

CompTIA®

Copyrighted Material

The Official CompTIA

**CASP+**

Study Guide

**Exam CAS-003**



**Official CompTIA Content Series** for CompTIA Performance Certifications

# The Official CompTIA® Advanced Security Practitioner (CASP+) Study Guide (Exam CAS-003)

Part Number: 093050

Course Edition: 1.1

## Acknowledgements

### PROJECT TEAM



Jason Nufryk, Author

Brian Sullivan, Media Designer

Peter Bauer, Content Editor

Thomas Reilly, Vice President Learning

Katie Hoenicke, Director of Product Management

James Chesterfield, Manager, Learning Content and Design

Becky Mann, Senior Manager, Product Development

James Pengelly, Courseware Manager

Rob Winchester, Senior Manager, Technical Operations

## Notices

### DISCLAIMER

While CompTIA, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with CompTIA. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). CompTIA is not responsible for the availability of, or the content located on or through, any External Site. Please contact CompTIA if you have any concerns regarding such links or External Sites.

### TRADEMARK NOTICES

CompTIA® and the CompTIA logo are registered trademarks of CompTIA, Inc., in the U.S. and other countries. All other product and service names used may be common law or registered trademarks of their respective proprietors..

### COPYRIGHT NOTICE

Copyright © 2018 CompTIA, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of CompTIA, 3500 Lacey Road, Suite 100, Downers Grove, IL 60515-5439.

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. If you believe that this book, related materials, or any other CompTIA materials are being reproduced or transmitted without permission, please call 1-866-835-8020 or visit **[www.help.comptia.org](http://www.help.comptia.org)**.



# The Official CompTIA® Advanced Security Practitioner (CASP+) Study Guide (Exam CAS-003)

<b>Lesson 1: Supporting IT Governance and Risk Management.....</b>	<b>1</b>
Topic A: Identify the Importance of IT Governance and Risk Management.....	2
Topic B: Assess Risk.....	7
Topic C: Mitigate Risk.....	18
Topic D: Integrate Documentation into Risk Management.....	28
 <b>Lesson 2: Leveraging Collaboration to Support Security</b>	<b>43</b>
Topic A: Facilitate Collaboration across Business Units.....	44
Topic B: Secure Communications and Collaboration Solutions.....	49
 <b>Lesson 3: Using Research and Analysis to Secure the Enterprise.....</b>	<b>55</b>
Topic A: Determine Industry Trends and Their Effects on the Enterprise.....	56

Topic B: Analyze Scenarios to Secure the Enterprise.....	66
 <b>Lesson 4: Integrating Advanced Authentication and Authorization Techniques.....</b>	<b>77</b>
Topic A: Implement Authentication and Authorization Technologies.....	78
Topic B: Implement Advanced Identity and Access Management.....	90
 <b>Lesson 5: Implementing Cryptographic Techniques.....</b>	<b>97</b>
Topic A: Select Cryptographic Techniques.....	98
Topic B: Implement Cryptography.....	113
 <b>Lesson 6: Implementing Security Controls for Hosts.....</b>	<b>123</b>
Topic A: Select Host Hardware and Software.....	124
Topic B: Harden Hosts.....	129
Topic C: Virtualize Servers and Desktops.....	137
Topic D: Protect Boot Loaders.....	145
 <b>Lesson 7: Implementing Security Controls for Mobile Devices.....</b>	<b>151</b>
Topic A: Implement Mobile Device Management.....	152
Topic B: Address Security and Privacy Concerns for Mobile Devices.....	159
 <b>Lesson 8: Implementing Network Security.....</b>	<b>171</b>
Topic A: Plan Deployment of Network Security Components and Devices.....	172
Topic B: Plan Deployment of Network-Enabled Devices.....	177
Topic C: Implement Advanced Network Design.....	182
Topic D: Implement Network Security Controls.....	189
 <b>Lesson 9: Implementing Security in the Systems and Software Development Lifecycle.....</b>	<b>203</b>

Topic A: Implement Security throughout the Technology Lifecycle.....	204
Topic B: Identify General Application Vulnerabilities.....	212
Topic C: Identify Web Application Vulnerabilities.....	219
Topic D: Implement Application Security Controls.....	225
<b>Lesson 10: Integrating Assets in a Secure Enterprise Architecture.....</b>	<b>237</b>
Topic A: Integrate Standards and Best Practices in Enterprise Security..	238
Topic B: Select Technical Deployment Models.....	243
Topic C: Integrate Cloud-Augmented Security Services.....	246
Topic D: Secure the Design of the Enterprise Infrastructure.....	250
Topic E: Integrate Data Security in the Enterprise Architecture.....	253
Topic F: Integrate Enterprise Applications in a Secure Architecture.....	257
<b>Lesson 11: Conducting Security Assessments.....</b>	<b>265</b>
Topic A: Select Security Assessment Methods.....	266
Topic B: Perform Security Assessments with Appropriate Tools.....	277
<b>Lesson 12: Responding to and Recovering from Incidents...289</b>	
Topic A: Prepare for Incident Response and Forensic Investigations.....	290
Topic B: Conduct Incident Response and Forensic Analysis.....	296
<b>Appendix A: Taking the Exams.....</b>	<b>305</b>
<b>Appendix B: Mapping Course Content to CompTIA® Advanced Security Practitioner (CASP+) Exam CAS-003.....</b>	<b>309</b>
<b>Solutions.....</b>	<b>333</b>
<b>Glossary.....</b>	<b>339</b>
<b>Index.....</b>	<b>365</b>



# About This Guide

Information security is a crucial field in the world of business. You have experience in this field, and now you're ready to take that experience to the next level. In this guide, you will expand on your knowledge of information security to apply more advanced principles that will keep your organization safe from the many ways it can be threatened. You'll apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement sustainable security solutions that map to organizational strategies; translate business needs into security requirements; support IT governance and risk management; architect security for hosts, networks, and software; respond to security incidents; and more.

Today's IT climate demands individuals with demonstrable skills, and the information in this guide can help you develop the skill set you need to confidently perform your duties as an advanced security practitioner.

## Guide Description

### Target Audience

This guide is designed for IT professionals in the cybersecurity industry whose primary job responsibility is to secure complex enterprise environments. You should have real-world experience with the technical administration of these enterprise environments.

This guide is also designed for learners who are seeking the CompTIA® Advanced Security Practitioner (CASP+) certification and who want to prepare for Exam CAS-003. Students seeking CASP+ certification should have at least 10 years of experience in IT management, with at least 5 years of hands-on technical security experience.

### Guide Prerequisites

To be fit for this advanced guide, you should have at least a foundational knowledge of information security. This includes, but is not limited to:

- Knowledge of identity and access management (IAM) concepts and common implementations, such as authentication factors and directory services.
- Knowledge of cryptographic concepts and common implementations, such as Secure Sockets Layer/Transport Layer Security (SSL/TLS) and public key infrastructure (PKI).
- Knowledge of computer networking concepts and implementations, such as the TCP/IP model and configuration of routers and switches.
- Knowledge of common security technologies used to safeguard the enterprise, such as anti-malware solutions, firewalls, and VPNs.

You can obtain this level of knowledge by training for *CompTIA® Security+ (SY0-501)* or by demonstrating this level of knowledge by passing the exam.

## Guide Objectives

In this guide, you will analyze and apply advanced security concepts, principles, and implementations that contribute to enterprise-level security.

You will:

- Support IT governance in the enterprise with an emphasis on managing risk.
- Leverage collaboration tools and technology to support enterprise security.
- Use research and analysis to secure the enterprise.
- Integrate advanced authentication and authorization techniques.
- Implement cryptographic techniques.
- Implement security controls for hosts.
- Implement security controls for mobile devices.
- Implement network security.
- Implement security in the systems and software development lifecycle.
- Integrate hosts, storage, networks, applications, virtual environments, and cloud technologies in a secure enterprise architecture.
- Conduct security assessments.
- Respond to and recover from security incidents.

## How to Use This Book

### As You Learn

This book is divided into lessons and topics, covering a subject or a set of related subjects. In most cases, lessons are arranged in order of increasing proficiency.

The results-oriented topics include relevant and supporting information you need to master the content. Each topic has various types of information designed to enable you to solidify your understanding of the informational material presented in the guide. Information is also provided for reference and reflection to facilitate understanding and practice.



At the back of the book, you will find a glossary of the definitions of the terms and concepts used throughout the guide. You will also find an index to assist in locating information within the instructional components of the book.

### As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

### Guide Icons

Watch throughout the material for the following visual cues.

<i>Icon</i>	<i>Description</i>
	A <b>Note</b> provides additional information, guidance, or hints about a topic or task.
	A <b>Caution</b> note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.

## 1

# Supporting IT Governance and Risk Management

**Lesson Time: 3 hours**

## Lesson Introduction

As a security professional, you are familiar with the ways in which information is vulnerable to theft, destruction, alteration, and unavailability. But good security is not just a process of reacting to individual threats when they appear or closing holes when they are discovered—you need to apply your security tasks in an overall framework of IT governance. In addition, you must understand how your information, by its very nature and the ways in which it is used, is at risk of being compromised. When you understand the risks you face from a foundational level, you can more effectively keep your day-to-day security operations aligned with business needs, and therefore provide optimal value to your organization.

## Lesson Objectives

In this lesson, you will:

- Identify the strategic value of IT governance and risk management.
- Assess risks that affect the organization.
- Translate risk assessment into specific strategies for mitigation.
- Integrate documentation into risk management.

# TOPIC A

## Identify the Importance of IT Governance and Risk Management

Every security-related task you perform on the job, and everything you'll do in this course, should build on a framework of IT governance. This is the guiding principle from which all of your actions should flow. In this topic, you'll be able to identify why IT governance is so important to protecting the enterprise, and why the supporting concept of risk management is just as vital.

### IT Governance

**Information technology governance (IT governance)** is a concept in which stakeholders ensure that those who govern IT resources in an enterprise are performing their duties in a way that fulfills the enterprise's strategies and objectives and creates value for the business. Other than evaluating IT management's performance, IT governance seeks to mitigate the risks that are associated with IT resources.

IT governance is concerned with *what* the organization can achieve by leveraging information technology. In order to do this, IT resources must align closely with business needs, and should support the business's overarching mission. Through this, governance enables IT management personnel to determine *how* to achieve this mission.

### IT Governance Frameworks

There are several existing frameworks of IT governance that businesses may adopt for easier integration. These frameworks can differ in terms of industry relevance, scope, and specific use cases. For example, the Control Objectives for Information and Related Technology (COBIT) framework is particularly popular for those enterprises that place a premium on risk management and mitigation.

### Impact of Good Governance

**Good governance** is generally defined as implementing processes that enable an organization to make the best possible decisions. An organization that exhibits good governance improves its likelihood of creating business value from its various assets, including IT resources. Security is no exception to this.

What exactly does it mean for security resources to "create value" for the business? Put another way, a security resource creates value by protecting the assets that are crucial in helping the business meet its strategic objectives. In order for security resources to align with the business strategy, they must be cost-effective and meet both high-level requirements set forth through governance and lower-level requirements that flow from these.

Security resources that contribute to good governance, therefore, contribute to the organization's success and survivability; and likewise, security resources that fail to uphold good governance may directly or indirectly harm an organization's ability to flourish.

### IT Governance and Risk Management

As a CompTIA® Advanced Security Practitioner (CASP+), you may not be directly in charge of guaranteeing good governance practices in your organization. However, a crucial element of good governance—and one that is most actively related to security activities—is risk management. IT governance and risk management lay the groundwork for all that you do as a CASP+, whether it's helping to train end-users on best practices, designing logically segmented network architecture,

configuring access control mechanisms on a host, and so on. You do these things to keep risk under control, which in turn supports good governance.

The stakeholders that oversee IT governance will expect the enterprise to adhere to a risk management framework that can both keep risk low and mitigate any growing risks. These principles will directly align with business objectives that mandate keeping the enterprise safe from threats and on good legal ground. To assuage the concerns of stakeholders, you may be called on to communicate how your IT department measures, responds to, and mitigates risks.

## Impact of Risk Management on Information Security

To meet the ever-evolving needs of information security, a CASP+ must be able to manage the risks that their information is exposed to. **Risk management** is typically defined as the cyclical process of identifying, assessing, analyzing, and responding to risks. This process is not meant to end; as long as information exists, it will need protecting. Therefore, risk management recurs indefinitely so that you may, at all times, keep your information as secure as possible. Without risk management, your security will be passive; and when you secure your information passively, it will be at the mercy of the quickly changing tides of technological advancement.



**Figure 1-1:** One way to represent the cycle of risk management.

## ERM

The comprehensive process of evaluating, measuring, and mitigating the many risks that pervade an organization is called **enterprise risk management (ERM)**. The ERM process is a vital part of any organization that strives to achieve its objectives by supporting good governance. Traditionally, the responsibility for an organization's ERM was placed in the hands of finance and actuarial science personnel. However, given that today's information landscape has a heavy focus on information and

interconnected systems across the world, the ERM responsibilities must now be shared by the IT department.

The amount and complexity of resources that enterprises provide can be overwhelming, and certainly a challenge to those responsible for keeping everything safe and secure. This enterprise approach to resource availability and accessibility introduces numerous ways in which attackers can compromise the operations of a business, and introduces just as many ways in which the enterprise's environment, employees, clients, and partners can unintentionally do likewise. By distributing the risk management functions across all levels of an organization, you can increase the awareness of cybersecurity issues and address all levels of risk management.

## Reasons to Implement ERM

The reasons that drive the adoption of ERM are numerous. The following are some examples:

- Keeping confidential customer information out of the hands of unauthorized parties.
- Keeping trade secrets out of the public sphere.
- Avoiding financial losses due to damaged resources.
- Avoiding legal trouble.
- Maintaining a positive public perception of the enterprise's brand/image.
- Ensuring the continuity of business operations.
- Establishing trust and liability in a business relationship.
- Meeting stakeholders' objectives.

Whatever the reasons may be, ERM is an increasingly important strategy in the business world and an intricate part of any CASP+'s duties.

## Risk Exposure

**Risk exposure** is the property that dictates how susceptible an organization is to loss. When quantified, risk exposure is usually defined as the product of the probability that an incident will occur and the expected impact or loss if it does occur.

An organization exposes itself to risk in every action it takes. These actions occur during the process of an organization conducting business, and the constant need for assessing those risks that has given rise to the security industry as a whole. Without risk, there would be no need for security, as there would be no consequences to poorly executed business processes. Since businesses are ever-increasing their dependence on technology, an increasing amount of risks involve computer security professionals as the primary means to manage those risks.

Through ERM, an organization can keep its risk exposure low, but it can never really avoid it entirely. This is why it is so critical for security professionals to constantly be vigilant for the elements of risk—including threats, attacks, and vulnerabilities—that have the potential to cause harm to the enterprise's assets. Ignoring your organization's exposure to risk will limit its ability to survive in any industry.

## Risk Analysis Methods

When determining how to protect computer networks, computer installations, and information, **risk analysis** is the security process used for assessing risk damages that can affect an organization. The risk analysis methods used to calculate for exposure can fall into one of three categories.

Method	Description
Qualitative	<b>Qualitative analysis</b> methods use descriptions and words to measure the likelihood and impact of risk. For example, impact ratings can be severe/high, moderate/medium, or low; and likelihood ratings can be likely, unlikely, or rare. Qualitative analysis is generally scenario-based. A weakness of qualitative risk analysis lies with its sometimes subjective and untestable methodology. You can also assign numbers between 0 and 9 for exposures and damage potential. However, you do not perform calculations on the numbers assigned to the risks. The goal of qualitative assessment is to rank the risks on a scale of 1 to 25, for example.
Quantitative	<b>Quantitative analysis</b> is based completely on numeric values. Data is analyzed using historic records, experiences, industry best practices and records, statistical theories, testing, and experiments. This methodology may be weak in situations where risk is not easily quantifiable. The goal of quantitative analysis is to calculate the probable loss for every risk.
Semi-quantitative	A <b>semi-quantitative analysis</b> method exists because it's impossible for a purely quantitative risk assessment to exist given that some issues defy numbers. For example, how much is your employee morale worth in terms of dollars? What is your corporate reputation worth? A semi-quantitative analysis attempts to find a middle ground between the previous two risk analysis types to create a hybrid method.

## Risks Facing an Enterprise

As an information assurance professional, you're likely to face risk in many different forms. Before you can even begin to mitigate risks, you need to know where they exist within your enterprise and identify how they can cause harm. The following table categorizes various types of risk that you may encounter in your enterprise. Keep in mind that cyber risks affect all areas and types of enterprise risks, and that they are not necessarily technical, but can be articulated in business terms.

Risk Type	Description
Legal	Every enterprise, no matter the industry, must comply with certain laws and regulations to stay within legal boundaries. Unethical business practices, unscrupulous employees, and negligent management can all place your enterprise in jeopardy. Even poor forensic practices can put your enterprise's ability to successfully prosecute attackers in court at risk.
Financial	Your organization likely has expected revenue and profit margins based on a number of calculations, and many different threats can cause your business to fail to meet monetary expectations. Financial risks may seriously affect your enterprise's survivability in a competitive marketplace.
Physical assets	Depending on your enterprise's size, you may have a great deal of valuable physical property stored in various company sites. Any physical product that your organization sells is your primary concern. Electronics such as computers, industrial machinery, and office appliances are also at risk of being stolen or otherwise damaged. Both human threats and environmental factors may put your physical resources at risk.

<b><i>Risk Type</i></b>	<b><i>Description</i></b>
Intellectual property	Organizations that create and own intellectual property, such as entertainment media, software, trade secrets, and product designs, all risk having these ideas and concepts destroyed or used in unauthorized ways. Although intellectual property is typically not stolen in the same sense as physical theft, a threat may infringe on trademarks and copyrights that you have in place. A threat that destroys or alters your intellectual property may make it extremely difficult or even impossible to recover.
Infrastructure	An organization must depend on its structure to function at maximum efficiency. Whether physical or abstract, the frameworks that hold an organization together are vulnerable to a number of threats. This is particularly true of any infrastructure that supplies power or facilitates transportation. Infrastructure risk affects the business at its foundational level.
Operations	Day-to-day operations are what keep your enterprise running and fulfilling not just its monetary expectations, but also its vision. Your organization is at risk of having its vision compromised if it cannot operate to the extent it needs to. Even if there are no immediate financial consequences, the enterprise risks losing its foothold in the marketplace, and its products or services may no longer be viable.
Reputation	The public's perception of an organization may greatly affect its success, and in some cases, may doom it to failure. Businesses must maintain great relationships with their customers and understand how society at large views the business. Your organization's brand may be devalued if the public reacts negatively to scenarios such as theft of personal data, unethical business practices, and a decline in the quality of products and services.
Health	Whether it's your employees or the customers they work with, people are at risk of harm as a result of your operations. Although high-risk industries like law enforcement have obvious health concerns, even typical businesses can put their personnel and customers at risk by providing unsafe, untested products and services. Physical assets like industrial machinery and electrical equipment may pose significant health risks to employees who use them.

# TOPIC B

## Assess Risk

Now that you've identified the importance of risk management in the context of IT governance, you can begin the management process by assessing how risk will impact your organization. For an enterprise, there are many different elements of normal business operations that may affect its risk profile. Being able to identify how these elements are relevant to your enterprise's security will prevent you from missing crucial information when the time comes to mitigate risk.

## ESA Frameworks

**Enterprise security architecture (ESA)** is a framework used to define the baseline, goals, and methods used to secure a business. When focused on risk, ESAs start with an assessment of the risk and quantify how internal and external threats and vulnerabilities manifest themselves to the organization; they then proceed to the mitigation of each specific threat, vulnerability, and risk. Beyond standard information security practices, ESAs are valuable for saving an organization time, money, and resources. This is possible because the cohesive design of an ESA framework is able to pull security practices together so that they work with one another.

Once an organization successfully implements an ESA, they can generate a roadmap by evaluating which risks pose the most liability to the organization. Based on the liabilities, it may be possible to get additional resources to mitigate those risks or it may demonstrate that the organization is adequately protecting itself from risk.

Examples of ESA frameworks include:

- National Institute of Standards and Technology Special Publication (NIST SP) 800-37
- Control Objectives for Information and Related Technology (COBIT®)
- Information Technology Assurance Framework (ITAF™)
- Information Technology Infrastructure Library (ITIL®)
- International Organization for Standardization (ISO®) 27001/ISO 27002
- Sherwood Applied Business Security Architecture (SABSA®)
- The Open Group Architecture Framework (TOGAF®)

## ESA Framework Assessment Process

Depending on how comprehensive the ESA framework is, there may be specific pre-defined steps the organization can follow to address the risk. The following is a list of assessment steps in an example ESA framework:

1. Develop a baseline assessment using internal resources and professional assessment software.
2. Conduct a thorough review of existing security policies.
3. Conduct an assessment of the physical and environmental elements of the enterprise.
4. Examine and assess the internal network for vulnerabilities.
5. Examine and assess external network connectivity and vulnerabilities.
6. Examine and assess connectivity and information sharing with third-party entities (supply chain, managed service providers, cloud services, etc.).
7. Examine and assess wireless connectivity and security.
8. Examine and assess resource accessibility and policies that govern resource access.
9. Examine and assess all hosts, host configurations, and host documentation.
10. Examine and assess all infrastructure devices and connectivity.
11. Identify human factors such as resource use, resource access, and policies that surround use and access.

12. Examine and assess security awareness and training policies.

## New and Changing Business Strategies

As the world adopts new technology, it brings about new forms of doing business. The best example of this is comparing the pre-Internet era with the current one. Prior to the Internet, companies performed most business-related functions themselves. Things like payroll, administrative duties, product development, and communications were all integrated and managed by each organization. Today's interconnected world, however, offers rich opportunities for companies to partner with other organizations, outsource their operations, rely on cloud providers for support, and merge and demerge assets with other business entities. For example, in a virtual organization, the mobility of its users, **crowdsourcing** of services, and the globalization of its network can result in wide open opportunities for cyber risk. All of these business models and strategies have an impact on computer security and management of risk in the enterprise.

## Partnership Strategies

A business partnership offers the partnering companies shared opportunities that either company might not have on its own. Partnership agreements are used to define the roles, responsibilities, and actions that each partner will take to make the partnership successful. Risk management is an important part of evaluating these agreements. Without this step, each of the partners may be exposing itself to risks which could put both companies in jeopardy of losing information or revenue, or by increasing liability past an acceptable limit. Your security team should be brought in prior to the partnership being finalized.

The partnership agreement should define how the organizations will still secure their private data, which sets of data each organization will have access to, and how that information should flow. Each organization, outside of the agreement, should conduct its own risk assessment of the processes proposed and what mitigating controls they should implement.

### Example

An example of risk within a partnership is when two organizations decide to approach a common goal, such as when an operating system manufacturer works with hardware vendors. Think of the complexities of Google™ working alongside a smartphone manufacturer like Samsung when creating Android phones. Both organizations have agreed to partner to create a device with a blend of each other's software and hardware. The organizations must be linked together in some way to facilitate operations, yet each organization has other business operations that they must secure and keep separate.

## Outsourcing Strategies

Outsourcing as a business practice can enable the organization to focus on core competencies while shifting high-cost, low-value, and non-core business processes to a service provider that can more efficiently run these processes. Risk management is a key component of outsourcing. Although the contracted organization is liable in part for the security risks of its operations, it is critical that organizations that decide to outsource evaluate and constantly audit the provider's actions. Audits should be performed to evaluate the provider's data handling, fulfillment of service-level agreement (SLA) criteria, and business conduct on behalf of the organization. Failing to perform recurring audits may lead to severe penalties against the parent organization. This is especially true when sensitive data is involved in the outsourcing arrangement or where legal regulations or compliance requirements are present.

A common pitfall in outsourcing arrangements is the depth to which an audit is conducted. In most cases, the outsourcing provider is contractually obligated to provide its yearly reports to clients, but those audits may not necessarily apply to all systems within the scope of the outsource provider's network. It is critical to understand the scope of all audit documents provided to your organization

from any provider and evaluate nuances in the report such as the use of (or lack thereof) the phrases "all systems" or "in scope systems." It is also important that you never assume that security reports given by the system provider necessarily encompass everything that they should. The provider might conduct a technical penetration test that comes back clean, but this is no guarantee that a social engineering attack wouldn't compromise their systems.

## Cloud Strategies

Cloud models are an increasingly common business strategy for organizations looking to offload technical components like data backups, server hosting, and virtualization platforms to an easily accessible Internet-based resource.

Like typical outsourcing, cloud-based solutions require an enterprise to rely on a third party to host and maintain these components. However, the cloud model differs in that it offers automation of components and processes to more easily facilitate the enterprise's needs. An outsourcing provider might simply take on a system already in place to lighten the burden on the enterprise, but a cloud provider might give the enterprise an entirely new set of options and services that could greatly affect the enterprise's operations.

The cloud might provide an entirely new software suite, or even an entirely new platform, and the enterprise must incorporate these unfamiliar elements into its ERM processes. For example, the cloud service may provide virtualized networking infrastructure that raises security issues for the flow of sensitive traffic. The auditing that the enterprise typically accepts from outsourcing providers may need to be reworked and targeted specifically for the cloud provider. Automating cloud resources provides a challenge to security administrators, as these resources may become more and more opaque to the client enterprise.

## Merger and Acquisition Strategies

Mergers and acquisitions occur when two organizations decide it is more profitable to operate under one banner rather than separately in a partnership. A merger provides an excellent time to conduct risk management activities since it gives both organizations a heightened sense of analysis and business management oversight to their operations. The two companies as a combined entity must consider influencers such as corporate culture, brands, business units, market opportunities, information consolidation, and numerous other components that drive ERM.

Mergers and acquisitions can also be challenging as one organization may have more strict security controls than the other. When merging, differing technology platforms will need to be integrated, controls will need to be aligned between the two organizations, security reporting structures will need to be streamlined, sensitive data governance will need to be reviewed, and more; all of which can have significant impact to both organizations if done poorly. It is best to conduct risk assessments before a merger so that each organization is aware of the other organization's risk portfolio.

### Example

As an example, a hosting company acquires a consulting company in another country. While the hosting company has many years of experience securing a network critical to its business, the consulting company has never had to secure its systems to the same degree. Most of its recurring security budget is spent on endpoint defense for the laptops being used in the field by its consulting personnel, and not on using advanced network intrusion detection systems, Internet gateway protection, host intrusion detection, or monitoring software. Once the merger is completed, the security team is brought in to integrate the systems. However, unbeknownst to both organizations, the consulting company's email systems had been breached many years prior to the merger. As a result, both organizations are now exposed to additional liability that could have been avoided had proper security activities taken place prior to the merger.

## Demerger and Divestiture Strategies

When an organization splits its business into several entities, it may be restructuring to strengthen its brand awareness, or it may be responding to government intervention through anti-trust regulations. Whatever the reason, demergers and divestitures require the careful application of ERM, just as much as mergers do.

Like mergers, enterprise components like company culture, brands, and market opportunities all have their place in a demerger. When the company splits, each entity may take their own components with them—and in many cases, each entity may wish to still share some of the same ones. A proper risk assessment will take into account that any assets—especially those of a sensitive nature—must be reconsidered in light of this restructuring. If both entities retain access to the same sensitive data, but have diverging security policies, then this may introduce risk to one or both of the new entities.

In addition, demergers and divestitures raise the issue of data ownership. Whoever owns a particular set of data is ultimately responsible for its security, and each split entity needs to be aware of and agree to the ownership terms laid out in the demerger. Likewise, data that transfers ownership may need to go through a reclassification process to ensure that it aligns with the split entity's unique data security policies.

## Integration of Diverse Industries

Sometimes enterprises that operate in different industries will find it beneficial to integrate business operations. There are various security concerns of integrating diverse industries which you can incorporate in your risk assessment.

<i>Integration Element</i>	<i>Security Concern</i>
Rules and policies	Crafting effective security rules and policies is all about fine-tuning them to your own specific needs as a business. A business that operates in a different industry will likewise customize their policies to fit their own needs. Therefore, integrating with a business that has policies that fail to meet your requirements, or outright contradict your rules, may pose a risk. It's important to assess where these rules and policies are divergent.
Legal requirements and regulations	Different industries are subject to different laws and government regulations. If your business integrates with another that fails to follow these laws and regulations, yours could also be held liable if this impropriety is discovered. In other situations, simply integrating with enterprises in certain industries could require you to observe these same laws and regulations. For example, an enterprise that integrates with a technology vendor may be subject to export controls that limit how information and technology is transferred outside of the country.
Geography	Certain industries may be more or less inclined to operate in specific geographic locations. For example, the transportation industry has a heavy presence in urban areas, and less so in rural locations. Your business may be unaccustomed to the increased security risks associated with congested, dense populations, so if you plan on integrating with a transportation business, you need to reassess your risk profile. Other geographic factors to take note of include: physical ease of access, strength of infrastructure (electricity, network cabling, etc.), climate, and natural disasters.

Integration Element	Security Concern
Foreign laws and customs	In addition to physical concerns, a geographically disperse enterprise also raises issues when it comes to foreign laws and customs. Your enterprise will be subject to the jurisdiction of any country where it operates. Since each country's laws differ—often in significant ways—the enterprise must adjust its security practices to account for these differences where applicable. Likewise, you should consider the issue of <i>data sovereignty</i> , or the sociopolitical outlook of a nation concerning computing technology and information. Some nations may look unfavorably on the data protection practices your security policies require, such as encryption.

## Third-Party Providers

When you assess risk in your own organization, you generally take into account the various ways in which a third party's lapse in judgment might impact your systems. But not every facet of the third party's operations might be open to you, and for good reason. They need to keep certain elements confidential, just as your organization does. So how do you assess risk in an environment you cannot completely and unrestrictedly survey?

One such approach is to ensure that third parties have a requisite level of information security through strong security training and awareness programs in place within their organization. You, as a CASP+, may have spent a good amount of time drafting a comprehensive policy for best security practices for employees, but your third-party provider may not have a comparable policy for any number of reasons. So, you should share best practices with third parties so that they may better inform their employees. After all, the human element is often the biggest risk in any organization.

Likewise, depending on your arrangements with the third party, you may even extend or provision security controls to them to strengthen their systems. A risk assessment might uncover an area of the third party's operations that poses an unacceptable amount of risk to your enterprise, but providing them with proper equipment and protocols could help mitigate the risk.

## De-perimeterization

*De-perimeterization* is the process of shifting, reducing, or removing some of the enterprise's boundaries to facilitate interactions with the world outside of its domain. In information security, this implies that a de-perimeterized business will shift its focus from creating a secure perimeter to incorporating security in other ways. For example, you might place more emphasis on encrypting your sensitive data rather than attempting to regulate access to your network from the outside (for example, remotely connecting to an internal server over the Internet).

The impact of de-perimeterization on risk depends on the ways the perimeter changes. The following table lists some of those ways, and the risk considerations of each one.

<i>Perimeter-Changing Concept</i>	<i>Risk Consideration</i>
Mobility	Remote employees may use a virtual private network (VPN) to tunnel into your network and access what they need, or they may simply use equipment and services that you provide to them. These remote employees expand your network's or business's boundaries, and may bring increased risk with them. Any external connection could compromise your network as a whole if it is not properly secured on both ends. This includes VPN services and remote authentication technology. Additionally, employees may use their own devices for their jobs, but these will not necessarily be as tightly controlled as the devices that are in your reach.
Cloud	Cloud services can reduce strain on your business by offloading business operations and resources to an Internet-based provider with distributed resources. However, this also reduces the amount of control you have over your environments that are hosted elsewhere. Reputable cloud providers will offer at least some security guarantee, but this may not be sufficient, depending on your risk appetite. Additionally, the cloud provider's security measures will be useless unless they are properly integrated with the security in your own enterprise. Being able to comprehensively assess a cloud provider's risks is also a challenge that you may not be able to complete.
BYOD	<i>Bring your own device (BYOD)</i> is a phenomenon in which employees use their personal mobile devices in the workplace. If your business tolerates this, you will need to recognize that work done while in the office may leave the office after close of business. This pushes your boundaries farther than you can totally manage. You may be able to enforce secure handling of sensitive data while employees are in the office, but once they are outside, that data will be at risk. This is because many users do not make the effort to secure their own personal devices, or in some cases, their devices may be inherently insecure.
Outsourcing	Like relying on a cloud service, outsourcing business operations to another enterprise will shift your security domain to an environment that you may not necessarily have control over. The company you outsource to may have its own set of security policies and procedures, or it may not have any at all. If you are unable to enforce your expected level of security, the assets you outsource could place the rest of the enterprise in jeopardy, especially if those assets hold information or infrastructure vital to the enterprise's survival.

## User Behaviors

Products, technologies, threats, and user behaviors are constantly changing within an organization, and with these changes come new risks. As new products and technologies are implemented, it is your job as a CASP+ to assess the risk to your organization and guide the implementation appropriately. Risk is not necessarily a negative, so you need to assess how these new elements can provide value to the business.

Users often present the largest risk to an organization. Users have access to data, are usually not as technically savvy as systems administrators or security personnel, and are frequently targeted by attackers through the use of social engineering methods. In any well-rounded risk management program, security professionals must analyze the ways in which the organization does business both

internally and externally with partners, outsourcers, and clients. By analyzing the business processes used, it is possible to find weaknesses which could be exploited by attackers.

For example, if an organization relies on email as a means to submit work requests through a trouble ticket system, it may be possible for attackers to use Simple Mail Transfer Protocol (SMTP) spoofing to submit fraudulent work requests such as system modifications or actions that will expose sensitive data. The ability of attackers to manipulate a company's human element is one of the best ways to gain access to an organization that has invested heavily in technical controls, but has not invested enough in employee training and awareness.

## New Products and Technologies

As new products are used by an organization, new vulnerabilities and threats are introduced, which increases risk. Depending on the prevalence of these products and the data they are associated with, the risks may be small or large. When evaluating new products, it is important to include the ERM process as well as consult with human resources (HR) and legal counsel for any regulatory or employment law requirements regarding how the products are used. At the beginning of the risk management process, you should evaluate products first for vulnerabilities and then for threats which may target those vulnerabilities. After that, you can quantify the risks and liabilities those threats present to your organization.

From one product to another, the risks are often fairly static. For example, while two different web platforms may not have identical security features, they suffer from the same potential sorts of risks: SQL injection, cross-site scripting, cross-site request forgery, and so on. If new products interoperate with legacy products, this may put either or both at risk, as their security protocols may be incompatible.

Similar to new products, new technologies must be evaluated for vulnerabilities and threats, but one technology might have markedly different risks from another. For example, mobile computing platforms like tablets and smartphones suffer from similar risks to traditional desktops, such as buffer overflows, yet have new risks, such as the ease of loss due to their small size and mobility. When implementing new technology, your organization should include HR and legal counsel to determine if any regulatory requirements exist.

In the ERM process, you may also draft certain policies that govern how new technology is deployed and used. For example, your policy might stipulate that all new technology be tested in a sandbox environment before being implemented live on the enterprise network. Like new products, new technologies that interoperate with older technologies may cause security issues.

## New Threats

Attackers are constantly inventing new attacks, and how organizations conduct business is always changing. This cycle of recurring change introduces new threats into an organization, and thus new risks. Even beyond human malice, other factors may unintentionally threaten the security of an organization in the midst of a change.

For example, if an organization sets up a new office in a coastal city, the prevalence of hurricanes may be a new threat the organization will need to analyze and develop a recovery plan for. Under a malicious threat, if a new weakness is found in an encryption protocol such as Secure Sockets Layer/Transport Layer Security (SSL/TLS), the organization will need to determine how to patch its systems or mitigate the threat in another way. You should always expect risk management to be a recurring process rather than a single static exercise performed periodically.

## Internal and External Influences

Many different types of events influence risk. Some of these influences are internal and some are external to the organization. You should assess how each influence aids or detracts from the risk management process.

<i><b>Influence Type</b></i>	<i><b>Risk Assessment Relevance</b></i>
Internal compliance	<p>Internally, all the employees of an organization are stakeholders that are concerned with the safety and security of the organization. When senior management signs off on an ERM plan, everyone should be expected to assist with its implementation; that is, be in compliance with the plan. This is not always easy to do, as a great deal of training may be required and numerous policies and procedures may be put in place to ensure full compliance.</p> <p>When done properly, internal compliance assessments can identify controls which are not operating as intended and are not reducing the risk to acceptable levels. Since internal users bring a high degree of risk to an organization's network and systems, including them in your assessment of risk will produce more accurate results. After all, they are the ones who access and use those systems on a daily basis and can help identify areas where additional risk treatment is necessary.</p>
External compliance	<p>All businesses must comply with external regulatory entities. It is important that your organization follows all applicable laws, regulations, and standards. The federal government will, for example, enforce the Health Insurance Portability and Accountability Act (HIPAA) in organizations that work in the healthcare industry. Even standards that are not necessarily legally binding, like those enforced by the International Organization for Standardization (ISO), are ubiquitous in the enterprise landscape.</p> <p>Although the goal of compliance regulations is to provide a minimum acceptable baseline for managing risks in a particular industry or organization, most regulations do not place requirements on the effectiveness of a control, but instead on whether or not the control is present. Without measuring a control and applying a baseline to the regulation, it is impossible to determine if the controls are effectively deployed within the enterprise. This is why simply being compliant will not necessarily produce an optimum risk assessment. Your organization may be compliant, but still may not be as secure as it should be under the intent of the regulation or standard.</p>
Internal client requirements	<p>Internal clients are often stakeholders in ERM planning and implementation because they are direct users of corporate resources. Internal clients should be involved in risk assessment, as they are at the forefront of recognizing risks that impact the enterprise. If they are not, it will be impossible to secure their environments, which in turn will lead to client dissatisfaction and reduced customer business.</p>
External client requirements	<p>The involvement of external clients depends on their needs. External clients have a vested interest in the ongoing activities of the organization with which they conduct business. In that regard, they are another front-line resource for identifying the threats and vulnerabilities of the business.</p> <p>At the same time, external clients who are part of ERM planning for their trading partners might demand that the ERM plan include business continuity protocols so that their source of supply can continue in the event of a loss. They might also insist on measures that protect the confidentiality that they share with their trading partners. Because of this vested interest, external clients can provide insight on the ways to assess risk in an organization that has business relationships.</p>

<i><b>Influence Type</b></i>	<i><b>Risk Assessment Relevance</b></i>
Audit findings	Audit findings influence risk by providing evidence that controls are adequate in reducing or eliminating risk. Where an auditor's results are below acceptable thresholds, the organization should assess the residual risk and determine if mitigation, transfer, or acceptance is the correct approach. In some cases, it is impossible to reduce risk further; for example, where the use of legacy systems is required as part of an established business function. In cases such as this, it may be necessary to change the business process or outsource the function entirely to avoid the risk. Likewise, it may be necessary to rethink your technology infrastructure.
Top-level management	Top-level management is one of the key stakeholders in the risk assessment process. Without proper risk assessment, they will be unable to make informed decisions about how to operate the business. When presenting both internal and external risk to executive management, quantitative analysis and accurate metrics are two of the key components that you must communicate effectively. When this is done, it will be easier for you to get buy-in from executive management for risk mitigation plans and the appropriate funding of security initiatives.
Competitors	Competitors can drive changes in business. In order to stay competitive, the organization may develop new products, incorporate new technology, and expand customer markets. All of these activities bring their own risk to the enterprise.

## System-Specific Risk Analysis

To understand the risks to an enterprise, a CASP+ must be able to analyze the enterprise systems to understand how those systems are used and how the confidentiality, integrity, and availability of the systems are threatened. A number of different frameworks and processes have been established to assist this analysis. Although how you go about your analysis will differ with respect to what you're analyzing, the following are some common questions to ask when trying to quantify a risk:

- How can an attack be performed?
- Can the attack be performed in the current network and are the assets accessible?
- Can the requirement for authentication diminish the possibility of attack?
- What is the potential impact to the **confidentiality**, **integrity**, and **availability** of the data?
- How exploitable is the flaw? Is it theoretical or does a working exploit exist?
- Are there workarounds or patches available?
- How confident is the report of the vulnerability? Is it an established and tested approach?
- What could be the potential damage to the organization?
- How many targets exist within the organization?
- What are the confidentiality, integrity, and availability requirements for the assets in question?
- How likely is the risk to manifest itself?
- What mitigating protections are already in place? How long will it take to put additional controls in place? Are those additional protections cost effective?
- How can the risk be articulated in terms that the business will understand (such as in the context of the risk to the overall architecture/system/service)? How can you translate technical risks into terms of how it could occur and what the effect would be on the business (for example, loss of revenue, reputation, legal repercussions)?

## Examples

If, for example, your enterprise is a cloud provider with multiple sites worldwide, your analysis should focus on the chances of an attack succeeding, what an attack can compromise in terms of the

data you host and its availability to your customers, and how exactly an attack can be performed. In this scenario, patches and software fixes may be irrelevant to stopping an attack, so you won't necessarily focus on that in your analysis. Likewise, you may be less concerned with the cost-effectiveness of any controls, since you have a considerable security budget.

If your organization is small and has primarily local customers, you'll want to approach your analysis differently. Cost-effectiveness becomes a significant factor in security controls, as your budget will likely be limited. Also, you may want to focus more on the damage an attack will do to your own systems, since you're unlikely to have the amount of redundancy that a large enterprise will. The point is, before you even begin your risk analysis, you should tailor it to your own situation to maximize its efficacy and dispense with irrelevant factors.

## Risk Determinations

A significant part of risk assessment is determining just how certain risks can specifically impact the enterprise. Two influential factors in risk determination are the likelihood of threats and the magnitude of impact.

You can determine the likelihood of a threat bringing risk to your organization by using the following methods:

- Discovering the threat's motivation, if it has any. What does an attacker stand to gain from conducting an attack? Note that some risks, like accidents and non-human factors (e.g., fires and floods) have no motivation.
- Discovering the source of the threat. Who is the threat? Is it an individual or a group? Where are they from, and what is their experience?
- Determining the threat's *annual rate of occurrence (ARO)*. How often does the threat successfully affect the enterprise?
- Conducting a trend analysis to identify emerging threats and threat vectors. How effective are these threat vectors and how have they been exploited before?

A quantitative assessment of risk attempts to assign a monetary value to the elements of risk, as in the following formula:

**AV (Asset Value) x EF (Exposure Factor) = SLE (Single Loss Expectancy)**

The *single loss expectancy (SLE)* value represents the financial loss that is expected from a specific adverse event. If you know how many times this loss is likely to occur in a year, you can calculate the cost on an annual basis:

**SLE (Single Loss Expectancy) x ARO (Annual Rate of Occurrence) = ALE (Annual Loss Expectancy)**

The *annual loss expectancy (ALE)* value is calculated by multiplying an SLE by its ARO to determine the financial magnitude of a risk on an annual basis.



**Note:** The ALE may be a moving target, as threats cannot necessarily be quantified as occurring annually, but rather on an individual basis.



**Note:** Two additional risk determination factors, return on investment (ROI) and total cost of ownership (TCO), are described in a later lesson.

## Guidelines for Assessing Risk

Follow these guidelines when you assess risk in the enterprise.

### Assess Risk in the Enterprise

When assessing risk:

- Implement an ESA to more easily define your security expectations.

- Evaluate new products and technologies in light of their new functionality and architecture, as well as how they interoperate with older systems.
- Stay up-to-date on the latest threats.
- Assess user behaviors as a point of weakness, especially due to social engineering threats.
- Draft security agreements for partnerships that include data handling requirements.
- Conduct thorough audits of outsourced assets.
- Conduct thorough audits of cloud providers that host your assets.
- Assess risk before a merger or acquisition occurs to look for any differences in security policies, data classification, procedures, or controls.
- Consider lost or continually shared assets in the event of a demerger or divestiture.
- Consider the rules and policies, regulations, and geographic issues associated with integrating with businesses in different industries.
- Consider how internal and external compliance, internal and external client requirements, and audit findings influence risk.
- Consider how practices like telecommunication and BYOD may impact your organization's network perimeter.
- Determine what a threat is, where it comes from, and what risk it poses to the enterprise.
- Calculate the SLE and ARO of a threat, then use the product of these two values to ascertain your ALE.
- Document your assessment results clearly and comprehensively.

# TOPIC C

## Mitigate Risk

After assessing how particular elements in your operations can bring risk to the enterprise, you're ready to actively respond to those risks. Mitigation is all about balancing your response capabilities with your tolerance for risk, and there are several different approaches that may work best for you. As a CASP+, you'll choose the most appropriate mitigation strategy to keep your enterprise as safe from harm as is feasible.

## Classes of Information

When developing a risk mitigation strategy, you need to classify the information that needs to be protected. The requirements to protect information will differ between jurisdictions, so you must examine the applicable regulatory requirements to ensure the classification takes this into account. Some information is more or less critical than other types. In general, there are four classes of information that organizations use:

- **Public** information, which presents no risk to an organization if it is disclosed, but does present a risk if it is modified or not available.
- **Private** information, which presents some risk to an organization if competitors were to possess it, if it were modified, or if it were not available.
- **Restricted** information, which might be limited to a very small subset of the organization primarily at the executive level (e.g., corporate accounting data), where unauthorized access to it might cause a serious disruption to the business.
- **Confidential** information, which would have significant impact to the business and its clients if it were disclosed. Client account information like user names and passwords, personally identifiable information (PII), protected health information (PHI), and payment card information/cardholder data (CHD) would be in this category.

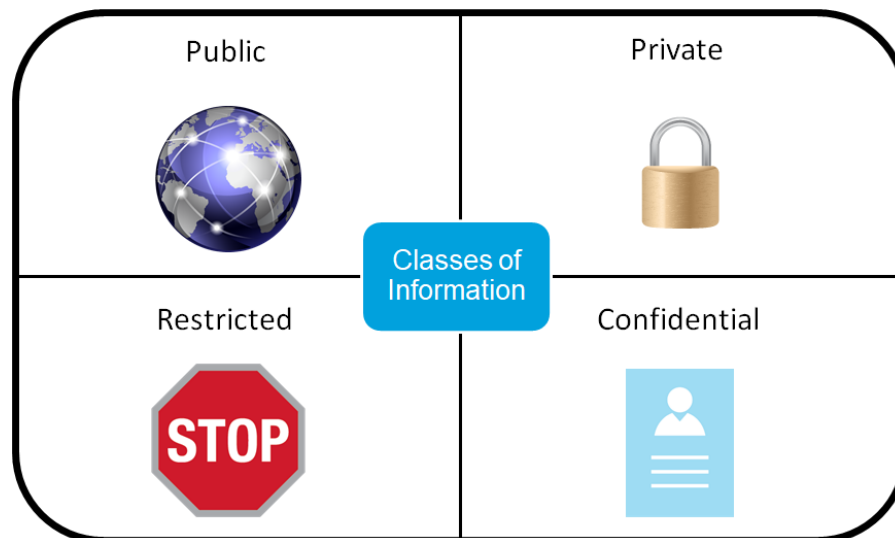


Figure 1–2: Classes of information.

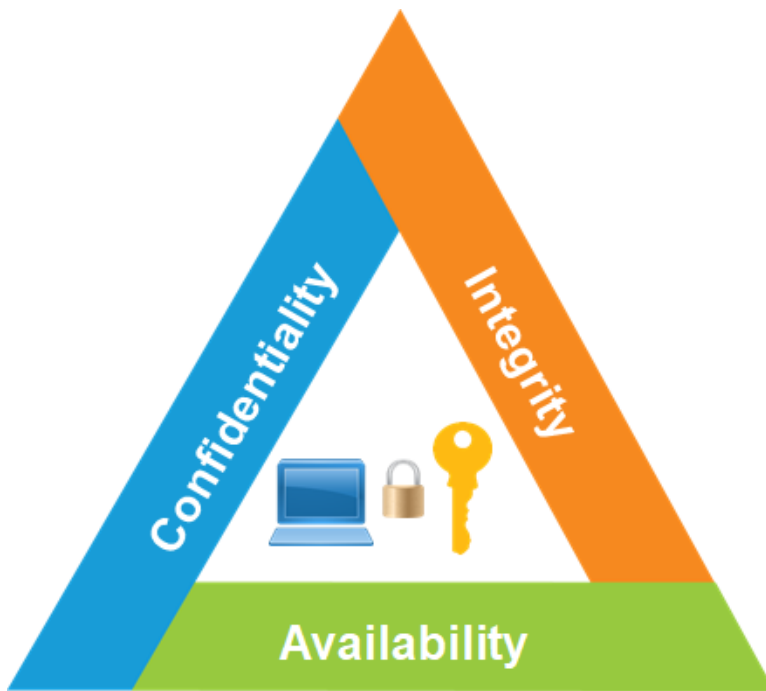
## Classification of Information Types into CIA Levels

Information is not categorized by access levels only; it can also be thought of in terms of how a compromise of that information can negatively impact the three core security attributes of the

**confidentiality, integrity, and availability (CIA) triad.** When surveying information within an organization, it is important not to solely judge the type of information, but how that information is used throughout the business as well. Public information, if disrupted, wouldn't necessarily cause problems from a confidentiality perspective. However, availability may drop significantly, compromising a very crucial part of any enterprise's security focus. Ultimately, you should investigate how each data category in your organization fits into the larger three goals of security so that you may be better prepared to respond to risk.



**Note:** The CIA triad is sometimes referred to as the AIC triad, CAI triad, etc., to differentiate it from the U.S. Central Intelligence Agency.



**Figure 1-3: The CIA triad.**

### Example

Imagine a large outsourcing company that runs payroll applications for its clients. This outsourcing provider would have massive quantities of confidential information, including names, addresses, bank account and routing numbers, Social Security numbers, and tax return data. It may also have self-administered health plan data that would be classified under HIPAA as PHI, bringing a regulatory and compliance element to its operations as well.

Now contrast that organization against a small company, where such data would be relative to the size of the company and there would be little to no required uptime to support it. By comparing these two companies, you can see how organizational perspective and scope can increase or decrease the risks associated with different types of data. While penalties and liability associated with a confidentiality and integrity breach of the payroll records would impact either organization, the outsourcing provider has significantly more at stake. Not only would brand damage result from the outsourcing provider's exposure or loss, but they would also lose immediate income through the refund component of their service-level agreement (SLA).

The smaller organization may be penalized for exposing data or failing to protect it from tampering; however, compared to the larger payroll provider, the smaller organization has less at stake.

## Stakeholder Input for CIA Decisions

When making security-related decisions based around CIA, it's important to incorporate stakeholder input as part of the process. Together, stakeholders may offer a more complete perspective on dimensions of the business you may be unaware of. Even small, seemingly unimportant dimensions may cause damage if they escape your notice. Because they may have more experience in certain areas, stakeholders will also be able to communicate their unique security concerns to you for your consideration. Whether it's employees, customers, or investors, stakeholders will keep you fully informed about the many ways in which the principles of CIA affect your enterprise.

## Select Controls Based on CIA Requirements

Once a specific risk has been quantified, it is possible to determine the best approach to mitigating the specific risk through various controls. Risks can be mitigated based on the specific CIA attribute targeted, and the technology used to reduce the risk does not always cover all three attributes. Consider the following table, in which examples of technical controls are reviewed and selected in terms of how they do or do not uphold the CIA principles.

<i>Technical Control</i>	<i>Upholds Confidentiality?</i>	<i>Upholds Integrity?</i>	<i>Upholds Availability?</i>
User permissions for network share	Yes, by keeping unauthorized users from accessing shared data	No	No
Load balancers for web servers	No	No	Yes, by routing traffic to hosts that are available and have capacity
Message authentication codes (MACs) used in digital signatures	No	Yes, by comparing the expected message digest with the actual message digest upon output	No

As you can see, no single technology in this list of examples addresses all three attributes. An organization has well-rounded security when it specifically upholds all three components of the CIA triad. Keep in mind, however, that CIA attributes are not the only criteria by which you can select the optimal controls for your organization. Ultimately, your organization must define which parameters it needs to uphold in order to mitigate risk—this will drive your process for selecting the right controls.

## Application of Controls That Address CIA Requirements

There are several approaches you can use to address risks to confidentiality; for example, encryption and access control. In both cases, the goal is to limit the readability of data to only authorized parties. What you implement will depend on your needs as an organization; access control may be enough to keep unwanted users from accessing somewhat sensitive data, but in scenarios where data is much more sensitive, you may want to aim for encryption to achieve the strongest confidentiality assurances.

Controls to address risks to integrity primarily rely upon data validation and auditing. This includes the use of read-only data stores and strong authentication controls in applications using multiple factors. Auditing controls function by monitoring the integrity of the data as it exists in the system and as data is passed through input and output routines. Auditing is a useful policy for essentially all organizations, though it isn't as active in maintaining integrity as forms of validation like hashing are.

Most commonly, organizations implement redundancy measures to mitigate hardware failures, which have a serious impact on availability. By using failover techniques such as active-passive and active-active, it is possible to seamlessly failover to backup hardware. However, not all threats are caused by hardware failure. In some situations, the consumption of resources is responsible for the system becoming unavailable. An example of this would be a denial of service (DoS) attack which leverages a flaw in the software to consume resources beyond the intended limits of the system or architecture. Once started, a DoS attack can be very difficult to recover from. There are various flood control mechanisms that may prevent successful DoS attacks, such as load balancers.

## Aggregate CIA Score

Once information critical to the business has been classified by the risk associated with its CIA attributes, and stakeholder input and technical controls are considered in the context of the CIA triad, it is possible to develop risk scores for the data. This is done subjectively and is based on a sliding scale of harm to the business, where:

- The highest risks are rated at a **10**.
- The lowest risks are rated at a **1**.
- Data having no risk (for example, public data) is rated at a **0**.

The CIA attributes of information are compared to the threat that each attribute faces, then multiplied to produce a total. The totals for each attribute are added to produce the aggregate CIA score for that entire risk.

## DoS Attack

Consider the following risk matrix. In this example, the threat of a DoS attack is being calculated on a network in terms of CIA. Although the analysis is subjective, you can still reliably and consistently quantify risk based on a sliding scale. This quantification is based on several factors, including how easy the attack is to perform, any controls that may already be in place to mitigate the attack, and the scope the attack is likely to cover.

<i>CIA Attribute</i>	<i>Value of Information</i>	<i>Threat Value</i>	<i>Total Risk</i>
Confidentiality	7	0	0
Integrity	3	0	0
Availability	8	10	80

The aggregate CIA score for a DoS condition is **80**. Using this score, you can compare it against other risks. Since enterprises have limited budgets and staff resources, not all risks may be able to be mitigated, so it is important to prioritize some responses over others.

## Database Intrusion

Compare the aforementioned DoS example with the database intrusion example in the following matrix.

<i>CIA Attribute</i>	<i>Value of Information</i>	<i>Threat Value</i>	<i>Total Risk</i>
Confidentiality	7	10	70
Integrity	3	5	15
Availability	8	5	40

The aggregate CIA score for the database intrusion condition is **125**. This is greater than the DoS attack from earlier (**80**), so you prioritize database intrusion over the DoS in the ERM process. In prioritizing, you are able to determine the minimum required security controls for each risk. This scenario dictates that you implement stricter requirements for intrusion protection than DoS attacks.

For certain assets, you might weigh the components of CIA differently. For example, confidentiality might matter more than availability for customer information because of the legal repercussions of stolen data.



**Note:** The previous examples are simplified, theoretical models for assessing and classifying risks to the enterprise. In the real world, such an assessment would be much more complex and involve many more factors and metrics.

## Articulate Risks Using Business Language

To ensure that the business stakeholders understand the risks, in addition to calculating an aggregate score, you should articulate the risk in business language such that the cause and effect can clearly be understood by the business owner of the asset. The DoS risk should be put into plain language that describes how the risk would occur and as a result what access is being denied to whom and the effect to the business. For example: "As a result of malicious or hacking activity against the public website, the site may become overloaded, preventing clients from accessing their client order accounts. This will result in a loss of sales for  $n$  hours and a potential loss of revenue of  $n$  dollars."

## CVSS

Risk scores depend on the integrated concept of risk. Vulnerabilities are a big part of that concept. Most vulnerabilities today are rated using the **Common Vulnerability Scoring System (CVSS)**. The CVSS is a risk management approach where vulnerability data is quantified and then the degrees of risk to different types of systems or information are taken into account. Since it is an open source formula for risk quantification, the CVSS is easily modified to fit a specific organization's needs. The CVSS is similar to the examples used previously, but it is much more granular.

The system consists of the three core metric groups (and their associated sub-metrics): base metrics that characterize fundamental components of a vulnerability, temporal metrics that qualify components of a vulnerability that change over time, and environmental metrics that qualify components of a vulnerability that depend on specific contexts and implementations. The following table lists these metrics and sub-metrics.

<b>Base Metrics</b>	<b>Temporal Metrics</b>	<b>Environmental Metrics</b>
Access vector	Exploitability	Collateral damage potential
Access complexity	Remediation level	Target distribution
Authentication	Report confidence	Confidentiality requirements
Confidentiality impact		Integrity requirements
Integrity impact		Availability requirements
Availability impact		

The strength of the CVSS is that it produces consistent results for the vulnerability's threat in the base and temporal metric groups, while allowing organizations to match those results with their specific computing environment. You can do this by using the CVSS calculator (available at <https://nvd.nist.gov/cvss.cfm?calculator&version=3>) and plugging in your own metric values.

## CVE

The CVSS is used to score vulnerabilities in the **Common Vulnerabilities and Exposures (CVE)** system, a public dictionary of vulnerabilities that facilitates the sharing of data among organizations, security tools, and services. In a sense, the CVE normalizes data about a vulnerability so that fixing or mitigating the issue is less of a challenge. The CVE is maintained by the non-profit **MITRE Corporation** and receives funding from the U.S. Department of Homeland Security.

There are several elements that make up a vulnerability's entry in the CVE:

- Each vulnerability has an identifier that is in the format: **CVE-YYYY-####**, where **YYYY** is the year the vulnerability was discovered, and **####** is at least four digits that indicate the order in which the vulnerability was discovered.
- A brief description of the vulnerability.
- A reference list of URLs that provide more information on the vulnerability.
- The date the vulnerability entry was created.

CVE-ID	
<b>CVE-2017-0144</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.	
References	
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"> <li>• EXPLOIT-DB:42030</li> <li>• <a href="https://www.exploit-db.com/exploits/42030/">URL:https://www.exploit-db.com/exploits/42030/</a></li> <li>• EXPLOIT-DB:42031</li> <li>• <a href="https://www.exploit-db.com/exploits/42031/">URL:https://www.exploit-db.com/exploits/42031/</a></li> <li>• EXPLOIT-DB:41891</li> <li>• <a href="https://www.exploit-db.com/exploits/41891/">URL:https://www.exploit-db.com/exploits/41891/</a></li> <li>• EXPLOIT-DB:41987</li> <li>• <a href="https://www.exploit-db.com/exploits/41987/">URL:https://www.exploit-db.com/exploits/41987/</a></li> <li>• CONFIRM:<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144</a></li> <li>• BID:96704</li> <li>• <a href="http://www.securityfocus.com/bid/96704">URL:http://www.securityfocus.com/bid/96704</a></li> <li>• SPECTRACK:1037991</li> <li>• <a href="http://www.securitytracker.com/id/1037991">URL:http://www.securitytracker.com/id/1037991</a></li> </ul>	

**Figure 1-4: CVE-2017-0144, which details a vulnerability in the Windows implementation of the Server Message Block (SMBv1) network-sharing protocol that enables an attacker to execute arbitrary code on a target host. EternalBlue, which exploits this vulnerability, was used to propagate the WannaCry ransomware attack in 2017.**



**Note:** Although the CVE is very useful for identifying weaknesses in your systems, in some circumstances, you may be unable to replicate the vulnerability.

## Extreme Scenario Planning and Worst-Case Scenarios

Planning for the worst is a necessity in any risk management strategy. Although extreme events are unlikely, they are often devastating enough to warrant some sort of plan of action. Some examples of extreme events include:

- The total DoS of your network and other systems.
- The theft of encryption keys.
- The theft, tampering, or destruction of trade secrets that keep your business competitive.
- The theft, tampering, or destruction of financial data.
- The theft, tampering, or destruction of national secrets.
- The total loss of systems through natural disasters, such as earthquakes, hurricanes, and floods.

To mitigate the risk of these worst-case scenarios, consider the following strategies:

- Gather intelligence to identify threats that can instigate extreme scenarios.
- Identify the motivations of these threats, if they have any.
- Identify the skill level required to carry out these threats and the probability that the perpetrators will be able to successfully carry out an attack.
- Identify what vectors these threats can take to instigate extreme scenarios.
- Determine what assets in your organization are the most critical and susceptible to extreme scenarios.
- Determine controls that will help prevent or mitigate an extreme scenario.
- Identify what exactly you risk by failing to prevent an extreme event.

## Enterprise Resilience

**Enterprise resilience** is the ability of an enterprise to adapt to changes that affect business operations, as well as its ability to evolve and meet future challenges with greater preparedness. Resilience is a comprehensive strategy that incorporates risk management and involves all aspects of the enterprise contributing to the security and viability of the enterprise as a whole. In other words, there is not just one single tactic that will make the enterprise resilient, but a combination of multiple integrated and collaborative tactics. In addition, tactics are not purely technical in nature, but must also include more abstract business practices to help support the survivability and growth of the enterprise.

Such tactics may include, but are not limited to:

- Ensuring the high availability of critical systems, especially public-facing systems that are a major source of revenue.
- Ensuring the redundancy of mission-critical systems so that an unrecoverable failure of the primary set can be compensated for by alternate sets.
- Ensuring the scalability and elasticity of infrastructure to anticipating ever-changing resource demands.
- Ensuring that stakeholders play an integral part in the process of identifying and assessing risks.
- Ensuring that the enterprise is able to anticipate and adapt to changes in the marketplace or industry in which it participates.
- Ensuring that the enterprise is adequately prepared to withstand changes to the local environment, politics, and economy.
- Ensuring that the enterprise and its personnel do not support or encourage unlawful business practices.

Resilience prevents changes from compromising the survivability of the business, whether those changes are inherently negative, positive, or neither. Rather than implementing mitigation tactics—like those in the previous list—in a vacuum, you can ensure that they serve the larger goal of contributing to a resilient enterprise.

## Risk Response Techniques

How an organization reduces or removes risk is based on the thresholds established for different risks and it is entirely dependent on the risk appetite of the organization. The following table describes the four possible approaches to risk response.

<b><i>Risk Response Technique</i></b>	<b><i>Description</i></b>
Avoid	<b>Risk avoidance</b> means that risk has been completely eliminated (reduced to zero). This is generally achieved by terminating the process, activity, or application that is causing the risk. For example, if you do not need a chat program to facilitate collaboration among employees, you might simply block access to it from within your systems, thus eliminating the risk it brings. Total risk avoidance is virtually impossible in any enterprise, as it would necessitate that you remove many vital systems that your business requires to function.

<b>Risk Response Technique</b>	<b>Description</b>
Transfer	<b>Risk transference</b> moves the responsibility for managing risk to another organization, such as an insurance company or an outsourcing provider. This external organization takes over and maintains the risks associated with data and other resources. Examples include purchasing natural disaster insurance to cover servers and the data present on them, and relying on cloud providers to store and secure data. You should choose the transference approach if the risks become larger and more complicated than your enterprise can manage without impeding your operations.
Mitigate	<b>Risk mitigation</b> is the process of implementing controls and countermeasures to reduce the likelihood and impact of risk to an organization. Organizations will mitigate risk so that the potential harmful outcomes do not exceed the organization's risk appetite. For example, if you have a high-traffic network, you may reduce the risk the traffic poses to the network by implementing an <b>intrusion prevention system (IPS)</b> . You might still have to deal with some residual risks after mitigation.
Accept	<b>Risk acceptance</b> is a response in which an organization identifies and analyzes a risk, then determines that the risk is within the organization's appetite and no additional action is needed. The ERM plan that an organization develops and implements will outline its risk appetite, so any risks that are accepted are within the parameters of what the enterprise deems unworthy of further response. As previously stated, not all risks can be avoided; likewise, not all risks can be transferred or mitigated. In your organization, you must decide what level of risk is unlikely or does not have enough potential for harm to warrant extra effort and cost.



**Note:** Ignoring risk is not the same as accepting it. When you accept a risk, you have evaluated it and decided not to transfer, reduce, or avoid it. When you ignore risks, you do not take the time to identify and evaluate them. Ignoring risks is a dangerous approach to take, and can lead to unforeseen disasters.



**Note:** Some responses will incorporate more than one technique. For example, you can begin to mitigate risk until it reaches an acceptable level, at which point you accept that risk.

## Additional Risk Management Strategies

There are several additional risk management processes that you can put into place to mitigate risk in your enterprise.

Strategy	Description
Identify exemptions	<p>Some legacy systems may be exempt from specific risk management processes because they do not have certain functionalities that other, newer systems do. Replacing these systems with newer ones may raise your risk profile from both a financial and security perspective, so you must be mindful of what systems have exemptions and how those exemptions may no longer apply in the event of change.</p> <p>Although a system may be exempt from certain risk management processes, you must remember to never ignore risk altogether—there are other ways that you can address the risk. For example, certain workstations may require older versions of an OS that don't have the same vulnerabilities that most of the newer workstations in the organization do. How those newer vulnerabilities are managed does not apply to the legacy OS, but there must still be a process in place to assess that legacy OS.</p>
Use deterrence	<p>It may be impractical or impossible to completely mitigate some risks. Deterrence is the process of influencing a threat's decision to exploit or not exploit these particular risks. You may convince a threat that carrying out a particular attack is not worth the cost, effort, or legal consequences. For example, a log-in screen may warn unauthorized users that they could face jail time if they log in under someone else's authorized credentials. If successful, this will keep vulnerable assets protected.</p>
Identify inherent risk	<p><b>Inherent risk</b> is the risk that an event will pose if no controls are put in place to mitigate it. Identifying the inherent risk of an enterprise asset or activity will aid you in assessing which controls to put in place to mitigate the risk.</p>
Identify residual risk	<p><b>Residual risk</b> is the risk that remains even after controls are put into place. Identifying the residual risk of an enterprise asset or activity will aid you in assessing the effectiveness of the controls you put in place to mitigate the risk.</p>

## Continuous Monitoring and Improvement

Risk is always changing within an enterprise due to new products, new technology, and new user behaviors. To address the constant flux of risk, organizations must continually evaluate their networks to ensure that implemented controls are operating as intended. A good example of this is the use of patch and vulnerability management software. Since new vulnerabilities are found regularly, and new patches are released for those vulnerabilities, organizations should expect to have a recurring process to update equipment. However, it is very time-consuming to quantify the recurring change in an organization with a regular risk assessment approach.

In light of this reality, many organizations have adopted a process of **continuous monitoring and improvement** to detect changes in an environment and then quickly and efficiently address them. When risk is mitigated in this fashion, the business will be able to improve its operational processes and cut down on costly risk assessments. There are software tools that provide this functionality by alerting security staff of unanticipated resource access, invalid or expired software licenses, and mobile devices that attach from anywhere and at any time.

## Guidelines for Mitigating Risk

Follow these guidelines when planning how you will mitigate risk in the enterprise.

## Mitigate Risk in the Enterprise

When mitigating risk:

- Categorize information into classes like public, private, restricted, and confidential.
- Classify information in terms of how it will impact your enterprise CIA.
- Incorporate stakeholder input for CIA-based decisions.
- Understand technical controls in terms of how they do or do not fulfill CIA.
- Create aggregate CIA scores to determine what threats to prioritize.
- Plan for worst-case scenarios by gathering intelligence on threats and how they could impact your enterprise.
- Integrate multiple technical and non-technical risk mitigation tactics into a comprehensive enterprise resiliency strategy.
- Avoid, transfer, mitigate, or accept risk based on factors like cost, viability, resources, and necessity.
- Identify exemptions and inherent and residual risk in the enterprise.
- Use deterrence techniques where mitigation fails.
- Implement continuous monitoring to quickly detect changes to an environment.
- Communicate to relevant stakeholders regarding how you measure, respond to, and mitigate risks.

## TOPIC D

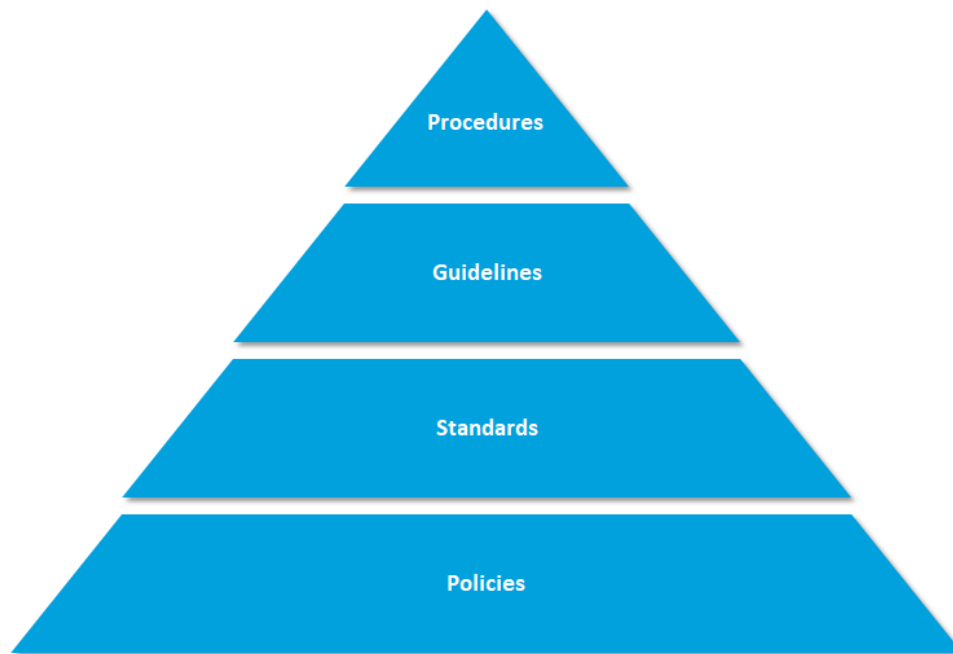
### Integrate Documentation into Risk Management

A less direct, but still important, part of risk management is developing documentation for future reference. Writing a policy and recording risk-related activity will move your ERM strategy from the conceptual to the concrete. This will provide the foundation on which to support your assessment and mitigation practices.

#### From Policies to Procedures

A policy identifies the organization's intentions. Policies are interpreted and made operational through standards, guidelines, and procedures. In regard to information security and compliance, these terms are used as follows:

- **Policies** are high-level statements that identify the organization's intentions.
- **Standards** consist of specific low-level mandatory controls that help enforce and support policies.
- **Guidelines** are recommended, non-mandatory controls that support standards or that provide a reference for decision making when no applicable standard exists.
- **Procedures** are step-by-step instructions on tasks required to implement various policies, standards, and guidelines.



**Figure 1–5: Policies are the foundation upon which standards, guidelines, and procedures are built.**

#### Policy Lifecycle

The policy lifecycle starts once an organization determines it needs a formal information security policy. The driver for an information security policy varies by organization; it could be for compliance reasons, the increasing size of the organization necessitating a written security policy to replace informal guidelines, to meet contractual obligations, or in response to a breach. Regardless

of the reasons for its development, ultimately, the policy must be approved by executive management, and in some cases the board of directors, should the organization be large enough.

Once the organization has identified a need, there are several ways to begin crafting a policy. One of the easiest methods is to download a free policy template available from various security organizations, then customize the policy to fit your organization. It is also common for organizations to bring in a security consulting company to aid them in policy development. Regardless of how you approach your company's policy, it is important to also compare and contrast the company's policy with those of other organizations; there may be topics or risks you did not previously consider which impact the elements of the policy.

Not all policies are created equal. It is best to use clear and concise language within the policy that is easy to understand. In other words, attempt to limit the legalese which pervades many policies. At the same time, it is important to understand that the organization's information security policy is a legal document, which you may provide to employees, customers, and in some cases, a court of law.

In conjunction with any laws or regulatory requirements the organization may be under, it is important to include business leaders in the development of the policy. If a policy is too strict, it may impair workers' ability to conduct business, which in turn impairs the organization. A well-developed policy should address all the risks the business may face; it is a living document that should be updated regularly as the business, technology, environments, and risks in an enterprise change. When emerging risks are identified, it's important that your policies clearly state when to report an incident and whom to report the incident to. Not all incidents require legal action, so it's necessary for the policy to cover when to report to law enforcement versus when to report to internal staff only.

### Acceptable Use Policy

#### 1. Overview

Infosec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Develetech's established culture of openness, trust and integrity. Infosec is committed to protecting Develetech's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Develetech. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Develetech employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

#### 2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Develetech. These rules are in place to protect the employee and Develetech. Inappropriate use exposes Develetech to risks including virus attacks, compromise of network systems and services, and legal issues.

**Figure 1-6:** An example security policy.

## Process and Procedure Lifecycle

To support the policies your organization has developed, it is important to create process and procedure documents which very clearly explain how the organization implements different security functions. These are the "how-to" documents used by systems administrators and company

employees that include the steps to implement and enforce the policies. They must be specific enough so that any user who is expected to follow them, can, regardless of their technical knowledge. If a predetermined level of technical prowess is required, then that should be explicitly stated. For example, a data handling procedure designed to be used by system administrators may make the assumption that the administrators are familiar with the platform they are supporting; however, a similar procedure designed for marketing and sales employees who have less technical familiarity may need more in-depth and explicit steps.

The style and contents of these documents will also vary considerably between commercial organizations and government bodies. It is common for documents relevant to military or similar agencies, such as emergency services, to be more prescriptive than those for standard businesses. In other words, you must understand your target audience and tailor the processes and procedures appropriately.

Process and procedure development is done in much the same way as policy development. Many standards organizations such as *National Institute of Standards and Technology (NIST)* or the *Center for Internet Security (CIS)* have pre-defined procedures or standards documents that you can use as a starting point, and then you can tailor them to fit your organization. Certain organizations will have specific types of standards they need to write to. Alternatively, you can bring in consultants to help define procedures or streamline business processes to make them compliant with particular policies. Regardless of the approach, it is always a good idea to compare and contrast policies with other organizations to see how they are implementing the "how-to" of information security. Many organizations, both commercial and government, publish their key policies online to enable potential users of their services to understand and gain confidence in how the organization manages information.

Just like the policies on which they are based, processes and procedures are living documents. If a policy changes in light of new business, technological, or environmental changes, then so too should processes and procedures. A policy that updates the enterprise's security posture in the face of new threats and risks is useless unless it is translated into practice through procedural documentation.

## CMS SSP Procedure

### 2.1. PHASE 1 - INITIATION (INTAKE)

During this phase the Business Owner works with the CMS CISO to determine if the system is either a GSS or a MA and by what FISMA system family it will be categorized. CMS has already established a number of FISMA system family categories for GSSs and MAs. In order to ensure continuity with the already identified inventory of systems, the OIS, Enterprise Architecture and Strategy Group (EASG) should be contacted for appropriate designation. Once the Business Owner has obtained this designation, the identification of the System Security Level by Information Type, which contains eleven (11) types, is determined. Upon establishing the level, the Business Owner will review the CMS PISP and CMS IS ARS for the level controls that must be employed in the system.

### 2.2. PHASE 2 - CONCEPT

At this phase of the life-cycle, the Business Owner will begin to identify business risks and the initial draft of the IS RA is developed. The business risks during this phase are defined as the vulnerabilities and threats that could be exploited and result in the loss of business functionality. The risks identified at this stage are documented within the IS RA and identified controls will be included within the appropriate sections of the SSP, which is initiated in Phase 4 Requirements Analysis of the Framework.

### 2.3. PHASE 3 - PLANNING

The Business Owner reviews the *CMS IS ARS*, which contains the minimum threshold for security controls based on the system security level that must be implemented to protect CMS' information and information systems. The Business Owner performs an evaluation of all IS areas within the CMS IS ARS and determines the appropriateness of the families for their system. The Business Owner will identify the expected minimum controls relative to the sensitivity level of the system, as defined in the CMS IS ARS using the SSP Workbook. Additional identified risks are used to support the development of the system requirements, including security.

**Figure 1-7: An example of a process document.**

## Topics to Include in Security Policies and Procedures

All information security policies and procedures contain topics specific to an organization and its requirements; however, there is a recommended list of topics that your security policies and procedures documentation should include. As you draft the documentation, be sure to obtain the approval and buy-in from top management for the following:

- The scope of what the policy covers.
- How information is classified.
- Goals for secure handling of information.
- How other management policies relate to the security policy.
- References to supporting documents.
- Specific instructions for handling security issues.
- The person or group who has specific designated responsibilities.
- Known consequences for security policy non-compliance.

## Best Practices to Incorporate in Security Policies and Procedures

Security documents that incorporate the previous topics will help to reduce your overall risk. Additionally, you should support the development of policies and procedures that contain the best practices listed in the following table. Note that the organization will not necessarily be able to, or should, incorporate all of these practices in the risk management process.

<i><b>Best Practice</b></i>	<i><b>Description</b></i>
<i><b>Separation of duties</b></i>	States that no one person should have too much power or responsibility. Duties and responsibilities should be divided among individuals to prevent ethical conflicts or abuses of power. Duties such as authorization and approval, and design and development, should not be held by the same individual because it would be far too easy for that individual to defraud or otherwise harm an organization. For example, it would be easier for an employee to make sure that the organization only uses specific software that contains vulnerabilities if they are the only one with that responsibility. In many typical IT departments, roles like backup operator, restore operator, and auditor are assigned to different people.
<i><b>Job rotation</b></i>	States that no one person stays in a vital job role for too long. Rotating individuals into and out of roles, such as the firewall administrator or access control specialist, helps an organization ensure that it is not tied too firmly to any one individual because vital institutional knowledge is spread among trusted employees. Job rotation also helps reduce the risk of individuals abusing their power and privileges, as well as preventing collusion between employees.
<i><b>Mandatory vacation</b></i>	A method of preventing fraud which provides you with an opportunity to review employees' activities. The typical mandatory vacation policy requires that employees take at least one vacation a year in a full-week increment so that they are away from work for at least five days in a row. During that time, your corporate audit and security teams have time to investigate and discover any discrepancies in employee activity. When employees understand the security focus of the mandatory vacation policy, the risk of fraudulent activities decreases.
<i><b>Least privilege</b></i>	Dictates that users or systems should only have the minimal level of access that is necessary for them to perform the duties required of them. This level of minimal access includes facilities, computing hardware, software, and information. When a user or system is given access, that access should still be only at the level required to perform the necessary tasks. If you give a user or system access that exceeds what they require, then that is one more vector that can be used to compromise your organization.
<i><b>Incident response</b></i>	Defines monitoring, response, and reporting requirements for incidents that involve security breaches or suspected breaches. Generally, this set of policies requires a response to all incidents and suspected incidents within a defined time period and according to a reporting hierarchy that might depend on the severity of the incident. Security awareness and training both play a role in incident response so that the personnel whose primary roles fall outside of information security know who and where to call for various levels of incidents, with a service desk or help desk being the first line in the reporting hierarchy. Without timely reporting to the right people, it will be much more difficult to mitigate the risk of a security breach causing harm to your enterprise.
Forensic tasks	Investigate from where a breach emanated, how a breach might have occurred, and who might be responsible for the breach. The forensics policy should include who is to be notified when forensics are required, under which conditions they are required, and how to contact individuals responsible for those duties. It is important to include legal counsel when formulating the forensics policy so that appropriate legal guidelines can be included, as necessary.

<b>Best Practice</b>	<b>Description</b>
Employment and termination procedures	Defines on-boarding and off-boarding procedures when employment both begins and concludes, respectively. Proper on-boarding involves acclimating new employees to the security practices that you expect them to follow. This ensures that there will be an expectation of liability in the arrangement. Likewise, when the employee leaves the organization, you should establish an off-boarding process. The terminated employee must agree to relinquish any access to company systems, data, and physical equipment. In some cases, terminating an employee may put your company secrets at risk of being leaked; to prepare for this, your policy should specify when you should enforce non-disclosure agreements (NDAs).
Continuous monitoring	Outlines what mechanisms and tools are used to continuously monitor systems for changes that could increase risk to the enterprise. This practice also defines exactly what events and environments should be monitored based on a prior risk analysis. Some policies will include provisions for continuous improvement so that the enterprise can take a proactive role in addressing detected risks.
Training and awareness for users	Without comprehensive education, user-based attacks, such as social engineering, will be a major source of risk for an organization. In addition to teaching users about the inherent risks of using technology, it is important to also educate them on the policies and procedures required for them to operate safely within the organization's systems. Training should also take into account the types of access and roles that employees have. For example, you wouldn't train a salesperson on the risks of SQL injection attacks, but you would educate your website developers on this topic. Specific training mechanisms can range from subtle reminders through on-screen messaging at login, through paper-based pamphlets on employee desks or common areas, to training for specific elements of enterprise operations (devices, software, building security, etc.).
Auditing requirements and frequency	Defines the types of audits performed, who performs those audits, and how frequently they are performed, and clearly delineates the authority for remediating audit issues found in the process. Auditing policies typically include provisions for event triggers that are based on enterprise risk assessments. The audit policy should also define the auditing requirements for business partners and subcontractors, which should be included in all contracts with third parties who could have an impact on the overall security of the organization.
Information classification	Information should be classified according to its sensitivity and criticality to business operations. This enables you to prioritize your data protection methods and apply those protections with regard to the CIA of that data. Industry-recognized categories like public, private, restricted, and confidential will fulfill most organization's needs, but you may wish to create your own categorization scheme if these are not adequate.

## Legal Compliance and Advocacy

There are many different stakeholders in an organization—employees, customers, regulatory agencies, legal counsel, and management. As you develop your security policy, you should consider the expertise of the various stakeholders, as each will offer different skills and perspectives in the creation of a strong policy that supports legal compliance and advocacy.

- Human resources can help guide the policy development in accordance with established labor laws and privacy requirements.
- Consulting legal counsel during policy development will ensure the policy does not violate any laws and is in accordance with any regulatory requirements the organization may fall under.
- You may also consult regulatory agencies to help ensure that the policy meets any regulatory or compliance requirements needed.
- For your policy to be successful, you must include management's input and approval. Their involvement will also allow the policy to fit within the goals of the business.
- You may consult employees to help identify areas of the policy that may not fit into current business processes and identify where projects are needed to alter current business practices.
- Industry organizations such as NIST, ISO, and other standards bodies, can help provide example policies or recommended best practices.

## General Privacy Principles

Privacy is the expectation that non-public data is protected from threats to confidentiality and integrity. When an organization fails to protect data, it reflects poorly on the organization and can have a lasting impact on its image. This is referred to as **brand damage**. It is important to keep in mind that different places in the world define what needs to be kept private differently and organizations may have different definitions of how data is classified. When regulations are involved, there is not any flexibility in how data is defined; however, when no regulations apply, then there is some latitude for organizations to leverage.

When drafting policies, you must be aware of what privacy expectations your clients have in working with the organization. **Personally identifiable information (PII)**, including full names, addresses, phone numbers, age, sex, and race, may or may not be considered sensitive information based on the context in which they are handled. Consider a website like LinkedIn that exists primarily as a social network for the business world. Full names and places of work are expected to be on pretty much everyone's profile, so a security breach that exposed those pieces of PII would not violate privacy policies, nor would it bring risk to the company. On the other hand, a dating website might discourage its users from associating their profiles with their real names and the companies they work for. If the site doesn't discourage this, then a breach that exposes this PII would put the site's reputation at risk and its users would worry about their privacy.

Regardless of how you define this information, you still have a responsibility to your customers, employees, and business partners to communicate how you plan to use their PII. Whether internal or public-facing, your privacy policy should be upfront, and you should even consider offering guidelines to your target audience on how they can help to ensure their own privacy.



**Note:** The abbreviation PII is widely accepted in the United States, but the phrase it abbreviates has four common variants based on word forms for personal (or personally) and identifiable (identifying). These variants are not identical from a legal standpoint. Each term's definition can change depending on the jurisdiction and the reason the term is being used.



**Figure 1-8: Example of PII.**

## Privacy Requirements

Every organization will have a specific privacy policy based on common business and legal requirements. The following table lists major U.S. federal privacy-related standards or laws that may be applicable to your enterprise. Note that individual states may have many of their own unique privacy laws, and that laws outside of the U.S., especially those in Europe, may enforce more stringent privacy requirements.

<b>Standard or Law</b>	<b>Description</b>
<b>SOX</b>	The Sarbanes-Oxley Act (SOX) of 2002 dictates requirements for the storage and retention of documents relating to an organization's financial and business operations, including the type of documents to be stored and their retention periods. It is relevant for any publicly traded company with a market value of at least \$75 million.
<b>GLBA</b>	The Gramm-Leach-Bliley Act (GLBA) of 1999 was primarily passed as a deregulation of banks, but also instituted requirements that help protect the privacy of an individual's financial information that is held by financial institutions and others, such as tax preparation companies. The privacy standards and rules created as part of GLBA safeguard private information and set penalties in the event of a violation. GLBA also requires a coherent risk management and information security process.

<i>Standard or Law</i>	<i>Description</i>
<b>FISMA</b>	<p>The Federal Information Security Management Act (FISMA) of 2002 was passed to address the evolutionary nature of information systems security in the federal government. Some of the act's key provisions require federal organizations to:</p> <ul style="list-style-type: none"> <li>• Define the boundaries of the systems to be protected and then identify the types of information found within those systems.</li> <li>• Document system information and perform a risk assessment to identify areas requiring additional protection.</li> <li>• Protect systems using an identified set of controls and certify systems before use. An approval for operation is issued upon certification.</li> <li>• Continuously monitor systems for proper operation.</li> </ul>
<b>COSO</b>	<p>The Committee of Sponsoring Organizations of the Treadway Commission (COSO) provides guidance on a variety of governance-related topics including fraud, controls, finance, and ethics. COSO's ERM-integrated framework defines risk and related common terminology, lists key components of risk management strategies, and provides direction and criteria for enhancing risk management practices.</p>
<b>HIPAA</b>	<p>The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 to establish several rules and regulations regarding healthcare in the United States. With the rise of electronic medical records, HIPAA standards have been implemented to protect the privacy of patient medical information through restricted access to medical records and regulations for sharing medical records. Visit <a href="http://www.hhs.gov">www.hhs.gov</a> for more information on HIPAA regulations.</p>

## Business Continuity Planning in ERM

**Business continuity planning (BCP)** is the process of defining how an organization will maintain normal day-to-day business operations in the event of a business disruption or crisis. A viable business continuity plan should ensure the survival of the organization by:

- Identifying critical at-risk systems and components to ensure that such assets are protected.
- Preserving key documents.
- Establishing decision-making authority.
- Communicating with internal and external stakeholders.
- Maintaining financial functions.
- Addressing infrastructure issues such as maintaining utilities service, utilizing high-availability or fault-tolerant systems that can withstand failure, and creating and maintaining data backups.

The enterprise should review the BCP and test it on a regular basis. The plan must have executive support to be considered authoritative; the authorizing executive should personally sign the plan.

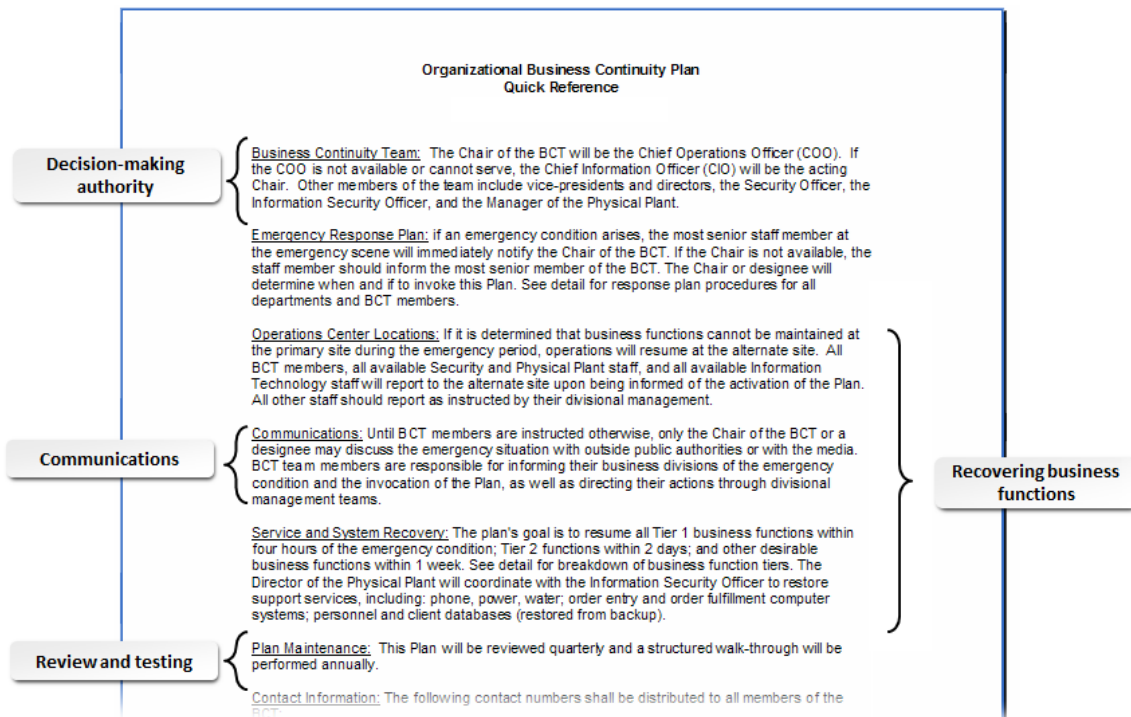


Figure 1–9: A BCP.

In enterprise risk management, the BCP will be your go-to documentation for keeping your organization financially and operationally afloat if risk becomes a reality. Beyond identifying key risks to critical systems and functions, BCPs often incorporate some form of risk mitigation strategies to prevent further damage to the organization. When an incident does occur, and you're able to mitigate the damage, you can update your BCP to reflect your success in addressing the problem. This will keep you better prepared for the next incident, and minimize the amount of disruption that will affect your business.

## BCP Metrics

As part of your BCP and related risk analysis activities, you should incorporate metrics that will help you assess the viability of your continuity operations. These metrics can also help you make more informed decisions about how to respond to risks that disrupt the business. Such metrics may include:

Metric	Description
<b>MTD</b>	Maximum tolerable downtime is the longest period of time that a business outage may occur without causing irrecoverable business failure.
<b>RPO</b>	Recovery point objective is the longest period of time that an organization can tolerate lost data being unrecoverable. The RPO determines how the organization schedules its backups.
<b>RTO</b>	Recovery time objective is the length of time within which normal business operations and activities can be restored following an event.
<b>MTTF</b>	Mean time to failure is the average time that a device or component is expected to be in operation. This assumes that the device cannot be repaired if it fails.
<b>MTTR</b>	Mean time to repair is the average time taken for a device or component to recover from an incident or failure.

<b>Metric</b>	<b>Description</b>
<b>MTBF</b>	Mean time between failures is the rating on a device or component that predicts the expected time it is in operation before needing to be repaired or replaced.

## Business Documents That Support Security Initiatives

There are several common types of business documents a CASP+ should expect to encounter in their normal duties. Many of these focus on business partnerships and alliances. Since all organizations do business with other entities, there are many types of common agreements used to govern those relationships. Some of these agreements specifically deal with security and risk management, whereas others may incorporate them secondarily or not at all.

<b>Document</b>	<b>Description</b>
<b>Master service agreement (MSA)</b>	This document lays the groundwork for any future business documents that two parties may agree to. The purpose of an MSA is to expedite the agreement process as the relationship between each business partner grows. Organizations may use an MSA to eliminate redundancies that arise when the partner organizations form multiple agreements, like those listed in the rest of the table.
<b>Statement of applicability (SOA)</b>	This document identifies the controls in place in an organization and explains their purpose. As SOAs identify why a particular control is being used, they are often directly influenced by the conclusions reached in a risk assessment. The SOA should reference the policies and procedures that will take advantage of the identified controls. It may be beneficial to not only explain why a certain control was included, but to also explain why certain controls were excluded.
<b>Business impact analysis (BIA)</b>	This document identifies present organizational risks and determines the impact to ongoing, business-critical operations and processes if such risks actually occur. BIAs contain vulnerability assessments and evaluations to determine risks and their impact. BIAs should include all phases of the business to ensure a strong business continuation strategy.
<b>Interoperability agreement (IA)</b>	This is the general term for any document that outlines a business partnership or collaboration in which all entities exchange some resources while working together.
<b>Interconnection security agreement (ISA)</b>	This type of agreement is geared toward the information systems of partnered entities to ensure that the use of inter-organizational technology meets a certain security standard for CIA. Because they focus heavily on security, ISAs are often written to be legally binding. ISAs can also support MOUs (see next entry) to increase their security viability. NIST provides a security guide for developing an interconnection plan, titled <i>Security Guide for Interconnecting Information Technology Systems Special Publication 800-47</i> .

Document	Description
<i>Memorandum of understanding (MOU)</i>	This type of agreement is usually not legally binding and typically does not involve the exchange of money. MOUs are less formal than traditional contracts, but still have a certain degree of significance to all parties involved. They are typically enacted as a way to express a desire for all parties to achieve the same goal in the agreed-upon manner. An MOU document might contain background information on each organization; the history of the relationship between the two organizations and circumstances that led to the partnership; and a general or specific timeline for collaborative business activities. Because they typically have no legal foundation, an MOU is not the most secure agreement for a partnership.
<i>Service-level agreement (SLA)</i>	This agreement clearly defines what services are to be provided to the client, and what support, if any, will be provided. Services may include everything from hardware and software to human resources. A strong SLA will outline basic service expectations for liability purposes. The document may include timeframes within which failures will be repaired or serviced; guarantees of uptime; or, in the case of a network provider, guarantees of data upload and download rates.
<i>Operating-level agreement (OLA)</i>	This agreement identifies and defines the working relationships between groups or divisions of an organization as they share responsibilities toward fulfilling one or more SLAs with their internal or external customers.
<i>Non-disclosure agreement (NDA)</i>	This is an agreement between entities stipulating that they will not share confidential information, knowledge, or materials with unauthorized third parties. NDAs also commonly state in which cases, if any, data may be used or processed by the receiving entity. For data acquired through public sources, an NDA is not enforceable.
<i>Business partnership agreement (BPA)</i>	This agreement defines how a partnership between business entities will be conducted, and what exactly is expected of each entity in terms of services, finances, and security. For security purposes, BPAs should describe exactly what the partners are willing to share with each other, and how any inter-organizational access will be handled.



**Note:** An example of an interconnection standard is the PSN Code of Interconnection (CoICo). This UK government standard applies to connectivity services provided by commercial suppliers. The standard can be found at <https://www.gov.uk/government/publications/psn-code-of-interconnection-coico>.

## Penalties for Non-Compliance

Failure to comply with certain business documents, especially those that are legally binding, may result in serious penalties to an organization or individual. For example, assume your organization has an ISA with another entity. If your security wanes too far from the requirements you agreed to in the ISA and a breach occurs, your organization will not only be liable for the breach, but the business entity you partnered with may file a lawsuit against your organization as well. This can lead to heavy fines that seriously impact business operations and profitability.

You may be subject to significant liability even for non-legally binding agreements. The negative effects are often more intangible; your organization could lose respect in the eyes of stakeholders and potential partners alike. This can impact the market influence your organization has.

Even individuals can be held accountable for non-compliance, especially with documents like an NDA. If your employer has you sign an NDA and you divulge sensitive information to unauthorized parties, you could lose your job and be sued for damages.

## Guidelines for Integrating Documentation into Risk Management

Follow these guidelines to integrate documentation into your ERM strategies.

### Integrate Documentation into ERM

When integrating documentation into your ERM strategies:

- Download free policy templates to make crafting a policy easier.
- Consider hiring a consultant if your organization can't support the internal development of policies.
- Use direct, concise language and dispense with legal jargon in policies.
- Include business leaders in policy development and make sure executive management approves of the policy before it is enforced.
- Support policies with clearly defined processes and procedures.
- Make processes and procedures easy to follow and tailor them toward your audience's technical aptitude.
- Compare and contrast policies, processes, and procedures with those of other organizations.
- Consider policies, processes, and procedures to be living documents; that is, subject to change as businesses and technology evolve.
- Incorporate best practices like job rotation, mandatory vacations, and user training, into your policies based on your specific enterprise requirements.
- Involve HR, legal counsel, management, and other entities in the policy development process to get unique perspectives.
- Ensure that policies have provisions for legal and regulatory compliance.
- Identify any sensitive PII that your organization handles.
- Be up front with your clients as to how their PII will be used and for what purpose it will be used.
- Advise your clients on best practices to maintain privacy.
- Draft a business continuity plan (BCP) to maintain day-to-day operations in the event of an incident.
- Define in the BCP what components are at risk and how they should be preserved.
- Review your BCP and test it on a regular basis.
- Identify the various business documents and agreements that are applicable to your enterprise needs.
- Use an agreement like an SLA in any partnership that requires strong security and legal and financial liability.

## ACTIVITY 1–1

### Supporting IT Governance and Risk Management Review

#### Scenario

Answer the following review questions.

---

1. At your workplace, what security risks are there, and what risks do you envision for the future of your company?
  
  2. What sort of documentation do you have in your company to support risk management? What other documentation should there be?
-

## Summary

In this lesson, you identified why the ERM process is important, and went through the process by assessing and mitigating risk across a wide range of factors. You also reinforced your ERM strategy through documentation. The information you learned in this lesson will give you a foundation for understanding and applying security in your enterprise, which you will build upon in later lessons.