CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Table 4-1 NIST SP 800-53 Control Categories

interest of brevity, we will only look at the first three controls (IR-1, IR-2, and IR-3) in the Incident Response, or IR family. You can see in Table 4-2 how these controls apply to the different SCs. Since the CRM is SC high, all three controls are required for it. You can also see that IR-2 and IR-3 have control enhancements listed.

Let’s dive into the first control and see how we would use it. Chapter 3 of SP 800-53 is a catalog that describes in detail what each security control is. If we go to the description

Control No.

Control Name
CONTROL ENHANCEMENT NAME

Control Baselines
Low

Mod.

High

X

IR-1

Policy and Procedures

X

X

IR-2

Incident Response Training

X

X

IR-2(1)

Simulated Events

X

IR-2(2)

Automated Training Environments

X

IR-2(3)

Breach

IR-3

Incident Response Testing

IR-3(1)

Automated Testing

IR-3(2)

Coordination with Related Plans

X

X

X

X

X

Table 4-2 Sample Mapping of Security Controls to the Three Security Categories in SP 800-53

a. Develop, document, and disseminate to [Assignment: organization-defined

personnel or roles]:
1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:
(a.) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(b.) Is consistent with applicable laws, executive orders, directives, regulations,
policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls;
b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and
c. Review and update the current incident response:
1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
Notice that there are assignments in square brackets in five of these requirements.
These are parameters that enable an organization to tailor the baseline controls

to its own unique conditions and needs. For example, in the first assignment (IR-1.a), we could specify who receives the policies and procedures; in the second (IR-1.a.1), we could specify the level(s) at which the incident response policy applies; in the third (IR-1.b), we could identify the individual (by role, not name) responsible for the policy; and in the last two assignments (IR-1.c.1 and IR-1.c.2), we could provide the frequency and triggering events for policy and procedure reviews. This is all a “fill in the blanks” approach to tailoring the controls to meet your organization’s unique conditions.

EXAM TIP You do not need to memorize the controls, control enhancements, or assignments of NIST SP 800-53. We provide them here to illustrate how a framework provides structure while still allowing you room to customize it.

CIS Controls

The Center for Internet Security (CIS) is a nonprofit organization that, among other things, maintains a list of 20 critical security controls designed to mitigate the threat of the majority of common cyberattacks. It is another example (together with NIST SP 800-53) of a controls framework. The CIS Controls, currently in Version 7.1, are shown in Figure 4-4.

of the baseline IR-1 (Incident Response Policy and Procedures) control, we see that it requires that the organization do the following:

Basic

Foundational

Organizational

1. Inventory and Control of Hardware Assets

7. Email and Web Browser Protections

12. Boundary Defense

17. Implement Security

Awareness and Training

2. Inventory and Control of Software Assets

8. Malware Defenses

13. Data Protection

18. Application Software Security

3. Continuous Vulnerability Management

9. Limit and Control Network Ports, Protocols, Services

14. Control Access Based on Need to Know

19. Incident Response and Management

4. Controlled Use of Administrative Privileges

10. Data Recovery Capabilities

15. Wireless Access Control

20. Penetration Tests and Red Team Exercises

5. Secure Configuration of Hardware and Software

11. Secure Configuration of Network Devices

16. Account Monitoring and Control

6. Maintenance, Monitoring and Analysis of Audit Logs

Figure 4-4 CIS Controls

Despite CIS's use of the word "controls," you should really think of these like the 20 families of controls in SP 800-53. Under these 20 controls, there are a total of 171 subcontrols that have similar granularity as those established by the NIST. For example, if we look into control 13 (Data Protection), we can see the nine subcontrols listed in Table 4-3.

Subcontrol	Title	IG1	IG2	IG3
13.1	Maintain an Inventory of Sensitive Information	X	X	X
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	X	X	X
13.3	Monitor and Block Unauthorized Network Traffic			
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers			
13.5	Monitor and Detect Any Unauthorized Use of Encryption			
13.6	Encrypt Mobile Device Data			
13.7				

Manage USB Devices

13.8

Manage System’s External Removable Media’s Read/Write Configurations

X

13.9

Encrypt Data on USB Storage Devices

X

X
X

X
X

X

Table 4-3 Data Protection Subcontrols Mapped to Implementation Groups

X

X

X

X

- Basic These key controls should be implemented by every organization to achieve minimum essential security.
- Foundational These controls embody technical best practices to improve an organization’s security.
- Organizational These controls focus on people and processes to maintain and improve cybersecurity.

A useful tool to help organizations match their implementation of controls to their resource levels are implementation groups (IGs). Version 7.1 of the CIS controls describes the following three IGs:

- Implementation Group 1 Small to medium-sized organizations with limited IT and cybersecurity expertise whose principal concern is to keep the business operational. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.

- Implementation Group 2 Larger organizations with multiple departments, including one responsible for managing and protecting IT infrastructure. Small organizational units. These organizations often store and process sensitive client or company information and may have regulatory compliance burdens. A major concern is loss of public confidence if a breach occurs.
- Implementation Group 3 Large organizations that employ security experts with different specialty areas. Their systems and data contain sensitive information or functions that are subject to regulatory and compliance oversight. Successful attacks against these organizations can cause significant harm to the public welfare.

You can see in Table 4-3 how subcontrols can be mapped to these implementation groups. This helps ensure that limited resources are focused on the most critical requirements.

COBIT 2019

COBIT 2019 (the name used to be an acronym for Control Objectives for Information Technologies) is a framework for governance and management developed by ISACA (which formerly stood for the Information Systems Audit and Control Association) and the IT Governance Institute (ITGI). It helps organizations optimize the value of their IT by balancing resource utilization, risk levels, and realization of benefits. This is all done by explicitly tying stakeholder drivers to stakeholder needs to organizational goals (to meet those needs) to IT goals (to meet or support the organizational goals). It is a holistic approach based on six key principles of governance systems:

1. Provide stakeholder value
2. Holistic approach

The CIS recognizes that not every organization will have the resources (or face the risks) necessary to implement all controls. For this reason, they are grouped into three categories, listed next. While every organization should strive for full implementation, this approach provides a way to address the most urgent requirements first and then build on them over time.

3. Dynamic governance system
4. Governance distinct from management
5. Tailored to enterprise needs

6. End-to-end governance system

Everything in COBIT is ultimately linked to the stakeholders through a series of transforms called cascading goals. The concept is pretty simple. At any point in our IT governance or management processes, we should be able to ask the question “why are we doing this?” and be led to an IT goal that is tied to an enterprise goal, which is in turn tied to a stakeholder need. COBIT specifies 13 enterprise and 13 alignment goals that take the guesswork out of ensuring we consider all dimensions in our decision-making processes.

These two sets of 13 goals are different but related. They ensure that we are aligned with the sixth principle of covering the enterprise end to end by explicitly tying enterprise and IT goals in both the governance and management dimensions, which is the fourth principle. These goals were identified by looking for commonalities (or perhaps universal features) of a large set of organizations. The purpose of this analysis is to enable a holistic approach, which is the second key principle in COBIT.

The COBIT framework includes, but differentiates, enterprise governance and management. The difference between these two is that governance is a set of higher-level processes aimed at balancing the stakeholder value proposition, while management is the set of activities that achieve enterprise objectives. As a simplifying approximation, you can think of governance as the things that the C-suite leaders do and management as the things that the other organizational leaders do. Figure 4-5 illustrates how the

Business
Goals
Requirements

M
by
ed
m
r
rfo
Pe

Responsibility
Accountability
Chart

Key
Activities

ce Fo
r

an

rm

m

at
fo
u
er For outcome rity

Audited with

su

re
d

by

IT Goals
IT Processes

ea

to
in
wn
o
d
en
ok
Br

Information

Control
Outcome
Tests

Figure 4-5 COBIT framework

Outcome
Measures

by

Derived
from
Control

Objectives
Audited with

rp
Fo

Performance
Indicators

Co
nt
ro
lle
d

Im
ple
me
nte
d

Based on
Maturity
Models

Control
Design
Tests

wi
th

Control
Practices

TIP Many people in the security industry mistakenly assume that COBIT is purely security focused, when in reality it deals with all aspects of information technology, security being only one component. COBIT is a set of practices that can be followed to carry out IT governance, which requires proper security practices.

Enterprise Architecture Frameworks

Organizations have a choice when attempting to secure their environment as a whole.
They can just toss in products here and there, which are referred to as point solutions
or stovepipe solutions, and hope the ad hoc approach magically works in a manner that
secures the environment evenly and covers all of the organization’s vulnerabilities. Most

organizations, particularly small and medium businesses, don’t start with a secure architecture. Instead, they focus on their core business, get just enough security to survive, and adjust things as they grow. This organic growth model lends itself to short-term measures that result in a “constantly putting out fires” approach. It is usually easier and cheaper for senior management to approve money for a new security tool than to approve the time, money, and business disruption needed to re-architect an information system to properly secure it.

The second approach to securing an organization’s environment would be to define an enterprise security architecture, allow it to be the guide when implementing solutions to ensure business needs are met, provide standard protection across the environment, and reduce the number of security surprises the organization will run into. The catch is that if a company has been following the first ad hoc approach for a while, it can be very challenging (and expensive) to rebuild its infrastructure without causing pain to a lot of people. Although implementing an enterprise security architecture does not necessarily promise pure utopia, it does tame the chaos and gets the security staff and organization into a more proactive and mature mindset when dealing with security as a whole.

Developing an architecture from scratch is not an easy task. Sure, it is easy to draw a big box with smaller boxes inside of it, but what do the boxes represent? What are the relationships between the boxes? How does information flow between the boxes? Who needs to view these boxes, and what aspects of the boxes do they need for decision making?

An architecture is a conceptual construct. It is a tool to help individuals understand a complex item (such as an enterprise) in digestible chunks. An example of an architecture

PART I

five governance and 35 management objectives defined by COBIT are organized into five domains. Governance objectives all fall within the Evaluate, Direct and Monitor (EDM) domain. Management objectives, on the other hand, fall into four domains: Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), and Monitor, Evaluate and Assess (MEA).

A majority of the security compliance auditing practices used today in the industry are based off of COBIT. So if you want to make your auditors happy and pass your compliance evaluations, you should learn, practice, and implement the control

objectives
outlined in COBIT, which are considered industry best practices.

is the Open Systems Interconnection (OSI) networking model, an abstract model used to illustrate the architecture of a networking stack. A networking stack within a computer is very complex because it has so many protocols, interfaces, services, and hardware specifications. But when we think about it in a modular framework (the OSI seven layers), we can better understand the network stack as a whole and the relationships between the individual components that make it up.

NOTE The OSI network stack will be covered extensively in Chapter 11.

An enterprise architecture encompasses the essential and unifying components of an organization. It expresses the enterprise structure (form) and behavior (function). It embodies the enterprise's components, their relationships to each other, and their relationships to the environment.

This section covers several different enterprise architecture frameworks. Each framework has its own specific focus, but they all provide guidance on how to build individual architectures so that they are useful tools to a diverse set of individuals. Notice the difference between an architecture framework and an actual architecture. You use the framework as a guideline on how to build an architecture that best fits your company's needs. Each company's architecture will be different because companies have different business drivers, security and regulatory requirements, cultures, and organizational structures—but if each starts with the same architecture framework, then their architectures will have similar structures and goals. It is similar to three people starting with a ranchstyle house blueprint. One person chooses to have four bedrooms built because they have three children, one person chooses to have a larger living room and three bedrooms, and the other person chooses two bedrooms and two living rooms. Each person started with the same blueprint (framework) and modified it to meet their needs (architecture).

When developing an architecture, first the stakeholders need to be identified, the people who will be looking at and using the architecture. Next, the views need to be developed, which is how the information that is most important to the different stakeholders will be illustrated in the most useful manner. The NIST developed a framework, illustrated in Figure 4-6, that shows that companies have several different viewpoints. Executives need to understand the company from a business point of view, business process developers need to understand what type of information needs to be collected to support business activities, application developers need to understand system requirements that maintain and process the information, data modelers need to know how to structure data elements, and the technology group needs to understand the network components required to support the layers above it. They are all looking at an architecture of the same company; it is just being presented in views that they understand and that directly relate to their responsibilities within the organization.

An enterprise architecture enables you to not only understand the company from several different views, but also understand how a change that takes place at one level will affect items at other levels. For example, if there is a new business requirement, how is it going to be supported at each level of the enterprise? What type of new information must

Business
architecture
Drives

Information
architecture
Feedback
Prescribes

Enterprise
discretionary and
non-discretionary
standards/
regulations

Information systems
architecture
Identifies

Data architecture
Supported by

Delivery systems architecture
hardware, software, communications

be collected and processed? Do new applications need to be purchased or current ones modified? Are new data elements required? Will new networking devices be required? An architecture enables you to understand all the things that will need to change just to support one new business function.
The architecture can be used in the opposite direction also. If a company is looking to do a technology refresh, will the new systems still support all of the necessary functions in the layers above the technology level? An architecture enables you to understand an organization as one complete organism and identify how changes to one internal component can directly affect another one.

Why Do We Need Enterprise Architecture Frameworks?
As you have probably experienced, business people and technology people sometimes seem like totally different species. Business people use terms like “net profits,” “risk universes,” “portfolio strategy,” “hedging,” “commodities,” and so on. Technology people use terms like “deep packet inspection,” “layer three devices,” “cross-site scripting,” “load balancing,” and so forth. Think about the acronyms techies like us throw around—TCP, APT, ICMP, RAID, UDP, L2TP, PPTP, IPSec, and AES. We can have complete

External discretionary
and nondiscretionary
standard/requirements

Figure 4-6
NIST enterprise
architecture
framework

conversations between ourselves without using any real words. And even though business people and technology people use some of the same words, they have totally different meanings to the individual groups. To business people, a protocol is a set of approved processes that must be followed to accomplish a task. To technical people, a protocol is a standardized manner of communication between computers or applications. Business and technical people use the term “risk,” but each group is focusing on very different risks a company can face—market share versus security breaches. And even though each group uses the term “data” the same, business people look at data only from a functional point of view and security people look at data from a risk point of view.

This divide between business perspectives and technology perspectives not only can cause confusion and frustration—it commonly costs money. If the business side of the house wants to offer customers a new service, as in paying bills online, there may have to be extensive changes to the current network infrastructure, applications, web servers, software logic, cryptographic functions, authentication methods, database structures, and so on. What seems to be a small change in a business offering can cost a lot of money when it comes to adding up the new technology that needs to be purchased and implemented, programming that needs to be carried out, re-architecting of networks, and the like. It is common for business people to feel as though the IT department is more of an impediment when it comes to business evolution and growth, and in turn the IT department feels as though the business people are constantly coming up with outlandish and unrealistic demands with no supporting budgets.

This type of confusion between business and technology people has caused organizations around the world to implement incorrect solutions because they did not understand the business functionality to technical specifications requirements. This results in having to repurchase new solutions, carry out rework, and waste an amazing amount of time. Not only does this cost the organization more money than it should have in the first place, business opportunities may be lost, which can reduce market share. So we need a tool that both business people and technology people can use to reduce confusion, optimize business functionality, and not waste time and money. This is where business enterprise architectures come into play. They allow both groups (business and technology) to view the same organization in ways that make sense to them.

When you go to the doctor’s office, there is a poster of a skeleton system on one wall, a poster of a circulatory system on the other wall, and another poster of the organs that make up a human body. These are all different views of the same thing, the human body. This is the same functionality that enterprise architecture frameworks provide: different views of the same thing. In the medical field we have specialists (podiatrists, brain surgeons, dermatologists, oncologists, ophthalmologists, etc.). Each organization is also made up of its own specialists (HR, marketing, accounting, IT, R&D, management, etc.). But there also has to be an understanding of the entity (whether it is a human body or company) holistically, which is what an enterprise architecture attempts to accomplish.

Zachman Framework

One of the first enterprise architecture frameworks that was created is the Zachman Framework, created by John Zachman. This model is generic, and is well suited to frame the work we do in information systems security. A sample (though fairly simplified) representation is depicted in Table 4-4.

🡅Data Models

Data
Management
Data Stores
Information

Technological
(Engineers)
Implementation
(Technicians)
Enterprise

Products

Conceptual
(Business Mgrs.)
Architectural
(System
Architects)

Assets and
Liabilities

Contextual
(Executives)

Functions

Programs

Systems Designs

Systems
Architectures

Business
Processes

Business Lines

Table 4-4 Zachman Framework for Enterprise Architecture

Perspective
(Audience)

How

Networks

Network Nodes
and Links

System Interfaces

Distributed
Systems
Architectures

Logistics and
Communications

Organizations

Access Controls

Human Interfaces

Use Cases

Workflows

Partners, Clients,
and Employees

Who

Interrogatives

Business Locales

Where

Schedules

Network/ Security
Operations

Process Controls

Project Schedules

Master Calendar

Milestones and
Major Events

When

Strategies

Performance
Metrics

Process Outputs

Business Rule
Models

Business Plan

Business Strategy

Why

What

The Zachman Framework is a two-dimensional model that uses six basic communication interrogatives (What, How, Where, Who, When, and Why) intersecting with different perspectives (Executives, Business Managers, System Architects, Engineers, Technicians, and Enterprise-wide) to give a holistic understanding of the enterprise. This framework was developed in the 1980s and is based on the principles of classical business architecture that contain rules that govern an ordered set of relationships. One of these rules is that each row should describe the enterprise completely from that row’s perspective. For example, IT personnel’s jobs require them to see the organization in terms of data stores, programs, networks, access controls, operations, and metrics.

Though they are (or at least should be) aware of other perspectives and items, the performance of their duties in the example organization is focused on these items.

The goal of this framework is to be able to look at the same organization from different viewpoints. Different groups within a company need the same information, but presented in ways that directly relate to their responsibilities. A CEO needs financial statements, scorecards, and balance sheets. A network administrator needs network schematics, a systems engineer needs interface requirements, and the operations department needs configuration requirements. If you have ever carried out a network-based vulnerability test, you know that you cannot tell the CEO that some systems are vulnerable to timeof-check to time-of-use (TOC/TOU) attacks or that the company software allows for client-side browser injections. The CEO needs to know this information, but in a language she can understand. People at each level of the organization need information in a language and format that are most useful to them.

A business enterprise architecture is used to optimize often fragmented processes (both manual and automated) into an integrated environment that is responsive to change and supportive of the business strategy. The Zachman Framework has been around for many years and has been used by many organizations to build or better define their business environment. This framework is not security oriented, but it is a good template to work with because it offers direction on how to understand an actual enterprise in a modular fashion.

The Open Group Architecture Framework

Another enterprise architecture framework is The Open Group Architecture Framework (TOGAF), which has its origins in the U.S. Department of Defense. It provides an approach to design, implement, and govern an enterprise information architecture.

TOGAF is a framework that can be used to develop the following architecture types:

- Business architecture
- Data architecture
- Applications architecture
- Technology architecture

TOGAF can be used to create these individual architecture types through the use of its Architecture Development Method (ADM). This method is an iterative and cyclic process that allows requirements to be continuously reviewed and the individual architectures

NOTE Many technical people have a negative visceral reaction to models like TOGAF. They feel it's too much work, that it's a lot of fluff, is not directly relevant, and so on. If you handed the same group of people a network schematic with firewalls, IDSs, and virtual private networks (VPNs), they would say, "Now we're talking about security!" Security technology works within the construct of an organization, so the organization must be understood also.

Military-Oriented Architecture Frameworks

It is hard enough to construct enterprise-wide solutions and technologies for one organization—think about an architecture that has to span many different complex government agencies to allow for interoperability and proper hierarchical communication channels. This is where the Department of Defense Architecture Framework (DoDAF) comes into play. When the U.S. DoD purchases technology products and weapon systems, enterprise architecture documents must be created based upon DoDAF standards to illustrate how they will properly integrate into the current infrastructures. The focus of the architecture framework is on command, control, communications, computers, intelligence, surveillance, and reconnaissance systems and processes. It is not only important that these different devices communicate using the same protocol types and interoperable software components but also that they use the same data elements. If an image is captured from a spy satellite, downloaded to a centralized data repository, and then loaded into a piece of software to direct an unmanned drone, the military personnel cannot have their operations interrupted because one piece of software cannot read another software's data output. The DoDAF helps ensure that all systems, processes, and personnel work in a concerted effort to accomplish its missions.

NOTE While DoDAF was developed to support mainly military missions, it has been expanded upon and morphed for use in business enterprise environments.

to be updated as needed. These different architectures can allow a technology architect to understand the enterprise from four different views (business, data, application, and technology) so she can ensure her team develops the necessary technology to work within the environment and all the components that make up that environment and meet business requirements. The technology may need to span many different types of networks, interconnect with various software components, and work within different business units. As an analogy, when a new city is being constructed, people do not just start building houses here and there. Civil engineers lay out roads, bridges, waterways, and zones for commercial and residential development. A large organization that has a distributed and heterogeneous environment that supports many different business functions can be as complex as a city. So before a programmer starts developing code, the architecture of the software needs to be developed in the context of the organization it will work within.

When attempting to figure out which architecture framework is best for your organization, you need to find out who the stakeholders are and what information they need from the architecture. The architecture needs to represent the company in the most useful manner to the people who need to understand it the best. If your company has people (stakeholders) who need to understand the company from a business process perspective, your architecture needs to provide that type of view. If there are people who need to understand the company from an application perspective, your architecture needs a view that illustrates that information. If people need to understand the enterprise from a security point of view, that needs to be illustrated in a specific view.

So one main difference between the various enterprise architecture frameworks is what type of information they provide and how they provide it.

Other Frameworks

Along with ensuring that we have the proper controls in place, we also want to have ways to construct and improve our business, IT, and security processes in a structured and controlled manner. The security controls can be considered the “things,” and processes are how we use these things. We want to use them properly, effectively, and efficiently.

ITIL

ITIL (formerly the Information Technology Infrastructure Library) was developed in the 1980s by the UK’s Central Computer and Telecommunications Agency (which was subsumed in the late 1990s by the now defunct Office of Government Commerce). ITIL is now controlled by AXELOS, which is a joint venture between the government of the UK and the private firm Capita. ITIL is the de facto standard of best practices for IT service management. ITIL was created because of the increased dependence on information technology to meet business needs. Unfortunately, as previously discussed, a natural divide exists between business people and IT people in most organizations because they use different terminology and have different focuses within the organization. The lack of a common language and understanding of each other’s domain (business versus IT) has caused many companies to ineffectively blend their business objectives and IT functions.

This improper blending usually generates confusion, miscommunication, missed deadlines, missed opportunities, increased cost in time and labor, and frustration on both the business and technical sides of the house.

ITIL blends all parts of an organization using a four-dimensional model built around the concept of value for the stakeholders. The dimensions in this model, illustrated in Figure 4-7, are organizations and people, value streams and processes, information and technology, and partners and suppliers. These exist in a broader context that is influenced by factors that can be political, economic, social, technological, legal, or environmental. Effective organizations must consider all four dimensions within their broader context when planning, developing, and offering products and/or services if they are to provide value.

Economical

Political
Organizations
and people

Information
and technology
du
Pro cts

Environmental

Social

Value

Partners

and suppliers
Legal

d s e r vice

s

an

Value streams
and processes
Technological

Six Sigma

Six Sigma is a process improvement methodology. Its goal is to improve process quality by using statistical methods of measuring operation efficiency and reducing variation, defects, and waste. Six Sigma is being used in the security assurance industry in some instances to measure the success factors of different controls and procedures. Six Sigma was developed by Motorola with the goal of identifying and removing defects in its manufacturing processes. The maturity of a process is described by a sigma rating, which indicates the percentage of defects that the process contains. While it started in manufacturing, Six Sigma has been applied to many types of business functions, including information security and assurance.

Capability Maturity Model

While we know that we constantly need to make our security program better, it is not always easy to accomplish because “better” is a vague and nonquantifiable concept. The only way we can really improve is to know where we are starting from, where we need to go, and the steps we need to take in between. Every security program has a maturity level, which could range from nonexistent to highly optimized. In between these two extremes, there are different levels. An example of a Capability Maturity Model (CMM) is illustrated in Figure 4-8. Each maturity level within this model represents an evolutionary stage. Some security programs are chaotic, ad hoc, unpredictable, and usually insecure. Some security programs have documentation created, but the actual processes are not taking place. Some security programs are quite evolved, streamlined, efficient, and effective.

EXAM TIP The CISSP exam puts more emphasis on CMM compared to ITIL and Six Sigma because it is more heavily used in the security industry.

Figure 4-7
ITIL

Figure 4-8 Capability Maturity Model for a security program

Security Program Development

No organization is going to put all the previously listed items (NIST RMF, OCTAVE, FAIR, ISO/IEC 27000, NIST CSF, NIST SP 800-53, CIS Controls, COBIT 2019, Zachman Framework, ITIL, Six Sigma, CMM) into place. But it is a good toolbox of things you can pull from, and you will find some fit the organization you work in better than others. You will also find that as your organization's security program matures, you will see more clearly where these various standards, frameworks, and management components come into play. While these items are separate and distinct, there are basic things that need to be built in for any security program and its corresponding controls. This is because the basic tenets of security are universal no matter if they are being deployed in a corporation, government agency, business, school, or nonprofit organization. Each entity is made up of people, processes, data, and technology, and each of these things needs to be protected.

A security program should use a top-down approach, meaning that the initiation, support, and direction come from top management; work their way through middle management; and then reach staff members. In contrast, a bottom-up approach refers to a situation in which staff members (usually IT) try to develop a security program without getting proper management support and direction. A bottomup approach is commonly less effective, not broad enough to address all security risks, and doomed to fail. A top-down approach makes sure the people actually responsible for protecting the company's assets (senior management) are driving the program. Senior management are not only ultimately responsible for the protection of the organization but also hold the purse strings for the necessary funding, have the authority to assign needed resources, and are the only ones who can ensure true enforcement of the stated security rules and policies. Management's support is one of the most important pieces of a security program. A simple nod and a wink will not provide the amount of support required.

The crux of CMM is to develop structured steps that can be followed so an organization can evolve from one level to the next and constantly improve its processes and security posture. A security program contains a lot of elements, and it is not fair to expect every part to be properly implemented within the first year of its existence. And some components, as in forensics capabilities, really cannot be put into place until some rudimentary pieces are established, as in incident management. So if we really want our baby to be able to run, we have to lay out ways that it can first learn to walk.

Putting It All Together

While the cores of these various security standards and frameworks are similar, it is important to understand that a security program has a life cycle that is always continuing, because it should be constantly evaluated and improved upon. The life cycle of any process can be described in different ways. We will use the following steps:

1. Plan and organize
2. Implement
3. Operate and maintain
4. Monitor and evaluate

Without setting up a life-cycle approach to a security program and the security management that maintains the program, an organization is doomed to treat security as merely another project. Anything treated as a project has a start and stop date, and at the stop date everyone disperses to other projects. Many organizations have had good intentions in their security program kickoffs, but do not implement the proper structure to ensure that security management is an ongoing and continually improving process.

PART I

Top-Down Approach

The result is a lot of starts and stops over the years and repetitive work that costs more than it should, with diminishing results.

The main components of each phase are provided here.

Plan and Organize:

- Establish management commitment.
- Establish oversight steering committee.

- Assess business drivers.
- Develop a threat profile on the organization.
- Carry out a risk assessment.
- Develop security architectures at business, data, application, and infrastructure levels.
- Identify solutions per architecture level.
- Obtain management approval to move forward.

Implement:

- Assign roles and responsibilities.
- Develop and implement security policies, procedures, standards, baselines, and guidelines.
- Identify sensitive data at rest and in transit.
- Implement the following blueprints:
- Asset identification and management
- Risk management
- Vulnerability management
- Compliance
- Identity management and access control
- Change control
- Software development life cycle
- Business continuity planning
- Awareness and training
- Physical security
- Incident response
- Implement solutions (administrative, technical, physical) per blueprint.
- Develop auditing and monitoring solutions per blueprint.
- Establish goals, SLAs, and metrics per blueprint.

Operate and Maintain:

Monitor and Evaluate:

- Review logs, audit results, collected metric values, and SLAs per blueprint.
- Assess goal accomplishments per blueprint.
- Carry out quarterly meetings with steering committees.
- Develop improvement steps and integrate into the Plan and Organize phase.

Many of the items mentioned in the previous list are covered throughout this book. This list is provided to show how all of these items can be rolled out in a sequential and controllable manner. Although the previously covered standards and frameworks are very helpful, they are also very high level. For example, if a standard simply states that an organization must secure its data, a great amount of work will be called for. This is where the security professional really rolls up her sleeves, by developing security blueprints. Blueprints are important tools to identify, develop, and design security requirements for specific business needs. These blueprints must be customized to fulfill the organization’s security requirements, which are based on its regulatory obligations, business drivers, and legal obligations. For example, let’s say Company Y has a data protection policy, and its security team has developed standards and procedures pertaining to the data protection strategy the company should follow. The blueprint will then get more granular and lay out the processes and components necessary to meet requirements outlined in the policy, standards, and requirements. This would include at least a diagram of the company network that illustrates the following:

- Where the sensitive data resides within the network
- The network segments that the sensitive data transverses
- The different security solutions in place (VPN, TLS, PGP) that protect the sensitive data
- Third-party connections where sensitive data is shared
- Security measures in place for third-party connections
- And more…

The blueprints to be developed and followed depend upon the organization’s business needs. If Company Y uses identity management, it needs a blueprint outlining roles, registration management, authoritative source, identity repositories, single sign-on solutions, and so on. If Company Y does not use identity management, it does not need to build a blueprint for this.

- Follow procedures to ensure all baselines are met in each implemented blueprint.
- Carry out internal and external audits.
- Carry out tasks outlined per blueprint.
- Manage SLAs per blueprint.

So the blueprint lays out the security solutions, processes, and components the organization uses to match its security and business needs. These blueprints must be applied to the different business units within the organization. For example, the identity management practiced in each of the different departments should follow the crafted blueprint. Following these blueprints throughout the organization allows for

standardization, easier metrics gathering, and governance. Figure 4-9
illustrates where
these blueprints come into play when developing a security program.
SECURITY EFFECTIVENESS

STRATEGIC ALIGNMENT

PERFORMANCE DASHBOARD

Privacy Blueprint
Identity Management Blueprint
Application Integrity Blueprint

Logging, Monitoring, and Reporting
Industry
and
Business
Standards

ISO/IEC
17799

TAILORED
BEST
PRACTICES

Systems and Network Infrastructure
Physical and Environmental
Information and Asset Baseline
Infrastructure Blueprint
Business Continuity Blueprint
Management Blueprint
SECURITY FOUNDATION

Figure 4-9 Blueprints must map the security and business requirements.

Compliance

Incident Response

Help Desk

Architecture Standards

Systems Development
Life Cycle

Specialized Architecture

Facilities

Applications

Internal Network

Security Strategy
and
Policy

Perimeter Network

Desired Risk Profile

Production Readiness

PROCESS ENHANCEMENT

BUSINESS ENABLEMENT
Legal/Regulatory
Requirements

Change Control

IT
Strategies

Project Management

Strategic
Business
Drivers

Chapter Review

This chapter should serve at least two purposes for you. First, it familiarizes you with the various frameworks you need to know to pass your CISSP exam. Though some of these frameworks don’t fit neatly into one category, we did our best to group them in ways that would help you remember them. So, we have risk management, information security, enterprise architecture, and “other” frameworks. Within information security, we further subdivided the frameworks into those that are focused on program-level issues and those that are primarily concerned with controls. You don’t have to know every detail of each framework to pass the exam, but you really should know at least one or two key points about each to differentiate them.

The second purpose of this chapter is to serve as a reference for your professional life. We focused our discussion on the frameworks that are most likely to show up in your work places so that you have a desktop reference to which you can turn when someone asks your opinion about one of these frameworks. While this second purpose of the chapter should apply to the whole book, it is particularly applicable to this chapter because frameworks are tools that don’t change very often (especially within an organization), so you may become very familiar with the one(s) you use but a bit rusty on the rest. Grouping them all in this chapter may help you in the future.

Quick Review

- A framework is a guiding document that provides structure to the ways in which we manage risks, develop enterprise architectures, and secure all our assets.
- The most common risk management frameworks (RMFs) are the NIST RMF, ISO/IEC 27005, OCTAVE, and FAIR.

To tie these pieces together, you can think of the NIST Cybersecurity Framework that works mainly at the policy level as a description of the type of house you want to build (ranch style, five bedrooms, three baths). The security enterprise framework is the architecture layout of the house (foundation, walls, ceilings). The blueprints are the detailed descriptions of specific components of the house (window types, security system, electrical system, plumbing). And the control objectives are the building specifications and codes that need to be met for safety (electrical grounding and wiring, construction material, insulation, and fire protection). A building inspector will use his checklists (building codes) to ensure that you are building your house safely. Which is just like how an auditor will use his checklists (like NIST SP 800-53) to ensure that you are building and maintaining your security program securely.

Once your house is built and your family moves in, you set up schedules and processes for everyday life to happen in a predictable and efficient manner (dad picks up kids from school, mom cooks dinner, teenager does laundry, dad pays the bills, everyone does yard work). This is analogous to ITIL—process management and improvement. If the family is made up of anal overachievers with the goal of optimizing these daily activities to be as efficient as possible, they could integrate a Six Sigma approach where continual process improvement is a focus.

- The seven steps of the NIST RMF are prepare, categorize, select, implement, assess, authorize, and monitor.
- Security controls in the NIST frameworks can be classified as common (if they exist outside of a system and apply to multiple systems), system-specific (if they exist inside a system boundary and protect only the one system), or hybrid (if they are a combination of the other two).
- Risks in a risk management framework can be treated in one of four ways: mitigated, accepted, transferred, or avoided.
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a team-oriented risk management methodology that employs workshops and is commonly used in the commercial sector.
- The Factor Analysis of Information Risk (FAIR) risk management framework is the only internationally recognized quantitative approach to risk management.
- The most common information security program frameworks are ISO/IEC 27001 and the NIST Cybersecurity Framework.
- ISO/IEC 27001 is the standard for the establishment, implementation, control, and improvement of the information security management system.
- The NIST Cybersecurity Framework's official name is the "Framework for Improving Critical Infrastructure Cybersecurity."
- The NIST Cybersecurity Framework organizes cybersecurity activities into five higher-level functions: identify, protect, detect, respond, and recover.
- The most common security controls frameworks are NIST SP 800-53, the CIS Controls, and COBIT.
- NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, catalogs over 1,000 security controls grouped into 20 families.
- The Center for Internet Security (CIS) Controls is a framework consisting of 20 controls and 171 subcontrols organized in implementation groups to address any organization's security needs from small to enterprise level.
- COBIT is a framework of control objectives and allows for IT governance.
- Enterprise architecture frameworks are used to develop architectures for specific stakeholders and present information in views.
- Blueprints are functional definitions for the integration of technology into business processes.
- Enterprise architecture frameworks are used to build individual architectures that best map to individual organizational needs and business drivers.
- The most common enterprise architecture frameworks are the Zachman and SABSA ones, but you should also be aware of TOGAF and DoDAF.
- Zachman Framework is an enterprise architecture framework, and SABSA is a security enterprise architecture framework.

Questions

Please remember that these questions are formatted and asked in a certain way for a reason. Keep in mind that the CISSP exam is asking questions at a conceptual level. Questions may not always have the perfect answer, and the candidate is advised against always looking for the perfect answer. Instead, the candidate should look for the best answer in the list.

1. Which of the following standards would be most useful to you in ensuring your information security management system follows industry best practices?
A. NIST SP 800-53
B. Six Sigma
C. ISO/IEC 27000 series
D. COBIT

2. What is COBIT and where does it fit into the development of information security systems and security programs?
A. Lists of standards, procedures, and policies for security program development
B. Current version of ISO 17799
C. A framework that was developed to deter organizational internal fraud
D. Open standard for control objectives

3. Which publication provides a catalog of security controls for information systems?
A. ISO/IEC 27001
B. ISO/IEC 27005
C. NIST SP 800-37
D. NIST SP 800-53

4. ISO/IEC 27001 describes which of the following?
A. The Risk Management Framework
B. Information security management system
C. Work product retention standards
D. International Electrotechnical Commission standards

- ITIL is a set of best practices for IT service management.
- Six Sigma is used to identify defects in processes so that the processes can be improved upon.
- A Capability Maturity Model (CMM) allows for processes to improve in an incremented and standard approach.

5. Which of the following is not true about Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)?
A. It is the only internationally recognized quantitative risk management framework.
B. It was developed by Carnegie Mellon University.
C. It is focused only on risk assessments.
D. It is a team-oriented risk management methodology that employs workshops.

6. What is a key benefit of using the Zachman Framework?
A. Ensures that all systems, processes, and personnel are interoperable in a

concerted effort to accomplish organizational missions

B. Use of the iterative and cyclic Architecture Development Method (ADM)

C. Focus on internal SLAs between the IT department and the “customers” it serves

D. Allows different groups within the organization to look at it from different viewpoints

7. Which of the following describes the Center for Internet Security (CIS) Controls framework?

A. Consists of over 1,000 controls, divided into 20 families, that are mapped to the security category of an information system

B. Balances resource utilization, risk levels, and realization of benefits by explicitly tying stakeholder needs to organizational goals to IT goals

C. Developed to determine the maturity of an organization’s processes

D. Consists of 20 controls divided into three groups to help organizations incrementally improve their security posture

8. Which of the following is not one of the seven steps in the NIST Risk Management Framework (RMF)?

A. Monitor security controls

B. Establish the context

C. Assess security controls

D. Authorize information system

9. The information security industry is made up of various best practices, standards, models, and frameworks. Some were not developed first with security in mind, but can be integrated into an organizational security program to help in its effectiveness and efficiency. It is important to know of all of these different approaches so that an organization can choose the ones that best fit its business needs and culture. Which of the following best describes the approach(es) that should be put into place if an organization wants to integrate a way to improve its security processes over a period of time?

i. ITIL should be integrated because it allows for the mapping of IT service process management, business drivers, and security improvement.

iii. A Capability Maturity Model should be integrated because it provides distinct maturity levels.

iv. The Open Group Architecture Framework should be integrated because it provides a structure for process improvement.

A. i, iii

B. ii, iii, iv

C. ii, iii

D. ii, iv

Use the following scenario to answer Questions 10–12. You are hired as the chief information security officer (CISO) for a medium-size research and development company. Its research file servers were recently breached, resulting in a significant loss of intellectual property. The company is about to start a critical research project and wants to ensure another breach doesn’t happen. The company doesn’t have risk management or information security programs, and you’ve been given a modest budget to hire a small team and get things started.

10. Which of the following risk management frameworks would probably not be well suited to your organization?

A. ISO/IEC 27005
B. NIST Risk Management Framework (RMF)
C. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
D. Factor Analysis of Information Risk (FAIR)

11. You decide to adopt the NIST Risk Management Framework (RMF) and are in the process of categorizing your information systems. How would you determine the security category (SC) of your research file servers (RFS)?

A. SCRFS = (probable frequency) × (probable future loss)
B. SCRFS = {(confidentiality, high),(integrity, medium),(availability, low)} = high
C. SCRFS = {(confidentiality, high),(integrity, medium),(availability, low)} = medium
D. SCRFS = Threat × Impact × Probability

12. When selecting the controls for the research file servers, which of the following security control frameworks would be best?

A. NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations
B. ISO/IEC 27002 code of practice for information security controls
C. Center for Information Security (CIS) Controls
D. COBIT 2019

ii. Six Sigma should be integrated because it allows for the defects of security processes to be identified and improved upon.

Answers

1. C. The ISO/IEC 27000 series is the only option that addresses best practices across the breadth of an ISMS. NIST SP 800-53 and COBIT both deal with controls, which are a critical but not the only component of an ISMS.

2. D. COBIT is an open framework developed by ISACA and the IT Governance Institute (ITGI). It defines goals for the controls that should be used to properly manage IT and ensure IT maps to business needs.

3. D. NIST Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations, catalogs over 1,000 security controls.

ISO/IEC 27005 and NIST SP 800-37 both describe risk management frameworks, while ISO/IEC 27001 is focused on information security management systems (ISMSs).

4. B. ISO/IEC 27001 provides best practice recommendations on information security management systems (ISMSs).

5. A. OCTAVE is not a quantitative methodology. The only such methodology for risk management we’ve discussed is FAIR.

6. D. One of the key benefits of the Zachman Framework is that it allows organizations to integrate business and IT infrastructure requirements in a manner that is presentable to a variety of audiences by providing different viewpoints. This helps keep business and IT on the same sheet of music. The other answers describe the DoDAF (A), TOGAF (B), and ITIL (C).

7. D. There are 20 CIS controls and 171 subcontrols organized so that any organization, regardless of size, can focus on the most critical controls and improve over time as resources become available. The other answers describe NIST SP 800-53 (A), COBIT 2019 (B), and Capability Maturity Model (C).

8. B. Establishing the context is a step in ISO/IEC 27005, not in the NIST RMF. While it is similar to the RMF’s prepare step, there are differences between the two. All the other responses are clearly steps in the NIST RMF process.

9. C. The best process improvement approaches provided in this list are Six Sigma and Capability Maturity Model. The following outlines the definitions for all items in this question:

- TOGAF Model and methodology for the development of enterprise architectures, developed by The Open Group
- ITIL Processes to allow for IT service management, developed by the United Kingdom’s Office of Government Commerce
- Six Sigma Business management strategy that can be used to carry out process improvement
- Capability Maturity Model (CMM) Organizational development for process improvement

11. B. The NIST RMF relies on the Federal Information Processing Standard Publication 199 (FIPS 199) categorization standard, which breaks down a system’s criticality by security objective (confidentiality, integrity, availability) and then applies the highest security objective category (the “high water mark”) to determine the overall category of the system.

12. A. Because you’re using the NIST RMF, NIST SP 800-53 is the best answer because the two frameworks are tightly integrated. None of the other answers is necessarily wrong; they’re just not as well suited as SP 800-53 for the given scenario.

10. D. The Factor Analysis of Information Risk (FAIR) framework uses a quantitative approach to risk assessment. As we discussed in Chapter 2, this approach requires

a lot more expertise and resources than quantitative ones. Since your organization is just getting started with risk management and information security and your resources are limited, this would not be a good fit.

⮝This page intentionally left blank

⮝PART II

Asset Security
Chapter 5
Chapter 6

Assets
Data Security

⮝This page intentionally left blank

⮝CHAPTER

Assets

This chapter presents the following:

- Identification and classification of information and assets
- Information and asset handling requirements
- Secure resource provisioning
- The data life cycle
- Data compliance requirements

You don’t know what you’ve got till it’s gone.
—Joni Mitchell

An asset is, by definition, anything of worth to an organization. This includes people, partners, equipment, facilities, reputation, and information. We already touched on the importance of some of these assets when we addressed risk in Chapter 2. While every asset needs to be protected, our coverage of the second CISSP domain in this chapter and the next one focuses a bit more narrowly on protecting information assets. This is because, apart from people, information is typically the most valuable asset to an organization. It lies at the heart of every information system, so precision focus on its protection makes a lot of sense.

Information, of course, exists in context; it is acquired or created at a particular point in time through a specific process and (usually) for a purpose. It moves through an organization’s information systems, sometimes adding value to processes and sometimes waiting to be useful. Eventually, the information outlives its utility (or becomes a liability) and must be disposed of appropriately. We start off our discussion of asset security by addressing two fundamental questions: “What do we have?” and “Why should we care?”

The first question is probably rather obvious, since we cannot protect that of which we’re not aware. The second question may sound flippant, but it really gets to the heart of how important an asset is to the organization. We’ve already tackled this (at least with regard to data) in Chapter 4 in our discussion of the categorize step of the NIST Risk Management Framework. Data and asset classification, as we will shortly see, is very similar to the categorization we’ve already explored. Let’s get to it!

EXAM TIP An information asset can be either the data, the device on which it is stored and used, or both. In the exam, when you see the term asset by itself, it typically means only the device.

Information and Assets

An asset can be defined as anything that is useful or valuable. In the context of products and services, this value is usually considered financially: how much would someone pay for it minus how much does the thing cost. If that value is positive, we call the thing an asset. However, if that value is negative (that is, the thing costs more than what someone would pay for it), then we call the thing a liability. Clearly, assets can be both tangible things like computers and firewalls and intangible things like data or reputation. It is important to narrow down the definition for purposes of the CISSP exam, so in this domain, we consider assets as tangible things and we deal with data separately.

Information is a set of data items, placed in a context, and having some meaning. Data is just an item. It could be the word “yes,” the time “9:00,” or the name “Fernando’s Café” and, by itself, has no meaning. Put this data together in the context of an answer to the question “Would you like to have coffee tomorrow morning?” and now we have information. Namely, that we’ll be sharing a beverage tomorrow morning at a particular place. Data processing yields information, and this is why we often use these two terms interchangeably when talking about security issues.

Identification

Whether we are concerned with data security or asset security (or both), we first have to know what we have. Identification is simply establishing what something is. When you look at a computing device occupying a slot in your server rack, you may want to know what it is. You may want to identify it. The most common way of doing this is by placing tags on our assets and data. These tags can be physical (e.g., stickers), electronic (e.g., radio frequency identification [RFID] tags), or logical (e.g., software license keys).

Using tags is critically important to establishing and maintaining accurate inventories of our assets.

But what about data? Do we need to identify it and track it like we do with our more tangible assets? The answer is: it depends. Most organizations have at least some data that is so critical that, were it to become lost or corrupted or even made public, the impact would be severe. Think of financial records at a bank, or patient data at a healthcare provider. These organizations would have a very bad day indeed if any of those records were lost, inaccurate, or posted on the dark web. To prevent this, they go to great lengths to identify and track their sensitive information, usually by using metadata embedded in files or records.

While it may not be critical (or even feasible) for many organizations to identify all their information, it is critical to most of us to at least decide how much effort should be put into protecting different types of data (or assets, for that matter). This is where classification comes in handy.

⮝Chapter 5: Assets

Classification

Data Classification

An important metadata item that should be attached to all our information is a classification level. This classification tag, which remains attached (and perhaps updated) throughout the life cycle of the data, is important to determining the protective controls we apply to the data.

Information can be classified by sensitivity, criticality, or both. Either way, the classification aims to quantify how much loss an organization would likely suffer if the information was lost. The sensitivity of information is commensurate with the losses to an organization if that information was revealed to unauthorized individuals. This kind of compromise has made headlines in recent years with the losses of information suffered by organizations such as Equifax, Sina Weibo, and Marriott International. In each case, the organizations lost trust and had to undertake expensive responses because sensitive data was compromised.

The criticality of information, on the other hand, is an indicator of how the loss of the information would impact the fundamental business processes of the organization. In other words, critical information is that which is essential for the organization to continue operations. For example, Code Spaces, a company that provided code repository services, was forced to shut down in 2014 after an unidentified individual or group deleted its code repositories. This data was critical to the operations of the company and, without it, the corporation had no choice but to go out of business.

Once data is segmented according to its sensitivity or criticality level, the organization can decide what security controls are necessary to protect different types of data. This ensures that information assets receive the appropriate level of protection, and classifications indicate the priority of that security protection. The primary purpose of data classification is to indicate the level of confidentiality, integrity, and availability protection that is required for each type of data set. Many people mistakenly only consider the confidentiality aspects of data protection, but we need to make sure our data is not modified in an unauthorized manner and that it is available when needed.

Data classification helps ensure that data is protected in the most cost-effective manner.

Protecting and maintaining data costs money, but spending money for the information that actually requires protection is important. If you were in charge of making sure Russia does not know the encryption algorithms used when transmitting information to and

Classification just means saying that something belongs to a certain class. We could say, for example, that your personnel file belongs to the class named “private” and that your organization’s marketing brochure for the latest appliance belongs to the class “public.” Right away, we would have a sense that your file has more value to your organization than the brochure. The rationale behind assigning values to different assets and data is that this enables an organization to gauge the amount of funds and resources that should go toward protecting each class, because not all assets and data have the same value to an organization. After identifying all important data, it should be properly classified. An organization copies and creates a lot of data that it must maintain, so classification is an ongoing process and not a one-time effort.

from U.S. spy satellites, you would use more extreme (and expensive) security measures than you would use to protect your peanut butter and banana sandwich recipe from your next-door neighbor.

Each classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed. For example, in a corporation, confidential information may be accessed only by senior management and a select few trusted employees throughout the company. Accessing the information may require two or more people to enter their access codes. Auditing could be very detailed and its results monitored daily, and paper copies of the information may be kept in a vault. To properly erase this data from the media, degaussing or overwriting procedures may be required.

Other information in this company may be classified as sensitive, allowing a slightly larger group of people to view it. Access control on the information classified as sensitive may require only one set of credentials. Auditing happens but is only reviewed weekly, paper copies are kept in locked file cabinets, and the data can be deleted using regular measures when it is time to do so. Then, the rest of the information is marked public. All employees can access it, and no special auditing or destruction methods are required.

EXAM TIP Each classification level should have its own handling and destruction requirements.

Classification Levels There are no hard and fast rules on the classification levels that
an organization should use. Table 5-1 explains the types of classifications available. An
organization could choose to use any of the classification levels presented in Table 5-1.
One organization may choose to use only two layers of classifications, while another
organization may choose to use four. Note that some classifications are more commonly
used for commercial businesses, whereas others are military classifications.
The following are the common levels of sensitivity from the highest to the lowest for
commercial business:

- Confidential
- Private
- Sensitive
- Public

And here are the levels of sensitivity from the highest to the lowest for military
purposes:

- Top secret
- Secret
- Confidential
- Controlled unclassified information
- Unclassified

Definition

Example

Public

- Disclosure is not welcome,

- How many people are

but it would not cause an
adverse impact to company
or personnel.

working on a specific
project
- Upcoming projects

- Requires special precautions

- Financial information
- Details of projects
- Profit earnings and

Sensitive

to ensure the integrity
and confidentiality of the
data by protecting it from
unauthorized modification
or deletion.
- Requires higher-thannormal assurance of
accuracy and completeness.

Private

- Personal information for use within a company.
- Unauthorized disclosure could adversely affect personnel or the company.

Confidential

- For use within the company only.
- Data exempt from disclosure under the Freedom of Information Act or other laws and regulations.
- Unauthorized disclosure could seriously affect a company.

Unclassified

- Data is not sensitive or classified.

Controlled
unclassified
information
(CUI)

- Sensitive, but not secret.
- Information that cannot

Secret

- If disclosed, it could cause

Commercial
business

Commercial

business

forecasts

- Work history
- Human resources

Commercial
business

information

- Medical information
-
-
-
-

Trade secrets
Healthcare information
Programming code
Information that
keeps the company
competitive

- Computer manual and

Commercial
business
Military

Military

warranty information
- Recruiting information

- Health records
- Answers to test scores

Military

- Deployment plans for

Military

legally be made public.

serious damage to national
security.
Top secret

Organizations That
Would Use This

troops
- Unit readiness
information

- If disclosed, it could cause

- Blueprints of new

grave damage to national
security.

weapons
- Spy satellite
information
- Espionage data

Table 5-1 Commercial Business and Military Data Classifications

Military

Classification

The classifications listed in Table 5-1 are commonly used in the industry, but there is a lot of variance. An organization first must decide the number of data classifications that best fit its security needs, then choose the classification naming scheme, and then define what the names in those schemes represent. Company A might use the classification level “confidential,” which represents its most sensitive information. Company B might use “top secret,” “secret,” and “confidential,” where confidential represents its least sensitive information. Each organization must develop an information classification scheme that best fits its business and security needs.

EXAM TIP The terms “unclassified,” “secret,” and “top secret” are usually associated with governmental organizations. The terms “private,” “proprietary,” and “sensitive” are usually associated with nongovernmental organizations.

It is important to not go overboard and come up with a long list of classifications, which will only cause confusion and frustration for the individuals who will use the system. The classifications should not be too restrictive either, because many types of data may need to be classified. As with every other issue in security, we must balance our

business and security needs.
Each classification should be unique and separate from the others and not have any overlapping effects. The classification process should also outline how information is controlled and handled through its life cycle (from creation to termination).
NOTE An organization must make sure that whoever is backing up classified data—and whoever has access to backed-up data—has the necessary clearance level. A large security risk can be introduced if low-level technicians with no security clearance have access to this information during their tasks.

Once the scheme is decided upon, the organization must develop the criteria it will use to decide what information goes into which classification. The following list shows some criteria parameters an organization may use to determine the sensitivity of data:

- The usefulness of data
- The value of data
- The age of data
- The level of damage that could be caused if the data were disclosed
- The level of damage that could be caused if the data were modified or corrupted
- Legal, regulatory, or contractual responsibility to protect the data
- Effects the data has on security
- Who should be able to access the data
- Who should maintain the data
- Who should be able to reproduce the data
- Lost opportunity costs that could be incurred if the data were not available or were corrupted

Applications and sometimes whole systems may need to be classified. The applications that hold and process classified information should be evaluated for the level of protection they provide. You do not want a program filled with security vulnerabilities to process and “protect” your most sensitive information. The application classifications should be based on the assurance (confidence level) the organization has in the software and the type of information it can store and process.

Asset Classification

Information is not the only thing we should classify. Consider that information must reside somewhere. If a confidential file is stored and processed in the CEO’s laptop, then that device (and its hard drive if it is removed) should also be considered worthy of more protection. Typically, the classification of an asset (like a removable drive or a laptop) used to store or process information should be as high as the classification of the most valuable data in it. If an asset has public, sensitive, and confidential information, then that asset should be classified as private (the highest of the three classifications) and protected accordingly.

Classification Procedures

The following outlines the necessary steps for a proper classification program:

1. Define classification levels.
2. Specify the criteria that will determine how data is classified.
3. Identify data owners who will be responsible for classifying data.
4. Identify the data custodian who will be responsible for maintaining data and its security level.
5. Indicate the security controls, or protection mechanisms, required for each classification level.
6. Document any exceptions to the previous classification issues.
7. Indicate the methods that can be used to transfer custody of the information to a different data owner.
8. Create a procedure to periodically review the classification and ownership. Communicate any changes to the data custodian.
9. Indicate procedures for declassifying the data.
10. Integrate these issues into the security awareness program so all employees understand how to handle data at different classification levels.

CAUTION The classification rules must apply to data no matter what format it is in: digital, paper, video, fax, audio, and so on.

Physical Security Considerations

We discuss data security in detail in Chapter 10. However, that data lives physically in devices and printed documents, both of which require protection also. The main threats that physical security components combat are theft, interruptions to services, physical damage, compromised system and environment integrity, and unauthorized access. Real loss is determined by the cost to replace the stolen items, the negative effect on productivity, the negative effect on reputation and customer confidence, fees for consultants that may need to be brought in, and the cost to restore lost data and production levels.

Many times, organizations just perform an inventory of their hardware and provide value estimates that are plugged into risk analysis to determine what the cost to the organization would be if the equipment were stolen or destroyed. However, the data held within the equipment may be much more valuable than the equipment itself, and proper recovery mechanisms and procedures also need to be plugged into the risk assessment for a more realistic and fair assessment of cost. Let’s take a look at some of the controls we can use in order to mitigate risks to our data and to the media on which it resides.

Protecting Mobile Devices

Mobile devices are almost indispensable. For most of us, significant chunks of our personal and work lives are chronicled in our smartphones or tablets. Employees who use these devices as they travel for work may have extremely sensitive company or customer data on their systems that can easily fall into the wrong hands. This problem can be mitigated to a point by ensuring our employees use company devices for their work, so we can implement policies and controls to protect them. Still, many organizations allow their staff members to bring their own devices (BYOD) to the workplace and/or use them for work functions. In these cases, it is not only security but also privacy that should receive serious attention.

There is no one-size-fits-all solution to protecting company, let alone personal, mobile devices. Still, the following list provides some of the mechanisms that can be used to protect these devices and the data they hold:

- Inventory all mobile devices, including serial numbers, so they can be properly identified if they are stolen and then recovered.
- Harden the operating system by applying baseline secure configurations.
- Stay current with the latest security updates and patches.
- Ensure mobile devices have strong authentication.
- Register all devices with their respective vendors, and file a report with the vendor when a device is stolen. If a stolen device is sent in for repairs after it is stolen, it will be flagged by the vendor if you have reported the theft.
- Do not check mobile devices as luggage when flying. Always carry them on with you.
- Never leave a mobile device unattended, and carry it in a nondescript carrying case.

- Engrave the device with a symbol or number for proper identification.
- Back up all data on mobile devices to an organizationally controlled

repository.

- Encrypt all data on a mobile device.
- Enable remote wiping of data on the device.

Paper Records

It is easy to forget that many organizations still process information on paper records. The fact that this is relatively rare compared to the volume of their electronic counterparts is little consolation when a printed e-mail with sensitive information finds its way into the wrong hands and potentially causes just as much damage. Here are some principles to consider when protecting paper records:

- Educate your staff on proper handling of paper records.
- Minimize the use of paper records.
- Ensure workspaces are kept tidy so it is easy to tell when sensitive papers are left exposed, and routinely audit workspaces to ensure sensitive documents are not exposed.
- Lock away all sensitive paperwork as soon as you are done with it.
- Prohibit taking sensitive paperwork home.
- Label all paperwork with its classification level. Ideally, also include its owner’s name and disposition (e.g., retention) instructions.
- Conduct random searches of employees’ bags as they leave the office to ensure sensitive materials are not being taken home.
- Destroy unneeded sensitive papers using a crosscut shredder, or consider contracting a document destruction company.

Safes

An organization may have need for a safe. Safes are commonly used to store backup data tapes, original contracts, or other types of valuables. The safe should be penetration resistant and provide fire protection. The types of safes an organization can choose from are

- Wall safe Embedded into the wall and easily hidden
- Floor safe Embedded into the floor and easily hidden

PART II

Tracing software can be installed so that your device can “phone home” if it is taken from you. Several products offer this tracing capability. Once installed and configured, the software periodically sends in a signal to a tracking center or allows you to track it through a website or application. If you report that your device has been stolen, the vendor of this software may work with service providers and law enforcement to track down and return your device.

- Chests Stand-alone safes
- Depositories Safes with slots, which allow the valuables to be easily slipped in
- Vaults Safes that are large enough to provide walk-in access

If a safe has a combination lock, it should be changed periodically, and only a small subset of people should have access to the combination or key. The safe should be in a visible location, so anyone who is interacting with the safe can be seen. It should also be covered by a video surveillance system that records any activity around it. The goal is to uncover any unauthorized access attempts. Some safes have passive or thermal relocking functionality. If the safe has a passive relocking function, it can detect when someone attempts to tamper with it, in which case extra internal bolts will fall into place to ensure it cannot be compromised. If a safe has a thermal relocking function, when a certain temperature is met (possibly from drilling), an extra lock is implemented to ensure the valuables are properly protected.

Managing the Life Cycle of Assets

A life-cycle model describes the changes that an entity experiences during its lifetime. While it may seem odd to refer to assets as having a “life,” the fact is that their utility for (and presence within) organizations can be described with clear start and end points. That is the lifetime of the asset within that organization (even if it gets refurbished and used elsewhere). After the asset departs, its utility is oftentimes transferred to its replacement even if the new asset is different than the original in meaningful ways. That new asset will, in turn, be replaced by something else, and so on.

The life cycle, which is shown in Figure 5-1, starts with the identification of a new requirement. Whoever identifies the new requirement either becomes its champion or

Figure 5-1
The IT asset
life cycle

Replace or
Dispose

Business
Case