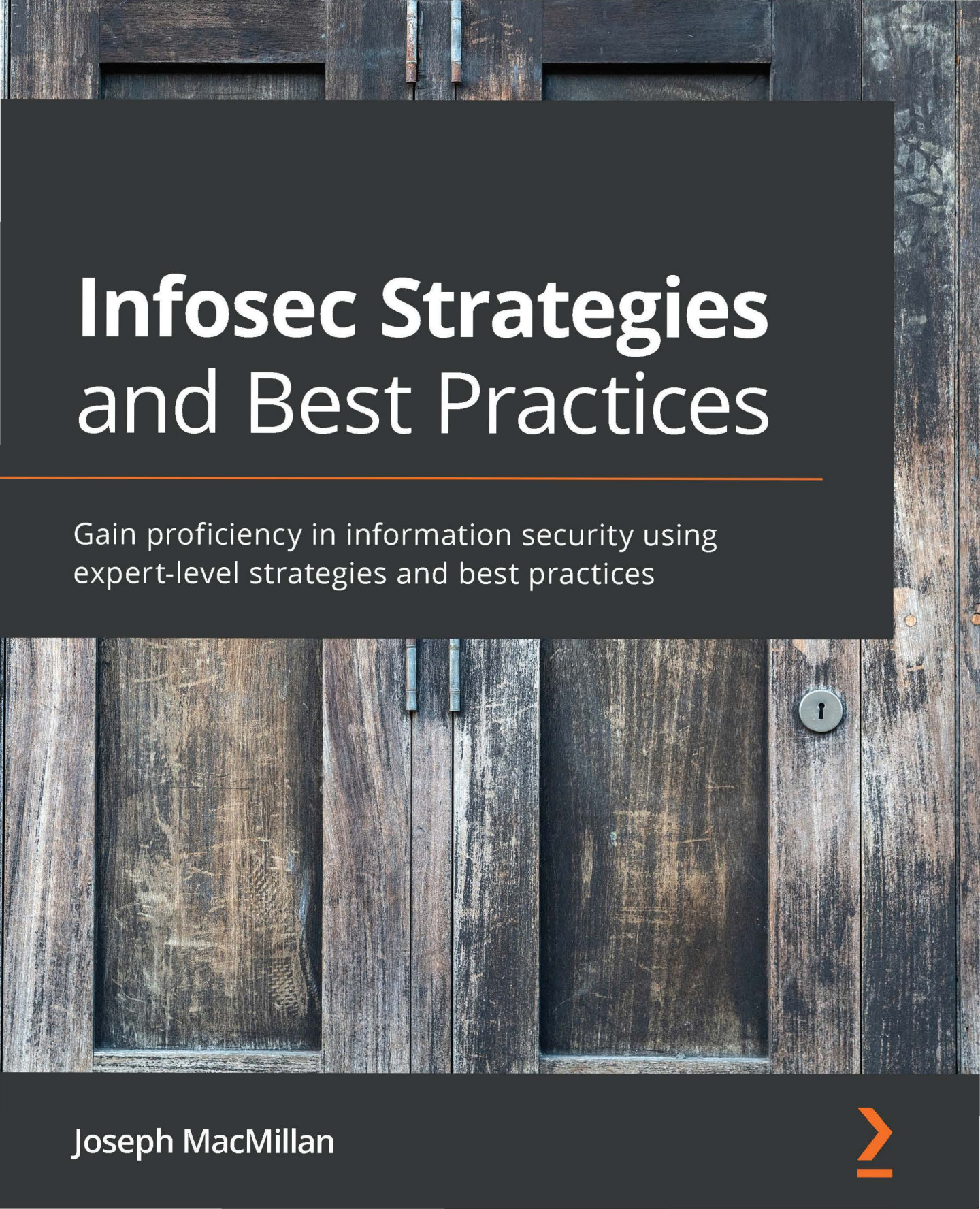

Infosec Strategies and Best Practices

Gain proficiency in information security using expert-level strategies and best practices

Joseph MacMillan

Infosec Strategies and Best Practices

Gain proficiency in information security using expert-level strategies and best practices

Joseph MacMillan

Packt

BIRMINGHAM—MUMBAI

Infosec Strategies and Best Practices

Copyright © 2021 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Group Product Manager: Wilson D'souza
Publishing Product Manager: Sankalp Khatri
Senior Editor: Shazeen Iqbal
Content Development Editor: Romy Dias
Technical Editor: Nithik Cheruvakodan
Copy Editor: Safis Editing
Project Coordinator: Shagun Saini
Proofreader: Safis Editing
Indexer: Rekha Nair
Production Designer: Shankar Kalbhor

First published: April 2021

Production reference: 1240521

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-80056-635-4

www.packt.com

Contributors

About the author

Joseph MacMillan is a technological utopian and cybersecurity junkie, currently living in Amsterdam.

Employed by Microsoft as a Global Black Belt for Cybersecurity, Joseph uses his experience in senior information security roles to transform businesses into secure organizations rooted in risk management principles to drive decision making.

Much of Joseph's work has been focused on enabling businesses to achieve their goals by removing the ambiguity surrounding risk, which enables the CEO and C-Suite to plan and achieve their goals in a secure manner with confidence.

Joseph holds various certifications, including the CISSP, CCSP, CISA, CSSLP, AlienVault Certified Engineer, and ISO 27001 Certified ISMS Lead Auditor.

I would like to take this opportunity to thank my wife and best friend, Helen, for her support and care along the way. Furthermore, I would like to thank all of the members of the Packt team who have supported me in the creation of this book, from beginning to end.

About the reviewer

Kyle Reidell has world-class experience leading, developing, and architecting cybersecurity and engineering solutions for numerous government agencies, as well as Fortune 500 companies, and cutting-edge technology start-ups. His background is truly multi-disciplinary: from developing and defending global operations centers to securing communications for the highest levels of government and designing cloud-native architectures while continuing to serve as a Cyber Officer in the Air National Guard.

Kyle is a Marine Corps veteran who is actively engaged as a mentor for aspiring youth and cybersecurity professionals. He holds multiple degrees and industry certifications, including a master's degree in information security.

I would like to thank my family, especially my wife and son, for the continuous support they have provided throughout my career and endeavors; I could not have done any of this without them!

2
Protecting the Security of Assets

Originally, the concept for the start of this chapter was to ask you *"How can you protect an organization if you don't know what assets they have?"*. We both know the answer to that question is *"You can't,"* and we've probably been asked this question a thousand times between the two of us, so I'm not going to ask it. Instead, I'm going to show you how you might structure the appropriate processes at your organization in order to discover and protect its assets.

These various processes combine to create what is known as an **Information Security Management System** (**ISMS**). We covered various key concepts in *Chapter 1*, *InfoSec and Risk Management*, but overall, there was much less structure than most organizations would require. What we want to be able to achieve with the ISMS is to appropriately identify and classify our organization's assets, and ensure the security of those assets is adequately protected by implementing the appropriate controls, taking into consideration *defense in depth* for each vertical of confidentiality, integrity, and availability.

This chapter focuses on those topics. We will look at utilizing effective processes to implement an effective ISMS. One that ensures, through policies and procedures determined by business requirements, that risk is reduced to an acceptable level.

With that goal in mind, I think it makes sense to follow these four stages in the structure of this chapter:

- How to implement an ISMS
- The appropriate process for the identification and classification of the information assets of an organization
- Securing those assets with the appropriate controls based on their value, monitoring for changes, and adapting to those changes
- Disposal of the assets, be it through archiving or destruction

All of these points will be covered in a way that helps you avoid the common pitfalls that InfoSec professionals often run into along the way.

Now that the housekeeping is in order, allow me to proceed to the actual content.

Implementing an ISMS

Implementing an ISMS requires *structure*, *planning*, *decisiveness*, and *collaboration*. There exists an extremely important question of *"Who is responsible for what?"*, which should be asked and documented. I'd like to briefly touch on the role of **top management**, and how we might translate our findings into effective communications about risk to the appropriate audience. Improving on this should allow you to act with authority in your mitigation strategies moving forward.

Once business goals are translated into IT goals, and the appropriate level of buy-in is attained, we can move onto the actual development of the policies, which will act as the information security "rules" for your organization. This is absolutely crucial in being able to systematically define "baselines" for security, organize assets, reduce risk, and communicate the information security requirements to members of your organization.

Next, I'd like to talk about evaluating and improving this policy, keeping in mind the rule of thumb for InfoSec is to *be continually improving and optimizing*. In such a rapidly changing field, keeping on top of things and adapting to changes will pay off.

So, buckle up! We're going to talk about governance and policies! I know how exciting that sounds.

Responsibilities of top management

To begin with, it's important to remember that when it comes to anything in information security, it's ultimately **senior management** who is responsible. What does this actually mean, in practice? Well, they hire you. Hiring an information security professional to delegate the responsibilities to is the most logical thing to do as a CEO who has been hearing of their growing responsibilities in information security.

Another aspect of top management's role in information security is to effectively communicate the organization's strategic objectives. With those objectives in mind, you are able to align all information security requirements to those goals.

So, now you've been hired, and it's been decided that it's your responsibility to understand the risks associated with your specific organization and communicate this to your CEO, or CIO, or CTO, or some other **C-level** in a digestible way. This is a pretty normal situation, but having said that, I've met folks who were responsible for security at their organizations who seemingly never report their findings to the C-level, and then complain that the company doesn't take security seriously. Yeah, of course not! How could they?

It is now your responsibility to assess the level of risk that faces the organization and turn it into a legitimate business case for senior management at your organization, in a way that is easy for them to understand. Keep in mind, these people are top management! Their childhood didn't consist of browsing the web; it consisted of playing stickball near Old Man River's house and drinking seltzer at the local pharmacy. As for their day-to-day use of "computers," they've probably been limited to email and (recently) a mobile device, and it all seems pretty magical to them.

My point is: You need to *know your audience*. While communicating risks to the IT department will allow for more technical references and discussions, presenting to the other business departments requires a more translated approach, focusing on organizational impact.

Generally speaking, from my experience, far too much time is spent on a technical description rather than presenting an understandable level of risk the business faces. Properly translating IT risk findings into organizational impact will ultimately add a lot of value to your career, because as it currently stands, very few IT and InfoSec professionals do this effectively.

When you're presenting your findings to the C-level, you might be able to use this example as a template for communicating risk:

- You stand to lose this much money this year: *£100,000+*
- Unless you protect this system: *NAS Server*
- From this threat: *External malicious actors accessing it through an unknown web app exploit*
- With this mitigation: *Web application firewall (WAF)*
- It will cost this much money to do it: *£84.42 / month, or £1,013.04 / year*
- And will take this long to implement: *3 days*

Now, with these communications in mind, I would like to talk about the **ISMS** we're going to create, and how we can implement structures into our organization. Then, we can gather the type of key information mentioned in the preceding template in order to communicate the level of risk, and ensure the security of organizational assets.

Developing an ISMS

An ISMS is a defined approach to handling information security at your organization. It ensures a systematic approach to accurately discover, measure, contain, and mitigate the information security risk at your organization in order to ensure your organization is adequately protected from malicious actors, accidental loss, and regulatory impact, with risk at the heart of the decision-making process.

The ISMS contains formalized documents determined by business needs, such as operational requirements, regulations, retention periods, the ability of the staff, and the business's solutions. These documents define your organization's policies, procedures, baselines, and guidance in relation to information security at your organization. This is an extremely important step in order to achieve your goal of a risk-focused, mature *information security program*. As a result, it is the information security team's responsibility to ensure this ISMS is in place and functional.

The rest of this book is going to help you in developing and adding to the content of these documents, as well as operationalizing the content, but the structure isn't set in stone in any specific way. You might want to structure these documents in a way that streamlines compliance with specific regulations. There are many information security frameworks and standards that are available, and structuring your policies to suit one or more of those will present a logical sequence of requirements. One way, for example, is to follow the requirements of the **ISO/IEC 27001** (ISO 27001) international standard for your ISMS. In this chapter, I'm going to leverage the ISO 27001 standard's requirements to help us create documents and define policies in order to build out our ISMS, but keep in mind that it's possible to leverage other standards and guidelines, as required by your organization and its context.

Essentially, we want to create a set of documents that will come together to define the organizational requirements and serve as our ISMS. The topics of these documents can include the following:

- How the responsible people within your organization create and update the information security policies, procedures, baselines, and guidance
- How the organization identifies, classifies, monitors, and disposes of information assets
- How the responsible people within your organization identify and measure the risks facing its information assets, and choose controls to mitigate those risks
- The levels of residual and unmitigated risk that exist for your organization's information assets

Often, documents in the ISMS are referenced in the configuration of new systems, during the onboarding of new employees, or in the day-to-day undertakings of various organizational members. For example, in the previous chapter, we covered various aspects of the *Risk Assessment Methodology, Risk Treatment Methodology, Risk Treatment Plan, and Risk Assessment Report* documentation that may be required for your ISMS.

To begin creating this system, we can start with a few key documents required by the ISO 27001 standard to specifically address the following topics, which I have divided into subsections. Keep in mind that it's your responsibility to understand your organization's requirements, and align the documentation and processes with those requirements to ensure the effective implementation of your ISMS.

High-level information security documentation

When it comes to high-level policies for information security and your ISMS, there are a few key documents you'll want to consider having, depending on the level of structure your organization requires. Keep in mind that with a structured approach to handling information security, we can more effectively reduce the level of risk facing our organization.

Context of the organization

In order to understand how to build your ISMS, you should be able to outline the context of the organization for which you're building the ISMS. You'll also use this document to define what the organization requires from the ISMS. By beginning with your organization's requirements, you're creating policies and procedures that align with the business goals of your organization, as defined by top management.

You might want to address any internal or external considerations that could impact the organization's goals for the ISMS. These could include the following:

- The nature of the organization, as in the type of work the organization takes part in. These questions (and more) are likely to have information security risks associated with them:

  - Is there a political nature to the organization?

  - What are the products and services the organization offers?

  - What is the growth outlook of the organization?

  - Which threats are currently facing it?

  - Which suppliers are being utilized?

  - What legislation does the organization need to consider?
- Information or assets, such as defining the crown jewels of the organization. Consider how the following affect your organization in terms of risk and information security:

  - What type of information does your organization process or control? PII, PHI, IP, financial information, or perhaps another type?

  - Which systems are currently being used to process and store information?

- People, including the nature of how work is done. Consider how the following affect your organization in terms of risk and information security:
  - How is recruitment done?
  - How are people trained?
  - When people change roles or leave the organization, how is that handled?

Having taken these things into consideration, you are better suited to design an information security management system that caters to your organizational needs.

Scope of the ISMS

Regardless of whether you're following the ISO 27001 standard or not, you will likely want to define the scope of your ISMS. The reason being that you will want to communicate to key stakeholders (such as top management, members of your organization, auditors, or potentially even your customers) which parts of your business are covered by your ISMS.

How can you define your ISMS's scope? You should align it with the scope of the organization, and any of its organizational requirements. Ask the question *"What aspects of the business will benefit from being in scope with the ISMS?"*. Liaising with key stakeholders at your organization about this topic will help you to understand the reasoning for wanting to (or needing to) implement this system to begin with, including understanding risk, regulatory pressure, or customer requirements.

You can also consider defining specific processes (or areas) of the organization that are "out of scope" with the ISMS. This could include external third-party processing activities that are out of your control – providing you still ensure that the third-party practices are in line with your risk appetite.

Generally speaking, the certification bodies that will end up evaluating your ISMS and certifying whether your business is compliant or not will prefer to see the "entire organization" fall under the scope of the ISMS, but it's not a hard-and-fast requirement to do so. Providing you "do what you say, and you say what you do" – as in, your organization follows the requirements set out in the ISMS in practice, and the practices are in line with the standard – you will be conformant with the requirements.

Statement of Applicability

Without things getting too complicated about how to structure this document, the **Statement of Applicability** is a summary of the relationship between your organization's risk, and the various controls available to reduce the risk scores to an acceptable level, and is often displayed in table form.

Considering we're taking a risk-based approach to selecting and applying controls at our organization, we will not be able to effectively complete the Statement of Applicability before performing a relevant risk assessment for our organization. However, creating the document and including a list of available controls will help provide context to that process.

Referring to ISO 27001, we would be looking at a list of 114 controls across 14 categories in what is known as Annex A, and defining whether each is applicable or not to your organization. It is possible for a control to be *applicable and implemented*, *applicable but not yet implemented*, or *not applicable*. The Statement of Applicability document should include a justification for the decisions made.

The controls found in this document include various methods of structuring your organization's ISMS and offer a great insight into how you could go about reducing risk at your organization through policies, procedures, and definitions. Utilizing ISO 27001's Annex *A* will help in the process of developing your ISMS, and bolstering your organization's security, but will not give you specifics on how you might implement the controls.

Refer to the following table with one entry included for how you may want to structure your Statement of Applicability table:

Ref	**Control**	**Control Description**	**Applicability**	**Implementation**	**Justification**
A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published, and communicated to employees and relevant external parties.	Applicable	A formal information security policy has been implemented, approved, published, and communicated. Link: information security policy	Control has been selected after analysis based on risk assessment.
...	...	...	...	...	...

In order to clearly define how your organization is taking a risk-based approach to handling information security, you will want to add an entry for each of the 114 Annex A controls. It must be decided why each control is (or is not) relevant to your organization, and if it is, how the organization has implemented (or plans to implement) that control.

For further guidance on how to go about implementing the 114 controls found in Annex A, you can refer to **ISO 27002**, a supplementary document to ISO 27001, which provides guidelines for the selection, implementation, and management of these controls.

Information security policy

A logical continuation of the high-level information security policy documents would be the **information security policy** itself.

As we saw in the preceding table, our Statement of Applicability table, the first Annex A control for mitigating information security risks is to define a set of policies for information security, and have those policies approved by management, published, and communicated to employees and relevant external parties.

The overall goal of the information security policy is to define the objectives for information security at your organization, including measurable requirements for the confidentiality, integrity, and availability of the organization's assets. Because of this, it is crucial to ensure the information security policy is applicable and relevant to your organization. There's no point in creating documents that nobody can or will abide by; these purely exist in order to reduce the level of risk facing the organization.

Another aspect of the information security policy is committing to the ideology of continual improvement that we mentioned towards the conclusion of *Chapter 1, InfoSec and Risk Management,* in order to ensure the organization remains protected as technologies, processes, and threats change.

Other key definitions and documents

Other definitions and documents you would be best suited to include in your ISMS include the following:

- A list of *security roles and responsibilities*, defining who is responsible for what, in terms of security at your organization. We want to ensure it's clear who is going to be implementing controls, or the responsibilities of data owners and data users, for example.
- A list of *legal, regulatory, and contractual requirements*, with specific references to key documents and web pages. If your organization must comply with a certain *SLA* for a specific customer, or if your organization's processed data is subject to *EU GDPR*, it will be important to keep track and document those requirements in a specific way in your ISMS.
- *Internal audit* policies and procedures, which include the specific processes internal auditors must follow in order to effectively check the effectiveness of the organization's ISMS and implemented controls.

- Policies and procedures for *corrective actions*, which include the specific and systematic processes to improve security at the organization. It should include how (and by whom) any information security issues are discovered, reported, documented, and actioned.

Furthermore, we will want to define a way to store and present the following information in our organization:

- Business impact analysis
- Records of training, skills, experience, and qualifications
- Results from monitoring and measurement
- Internal audit results
- Management review results
- Corrective action results
- Logs of user activities, exceptions, and security events

Once we have those specific definitions, we can proceed to the other parts of the ISMS, including asset management, risk management, and business continuity and incident response. Let's begin with the key topic of asset management.

Asset management documentation

Part of the reason I've started with asset management instead of risk management is that old trope you might have heard in the past: *"How can you protect your organization's assets if you don't know what assets your organization has?"*.

It's a cliché, but that doesn't make it any less true. In your ISMS, you must define a way to understand not only the information assets your organization has, but also how information should be classified, and the way those assets should be handled securely. Only then will you begin to fully understand the risk facing your organization, and be able to apply controls to reduce that level of risk to an appropriate level.

Generally, the life cycle of managing information assets at your organization will follow these four steps. I've mapped ISO 27001's requirements to each stage in parentheses:

- Adding the information asset to the asset inventory (A.8.1.1)
- Classifying that information, based on legal requirements, asset value, criticality, and sensitivity (A.8.2.1)

- Labeling that information (A.8.2.2)
- Handling that information in a secure way (A.8.2.3)

I'll begin with the first stage, the asset inventory.

Asset inventory

You will absolutely want to have a way to effectively catalog and continually update the **asset inventory** of your organization. In the first chapter, we discussed the various categories that assets can fall into, and the reason for those definitions was in order to ensure you are considering anything that is of value to the organization that can fall into the ISMS's scope, or in plainer words: any information, as well as the devices or systems where information is stored, processed, or accessed from.

Once you have a list of assets for your organization, what you will want to do is to categorize and prioritize the assets, and then assign an **asset owner** to each asset (or asset group). It's up to you and your organization's requirements as to how you might structure this, but keep in mind that the asset owner is the one who has the responsibility (and the authority) to protect the asset. This doesn't mean daily activities can't be delegated by the asset owner, but it's their responsibility to do so.

Additionally, you might want to assign values or criticality *scores* to your assets, in order to streamline the prioritization and risk management processes. Asset criticality can allow for a better understanding of what is at stake and make for more accurate impact scores. As a result, this can help prioritize which controls get applied, in which order. With that said, asset criticality is not a requirement from ISO 27001, so ensure you're making sure it's fit for purpose for your organization, and remember that complexity is the enemy of security.

One more point to remember when it comes to your asset inventory is keeping it up to date. This inventory acts as a tool for reducing risk at your organization, and as a result, it must be continually updated to reflect any changes to assets, asset owners, values, criticality scores, or any other information that is required for a complete asset inventory at your organization.

We will delve deeper into how you might want to classify assets or information at your organization, and the roles for information assets, later on in this chapter, so let's move on to the next requirement for the ISMS documentation, the information classification policy.

Information classification policy

This policy sets out to define the requirements and processes for classifying information assets at your organization. It is a key document in the ISMS, and must (yet again) cater to your organization's needs, and be proportionate to the level of risk the organization faces.

We aim to classify information assets based on the organization's legal requirements, as well as the asset's value, criticality, and sensitivity. From general experience, I've found that most organizations will have around four classification options, to allow for flexibility without being overcomplex, but depending on the organization, there could be a wider (or narrower) range of classifications.

There are no specific requirements in ISO 27001 for what levels of classification are required, but you can align the classifications with other requirements or best practices, depending on your geographic location or industry.

A typical set of classification levels could include the following:

- Confidential
- Restricted
- Internal
- Public

In your policy, you might define that the asset owner is responsible for the appropriate classification of information, based on the definitions set out in this document.

Labeling based on classification

Your organization may commit to labeling physical and digital information assets based on their classification, and you are able to set out the requirements for doing so in the **information classification policy**.

In the later stages of this chapter (and throughout the book), I will go through various ways we can classify, handle, and protect information based on its classification and risk, but as you might have noticed, everything in your ISMS should reflect your organization and its requirements, there is no hard-and-fast way of going about this.

Acceptable use policy

Now that we have an inventory of the organization's assets, and understand how those assets are classified and labeled, we should specify how those assets should be used by members of your organization, contractors, and third parties in order to comply with the information security requirements defined in your ISMS. This acceptable use policy should be part of the information security training and education for members of your organization and should be accessible to all members who are subject to its requirements.

Some examples of what might be included in an **acceptable use policy** include any security rules applicable to employees, such as the following:

- General use and asset ownership policies
- Policies for email security
- Policies for company assets, such as laptops and mobile devices
- Policies for using third-party software
- Policies for returning assets upon termination of employment
- Policies for handling removable media, such as USB drives
- Policies for the secure disposal of media

This document should cater to your organization's needs and the nature of how members of the organization interact with information systems in their daily activities. Further, the policies should be proportionate to the level of risk the organization faces. In order to ensure the appropriate handling of information assets, the asset classifications should be taken into account, and appropriate policies for how to handle assets with each classification should be defined.

Risk management documentation

Now that we understand the organization's assets, we are able to define a policy for how we assess, treat, and report on the risks facing those assets. In order to ensure the effectiveness of your ISMS, this risk management documentation must be clear and absolutely *must cater to your organization's requirements and abilities*. If it does not, your ISMS will likely fail to protect your organization from the threats it faces. It is also crucial to remember that complexity is the enemy of security, and as a result, it is crucial to reduce any complexity in these documents and processes to the minimum amount.

I have already taken an opportunity in *Chapter 1, InfoSec and Risk Management*, to cover important risk management topics, but to skim over what we covered in the previous chapter, we want to perform risk assessments in order to understand the risks the organization faces, including determining the impact and likelihood of those risks. I assure you that I will expand on these topics throughout the book, including covering threats and control types in *Chapter 3*, *Designing Secure Information Systems*. For now, we're simply looking at documentation and processes.

In a general sense, the process that your organization will follow to manage risk can be reduced to the following steps:

- Risk identification
- Risk assessment (and prioritization)
- Risk treatment, including storing documented evidence
- Monitoring and reviewing the risks, including management reviews

To begin with, let's talk about risk identification, assessment, and treatment documentation.

Risk assessment methodology and risk treatment methodology

By creating **risk assessment methodology** and **risk treatment methodology** documents, you're able to define specifically how and when your organization performs a risk assessment, who is responsible for each step, how to calculate the risk level, and how we may reduce any unacceptable risk to an appropriate level.

You might decide that, in order to meet your organization's needs, a risk assessment is required annually, or upon significant change. That's a pretty typical choice I've seen quite often, but it's not necessarily the best choice for every organization. As we've said several times, it's all about catering each policy and procedure to your organization.

If we recall that one long sentence about risk from *Chapter 1, InfoSec and Risk Management*:

Information Security Risk is the potential for loss as measured through the combined impact and likelihood of a threat exploiting a vulnerability in one or more information system assets.

We remember that we cannot have a risk without an asset and a threat. In these documents, we can define how we identify and measure risk, and whether we perform risk assessments based on threat scenarios, or by each information asset associated with the organization. You have a list of assets at your organization, in your asset inventory, so you should leverage that inventory and reference it in your risk management documentation.

Furthermore, we can define the scale and definitions for likelihood and impact in this document. I covered an example of how you might do that in *Chapter 1, InfoSec and Risk Management,* and this is your chance to either use that example, leverage another framework, or create your own ad hoc system for assessing those levels.

You might also want to include the risk matrix, with the defined risk appetite *level* clearly displayed on it, as defined by top management.

When we're looking at risk treatment, you might remember that it's possible to do the following:

- Avoid the risk
- Reduce the risk through security controls
- Transfer the risk
- Accept the risk

You can describe these processes in your documentation, in order to ensure other members of your organization understand how and when they might choose each treatment. Keep in mind that you have a Statement of Applicability document that lists any applicable controls for your organization, and ensure that you reference it in your risk treatment methodology. You can also define how your organization accepts risks (and documents that acceptance) once the risk level has been reduced to an acceptable level.

By defining an effective risk management process for your organization, and applying the principles of continual improvement, you improve the effectiveness of your ISMS by increasing the visibility of the risks that your organization faces.

Risk assessment report

You need to be able to plan and prioritize risk treatments, as well as to communicate the results from risk assessments to relevant stakeholders. This implies that you should have various reports based on risk management activities, depending on the audience.

For example, in your regular updates to top management, you could provide a high-level overview of the risk assessment, as this audience is ultimately responsible for ensuring the ISMS is effectively implemented at their organization, but not necessarily interested in the specific details. You might include the most important assets and their inherent risk levels, the risk treatment applied (or proposed), and the resulting residual risk after the treatment.

In the more detailed report, it might make sense to provide a status for each of your organization's assets, as well as the Statement of Applicability controls and their status. Additionally, if a control is in the process of being implemented, you can report on the progress of that implementation.

Third-party security documentation

In *Chapter 1*, *InfoSec and Risk Management*, we discussed the importance of managing third-party risk at our organization, as a result of the growing reliance on suppliers to provide information systems, and cloud solutions for performing business activities.

In our third-party security policy, we want to define specifically how our organization handles the management of third-party risk, and describe how we can monitor, review, and audit a supplier's security.

This could include definitions and methodologies surrounding service-level agreements, vendor security assessments, and due care at your organization.

Furthermore, you should consider how you might catalog each asset used by your organization that is managed or controlled by a third party, and how you might structure your ISMS and information security strategy to cater to the shared responsibility model.

Incident management documentation

When we focus on incident management documentation, we want to be clear on what is required in a specific type of event. As the information security professional, you will need to work together with your organization's leadership to define the thresholds necessary to declare an information security event an incident, and the appropriate response.

The best way to document this is to create a high-level incident management policy, which defines the appropriate roles and responsibilities and includes references for any supporting documents, such as playbooks. The incident management policy should be the central document in any incident management activity, and the first reaction of any staff member in the event of an information security event should be to refer to it.

With the knowledge that this suite of documents is going to be required during incidents such as an outage, it's valuable to note that the incident management policy, and all other incident management and business continuity documents, should be stored in a way that is accessible regardless of whether availability to the information systems is affected. If ransomware spreads through your organization, you can't access the documents stored on your NAS anymore. Do you have printed copies? The same goes for physical copies: If your printed copies are now underwater, do you have a way to access those policies through cloud storage?

After the high-level incident management policy has been created, two areas in which a defined, easily-followed, structured approach to information security is incredibly valuable are **incident response plans (IRPs)** and **Business Continuity Management (BCM)**.

As we have defined how we're going to discover and classify our assets, and how we're going to perform risk assessments based on our asset criticality, we have achieved much of the progress required in order to structure these processes into our organization.

By understanding asset criticality, and the threats associated with the risks your business faces, you can ascertain and define the organizational requirements for business continuity and incident response.

We will delve deeper into various aspects of business continuity and incident response in *Chapter 7*, *Owning Security Operations*, and so I will do my best to avoid repeating myself too much here, and instead focus on the high-level requirements for the documentation and planning required to ensure your organization is prepared to respond to incidents.

Incident response and business continuity playbooks

Always remember that in the event of an information security incident, heart rates will have risen, palms will be sweaty, and there will be many people involved in the "what's next?" discussion.

Incident response playbooks should be simple, easy-to-follow for anyone, and accurate to the most recent changes in business processes or versions. This is much more difficult than it sounds. Think of it as a "picture book," where the first page is the first step, the second page is the second step, and so on. This is a highly effective method that increases the likelihood of a successful response.

You can have a playbook for the various threat scenarios, such as "Our server has been damaged," or "Ongoing DDoS attack on our website," and so on. All threats that are viable and require a response that is repeatable can be turned into playbook form, and it's not something that should be skipped over.

Furthermore, you can't just assume these playbooks are effective. We can't trust that the person who is accountable for executing the plan is going to be able to do so. It's important to run through the plan and see whether it will actually pan out the way it should, by holding incident management training, awareness sessions, and performing regular **tabletop exercises**. Tabletop exercises are simulations where members of the organization get together in a conference room and walk through realistic incidents at their organization, discussing their responsibilities and looking for gaps in the documented plans and procedures. The advantage of a tabletop exercise is that they're inexpensive and easy to facilitate, while still measuring the impact of various events. In order to make tabletop exercises more interesting, you as the information security professional should throw in curveballs occasionally. When people start following along and become bored with the activity, throw in a "The card is declined. Now what?". It keeps the members of the team on their toes and engaged, and simulates the messy real world where nothing goes to plan.

By documenting and optimizing the response process and applying findings from tabletop exercises and simulations, you are able to reduce the amount of time it would take to diagnose the cause of an incident, and the stress level experienced by the members of the response team.

IT management documentation

Due to the close-knit relationship between information technology and information security, your ISMS will likely contain several references to IT management documentation that may already exist at your organization or may need to be created with input from the relevant stakeholders.

This documentation could include the following:

- Operating procedures for IT management
- Secure system engineering policy
- Access control policy
- Bring your own device and mobile device policies
- Password policy
- Information disposal and destruction policy
- Maintenance and review plan
- Change management policy
- Backup policy
- Exercising and testing plan
- Information transfer policy
- Procedures for working in secure areas
- Clear desk and clear screen policies

It's crucial that these documents state the reality of your organization's approach, and are in line with the level of risk determined as acceptable.

Educating members of your organization

Although it's a great start to define the requirements of the ISMS in a set of documents and to use those documents to implement a systematic process for securing your organization's assets, users may feel arbitrarily restricted if a solution is rolled out that prevents them from working the way they always have, without any communication about the reasoning.

Even the most intelligent systems are able to be circumvented or destroyed, and your users might be compelled to find ways to get around the policies or controls in order to make their lives easier. Your organization has a requirement to train its users on the ISMS, and educate them on its impact on them in their role. It's important to help them see that you're trying to make their jobs easier by removing the burden of ambiguity from their daily working lives.

As we've said earlier, these policies need buy-in from top management, with repercussions for when the policies aren't followed. You are doing this to protect their organization, and so top management needs to care, and they need to be champions for your ISMS. Try to get the leadership team involved in the communications that you would normally send out yourself. By having a sponsor in the form of a CEO, MD, CTO, CFO, or similar, you will have notoriety among the staff that there is a method and a strategy, and it's not just you as a lone wolf "security dude" being paranoid and harping on at them about not installing browser add-ons, or randomly tricking them with phishing exercises. Getting the VIPs to do the heavy lifting is an especially important concept to embrace in order to increase effectiveness.

Furthermore, it's important to raise general information security awareness with all members of your organization. A good awareness initiative will enable users to identify various types of control circumvention, and potentially even prevent such activity by reporting a non-compliance scenario. That's an important aspect of ensuring the security of your organization is maintained and effective.

As with everything, optimization is key, so let's move on to evaluating your ISMS's effectiveness.

Evaluating the effectiveness of the ISMS

Evaluating the effectiveness of your ISMS, and whether it is fit for the purposes of your organization is crucial in the optimization of your organization's wider information security maturity. There should be a requirement set to review the effectiveness of the ISMS on a regular basis, such as annually, and to perform an internal audit as defined by your internal audit procedure, previously defined. Any **non-conformities** or **findings** should be subject to the corrective action procedure that we've also previously defined.

Additionally, by including findings from discussions and dialogs on a daily basis, and subjecting them to the same corrective action requirements, you enable continual improvement by defining the future changes required.

If your organization must comply with several standards and regulations from global bodies, it's important to consider the potential to leverage technological solutions to manage your requirements for your implementations. There are several tools available to align your ISMS and security controls with multiple regulations, and utilizing those can increase the coverage and effectiveness of your ISMS.

Improving the policy

The improvement phase of your ISMS is where we identify present gaps and plan for the next version of the policy. Always remember that this policy is acting as a structure for you to organize and plan your organization's information security program. It's just as important as anything else in the job, and there's a reason I started with this (extremely not-dry, but rather highly interesting and entertaining) topic.

Without fail, I'm going to mention the ideology of continual improvement with every step of this book. It's integral to keep up to date by regularly measuring risk, and applying controls to ensure the organization is not exposed to an unnecessary or unacceptable level of risk.

To summarize, in order to be able to implement an ISMS that ensures the appropriate identification, classification, and protection of the information assets of an organization, we must start with policies that reflect the organization's requirements from an organizational and IT perspective. It's critical to ensure the members of your organization are educated on the ISMS in order to avoid an increased level of unknown risk, such as **shadow IT**, which is a term to describe any IT systems that have been deployed without the IT department's oversight, and therefore circumventing the policies, processes, and controls that have been implemented to keep the organization secure.

Let's proceed toward the topic of identifying and classifying information assets next.

Identifying and classifying information assets

In your asset management policies, it's likely that you have defined the way your organization is going to identify and classify information assets based on the value, criticality, sensitivity, and legal obligations, but not specifically discussing *how* your organization might do that from an IT perspective.

While creating that policy and defining those motives is a huge leap forward in understanding the overall position your organization takes when it comes to their risk appetite and what is considered to be the most valuable information they have, remember that it's also just the "rule," and not the actual action of identifying and classifying those assets or protecting them for that matter.

In this section, I would like to detail the ways we can structure the rules, as well as the actual "doing" part of an effective identification and classification phase of an ISMS.

This includes the following topics:

- Structuring information asset classifications
- Determining the roles for assets
- Identifying and protecting information assets
- Retention policies

You're about to learn some key information security principles! Get ready!

Structuring information asset classifications

In your documentation, it is likely that you have defined classifications for your information assets, based on the value, criticality, sensitivity, and legal obligations determined by the organization.

You might have arrived at a hierarchy of classifications such as the following:

- Confidential
- Restricted
- Internal
- Public

How are you going to ensure the appropriate classification is applied to the relevant information assets, and how are you able to ensure the assets are protected and secured appropriately?

Generally, you will want to define specific roles for each of your assets. Each of these roles should have various responsibilities in the identification, protection, and disposal of information assets. The **Information Owner** could be responsible for ensuring the data is properly classified, and that the appropriate data protection has been applied, in line with regulatory and organizational requirements, for example.

Determining the roles for assets

If you want to be structured with the way your organization handles the identification and classification of its information assets, you must consider defining the roles listed in the following table for each asset. As with everything, the level of structure you create and implement should be acceptable for the organization you're working with.

Some roles to consider documenting for each asset are the following:

Information Owner	Responsible for data protection and ensuring the data is properly classified.
System Owner	Controls the software and hardware configurations for the processing and storage assets that the information lives in.
Information Custodian	Responsible for backups and restoration.
Security Administrator	Assigns the permissions for the network.
Users	Must comply with all policies and rules when sharing information with others.
User Manager	Responsible for overseeing the activity of all of the above-mentioned roles.

While it may not be feasible for a small company to have dedicated roles to accomplish each of these tasks, these roles (and several others) could exist in a large organization. Additionally, you could have several types of information owners, and each system could have a respective system owner, split, for example, by vendor.

With that said, if it's possible, use the KISS principle, which is a term recognized by the software engineering community as a design principle meaning *"Keep it simple, stupid"*. You want to ensure less work and maintenance is required to be successful in your ISMS. There's already a lot of work to be done without the extra complexity.

Methods of identifying and protecting information assets

Great! We have now defined our categories for classifying information assets. An additional consideration, and potentially the most important of all is the matter of *how* you can ensure the information is properly classified.

The manual identification, classification, and protection of information assets isn't a scalable or dependable solution. Loss, modification, or disclosure of these assets can carry significant financial and reputational risk. It makes very little sense to make non-InfoSec people responsible for appropriately identifying, classifying, and protecting the information assets of your organization during their day-to-day work.

Luckily, there exists **Data Loss Prevention (DLP)** or **Information Protection** technology to help the process of properly identifying and classifying our organizational information. We can leverage "built-in" models for discovering and classifying information, or create our own rules.

The "built-in" models can automatically identify specific types of information, no matter where it lives, or the format. This means we can configure our DLP or information protection solution to "find" credit card numbers sent in chat messages, or passport numbers detected in a `.jpeg` file on a corporate laptop's hard drive, as a couple of examples.

Beyond this, by creating our own model (or definition) of an information type, administrators are able to use regex and complex filters to locate any files that include information that is specific to the organization, such as keywords like Project Neptune, for example.

After locating this data, an automatic metadata "label" for the information classification is be applied, along with any appropriate restrictions for access, protections through encryption, as well as watermarks or notices that are visually apparent while users are accessing the information. The operating system or mail solution can even show the user a notification to explain why they aren't able to send a file outside of their organization, and link to any relevant training.

Through automation in the discovery, classification, and protection of our information assets for our organization's estate, we ensure that information is available to only those who need to access it, that the information has only been changed by those approved to, and that those changes are tracked and stored in a way that is auditable.

This type of solution is an absolute dream compared to even 5 years ago when DLP was still extremely antiquated and didn't offer anywhere near this level of automation. Now, if a user is creating a file on their laptop that discusses a sensitive topic, or contains PII, a label is automatically applied to that document, which, in turn, activates encryption and restricts access to the appropriate group of users. It should be the asset owner's responsibility to ensure the appropriate classification is automatically applied.

Administrators of this system should be able to see metrics of the users, locations, or programs and services that have each type of data associated with them. By using a technological solution to aid in this process, you can monitor the changes, detect new requirements, and measure the efficacy of your policy, based on the results from the monitoring over the entire lifespan of all of your organization's information assets.

Outside of the digital realm, in your information classification policy, you could (for example) require that the classification is indicated in the top-right corner of each physical document page and that it is also to be indicated on the front of the cover or envelope carrying such a document. As we've previously said, the policy should suit the organization, and as a result, there should be processes to follow the requirements set out from the policy, and repercussions for not complying with those requirements. Whether we can or cannot automate the process, ensuring the appropriate classification and labeling of information is usually the responsibility of the asset owner.

Luckily, we have defined a policy in plain language, to help those responsible for selecting, implementing, and configuring the systems that regulate these requirements. By setting those requirements in the information classification policy, we are able to select a technology that mitigates against the risks associated with data exfiltration, insider threats, retention policy breach, and so on, as required by your organization.

Retention policies

I'd like to briefly talk about retention policies, and considering them while developing and implementing your ISMS. There exist regulations in many jurisdictions that require that any sensitive data, when processed for any purpose, is not retained for any longer than the prescribed amount of time. What is the prescribed amount of time, you ask? Well, unfortunately, that depends on the jurisdiction, and type of data.

In our policies, it's important to consider the retention requirements for our organization, and ensure that a retention policy is defined. With these definitions, you can leverage technological solutions that exist to do the following:

- Ensure you aren't allowing users to dispose of information that must be retained due to a specific regulatory requirement.
- Ensure information that is able to be disposed of is disposed of in a timely and compliant manner.

Some of the requirements you should be looking to define are the following:

- How should we store and retain data in a way that makes it accessible whenever it is required, in a way that is easily searched and classified? This includes audio files, video files, and so on.
- What data must be retained? Business management, third-party dealings, partnerships, employment records. These are just the tip of the iceberg. Split the data into categories and consider a solution that allows tagging into these categories (along with sensitivity labeling).
- How long must the data be retained? Consider each classification or category, as they can differ.
- How do we apply ownership to information and assets? This can be done by policy only, but it would be better to automate it, as with almost anything, if you find a reliable solution.

With the same information protection technological solutions from the previous section, we are able to automate the retention policies defined by your organization and remove a file from access after 7 years of inactivity, for example.

Securing information assets

This section is all about implementing the appropriate information security controls for assets. I've been thinking about this section for a while, trying to understand how to tackle it best for you.

I know you probably have experience with choosing and implementing controls, and I don't want this section to end up being half of the entire book, just droning on and on about different types of controls or all of the great vendors out there who want to sell you a silver bullet to fix all of your issues. I'm going to go into many different controls and ideologies in the following chapters, anyway.

Instead, in this chapter, I want to make sure that we focus on heavy-hitting, effective ideologies to understand in order to select the appropriate controls, meaning that the asset is considered "secure enough" based on its criticality and classification.

There are different **classes** that split up the types of controls:

- **Administrative/Managerial Controls** are the policies and procedures I'm always talking about. They aren't as "cool" as a new software control, but they exist to give structure and guidance to individuals like you, and other members of your organization, ensuring nobody gets fined or causes a breach.

- **Physical Controls** limit the access to systems in a physical way; fences, CCTV, dogs... and everybody's favorite: fire sprinklers.
- **Technical/Logical Controls** are those that limit access on a hardware or software basis, such as encryption, fingerprint readers, authentication, or **Trusted Platform Modules** (**TPMs**). These don't limit access to the physical systems the way physical controls do, but rather access to the data or contents.
- **Operational Controls** are those that involve people conducting processes on a day-to-day level. Examples could include awareness training, asset classification, and reviewing log files.

There are so many specific controls, there's just no way we can go into each of them in this chapter. Beyond the Annex A controls from ISO 27001, further expansion on controls and the categories of controls can be found in the links on this page: `NIST SP 800-53 Rev 5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final)`, including control mappings between the ISO 27001 standard, and *NIST SP 800-53*.

What I can cover are the types of controls that you'll be able to categorize and apply as mitigation against risk, depending on the threat and vertical:

- **Preventative Controls** exist to not allow an action to happen and include firewalls, fences, and access permissions.
- **Detective Controls** are only triggered during or after an event, such as video surveillance, or intrusion detection systems.
- **Deterrents** discourage threats from attempting to exploit a vulnerability, such as a "Guard Dog" sign, or dogs.
- **Corrective Controls** are able to take an action from one state to another. This is where fail open and fail closed controls are addressed.
- **Recovery Controls** get something back from a loss, such as the recovery of a hard drive.
- **Compensating Controls** are those that attempt to make up for the shortcomings of other controls, such as reviewing access logs regularly. This example is also a detective control, but compensating controls can be of various different types.

Generally, the order in which you would like to place your controls for adequate defense in depth is the following:

1. **Deter** actors from attempting to access something that they shouldn't be.
2. **Deny/Prevent Access** through a preventative control such as access permissions or authentication.

3. **Detect** the risk, making sure to log the detection, such as with endpoint protection software.
4. **Delay** the process of the risk from happening again, such as with a "too many attempts" function for a password entry.
5. **Correct** the situation by responding to the compromise, such as with an incident response plan.
6. **Recover** from the compromised state, such as a backup generator restoring availability to a server.

Furthermore, in the realm of continual improvement, we should monitor the value of each asset for any changes. The reason being that we may need to rethink our controls for protecting those assets if they become more or less valuable over time, or in certain major events at your organization.

Additionally, as a footnote, when we're looking at controls, we should also be thinking about recovery. What I mean is that we want to be able to recover from any adverse situations or changes to assets and their value. Just as examples, we're talking about backups, redundancy, restoration processes, and the like.

A concept to keep in mind, especially in the era of the cloud, SaaS, PaaS, IaaS, third-party solutions, and all other forms of "somebody else's computer" is to ensure that **Service-Level Agreements** (**SLAs**) are clearly defined, and have agreements for maximum allowable downtime, as well as penalties for failing to deliver on those agreements. This is an example of a compensating control.

As a consumer of third-party solutions, you'll want to fight for SLAs that reflect your risk appetite. Simultaneously, you'll also want to consider the idea that by chaining those assets together, you are creating a higher level of risk to availability. If just one of the services isn't online, and you can't perform a task, that's a loss of availability. If you're a vendor of cloud services, you need to consider your availability and what can be offered to your customers realistically, and what is required from a commercial perspective.

Data security

When we're looking at data security specifically, there are three key **states** of data that present unique security requirements: data in transit, data at rest, and data in use.

Data in transit

Data in transit or data in motion is data that is being transmitted either inside the network, or out of the network onto the web, either through physical cables or wireless connections, or from one application to another sitting on the same computer, or whatever other type of data transfer can occur, which I'll avoid going into before this sentence makes both of us lose our minds.

There's also the concept of **information in transit** being something like people speaking at a water cooler, or a USB drive being moved to another desk... but let's not be ridiculous. There's a reason I said "data" and not "information" in this case.

Data at rest

Without complicating things too much, let's just define **data at rest** as data that is being stored, not currently utilized. It begins to get a bit complicated when you consider databases as constantly growing and changing entities, with machine learning models utilizing the data in an evolving, living amoeba of logic. But as I've said, let's keep it simple.

Data in use

Data in use is data that is being processed by a system or user and is usually stored and referenced in a non-persistent memory form such as a CPU cache or RAM.

Encryption for data in various states

Encryption is one of the ultimate controls that we can discuss, for both data at rest, and data in transit. In order to effectively keep data secret, employing encryption is likely going to be a necessity. Actually, it must be used in order to satisfy the requirements set forth by standards such as PCI-DSS or ISO 27001.

Beyond the requirements, cryptographic controls are incredibly useful as a mitigation tactic. Make sure you're aware of the different types of encryption, and that doesn't only mean understanding "symmetric" versus "asymmetric" encryption, but also different encryption standards, and which mechanisms are used for securing data in transit, such as *TLS*, as opposed to securing data at rest, such as *AES-256*.

Hashing is a cryptographic function for integrity, which (for example) allows storing passwords in a way that ensures the input is the same as the compared data but without storing the plaintext of the input. Furthermore, hashing helps to ensure that data hasn't been changed, by using a checksum or message digest. Being up to speed with these topics should be at the top of your priorities, as you will use encryption more and more as a control moving forward.

Defense in depth

A major focus for you at your organization should be the consideration of **defense in depth**, a concept I touched on briefly in the last chapter, but wanted to re-iterate on here. We don't want a single point of failure to allow a complete loss of confidentiality, availability, or integrity. If we're protecting our assets adequately, it means that we can have a control fail, and still have the peace of mind that we have other controls in place that mitigate against the risk, (or at least some of it). It's difficult to achieve in practice, due to usability concerns, budget constraints, or a lack of options.

For an example of how defense in depth might look for a specific system, let's say your organization creates a web app allowing internal users to log in and create, read, update, or delete data in a database. How can you be sure that unauthorized users aren't able to read or update the data through a vulnerability? How can you ensure the app stays online and the data remains available?

Let's take a look at some of the controls we might put into place for the app:

- To prevent unauthorized access, and to enforce the appropriate levels of access based on the type of user, you might want to implement a form of authentication with varying levels of authorization. To protect against the breach of passwords, they should be stored as salted hashes, created with a secure function, with no way to reverse them back into plaintext.
- To prevent unauthorized changes to the web app's source code, the code base could be stored in a source control solution, such as GitHub or GitLab. Each developer could be given a unique login and be made to choose a strong password and utilize two-factor authentication.
- To prevent backdoors and common flaws from being implemented in the source code by a developer, you could run static code analysis on the code base. To check for vulnerabilities in any imported software used in the app, you could run a *dependency scanner* for the included imports also.
- To look for vulnerabilities in the app once it's running, you could run a vulnerability scanner on it, which pokes at it for common flaws to check for issues with versions, headers, and input sanitation, among other things.
- In order to detect whether there has been a breach, and to investigate and mitigate against the vulnerability being exploited again, logging, auditing, and monitoring policies and solutions could be implemented.
- Do you know whether your users are only going to be accessing the application in a certain context, such as from a specific IP address? You can implement firewall rules to whitelist (or only allow) that access, blocking everywhere else.

- You could also use a **Web Application Firewall** *(***WAF***)* to protect against common injections and cross-site-scripting attacks, among other things.
- How can you ensure that the application is available when it needs to be? You should probably look at load balancing and deploying across multiple locations.

So, that scenario gave various different examples of technical security controls, with administrative controls as policies for how they are configured. Is this a good example of defense in depth for the web app? Are you adequately protected?

It depends on the risk appetite! You might not need all of these controls, or they might not be enough, depending on the asset classifications, criticalities, and how much risk the organization is willing to accept. That's why in the first two chapters we've focused on that so heavily: Without understanding our risk level, there is no way we could understand whether we're spending too much (or not enough) time, effort, and money on mitigating against risk.

Monitoring for changes

You should be monitoring your organization's information *assets* for changes, and adapting to those changes, following the principle of continual improvement. One way you might handle this is through a regular risk assessment process, in which you perform risk assessments annually, or upon significant change, for example.

Another way would be to implement technological solutions to keep track of configuration changes, vulnerabilities and updates, or active threats. I cover configuration management and monitoring for security purposes in *Chapter 7*, *Owning Security Operations*, and as a result, I'm going to let that chapter do the heavy lifting on this topic.

Eventually, from your monitoring activities, you will discover it is time to retire an asset and dispose of it, which I'll move on to now.

Disposing of assets

We have several different physical and digital information assets in our control at our organization, all of which are likely to reach the end of their life cycle eventually.

How do we go about ensuring the secure disposal of those assets? It's likely we're not able to just throw sensitive financial documents or the CEO's laptop into the trash, making those information assets unprotected, waiting for a **dumpster-diving** malicious actor.

ISO 27001 mentions two controls on the topic of information disposal:

- *"Media shall be disposed of securely when no longer required, using formal procedures."* (A.8.3.2).
- *"All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use."* (A.11.2.7).

As a result, in order to comply with the standard, you should define your organization's requirements for the secure disposal of information assets based on classification, and you should provide specific processes for how your organization recommends its members abide by those requirements. Furthermore, you should keep a record of securely disposed of information assets.

Additionally, the disposal or reuse of storage media or devices should include a process to ensure the effective removal of any data remnants from the device.

Data remnants

Data remnants are a result of deleting data in a system but the system simply marking that space as "available for use," without actually erasing it. It is very simple to recover this data, with both commercial and open source solutions available to anybody with the most basic knowledge of installing software onto a computer.

This type of threat can be mitigated by structuring some sort of **defensible destruction** in your organization, which is the controlled, compliant, legal method of destroying data through one of the following methods:

- **Overwriting**, which causes the original data to be replaced with new or random data. The US standard is a minimum of seven times.
- **Degaussing**, or removing the magnetic imprint on disk drives, which wipes the drives. This could potentially be useful for old-school HDD drives.
- **Encryption** is not only a way to protect data at rest and data in transit, but also a potential way to make data unrecoverable by using a secret key that isn't stored, as in "throwing away the key." Cryptoshredding is a term used for when you encrypt your data and then encrypt the recovery key so it can never be used again.
- And then, of course, the **physical destruction** of a disk, usually by putting it into a woodchipper-like device, sort of like Steve Buscemi in Fargo. Other examples could include incineration, shredding, disintegrating, and pulverizing.

When we talk about **data disposal**, we don't always mean defensible destruction, however. Sometimes, when we dispose of data, we archive it into long-term storage. We won't use the data, but if it's required in the future, we have it securely stored, usually in a way that is the most cost-effective for the use case. This method is valuable for data that could be required for legal proceedings, for example. The retention periods and requirements for your organization must be understood and considered in order to make an appropriate decision on how to store this data and remain compliant with local laws and regulations.

Summary

In this chapter, we focused on the various topics surrounding protecting the security of assets. We had our hair blown back with the enthralling topic of implementing an ISMS, which covered everything from the responsibilities of top management to developing an ISMS, educating members of your organization, evaluating the policy's effectiveness, and improving the policy for the next iteration.

Then we moved on to identifying and classifying information assets – from structuring the information asset classifications to determining the roles for assets, methods for identifying and protecting information assets, and retention policies.

We moved on to a high-level overview of securing information assets, data security, encryption, defense-in-depth, and monitoring for changes, before moving on to the final topic of disposing of assets and data remnants.

And, just like that, we are through this chapter. I am not even sure how you managed to take in all of that information, but somehow you did, and you're all the better for having done it. Now let's move on to the next chapter, where we'll talk about designing secure information systems.