorized users from making modifications 2. prevent

authorized users from making unauthored changes 3. maintain internal and external consistency - these three goals are achieved through a separation of duties and well-formed transactions. utilizes the access triple known as "subject - program - object"

class

oop concept of a template that consist of attributes and behaviors

classification

the assignment of a level of sensitivity to data (or information) that results in the specification of controls for each level of classification

classification scheme

a systematic method of determining and assigning a level of protection to data or information

clean room approach

the approach to produce a program that has no flaws

cleartext

information in a readable format

clipping level

the threshold for when to begin logging or when to stop logging

closed system

system designed to utilize proprietary interfaces

cloud computing

a model for on-demand access to computing resources owned and operated by another entity, it could be either public or private

CMMI

a process improvement framework

coaxial cable

a cable consisting of a copper core surrounded by insulation and grounded,

braided shielding. the shielding minimizes emanations as well as interference

COBIT 2019

a framework for developing, implementing, monitoring, and improving IT governance and management practice

code

substitution at the word or phrase level

CODEC

used to code/decode a digital data stream

cold site

a long-term disaster recovery alternative consisting of a building with sufficient power, HVAC and communication and power lines from the carriers, and little more

collisions

outputs within a given function are the same result

common criteria (CC)

see ISO 15408

common law

system of law based upon precedence, with major divisions of criminal, tort, and administrative

compartmentalize

divide into sections or categories for the purpose of providing the appropriate level of protection to each category

compensating control

a control designed to make up for a deficiency or lack of another existing control

compiler

converts source code to an executable

complete

pertaining to law, no omissions

component based development

standardized building block approach

compression

a technology that reduces the size of a file

computer aided software engineering (CASE)

software development tools designing and building applications. Used for large, complex projects

computer forensics

a subset of forensics examination focusing on digital evidence - see forensics examination

concatenation

joining two pieces of text

concentrator

layer 1 network device that is used to connect network segments together but provides no traffic control (a hub)

confidence value

a value an organization places on an IDS based on past performance and analysis to help determine its ability to effectively identify an attack

confidentiality

keeping secrets secret

configuration management (CM)

a process of recording and preserving device information in order to provide stability. all changes to the configuration must be documented, tracked and confirmed

conflict of interest

a situation that occurs when one entity acts with two competing allegiances

consistency

property that data is represented in the same manner at all times

contact list

a list of team members and/or key players to be contacted including their alternates. the list will include the necessary contact information (i.e., home phone, pager, cell, etc.) and in most cases be considered confidential

containment

a method to mitigate damage from spreading by isolating compromised systems from the network

content dependent access control

system mediation of access with the focus on the context of the request

contingency plan

a plan used by an organization or business unit to respond to a specific system failure or disruption of operations. see business continuity plan see disaster recovery plan

continuous monitoring (CM)

ongoing observation of organizational resources to provide an updated picture of the organizations risk status

control

mechanisms designed to constrain or restrict access to resources

control category

organization of controls based upon functional design e.g., preventive, detective, corrective, etc.

control type

organization of controls based upon form factor e.g., physical, logical,

administrative

convincing

pertaining to law, lending itself to one side of an argument

cookie

small data files written to a user's hard drive by a web server

cookie poisoning

the alteration of the cookie for malicious purposes

copyright

intellectual property protection for the expression of an idea

corporate governance

see governance

corrective control

to stop bad behavior from continuing or to restore to a functional condition, not usually to normal, just simply working. e.g., UPS, diesel generator

COSO

Committee of Sponsoring Organizations

cost benefit analysis (CBA)

a systematic method of comparing the pro's and con's associated with spending money on a particular resource

counter (CTR)

a block cipher mode

countermeasure

a control put in place before a threat is realized that will help after the threat is realized. data backups would be an example

covert channel

a communication channel that is in violation of policy. this is done through timing or storage

CPU cache

dedicated fast memory located on the same board as the CPU

criminal law

wrong against society

crisis

a critical event, which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation, or ability to operate

critical functions

business activities or processes that cannot be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization

critical infrastructure

systems whose incapacity or destruction would have a debilitating impact on the economic security of an organization, community, nation, etc.

critical records

records or documents that, if damaged or destroyed, would cause considerable inconvenience and/or require replacement or recreation at considerable expense

cross certification

two certificate authorities that trust each other

cross site request forgery (CSRF)

attack where an HTML request sent from a malicious site, through a user's web browser to a second site with the goal of tricking the second site to think that the request was initiated by the browser CSRF tricks a user into

making a request from one site to another. the target site believes the request was initiated by the user not the original site

cross site scripting (XSS)

an attack achieved by hosting a (malicious) script on site a but having it displayed or presented at (trusted) site b. the target web browser runs the script as if it were from site b

cross training

ensuring that people are trained in multiple jobs. the main function is to ensure that critical jobs will always be covered even if the primary operator is unavailable

crossover error rate (CER)

the sensitivity tuning point where the FAR matches the FRR

cryptanalysis

code breaking, looking for weaknesses in a cryptographic system, practice of defeating the protective properties of cryptography. this includes ethical and unethical activities

cryptogram

encrypted or scrambled text, see ciphertext

cryptography

the art and science of creating encoded/encrypted/enciphered information often with the purpose of protecting the confidentiality and integrity of data, both at rest and in transit

cryptology

the study of cryptography and cryptanalysis

cryptovariable

the key used in cryptography for the purpose of encrypting or decrypting data

custodian

an entity that has possession of an asset(s)

customary law

a type of legal system built upon the traditions of the country, the laws may be written or not

damage assessment

the process following a disaster to computer hardware, vital records, office facilities, etc. that determines what can be salvaged or restored and what must be replaced. damage assessment also allows management to determine if disaster recovery procedures (DRP) must be initiated or if the business can return to normal operations within a reasonable time frame through normal process

dangling pointer

false memory reference

data backup strategies

those actions and backup processes determined by an organization to be necessary to meet its data recovery and restoration objectives. data backup strategies will determine the timeframes, technologies, media and offsite storage of the backups, and will ensure that recovery point and time objectives can be met

data backups

the backup of system, application, program and/or production files to media that can be stored both on and/or offsite. data backups can be used to restore corrupted or lost data or to recover entire systems and databases in the event of a disaster. data backups should be considered confidential and should be kept secure from physical damage and theft

data classification

see classification

data custodian

individuals and departments responsible for the storage and safeguarding of computerized data

data dictionary

a database that contains the name, type, range of values, source and authorization for access for each data element

data diddler

malware that makes small random changes to many data points

data hiding

a software design technique for abstraction of a process

data integrity

the property that data is in its original form and that it can be proven not to have been changed or modified in an unauthorized manner

data leakage

see data loss prevention

data loss prevention (DLP)

a program designed to safeguard intellectual property by controlling the flow of sensitive information out of a business with the goal of ensuring sensitive information such as PII are not leaked

data marts

small data warehouse, a specialized collection of data

data owner

individual ultimately responsible for the protection of the data

data recovery

the restoration of computer files from backup media to restore programs and production data to the state that existed at the time of the last successful backup

data warehouse

a federated repository of multiple databases used to identify trends that might be useful for business decisions

database management system (DBMS)

the control between a user and the raw database that controls access and organizes data

database replication

the partial or full duplication of data from a source database to one or more destination databases

database shadowing

real-time data backup (data mirroring)

databases

a central repository of data designed to reduce duplication and increase integrity

deadlock

a condition in which two subjects are attempting to access the same object at the same time. both subjects are prevented from completing their transaction

debriefing/feedback

communicate to stakeholders

decentralized

distributed across multiple device/locations, controlled and managed under multiple authorities

decipher

decrypting the encrypted message with the corresponding key

declaration

a formal announcement by pre-authorized personnel that a disaster or severe outage has occurred. the announcement triggers pre-arranged mitigating actions (e.g., a move to an alternate site.)

decode

to change ciphertext into plaintext

decrypt

to change ciphertext into plaintext

dedicated system

a system that processes only one level of classification e.g., a dedicated secret system containing secret documents being used by people with a secret clearance

defense in depth

a collection of security controls that work together to provide an elevated level of protection also known as layered defense

degauss

protection of stored or displayed information by removal/reduction of the magnetic field (demagnetization)

deleted file disk

space it used to occupy has been designated by the computer as available for reuse. the deleted file remains intact until it has been overwritten with a new file

deletion process

whereby data is removed from active files and other data storage structures

demilitarized zone (DMZ)

an area of partial trust containing resources owned by one entity but are accessible by the public

denial of service (DoS)

causing a user to not be able to perform their job because they are unable to reach something that they need to perform their job

desk check

see checklist

detective control

to record or alert, often used to inform security personnel that an event occurred, e.g., a log file

deterrent control

used to discourage desire to perform an action, e.g., the part of a policy that states that negative actions will be taken against individuals who violate the policy

diameter

a layer 7 centralized access control protocol that utilizes TCP

dictionary attack

using a list of potential passwords ('dictionary') to hash and attempt to match to a captured hash to uncover the password. a form of brute force

digital certificate

an electronic attestation of identity that is issued by a certificate authority

digital forensic science (DFS)

the study of media, software and network analysis for forensic purposes

digital signature

a cryptographic tool that proves the authenticity (integrity and proof of origin) of a message. the user will hash a document and then encrypt (sign) that hash with their asymmetric private key. often used to provide non-repudiation

directive control

controls that have a specific consequence if they are not followed. e.g., a policy that states failure to comply could result in anything up to and including termination of employment

disaster

a potentially catastrophic event which may disrupt critical services in

excess of the maximum tolerable downtime

disaster recovery institute (DRI)

international organization working with disaster recovery planning

disaster recovery plan (DRP)

the document that defines the resources, actions, tasks and data required to manage the recovery process in the event of a business interruption. the plan is designed to assist in restoring the business process within the stated disaster recovery goals

disaster recovery tape

portable media used to store data that is not presently in use by an organization to free up space but still allow for disaster recovery. may also be called “backup tapes”

disaster recovery teams

a structured group of teams ready to take control of the recovery operations if a disaster should occur. see business recovery teams

discretionary access control (DAC)

a manner of controlling access from the subject to the object based solely on the owner’s discretion or desires

disk mirroring

disk mirroring is the duplication of data on separate disks in real time to ensure its continuous availability, currency and accuracy. disk mirroring can function as a disaster recovery solution by performing the mirroring remotely. true mirroring will enable a zero-recovery point objective. depending on the technologies used, mirroring can be performed synchronously, asynchronously, semi-synchronously, or point-in-time

distributed denial of service (DDoS)

an attack against availability that comes from multiple vectors and consumes resources to the point of exhaustion. a DOS attack that is launched from many, perhaps thousands of points at once against a single target by bots

distributed processing

a computing technique that uses two or more computers to work together to run an application

domain

sphere of influence

double blind

testing of a system without prior knowledge by the tester or the tested

double door system (mantrap)

a physical enclosure for verifying identity before entry to a facility by routing people through one door that should close behind them, then using a second factor of authentication to allow passage through a second locked door. also used to prevent tailgating

DR or BC coordinator

the person responsible for overall recovery strategy and plans of an organization or business unit(s)

due care

performing in a way that matches the behavior of someone else (reasonable person rule) in a similar situation with similar knowledge

due diligence

an ongoing display of due care often implemented via investigation/review/analysis

durability

what is will remain, persistence

e-mail spoofing

forgery of the sender's email address in an email header

eavesdropping

a passive network attack involving monitoring of traffic

education

long term knowledge building

electronic code book (ECB)

a block cipher mode

electronic vaulting

electronically forwarding backup data to an offsite server or storage facility. vaulting eliminates the need for tape shipment and therefore significantly shortens the time required to move the data offsite

electrostatic discharge

power surge

emanations

potentially compromising leakage of electrical or acoustical signals

embedded

hardware or software that is part of a larger system

emergency

a sudden, unexpected event requiring immediate action due to potential threat to health and safety, the environment, or property

emergency operations center (EOC)

location where coordination and execution of BCP or DRP is directed

emergency procedures

a plan of action to commence immediately to prevent the loss of life and minimize injury and property damage

EMI

disruption of operation of an electronic device due to a competing

electromagnetic field

encapsulation

concept of a class's details to be hidden from an object, or in networking to place something like a TCP datagram within an IP packet

encipher

see encryption

encryption

a procedure that renders the contents of a message or file unintelligible to anyone who does not have the proper decryption key

enterprise security architecture

overall planning and strategy for an organization standardizing information security efforts in all areas. architecture is high level

equity law

under Napoleonic code it is the practice of lawsuits

escrow

to place something, usually software source code, with a trusted third party. usually for the purpose of protection from bankruptcy

ethics

the principles of behavior or beliefs that an individual or group sets for themselves to follow

European Union privacy principles

8 fundamental privacy protection principles

evaluation assurance level (EAL)

a resulting grade at the end of the ISO 15408 testing and evaluation process. there are 7 levels (1-7) where 7 is the highest grade

event

an observable occurrence, a change of state

executable content

content that is usually launched from a server and installs or performs something on the client device. aka mobile code

exclusive-or (XOR)

mathematical property whereby two binary numbers are combined resulting in a single bit output for every two bits of input. two separate inputs are combined to create a single output of the same length. uses the BOOLEAN "AND" function to combine but drops the carry. i.e. 1 and 1 = 0, 0 and 1 = 1, 1 and 0 = 0, 0 and 0 = 0

executive succession

the plan for who will step into leadership roles when those individuals have been lost to us

exercise

an activity that is performed for the purpose of training and conditioning team members, and improving their performance

exploitation

the action of launching a threat against an asset

exploratory model

research is used to enhance existing model

exposure

the condition of being revealed so that an attack or other type of incident may occur

exposure factor (EF)

percentage of loss when an incident occurs

external control

mandate by outside entities requiring policies, procedures and activities be implemented to ensure the best interests of the public are served by the organization

extreme programming

an application development methodology in which much of the functionality is coded in a very short amount of time by using several small teams

fail closed

a failure state for a control where it fails into a mode that does not allow the passage of anything

fail open

a failure state for a control where it fails into a mode that allows the passage of everything

fail safe

the failure state that ensures life safety

fail secure

a failure state that maintains the 'secure state' which could be either fail open or fail closed. see secure state

failover

the process of switching from a primary system or site to an alternate system or site following an incident

false positive

an alert or alarm that is triggered when no actual attack has taken place

false acceptance rate (FAR)

the rate a biometric system would allow unauthorized users into a system

false attack stimulus

the event signaling an IDS to produce an alarm when no attack has taken place

false negative

a failure of an ids to detect an actual attack

false rejection rate (FRR)

the rate a biometric system would deny access to authorized users into a system

faraday cage/ shield

a shield against leakage of electromagnetic signals

fast flux botnet

distributed denial of service attack where the attackers are constantly changing making it very difficult to filter or block the attack

fault

momentary loss of power

fault tolerance

mitigation of system or component loss or interruption through use of backup capability

fiber optics

bundles of long strands of pure glass that efficiently transmit light pulses over long distances

file

a unit or collection of data or information

file extension

a tag of three or four letters, preceded by a period, which identifies a data file's format, or the application used to create the file. file level deletion on the file level renders the file inaccessible to the operating system, available to reuse for data storage

file server

when two or more computers are networked together in a LAN situation, one computer may be utilized as a storage location for files for the group

file shadowing

the asynchronous duplication of the production database on separate media to ensure data availability, currency and accuracy. file shadowing can be used as a disaster recovery solution if performed remotely, to improve both the recovery time and recovery point objectives

file sharing

one of the key benefits of a network is the ability to share files stored on the server among several users

fire detection

alerts personnel to the presence of a fire

fire prevention

reduces causes of fire

fire suppression

to reduce fire

firewall

a control device installed to protect networks from each other by either blocking or allowing traffic as configured

firmware

reprogrammable basic startup instructions

FISMA

federal government requirement for federal agencies to create an information security program

forensic copy

an exact bit-by-bit copy of the entire physical hard drive or floppy disk, including slack and unallocated space. only forensic copy quality should hold up in court

forensic examination

a scientific analysis of evidence, physical or digital, in a manner that meets legal requirements

forward recovery

the process of recovering a database to the point of failure by applying active journal or log data to the current backup files of the database

Fraggle

a denial-of-service attack initiated by sending spoofed UDP echo request to IP broadcast addresses. (see Smurf)

fragmented data

live data that has been broken up and stored in various locations on a single hard drive or disk

framework

third party processes used to organize the implementation of an architecture

freeware

software distributed free of charge

frequency analysis

a cryptography attack that looks for patterns in the ciphertext that would reveal the patterns in the plaintext

full interruption test

a test for BCP or DRP that shuts down operation at the primary site and fails over to the alternate site such as the hot site

garbage collector

in software programming a garbage collector is used to "clean up" after an operation. as an example, a garbage collector could remove temporary installation files upon install, or wipe an area of memory prior to freeing it back to operation

gateway

a secure connection to another network

generator

fault tolerance for power

governance

executive responsibilities of guiding a business through goal setting, delegation and verification, based upon the mission of the business

guideline

a set of recommendations and good practices typically informative, but not mandatory in nature

hacker someone who wants to know how something works, typically by taking it apart

hard disk

a peripheral data storage device that may be found inside a desktop or laptop as permanent storage solution. the hard disk may also be a transportable version and attached to a desktop or laptop

harden

a process that secures a device by turning off unnecessary services, changing default passwords, closing unused ports etc.

hash function

a mathematical process that creates a representation of the data for integrity checking purposes

hearsay

evidence that is inadmissible because it is not cross examinable

high-risk areas

heavily populated areas, particularly susceptible to high-intensity earthquakes, floods, tsunamis, or other disasters, for which emergency response may be necessary in the event of a disaster

highly confidential

information that, if made public or even shared around the organization, could seriously impede the organization's operations

hijacking

interception of a communication session by an attacker

honeynet

a group or network of honeypots

honeypot

a computer designed for the purpose of distracting hackers, often placed in the DMZ. also useful for gathering information about attack techniques

host based intrusion detection system (HIDS)

software placed on an end device (server, pc, etc.) that looks for access attempts that are not permitted. it usually analyzes log files

host based intrusion prevention system (HIPS)

software placed on an end device (server, pc, etc.) that looks for access attempts that are not permitted and then attempts to block access

hot site

a recovery alternative that includes everything needed for all critical business function to recover, except people and at least some data

hot spares

redundant component that provides failover capability in the event of failure or interruption of a primary component

HTTP response splitting

also referred to as a carriage feed line return vulnerability, the HTTP response splitting allows the attacker to create two responses to one request. the first response is most often controlled by the destination web server while the second response (although it comes from the same server) is entirely under the control of the attacker

hub

layer 1 network device that is used to connect network segments together but provides no traffic control (a concentrator)

hypertext transfer protocol (HTTP)

a layer 7 protocol for transferring HTML web pages

identification

the assertion of your name (or userid) credentials to an authentication system

iframe

one HTML document embedded within another HTML document

incident

an event(s) that has the potential to cause harm

incident handling

the process of following a documented battle plan for coordinating response to an incident

incident management plan

high level (strategic) part of the business continuity plan that is used to manage the overall incident response process

incident manager

the person with the highest level of authority at EOC with knowledge of the business process and the resources available

incident response

the response of an organization to a disaster or other significant event that may significantly impact the organization, its people, or its ability to function productively

incomplete parameter check

failure to verify incoming data into a program

inference

to deduce information that you are not supposed to know from information you are allowed to know, to make a mental leap, often a concern with

databases

information disclosure

intellectual property that is no longer under the proper protections and has been seen by people that should not view this data

information flow model

mediation of covert channels must be addressed

information owner

the one person responsible for data, its classification and control setting. assigns "need to know" to the data

information security

protection of the confidentiality, integrity and availability of information

information security architecture

see enterprise security architecture

information security forum

a group that companies can join for the sake of sharing security best practices www.securityforum.org

information security governance

oversight provided by management to ensure that information is protected appropriately

information security management system (ISMS)

the security program built for a specific company

information security program

ongoing events, actions and activities employed within the organization to protect information

infrastructure

specific format of technical and physical controls that support the chosen framework and the architecture

inheritance

OOP concept of a taking attributes from the original or parent

initialization vector (IV)

randomly generated value used by many cryptosystems to ensure that a unique ciphertext is generated

inrush current

initial surge of current

instance

OOP concept of an object at runtime

integrated test

a test conducted on multiple components of a plan, in conjunction with each other, typically under simulated operating conditions

integrity

the correctness of the data

intellectual property (IP)

information that is critical or sensitive to a business

interception

unauthorized access of information (e.g., tapping, sniffing, unsecured wireless communication, emanations)

interference

noise, natural occurrence in circuits that are in close proximity

internal controls

the policies, procedures and activities put in place by the organization to ensure business goals and objectives are met

internal use

loss would inconvenience the organization, but disclosure is unlikely to

result in financial loss or serious damage to credibility

international organization on computer evidence (IOCE)

international forum for law enforcement agencies to exchange information on computer evidence

internet protocol version 4 (IPv4)

the current most widely used version of IP. IPv4 has a 32-bit address field and is used by most end users today for logically addressing computers and network

internet protocol version 6 (IPv6)

the new and improved version of IP. IPv6 has a 128-bit address field and is often used in the backbone of the Internet. offers many improvements over IPV4 including built in security and quality of service

interpreter

line by line translation from a high-level language to machine code

interrogate

to question a suspect or a person of interest in an intimidating environment

interview

to gather information through a discussion

intrusion detection systems (IDS)

a security system that is connected to a network or operates on a host watching for and logging any intrusion attempts based upon signatures, anomalies or heuristics

intrusion prevention systems (IPS)

a security system that is connected to a network or operates on a host watching for and blocking any intrusion attempts it can

invalid hyperlink

an erroneous web link that takes a user to the wrong, or a non-existent location. may result in a 404-type error

investigation

methodical research of an incident with the purpose of finding the root cause

IP address spoofing

forging of an IP address

IP fragmentation

an attack that breaks up malicious code into fragments, in an attempt to elude detection

IPSEC

a suite of security protocols to provide confidentiality, integrity and authentication of data over an IP network. often used with a VPN to protect data in transit

ISO/IEC 15408

international standard for evaluating security products. aka common criteria

ISO/IEC 17799

See ISO 27002

ISO 20000

a standard for proving that the organization is continually improving its IT management activities. This is a support document for implementing ITIL

ISO 22301

Societal security -- Business continuity management systems --- Requirements

ISO/PAS 22399

Societal security - Guideline for incident preparedness and operational continuity management

ISO/IEC 27000

an international standard providing information security vocabulary words and definitions

ISO/IEC 27001

an international standard defining requirements for creating, managing and maintaining an information security management system

ISO/IEC 27002

Information Technology - Security Techniques - Code of Practice for Information Security Management. an international standard that contains best practices to be used as a reference for selecting controls to be used within an Information Security Management System

ISO/IEC 27003

ISMS - Implementation guidance

ISO/IEC 27004

ISMS - Measurement

ISO/IEC 27005

an international standard for risk management within an information security management system

ISO/IEC 27006

ISMS - Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27031

Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity

ISO/IEC 27034

Guidelines for Application Security (draft) - This is a project to develop information-security guidance for those specifying, designing/programming, procuring, or implementing application systems

ISO 27799

Health informatics -- Information security management in health using ISO/IEC 27002

ISO 31000

Risk management – Principles and guidelines

ISO/IEC 42010

Systems and software engineering - Architecture description

ISO 7498

international standard for network protocols

isolation

another subject cannot see an ongoing or pending update until it is complete

iterative development

multiple waterfall approach

ITIL

a comprehensive set of best practices for IT services management

ITSEC

the past internationally accepted set of standards and processes for information security products evaluation and assurance, which separates function and assurance requirements

job rotation

to move from one location to another either keeping the same function or changing function. the purpose is cross training to avoid the problem of someone not showing up to work that is critical to the business leaving a function uncovered

job training

work done to ensure that an employee has the skills they need to perform their day-to-day job activities

joint analysis development (JAD)

users and developers working together to develop software that meets business needs

journaling

the process of logging changes or updates to a database since the last full backup. journals can be used to recover previous versions of a file before updates were made, or to facilitate disaster recovery, if performed remotely, by applying changes to the last safe backup

JPEG (joint photographic experts' group)

an image compression standard for photographs

Kerberos

authentication protocol which only uses symmetric session keys between principals distributed by a 3rd party using different pre-shared symmetric keys

Kerckhoff's principle

only the key protects the encrypted information

kernel

the core logic engine of an operating system which almost never changes

key

the variable that is applied to an algorithm that allows encryption or decryption to take place. aka cryptovvariable

key clustering

two different keys decrypt the same ciphertext

key distribution center (KDC)

one of the three names for the server in Kerberos. this function stores, creates and distributes symmetric keys for use within the Kerberos protocol

key escrow for PKI

to store another copy of a key

key goal indicator (KGI)

a metric, usually after the fact or lagging, used to tell management if the organizational business requirements have been met

key management

the management of the cryptographic keys over the life cycle of their existence from creation to zeroization

key performance indicator (KPI)

a leading indicator used to tell management if the process is working at an appropriate level to achieve the organizational goals

key risk indicator (KRI)

a metric used to indicate the probability that the acceptable level of risk is going to be exceeded

key space

total number of keys available that may be selected by the user of a cryptosystem

keyed hashing for message authentication

a hash that has been further encrypted with a symmetric algorithm

keystroke logging

recording activities at the keyboard level

known plaintext attack

a cryptography attack where the attacker has some of the plaintext and the corresponding ciphertext. if the algorithm and key can be uncovered the rest of the ciphertext can then be decrypted and read

labeling

to set the clearance of a subject or the classification of an object

lattice based model

a one way, directed graph which indicates confidentiality or integrity flow

layered defense

see defense in depth

layering

a programming design concept which abstracts one set of functions from another in a serialized fashion

least privilege

just enough permissions to be able to do the job at hand, minimum amount of access required to do the job

legacy data

information in the development of which an organization may have invested significant resources and which has retained its importance, but which has been created or stored by the use of software and/or hardware that has been rendered outdated or obsolete

liability

responsibility for actions

likelihood

the chance something will occur

Lockard's principle

a perpetrator leaves something behind or takes something with them at the scene of a crime

log

record of system activity, which allows for monitoring and detection of incidents, hacking, unauthorized activity, etc.

logic bomb

a program that waits for a condition or time to occur that executes an inappropriate activity

logical control

security controls executed in the hardware and or software mechanisms of a system. see technical control

machine language (machine code)

program instructions based upon the CPU's specific architecture

malformed input

inappropriate data

malware

malicious software written with the intent to cause harm (not a mistake in programming)

man-in-the-middle (MitM) attack

adversary intercepts communications, possibly decrypting, copying or even changing the data before sending it along to the true destination

mandatory access control (MAC)

a manner of controlling access that is very strict and rigid. It requires labeling of users and data as well as system enforcement of the corporate policy

mandatory vacations

requirement to take time off so that an audit can be performed against your work, usually a surprise vacation

mantrap

see double door system

maritime law

the law of the seas

marking

physical description on the exterior of an object that communicates the existence of a label

masked/interruptible

cooperative hardware and operating system notification process for prioritizing execution due to the change in state of components

masquerading

often described as spoofing your identity. most commonly used in terms of personal identities such as name. e.g., wear a brown uniform with the name UPS on the shirt. see spoofing

maximum tolerable downtime (MTD)

the maximum length of time a business system can be stopped before irreparable harm occurs

maximum tolerable outage (MTO)

the maximum length of time a business process can be stopped before irreparable harm occurs

memory management

a program in the operating system responsible for maintaining the hierarchical storage relocation requirements for processes and data from ram to hard drives

message digest

a condensed representation of a message that allows for integrity checking to be done to detect accidental changes can also be referred to as a hash value

metadata

information about a particular data set

method

OOP concept of an object's abilities, what it does

microwave

high frequency, highly directional radio signals. attackers target interception attempts at transmission and relay stations

mirrored site

recovery alternative, complete duplication of services including personnel

mirroring

the duplication of data for purposes of backup or to distribute network traffic among several computers with identical data

mission-critical application

an application that is essential to the organization's ability to perform necessary business functions. loss of the mission-critical application would have a negative impact on the business, as well as legal or regulatory impacts

mitigate

a choice in risk management, to implement a control that limits or lessens negative effects

mobile code

see executable content

mobile recovery

see mobile site

mobile site

a movable recovery location option that is usually used for short-term needs but can be high in cost

mock disaster

one method of exercising teams in which participants are challenged to determine the actions they would take in the event of a specific disaster scenario. mock disasters usually involve all, or most, of the applicable teams

modems

a network communication device that converts between digital and analog data

modification

a type of attack involving attempted insertion, deletion or altering of data

modified prototype model

a dynamic model

monitor

continuous surveillance, to provide for detection of any failure in controls

Moore's law

the founder of intel predicted that computing power will double every 18 months

multi-core

more than one CPU on a single board

multi-party control for PKI

to have more than one person in charge of a sensitive function

multi-processing

to execute more than one instruction at an instant in time

multi-tasking

more than one process in the middle of executing at a time

multilevel system (MLS)

systems capable of handling multiple levels of data classification while maintaining the appropriate levels of security. e.g., a system that contains both government secret and top secret data with users who have either secret or top secret clearanc

multiplexers

a device that sequentially switches multiple inputs to the output

multiprocessor

more than one processor sharing same memory, also known as parallel systems

multiprogramming

rapid switching back and forth between programs from the computer's perspective and appearing to do more than one thing at a time from the user's perspective

Napoleonic code

the legal system that is based on the ancient Roman system that requires laws to be written. aka civil law or Roman law

near site

a backup storage location in close proximity to the primary processing location that provides easy access to the data

need-to-know

requirement of access to data for a clearly defined purpose

network attached storage (NAS)

server optimized for providing file-based data storage to the network. unlike a file server, a NAS unit has no input or output devices, and the OS is dedicated for providing storage services

network based intrusion detection system (NIDS)

software or hardware that looks for access attempts that are not permitted and then logs it. the software could be placed on the router, firewall, switch, etc. the hardware would be a device sitting beside the router, firewall, switch, etc. in the network

network based intrusion prevention system (NIPS)

software or hardware that looks for access attempts that are not permitted and then attempts to block those attempts. the software could be placed on the router, firewall, switch, etc. the hardware would be a device sitting beside the router, firewall, switch, etc. in the network

noise

data or interference that can trigger a false positive

non-discretionary (NDAC)

system directed mediation of access without labels

non-interference

subjects will not interact with each other's objects

non-repudiation

you cannot deny or argue that you created, sent or received a piece of data

notification

communication of a security incident to stakeholders and data owners

object

passive entity in a subject object relationship. e.g., data, application, OS see subject

object

OOP concept of a distinct copy of the class

object oriented programming (OOP)

a programming design philosophy and a type of programming language, which breaks a program into smaller units. each unit has its own function

object reuse

the problem of reusing something that stores information (i.e., RAM, hard drive, CD). if the object is not properly cleaned residual data may be accessible by the next application. uncleared buffers or media

off-site

a location where staff cannot gain access readily and a regional disaster will not cause harm, usually a significant distance away. Often where an alternate site would be located or where data backups would be stored. see off-site storage

off-site storage

alternate facility, other than the primary production site, where duplicated vital records and documentation may be stored for use during disaster

recovery. see off-site

on-site

a location usually discussed in relationship to a copy of data backups located where staff can gain access immediately, because it is located within the primary location

one time pad (OTP)

a running key using a random key that is never used again

open mail relay servers

a mail server that improperly allows inbound smtp connections for domains it does not serve

open system

system design that allows for standardized interfaces

operating

state of computer, to be running a process

operational

intermediate level, pertaining to planning strategic - long term, operational - intermediate level, tactical – day-to-day

operational exercise

one method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation. operational exercises, which may involve one or more teams, are typically performed under actual operating conditions at the designated alternate location, using the specific recovery configuration that would be available in a disaster. see parallel test

operational impact analysis

determines the impact of the loss of an operational or technological resource. the loss of a system, network or other critical resource may affect a number of business processes

operational test

see operational exercise

organization for economic cooperation and development (OECD)

37 member countries working together to stimulate economic process

output feedback (OFB)

a mode of operation for symmetric block ciphers

overlapping fragment attack

a denial-of-service attack that manipulates the IP offset field of fragmented packets resulting in an overlap when the resulting systems attempts to reassemble the packet ex. teardrop

owner

an individual responsible for the protection of resources see data owner

packet filtering

an access control technique that permits some communication while preventing others based upon information contained in the IP packet header

parallel test

one method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation. operational exercises, which may involve one or more teams, are typically performed under actual operating conditions at the designated alternate location, using the specific recovery configuration that would be available in a disaster. see operational exercise

passive attack

where the attacker gains access to information. no change of the data is done. think eavesdropping

password cracking

to reveal authentication credentials

patch management

a management process of applying security software updates in a controlled

and documented manner

patch panels

provides a physical cross connect point for devices

patent

the registration of a novel, useful and non-obvious idea to protect the creator of that idea for a period of approximately 20 years

payload

final purpose or result

PBX

a private branch exchange is telephone exchange for a specific office or business

penetration testing

authorized security personnel using the tools and techniques of attackers to determine and confirm vulnerabilities of systems for the purpose of remediation

permission

authorization for a subject to interact with an object. see subject and object

permutation /transposition

moving letters around

personally identifiable information (PII)

any information that can be used to distinguish or trace an individual. e.g., name, social security number, phone number

pharming

poisoning the DNS cache on the host device

phishing

a social engineering attack that uses spoofed email addresses or websites to persuade people to divulge information

physical control

tangible control, such as a lock or guard

physical tampering

unauthorized access of network devices

plaintext

data that is in a natural or human-readable form

plan maintenance procedures

maintenance procedures outline the process for the review and update of business continuity plans

pointer

an index entry in the directory of a disk (or other storage medium) that identifies the space on the disk in which an electronic document or piece of electronic data resides, thereby preventing that space from being overwritten by other data. in most cases, when an electronic document is "deleted," the pointer is changed to a form that allows the document to be overwritten, but the document is not actually erased

policy

strategic, brief, high level statement from senior management that conveys their goals and objectives, the general "do's and don'ts" of the organization

polyalphabetic

encryption using many alphabets

polymorphism

objects or programming that looks the different but act same

preemptive

a type of multitasking that allows for more even distribution of computing time among competing requests

preventive control

controls deployed to avert or stop unauthorized and/or undesired actions

primary storage

memory - ram, registers, cache

privacy

a state of being hidden from public view

privacy-aware role-based access control (RBAC)

system mediation of access with the focus on the object's privacy

private key

a cryptographic variable that must be available only to its owner. the protected half of a public/private key pair. see symmetric see asymmetric

privileged programs

applications running with a high level of privileges e.g., a scheduler running with system level privileges

procedure

written step-by-step actions to accomplish a task

process isolation

an operating system function to prevent running threads of execution from using each other's memory. see sandbox

proprietary

define the way in which the organization operates

protection

memory management technique that allows two processes to run concurrently without interaction

protection profile (PP)

part of the Common Criteria requirements. a protection profile is generated by a user or user groups to define a category of product and the desired requirements of that product category. the protection profile will often be

used as the basis for the vendor created security target

prototyping method

build a simple version first then refine

proxy server

mediates communication between untrusted hosts on behalf of the hosts that it protects

prudent person rule

the legal concept that a person with reasonable knowledge would consider something to be a logical step to take

public key

a cryptographic variable that can be available to anybody in the world. It is one half of a mathematically linked set of keys in asymmetric cryptography systems, public/private key pair

public key infrastructure (PKI)

a pervasive infrastructure that includes a cooperative collection of business processes and technologies used for the purpose of binding a public key to an individual

purchase key attack

bribery or extortion of the key holder

qualitative

a subjective risk assessment method that involves comparing scenarios based upon the likelihood and the impact of a specific event

quantitative

a risk assessment method that involves calculating the actual cost in monetary values when a specific event occurs

race condition

a state where two subjects can access the same object without proper mediation

radio frequency interference (RFI)

lower frequency noise sag/dip short period of low voltage

RADIUS

a centralized authentication protocol from layer 7 of the OSI model that utilizes UDP

rainbow table attack

a precomputed dictionary attack

rapid application development (RAD)

a fast method of prototyping

reciprocal agreement

agreement between two organizations (or two internal business groups) with basically the same equipment/same environment that allows each one to recover at each other's site

record level deletion

renders the record inaccessible to the database management system

recovery

actions taken to resume critical functions following an incident

recovery control

to return to a normal condition e.g., restoring from backup

recovery period

the time period between a failure and a return to a functional condition

recovery point objective (RPO)

the moment in time to which systems and data must be recovered after an outage. usually stated in terms of acceptable or tolerable amounts of data lost as a measurement of time. e.g., 24 ms of lost data or 2 hours of lost data is tolerable

recovery strategy

a plan by an organization that will ensure its continuity in the face of a disaster or other major outage

recovery time objectives (RTO)

this is the amount of time left to actually do the work of recovering a server or function within the business after failure. recommended to be 1/2 MTD. see maximum tolerable downtime

redundant array of independent drives (RAID)

a group of hard drives working as one storage unit for the purpose of speed and fault tolerance

RAID 0

stripping across 2+ drives

RAID 1

mirroring to a second drive

RAID 2

requires 39 drives, then stripes with a hamming code added

RAID 3

Striping across two drives and parity added to a third drive

RAID 4

Striping across two drives and parity added to a third drive

RAID 5

Striping across three drives with parity interleaved

redundant servers

two servers (possibly more), one server in an active status and the second in a passive status. the passive server is ready to take over when the active server fails

redundant site

a backup location that business processes can failover to after a serious incident occurs

reference monitor (RM)

the hardware and software mediator of all subject and object interactions which has as its primary goal security policy enforcement

registration authority (RA)

the concept within public key infrastructure (PKI) where a user verifies their identity

religious legal system

a legal system based on the religious teachings. the religious leaders have a function within the legal system

relocation

memory management technique which allows data to be moved from one memory address to another

remote access trojan (RAT)

a trojan horse with the express underlying purpose of controlling host from a distance. software that allows remote control over a system. aka remote access tool

remote journaling

a database backup technique that periodically sends transaction data to a remote location

repeaters

layer 1 network device that is used to connect network segments together but provides no traffic control (a concentrator)

replication

a backup type which creates a complete copy. also known as database replication

residual data

refers to data that has been left behind after deletion

residual risk

quantity of risk remaining after a control is applied. often written as "risk - control = residual risk"

restoration

process to repair and return systems, facilities, people and processes to normal operations at the primary site

resumption

the process of recovering business functions after a failure of some kind

return on investment (ROI)

the financial consequences for actions or expenditures

reuse model

object oriented programming method that reuses objects in the new product

revocation for PKI

decertify an entity's certificate

ring protection

implementation of operating system protection mechanism, where more sensitive built upon the layering concept

risk

the chance that something negative will occur and the impact it will have on the organization

risk acceptance

management formally choosing to bear the burden of the loss should it occur. see risk mitigation, risk avoidance, risk transference, residual risk

risk analysis

see threat analysis

risk appetite

amount of risk a company is willing to take on

risk assessment

see threat assessment

risk avoidance

when an activity is potentially just too dangerous the organization makes a conscious decision to not engage in that activity

risk management

the process of assessing, analyzing and mitigating risks to business processes, systems and information

risk mitigation

controls placed within a business in order to reduce the chance or reducing the impact of a threat being realized

risk reduction

see risk mitigation

risk tolerance

acceptable level of deviation from risk appetite

risk transference

involving someone else in the absorption of the damage from a threat being realized. e.g., insurance

rogue access points

unauthorized wireless network access device

role based access control (RBAC)

to control access based on the function or role of the subject

rootkit

malware that subverts the detective controls of an operating system

routers

a layer three device that used to connect two or more network segments and regulate traffic

rubber hose attack

assault and battery of the key holder

rule based access control (RBAC)

to control access based on a configured set of rules. e.g., IP address, time of day, etc.

running

a process state, to be executing a process on the CPU

running key

an encryption method that has a key as long as the message

SABSA

a methodology for developing business-driven, risk and opportunity focused security architectures

safeguard

a preventive control that is intended to work to reduce the chance of an attack, proactive

salami

malware that makes many small changes over time to a single data point or system

sampling process

of statistically testing a data set for the likelihood of relevant information

sandbox

an isolated or quarantined environment within a system or organization used to isolate potentially unsafe elements

satellite

a specialized wireless receiver/ transmitter placed in orbit that facilitates long distance communication

scientific working group on digital evidence (SWGDE)

a group that "brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as ensuring quality and consistency within the forensic community"

Scytale

an ancient form of cryptography that was used in ancient Sparta

search warrant

a legal document issued by a judge or magistrate that allows law enforcement officials to search a residence or other location

secondary storage

the hard drive

secure socket layer (SSL)

an outdated secure networking protocol that operates at layer 4 of the OSI model that provides encryption and authentication features for client-server communications

secure state

a defined state of security as defined in the corporate policies

security blueprint

a template for the designing the security architecture within a business

security clearance

the level and label given to an individual for the purpose of accessing data that is compartmentalized and protected (classified)

security domain

an administrative unit or a group of objects and subjects controlled by one reference monitor

security kernel

the hardware, firmware and software of the TCB that houses and enforces the reference monitor

security metrics

a clearly defined, specific and repeatable measurement used to track security status

security program

companies plan to implement security into the organization. the security program defines what is important to the organization and how those things are going to be protected

security target (ST)

the vendor created document used as the basis for a Common Criteria evaluation. what the vendor claims their product can do and how to test it

sensitivity

an indication of the level of protection that must be placed around an item such as data, server, network

separation of duties (SoD)

to break a business process into separate steps and assign some steps to one person and some steps to another person requiring at least two different people to complete that process

sequence attacks

an attack involving the hijacking of a TCP session by predicting a sequence number

service bureau

recovery alternative which outsources a business function at a cost

service delivery objective (SDO)

the desired level of service to restore at an alternate site after a failure

service level agreement (SLA)

contractual agreement, usually from vendor or service provider, in which they promise a certain level of service delivery. e.g., a replacement device within the next 24 hours or up time of 99.999% of the time

SESAME

secure European system for applications in a multi-vendor environment. authentication protocol which uses both asymmetric and symmetric keys

session key

the key utilized in symmetric encryption to encrypt data, often used for data in transit. two devices will negotiate a session key to use for passing sensitive data

shadowing (file shadowing)

a database backup technique that creates a secondary copy of the database that is intentionally slightly lagging behind the primary

shareware

software licensing that allows a "trial" period at no cost

sharing

memory management technique which allows subjects to use the same resource

shielding

enclosure of electronic communication devices to prevent leakage of electromagnetic signals

shift cipher (Caesar)

encrypting by moving down the alphabet, leaving it intact, a certain number of spaces

shoulder surfing

to physically view another's keyboard and monitor activities

side channel attack

inference about encrypted communications

simulation

a type of BCP test designed to mimic the actual actions that would happen if a real event were to occur. e.g., fire drill

single level system

a computer system that processes all data at one level of security; the highest level

single sign-on (SSO)

an identification and authentication technique that relies on one account, one userid/password combo, and is used to access many or all resources within a network or business environment

slack

space unused storage capacity

Smurf

a denial-of-service attack initiated by sending spoofed ICMP echo request to IP broadcast addresses. (see Fraggle)

sniffing

eavesdropping on network communications by a third party

social engineering

actions to manipulate or influence another to take actions not in their own best interest

source route exploitation

a vulnerability in IP that allows an attacker to dictate the path of a communication and thereby access an internal network

spam

unsolicited commercial mail

spear phishing

phishing attacks that go after very specific targets

spam over instant messaging (SPIM)

SPAM that is sent by instant messenger

spiral

an application development methodology which addresses risk early and often

spam over internet telephony (SPIT)

SPAM that is sent by short message service (SMS)

spoofing

often stated as masquerading as another. most commonly used in terms of technical identities such as IP addresses. see masquerading

spyware

program that inappropriately collects private data or activity

SQL injection

an attack technique that exploits systems that do not perform input validation by embedding partial SQL queries inside input

standalone test

a test conducted on a specific component of a plan, in isolation from other components, typically under simulated operating conditions

standard

written document stating the authorized security actions. can be created either internally or externally, compliance is mandatory either way

state machine model

abstract and mathematical in nature, defining all possible states, transitions and operations

steering committee

a committee of decision makers, business owners, technology experts and continuity professionals, tasked with making strategic recovery and

continuity planning decisions for the organization

steganography

hiding the fact that communication has occurred

stopped

a process state, to be either be unable to run waiting for an external event or terminated

storage area network (SAN)

a subnetwork with storage devices servicing all servers on the attached network

strategic

high level planning and actions designed meet long term goals and objectives

strategy

an overall plan designed to meet long term goals and objectives

structured programming development

a modular development method that concentrates on high quality

structured walkthrough

a procedure for a group of peers to walk the business continuity plan as a verbal exercise through one scenario at a time. See walkthrough or tabletop test

subject

active entity in a subject object relationship. e.g., user, script, process see object

substitution

trading one for another, to replace

supervisor mode

a processor execution state in which instructions are executed by the CPU at a high privilege level

surge

sudden rise in voltage in the power supply

surge suppressor

to reduce sudden rises in current surveillance high degree of visual control

switches

a layer 2 device that used to connect two or more network segments and regulate traffic

symmetric

encryption system using a shared single key for encryption and decryption aka private key/single key/secret key/session key

syn flooding

a denial-of-service attack that overwhelms the target system with TCP connection requests that are not finalized

system downtime

a planned or unplanned interruption in system availability

system life cycle (SLC)

robust project management process of new systems with at least the following phases: design and development, creation, distribution, operation, maintenance, retirement, and disposal

system owner

individual responsible for the protection of the system

tabletop test

a procedure for a group of peers to walk the business continuity plan as a verbal exercise through one scenario at a time. see walkthrough or structured walkthrough

TACACS+

a layer 7 protocol for centralized authentication that utilizes TCP and encrypts the full authentication session

tactical

low level planning and actions designed to accomplish a task

tapping

eavesdropping on network communications by a third party

tar pits

mitigation of spamming and other attacks by delaying incoming connections as long as possible

target of evaluation (TOE)

the product that is being tested under ISO 15408

targeted testing

narrow scope examination of a system

TCSEC (orange book)

trusted computer system evaluation criteria. the past US military accepted set of standards and processes for computer systems evaluation and assurance, which combines function and assurance requirements

teardrop

an example of an overlapping fragment attack

technical control

hardware and or software mechanisms which require system interaction to gain access

tempest

a codename that refers to the study and mitigation of information disclosure via electromagnetic emanations from electronic equipment

temporal (time-based) isolation system

mediation of access with the focus on the time of day

territoriality

people protect their domain

test plan

a document designed to periodically exercise specific action tasks and procedures to ensure viability in a real disaster or severe outage situation

threads

a unit of execution

threat

potential danger to information or systems that will impact at least one element of CIA triad

threat agent

individual or group that creates a threat or causes a threat to be realized

threat analysis

the steps performed to enable a full understanding of the extent that a threat can cause damage

threat assessment

to understand threats as they exist

threat model

a tool that provides a perspective that allows us to see the harm a given threat can do if there is an exploitable vulnerability

threat source

the source or agent that launches the attack against an asset that would realize the threat

TIFF (tagged image file format)

one of the most widely supported file formats for storing bit-mapped images. files in tiff format often end with a .tif extension

time of check/time of use (TOC/TOU)

a race condition where the security changes during the object's access

timing and power analysis attacks

a cryptography attack that analyzes the time something occurs and the power that was output in an attempt to uncover the algorithm and key. collectively called side channel attacks

TNI (red book)

the past US military accepted set of standards and processes for network evaluation and assurance, which combines function and assurance requirements

TOGAF

the open group architecture framework. a set of tools and methodologies to developing an enterprise architecture

top secret

highly sensitive internal documents that could seriously damage the organization if such information were lost or made public

tort

a legally enforceable agreement between two people, two organizations, a person and an organization

tort law

the section of the legal system where lawsuits are filed under common law

total cost of ownership (TCO)

the cost of a control that includes not just the cost of the product but also the licenses, training costs, power, etc.

total risk

calculation encompassing threats, vulnerabilities and asset value

tracking

record history of incident

trade secret

intellectual property protection for a confidential and critical process

trademark

intellectual property protection for marketing efforts

training

a process designed to equip users with the necessary skills to accomplish a task, usually classroom based

transfer

a choice in risk management, to convince another to assume risk, typically by payment

transients

line noise that is superimposed on the supply circuit

transport layer security (TLS)

a layer 4 protocol for encryption and authentication within a client - server communication channel

trap doors (back doors, maintenance hooks)

a programming device use in development to circumvent controls

treaty

an agreement between countries

triage

an initial assessment of a situation to determine severity and to properly classify the incident. it also includes categorization of all events occurring at this moment for the purpose of prioritization

trojan horse

an application with a primary legitimate purpose known by the user and a secondary illegitimate, often nefarious purpose not known by the user. e.g.,

About The Author

Gwen Bettwy



wen Bettwy, CISM, CISA, CISSP-ISSAP, CCSP, SSCP is an information security specialist and trainer with Tactical Security. She has nearly three decades of information technology and security experience, both in the classroom and out. She has worked with thousands of students assisting them in their pursuit of industry certifications. Gwen lives in North Carolina with her two dogs.

About The Author

Mark Williams



Mark Williams, CISM, CISA, CISSP, is an information security trainer with Tactical Security. He has over 20 years of information technology and security training experience. In this time, using the proper combination of knowledge, experience, and test-taking tips, he has helped thousands of students to successfully pass industry leading security certification exams. Prior to becoming an instructor, Mark served in the U.S. Navy and also worked as a defense contractor.

About The Author

Mike Beevers

Mike Beevers, CISM, CISA, CISSP, is an information security trainer with Tactical Security. Mike been in the training industry for over 20 years and has received several awards for excellence. In addition to in class and online instruction, Mike has developed security training courses, security awareness training, and exam study questions for many information security exams. His roots in security began with a fundamental understanding of the value of protecting information while holding a security clearance in the United States Navy and as a DoD contractor.