audience, because these metrics are not technical. They are also forward-looking because they address things that may happen in the future. For these reasons, risk metrics are the best ones to support strategic analyses.

Depending on your organization's risk management program, you may already have risk metrics defined. Recall from Chapter 2 that quantitative risk management requires that you identify and capture risk metrics. Even if you use a qualitative approach, you probably have a good place from which to start. All you have to do is identify the variables that make your risks more or less likely to be realized and then start tracking those. Here are some examples of commonly used risk metrics:

- The percentage of change in your aggregated residual risks
- The percentage of change in your current worst-case risk
- The ratio of organizational security incidents to those reported by comparable organizations

Preparedness Metrics

There is another type of metric that indicates how prepared your organization is to deal with security incidents. These metrics are sometimes useful when dealing with executives, but they are more commonly used to monitor the security program as a whole. Preparedness metrics look at all your controls and how well they are being maintained. For example, are your policies and procedures being followed? Do your staff members know what they're supposed to (and not supposed to) do? What about your business partners?

Given the importance (and difficulty) of securing your organization's supply chain, your preparedness metrics should include the preparedness of organizations that are upstream from yours (in other words, your organization's suppliers of goods and services).

Depending on your organization's relationship with them, you may have a lot of visibility into their security programs, which makes your assessment and measuring of them a lot easier. Even if they are fairly opaque and unwilling to give you enough information, you should develop a mechanism for rating their security, perhaps using an external or thirdparty audit, as discussed in Chapter 18.

Here are some examples of preparedness metrics used by many organizations:

- Monthly change in the mean time to patch a system
- Percentage of systems that are fully patched
- Percentage of staff that is up to date on security awareness training

• Ratio of privileged accounts to nonprivileged accounts
• Annual change in vendor security rating (i.e., how prepared is your organization's supply chain)

Performance Metrics

• Number of alerts analyzed this week/month compared to last week/month
• Number of security incidents declared this week/month compared to last week/month
• Percent change in mean time to detect (MTTD)
• Percent change in mean time to resolve (MTTR)

Key Performance and Risk Indicators
There is no shortage of security metrics in the industry, but not all are created equal.
There are some that are important for tracking our processes and day-to-day operations.
Other metrics, however, can tell us whether or not we are meeting strategic business goals.

PART VI

If risk metrics are fairly strategic and preparedness metrics are more operational, performance metrics are as tactical as they come. They measure how good your team and systems are at detecting, blocking, and responding to security incidents. In other words, performance metrics tell you how good you are at defeating your adversaries day in and day out.
If you've ever worked in or led a security operations center, performance metrics are the metrics you're probably most used to seeing. Some examples are listed here:

These are the key performance indicators (KPIs) and key risk indicators (KRIs). KPIs measure how well things are going now, while KRIs measure how badly things could go in the future.

Key Performance Indicators
A key performance indicator is an indicator that is particularly significant in showing the performance of an ISMS compared to its stated goals. KPIs are carefully chosen from among a larger pool of indicators to show at a high level whether our ISMS is keeping pace with the threats to our organization or showing decreased effectiveness. KPIs should be easily understood by business and technical personnel alike and should be

aligned
with one or (better yet) multiple organizational goals.
Choosing KPIs really forces us to wrestle with the question “What is it that we’re
trying to accomplish here?” The process by which we choose KPIs is really driven by
organizational goals. In an ideal case, the senior leadership sets (or perhaps approves)
goals for the security of the organization. The ISMS team then gets to work on how
to show whether we are moving toward or away from those goals. The process can be
summarized as follows:
1. Choose the factors that can show the state of our security. In doing this, we want
to strike a balance between the number of data sources and the resources required
to capture all their data.
2. Define baselines for some or all of the factors under consideration. As we do this,
it is helpful to consider which measurements will be compared to each other
and which to some baseline. Keep in mind that a given baseline may apply to
multiple factors’ measurements.
3. Develop a plan for periodically capturing the values of these factors, and fix the
sampling period. Ideally, we use automated means of gathering this data so as to
ensure the periodicity and consistency of the process.
4. Analyze and interpret the data. While some analysis can (and probably should)
be automated, there will be situations that require human involvement. In some
cases, we’ll be able to take the data at face value, while in others we will have to
dig into it and get more information before reaching a conclusion about it.
5. Communicate the indicators to all stakeholders. In the end, we need to package
the findings in a way that is understandable by a broad range of stakeholders. A
common approach is to start with a nontechnical summary that is supported by
increasingly detailed layers of supporting technical information. On the summary
side of this continuum is where we select and put our KPIs.

This process is not universally accepted but represents some best security industry
practices. At the end of the day, the KPIs are the product of distilling a large amount
of information with the goal of answering one specific question: “Are we managing our
information security well enough?” There is no such thing as perfect security, so what
we are really trying to do is find the sweet spot where the performance of the ISMS is

adequate and sustainable using an acceptable amount of resources. Clearly, this

spot is a
moving target given the ever-changing threat and risk landscape.

Key Risk Indicators
While KPIs tell us where we are today with regard to our goals, key risk indicators tell us
where we are today in relation to our risk appetite. They measure how risky an activity is
so that leadership can make informed decisions about that activity, all the while taking
into account potential resource losses. Like KPIs, KRIs are selected for their impact on
the decisions of the senior leaders in the organization. This means that KRIs often are not
specific to one department or business function, but rather affect multiple aspects of the
organization. KRIs have, by definition, a very high business impact.
When considering KRIs, it is useful to relate them to single loss expectancy (SLE)
equations. Recall from Chapter 2 that SLE is the organization's potential monetary loss
if a specific threat were to be realized. It is the product of the loss and the likelihood
that the threat will occur. In other words, if we have a proprietary process for building
widgets valued at $500,000 and we estimate a 5 percent chance of an attacker stealing
and monetizing that process, then our SLE would be $25,000. Now, clearly, that
5 percent figure is affected by a variety of activities within the organization, such as IDS
tuning, IR team proficiency, and end-user security awareness.
Over time, the likelihood of the threat being realized will change based on multiple
activities going on within the organization. As this value changes, the risk changes too.
A KRI would capture this and allow us to notice when we have crossed a threshold that
makes our current activities too risky for our stated risk appetite. This trigger condition
enables the organization to change its behavior to compensate for excessive risk. For
instance, it could trigger an organizational stand-down for security awareness training.
In the end, the important thing to remember about KRIs is that they are designed to
work much as coal mine canaries: they alert us when something bad is likely to happen
so that we can change our behavior and defeat the threat.
EXAM TIP KPIs and KRIs are used to measure progress toward attainment of
strategic business goals.

Most of our metrics and indicators come from the security processes that make up our
ISMS. There are other sources of measures, of course, but if we want to assess

the effectiveness of our security controls, clearly we have to look at them first. To determine whether our controls are up to speed, we need to collect security process data from a variety of places. From how we manage our accounts to how we verify backups to the security awareness of our employees, administrative controls are probably more pervasive and less visible than our technical controls. It shouldn’t be surprising that sophisticated threat actors often try to exploit administrative controls.

PART VI

Security Process Data

We covered a number of technical processes in the previous chapter. These included vulnerability assessments, various forms of attack simulations, and log reviews, to name a few. In the sections that follow, we look at some of the more administrative processes from which we can also collect data to help us determine our current posture and help us improve it over time. This is by no means an exhaustive list; it is simply a sampling that (ISC)2 emphasizes in the CISSP exam objectives.

Account Management

A preferred technique of attackers is to become “normal” privileged users of the systems they compromise as soon as possible. They can accomplish this in at least three ways: compromise an existing privileged account, create a new privileged account, or elevate the privileges of a regular user account. The first approach can be mitigated through the use of strong authentication (e.g., strong passwords or, better yet, multifactor authentication) and by having administrators use privileged accounts only for specific tasks. The second and third approaches can be mitigated by paying close attention to the creation, modification, or misuse of user accounts. These controls all fall in the category of account management.

Adding Accounts

When new employees arrive, they should be led through a well-defined process that is aimed at ensuring not only that they understand their duties and responsibilities, but

also that they are assigned the required organizational assets and that these are properly configured, protected, and accounted for. While the specifics of how this is accomplished vary from organization to organization, there are some specific administrative controls that should be universal.

First, all new users should be required to read through and acknowledge they understand (typically by signing) all policies that apply to them. At a minimum, every organization should have (and every user should sign) an acceptable use policy (AUP) that specifies what the organization considers acceptable use of the information systems that are made available to the employee. Using a workplace computer to view pornography, send hate e-mail, or hack other computers is almost always specifically forbidden in the AUP. On the other hand, many organizations allow their employees limited personal use, such as checking personal e-mail or surfing the Web during breaks. The AUP is a useful first line of defense, because it documents when each user was made aware of what is and is not acceptable use of computers (and other resources) at work. This makes it more difficult for a user to claim ignorance if they subsequently violate the AUP.

Testing that all employees are aware of the AUP and other applicable policies can be the first step in auditing user accounts. Since every user should have a signed AUP, for instance, all we need is to get a list of all users in the organization and then compare it to the files containing the signed documents. In many cases, all the documents a new employee signs are maintained by human resources (HR) and the computer accounts are maintained by IT. Cross-checking AUPs and user accounts can also verify that these two departments are communicating effectively.

The policies also should dictate the default expiration date of accounts, the password policy, and the information to which a user should have access. This last part becomes difficult because the information needs of individual users typically vary over time.

Modifying Accounts

Suppose a newly hired IT technician is initially assigned the task of managing backups

for a set of servers. Over time, you realize this individual is best suited for internal user
support, including adding new accounts, resetting passwords, and so forth. The privileges needed in each role are clearly different, so how should you handle this? Many
organizations, unfortunately, resort to giving all privileges that a user may need. We
have all been in, seen, or heard of organizations where every user is a local admin on
his or her computer and every member of the IT department is a domain admin. This
is an exceptionally dangerous practice, especially if they all use these elevated credentials by default. This is often referred to as authorization creep, which we discussed in
Chapter 17.
Adding, removing, or modifying the permissions that a user has should be a carefully
controlled and documented process. When are the new permissions effective? Why are they needed? Who authorized the change? Organizations that are mature in their
security processes have a change control process in place to address user privileges. While
many auditors focus on who has administrative privileges in the organization, there are
many custom sets of permissions that approach the level of an admin account. It is
important, then, to have and test processes by which elevated privileges are issued.

The Problem with Running as Root

• Windows operating systems allow you to right-click any program and select Run As to elevate your privileges. From the command prompt, you can use the command runas /user:<AccountName> to accomplish the same goal.
• In Linux operating systems, you can simply type sudo<SomeCommand> at the command line to run a program as the super (or root) user. Some Linux GUI desktop environments also offer the user the option of running with sudo (usually by checking a box) and prompting for a password.
• In macOS, you use sudo from the Terminal app just like you would do from a Linux terminal. However, if you want to run a GUI app with elevated privileges, you need to use sudo open –a <AppName> since there is no gksudo or kdesudo command.

PART VI

It is undoubtedly easier to do all your work from one user account, especially if that
account has all the privileges you could ever need. The catch, as you may well know,
is that if your account is compromised, the malicious processes will run with whatever privileges the account has. If you run as root (or admin) all the time, you can
be certain that if an attacker compromises your box, he instantly has the privileges

to do whatever he needs or wants to do.
A better approach is to do as much of your daily work as you can using a restricted account and elevate to a privileged account only when you must. The way in which you do this varies by operating system:

Suspending Accounts

Another important practice in account management is to suspend accounts that are no longer needed. Every large organization eventually stumbles across one or more accounts that belong to users who are no longer part of the organization. In extreme cases, an organization discovers that a user who left several months ago still has privileged accounts.
The unfettered presence of these accounts on our networks gives adversaries a powerful means to become seemingly legitimate users, which makes our job of detecting and repulsing them that much more difficult.
Accounts may become unneeded, and thus require suspension, for a variety of reasons, but perhaps the most common one would be that the user of the account was terminated or otherwise left the organization. Other reasons for suspension include reaching the account's default expiration date, and temporary, but extended, absences of employees (e.g., maternity leave, military deployment). Whatever the reason, we must ensure that the account of someone who is not present to use it is suspended until that person returns or the term of our retention policy is met.
Testing the administrative controls on suspended accounts follows the same pattern already laid out in the preceding two sections: look at each account (or take a representative sample of all of them) and compare it with the status of its owner according to our HR records. Alternatively, we can get a list of employees who are temporarily or permanently away from the organization and check the status of those accounts. It is important that accounts are deleted only in strict accordance with the data retention policy. Many investigations into terminated employees have been thwarted because administrators have prematurely deleted user accounts and/or files.

Backup Verification

Modern organizations deal with vast amounts of data, which must be protected for a variety of reasons, including disaster recovery. We have all been in at least

one situation in which we have lost data and needed to get it back. Some of us have had a rude awakening upon discovering that the data was lost permanently. The specific nature of the backup media is not as important as the fact that the data must be available when we need it most.

Magnetic tapes are now able to hold over 180 terabytes of data, which makes this seemingly antiquated technology the best in terms of total cost of ownership. That being said, many organizations prefer other technologies for daily operations, and relegate tapes to the role of backup to the backup. In other words, it is not uncommon for an organization to back up its user and enterprise data to a storage area network (SAN) on a daily basis, and back up these backups to tape on a weekly basis. Obviously, the frequency of each backup (hourly, daily, weekly) is driven by the risk management process discussed in Chapter 1.

Whatever the approach to backing up our organizational data, we need to periodically test it to ensure that the backups will work as promised when we need them. There are some organizations that have faced an event or disaster that required them to restore some or all data from backups, only to discover that the backups were missing, corrupted, or outdated. This section discusses some approaches to assess whether the data will be there when we need it.

CAUTION Never back up your data to the same device on which the original data exists.

Types of Data

Not all data is created equal, and different types may have unique requirements when it comes to backups. The following sections discuss some of the major categories of data that most of us deal with and some considerations when planning to preserve that data.

Keep in mind, however, that there are many other types of data that we will not discuss here for the sake of brevity.

User Data Files This is the type of data with which most of us are familiar. These are the documents, presentations, and spreadsheets that we create or use on a daily basis. Though backing up these files may seem simple, challenges arise when

users put
“backup” copies in multiple locations for safekeeping. Users, if left to their own devices,
may very well end up with inconsistently preserved files and may even violate retention
requirements. The challenge with this type of data is ensuring that it is consistently
backed up in accordance with all applicable policies, regulations, and laws.
Databases Databases are different from regular files in that they typically store the
entire database in a special file that has its own file system within it. To make sense of
this embedded file system, your database software uses metadata that lives in other files
within your system. This architecture can create complex interdependencies among files
on the database server. Fortunately, all major database management systems (DBMSs)
include one or more means to back up their databases. The challenge is in ensuring
that the backup will be sufficient to reconstitute the databases if necessary. To verify
the backups, many organizations use a test database server that is periodically used to
verify that the databases can be recovered from backup and that the queries will execute
properly from the restored data.

Many organizations have virtualized their server infrastructure for performance and
maintenance reasons. Some are also virtualizing their client systems and turning
their workstations into thin clients on a virtualization infrastructure. The next step
in this evolution is the use of virtual machine (VM) snapshots as a backup strategy.
The main advantage to this approach is that restoration is almost instantaneous.
All you typically have to do is click a button or issue a scripted command and the
VM will revert to the designated state. Another key advantage is that this approach
lends itself to automation and integration with other security systems so that if, for
example, a workstation is compromised because the user clicked a link and an IDS
detected this incident, then the VM can be instantly quarantined for later analysis
while the user is dropped into the most recent snapshot automatically with very
little impact to productivity.

PART VI

Virtualization as a Backup and Security Strategy

Mailbox Data By some estimates, as much as 75 percent of an average organization's data lives in its mailboxes. Depending on the mail system your organization is running, the backup process may be very different. Still, some commonalities exist across all platforms, such as the critical need to document in excruciating detail every aspect of the configuration of the mail servers. Most medium-sized to large organizations have multiple mail servers (perhaps backing each other up), so it is a good idea not to back them up at the same time. Finally, whatever backup mechanism you have in place for your mail servers should facilitate compliance with e-discovery.

Verification
Having data backups is not particularly helpful unless we are able to use them to recover from mistakes, accidents, attacks, or disasters. Central to verifying this capability is understanding the sorts of things that can go wrong and which of them would require backups. Recall from our discussion on threat modeling in Chapter 9 that an important step in understanding risk is to consider what can happen or be done to our systems that would destroy, degrade, or disrupt our ability to operate. It is helpful to capture these possibilities in scenarios that can then inform how we go about ensuring that we are prepared for the likely threats to our information systems. It is also helpful to automate as much of the testing as possible, particularly in large organizations. This ensures that we cover the likely contingencies in a very methodical and predictable manner.
Some tests may cause disruptions to our business processes. It is difficult to imagine how a user's backups can be fully tested without involving that user in the process to some extent. If, for instance, our users store files locally and we want to test Mary's workstation backup, an approach could be to restore her backup to a new computer and have Mary log into and use the new computer as if it were the original. She would be in a better position than anyone else to determine whether everything works as expected.
This kind of thorough testing is expensive and disruptive, but it ensures that we have in place what we need. Obviously, we have to be very selective about when and how we impact our business processes, so it becomes a trade-off.
However you decide to implement your backup verification, you must ensure that

you
are able to assert that all critical data is backed up and that you will be able to restore it
in time of need. This means that you probably have to develop an inventory of data and
a schedule for testing it as part of your plan. This inventory will be a living document,
so you must have a means to track and document changes to it. Fortunately, major items such as mail and database servers don’t change very frequently. The challenge is in
verifying the backups of user data.
This brings us back to our policies. We already discussed the importance of the organization’s data retention policy, but an equally important one is the policy that
dictates how user data is backed up. Many organizations require their staff to maintain
their files on file shares on network servers, but we all know that users don’t necessarily
always do this. It is not uncommon for users to keep a local folder with the data that is
most important to them. If the local files are not being backed up, then we risk losing the
most critical files, particularly if backups can be disabled by the user. The point of this
is that policies need to be carefully thought out and aggressively enforced if we are to be
ready for the day when things go badly for us.

Testing Data Backups

It is important to develop formal processes for testing your data backups to ensure
they are available when needed. The following are some elements that should be included in these processes:

- Develop scenarios that capture specific sets of events that are representative of
the threats facing the organization.
- Develop a plan that tests all the mission-critical data backups in each of the scenarios.
- Leverage automation to minimize the effort required by the auditors and ensure tests happen periodically.
- Minimize impact on business processes of the data backup test plan so that it can be executed regularly.
- Ensure coverage so that every system is tested, though not necessarily in the same test.
- Document the results so you know what is working and what needs to be worked on.
- Fix or improve any issues you documented.

Security Training and Security Awareness Training

PART VI

As should be clear from the preceding discussions, having a staff that is well trained in security issues is crucial to the security of our organizations. The terms security training and security awareness training are often used interchangeably, but they have subtly different meanings. Security training is the process of teaching a skill or set of skills that enables people to perform specific security functions better. Security awareness training, on the other hand, is the process of exposing people to security issues so that they are able to recognize and respond to them better. Security training is typically provided to security personnel, while security awareness training should be provided to every member of the organization.

Assessing the effectiveness of our security training programs is fairly straightforward because the training is tied to specific security functions. Therefore, to test the effectiveness of a training program, all we have to do is test the performance of an individual on those functions before and after the training. If the performance improves, then the training was probably effective. Keep in mind that skills atrophy over time, so the effectiveness of the training should be measured immediately after it concludes. Otherwise, we are assessing the long-term retention of the functional skills.

We now turn our attention to the somewhat more difficult issue of assessing the effectiveness of a security awareness training program. As we broach this subject, keep in mind that the end state is to better equip our teammates to recognize and deal with

security issues that arise while they are performing their everyday tasks. This implies that a key measure of the effectiveness of the security awareness program is the degree to which people change their behaviors when presented with certain situations. If this change is toward a better security posture, then we can infer that the program was effective. In the following sections, we take a look at specific components of a security awareness training program that are common to many organizations.

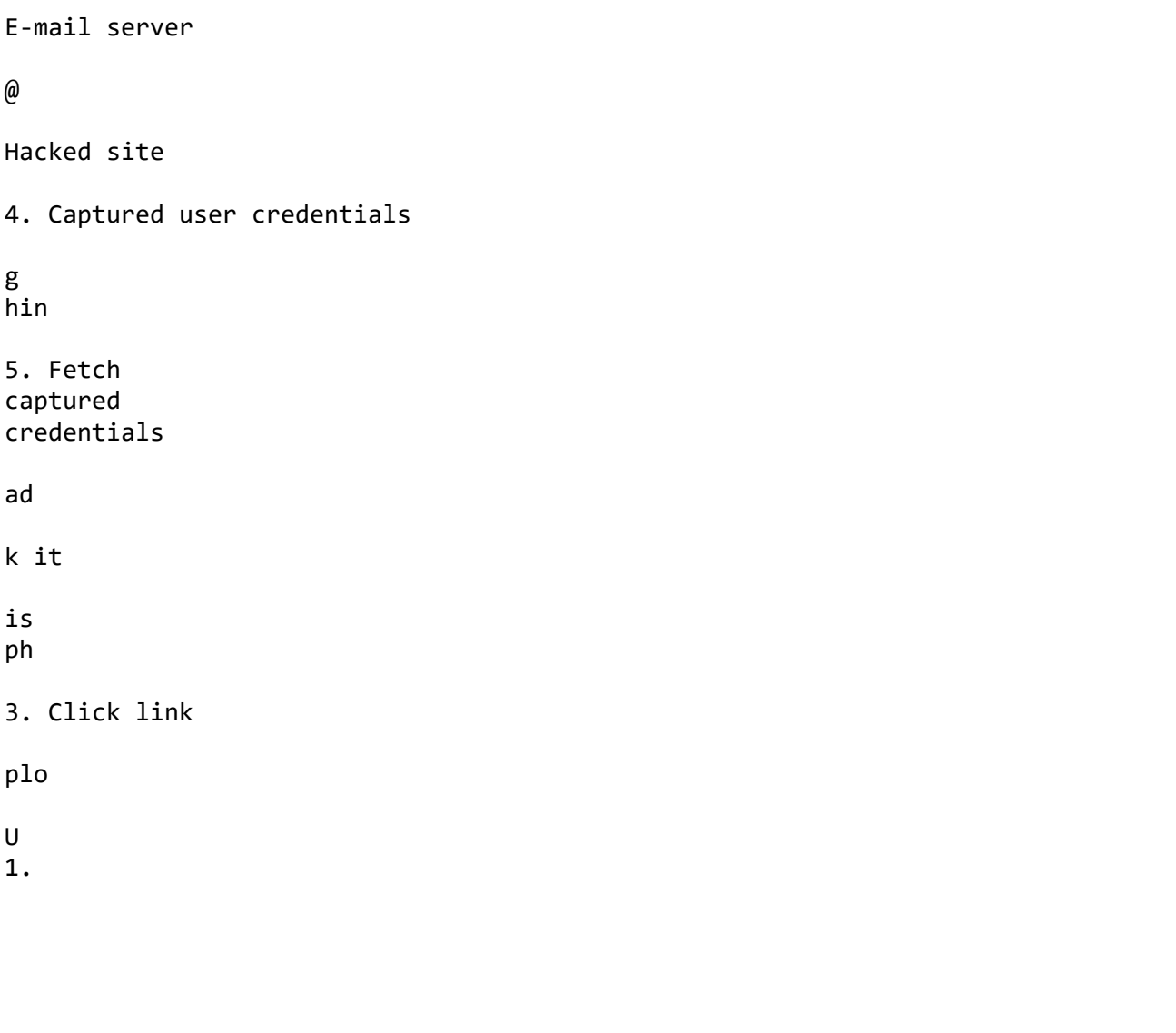
EXAM TIP Security awareness (and the training required to attain it) is one of the most critical controls in any ISMS. Expect exam questions on this topic.

Social Engineering

Social engineering, in the context of information security, is the process of manipulating individuals so that they perform actions that violate security protocols. Whether the action is divulging a password, letting someone into the building, or simply clicking a link, it has been carefully designed by the adversaries to help them exploit our information systems. A common misconception is that social engineering is an art of improvisation. While improvising may help the attacker better respond to challenges, the reality is that most effective social engineering is painstakingly designed against a particular target, sometimes a specific individual.

Perhaps the most popular form of social engineering is phishing, which is social engineering conducted through a digital communication. Figure 19-2 depicts the flow of a typical e-mail phishing attack. (While e-mail phishing receives a lot of attention, text messages can also be used to similar effect.) Like casting a baited fishing line into a

Figure 19-2
Typical phishing
attack



2. Send phishing e-mail

Phisher

Victim

pond full of fish, phishing relies on the odds that if enough people receive an enticing or believable message, at least one of them will click an embedded link within it. Some adversaries target specific individuals or groups, which is referred to as spearphishing. In some cases, the targets are senior executives, in which case it is called whaling.

In whatever variety it comes, the desired result of phishing is usually to have the target click a link that will take them to a website under the control of the attacker. Sometimes the website looks like the legitimate logon page of a trusted site, such as that of the user's bank. Other times, the website is a legitimate one that has been compromised by the attacker to redirect users somewhere else. In the case of a drive-by download, the site invisibly redirects the user to a malware distribution server, as shown in Figure 19-3.

Pretexting is a form of social engineering, typically practiced in person or over the phone, in which the attacker invents a believable scenario in an effort to persuade the target to violate a security policy. A common example is a call received from (allegedly) customer service or fraud prevention at a bank in which the attacker tries to get the target to reveal account numbers, personal identification numbers (PINs), passwords, or similarly valuable information. Remarkably, pretexting was legal in the United States until 2007, as long as it was not used to obtain financial records. In 2006, HewlettPackard became embroiled in a scandal dealing with its use of pretexting in an effort to identify the sources of leaks on its board of directors. Congress responded by passing the Telephone Records and Privacy Protection Act of 2006, which imposes stiff criminal penalties on anyone who uses pretexting to obtain confidential information.

So how does one go about assessing security awareness programs aimed at countering social engineering in all its forms? One way is to keep track of the number of times users fall victim to these attacks before and after the awareness training effort. The challenge with this approach is that victims may not spontaneously confess to

falling for

1. Attacker modifies
vulnerable website.

2. Victim visits
tampered good
website.

3. Victim is secretly
redirected to
malware server.

PART VI

4. Malware server gets
browser specs, finds the
right exploit for it.
6. Malware phones
home to attacker,
ready to send data
or be used in other
attacks.

Figure 19-3

Drive-by downloads

5. Malware gets
installed without
the victim noticing.

these tricks, and our security systems will certainly not detect all instances of successful attacks. Another approach is to have auditors (internal or external) conduct benign social engineering campaigns against our users. When users click a link inserted by the auditors, they are warned that they did something wrong and perhaps are redirected to a web page or short video explaining how to avoid such mistakes in the future. All the while, our automated systems are keeping tabs on which users are most susceptible and how often these attacks are successful. Anecdotal evidence suggests that there is a group of users who will not respond to remedial training, so the leadership should decide what to do with individuals who repeatedly make the wrong choices.

Online Safety

Oftentimes users don’t have to be tricked into doing something wrong, but willingly go down that path. This is often the result of ignorance of the risks, and the remediation of this ignorance is the whole point of the security awareness campaign. An effective security awareness program should include issues associated with unsafe online behavior that could represent risk for the organization.

Perhaps one of the most important elements of safe online behavior is the proper use of social media. A good starting point is the proper use of privacy settings, particularly considering that all major social media sites have means to restrict what information is shared with whom. The default settings are not always privacy-focused, so it is important for users to be aware of their options. This becomes particularly important when users post information concerning their workplace. Part of the security awareness program should be to educate users about the risks they can pose to their employers if their posts reveal sensitive information. Once posted, the information cannot be recalled; it is forevermore out there.

Sometimes it is not what goes out to the Internet but what comes in from it that should concern users. Simply surfing to the wrong website, particularly from a workplace computer, may be all it takes to bring down the whole organization. In the case of a drive-by download, the attack is triggered simply by visiting a malicious website. While the mechanisms vary, the effect can be the execution of malware on the client computer, with or without additional user interaction. While web filters can mitigate some of the risk of surfing to inappropriate sites, malicious websites sometimes are legitimate ones that have been compromised, which means that the filters may not be effective.

While some downloads happen without user knowledge or interaction, others are intentional. It is not unusual for naïve users to attempt to download and install unauthorized and potentially risky applications on their computers. Unfortunately, many organizations do not use software whitelisting and even allow their users to have administrative privileges on their computers, which allows them to install any application they desire. Even benign applications can be problematic for the security of our systems, but when you consider that the software may come from an untrusted and potentially malicious source, the problem is compounded.

Assessing the effectiveness of an awareness campaign that promotes users’ online

safety
is not easy and typically requires a multipronged approach. Social media posts may be
detected using something as simple as Google Alerts, which trigger whenever Google’s

robots find a term of interest online. A simple script can then filter out the alerts by
source in order to separate, say, a news outlet report on our organization from an illadvised social media post. The software download problem (whether intentional or not)
can be assessed by a well-tuned IDS. Over time, with an effective awareness campaign, we
should see the number of incidents go down, which will allow us to focus our attention
on repeat offenders.

Data Protection

We already covered data protection in Chapter 6, but for the purposes of assessing a security awareness program, it bears repeating that sensitive data must always be encrypted
whether at rest or in transit. It is possible for users to circumvent controls and leave this
data unprotected, so awareness is a key to preventing this type of behavior. Unencrypted
data is vulnerable to leaks if it is stored in unauthorized online resources or intentionally
(but perhaps not maliciously) shared with others. Another important topic is the proper
destruction of sensitive data when it is no longer needed and falls out of the mandatory
retention period (see Chapter 5).
Testing the degree to which our users are aware of data protection requirements and
best practices can best be done by using tags in our files’ metadata. The information
classification labels we discussed in Chapter 5 become an effective means of tracking
where our data is. Similarly, data loss prevention (DLP) solutions can help stop leaks
and identify individuals who are maliciously or inadvertently exposing our sensitive
information. This allows us to target those users either with additional awareness training
or with disciplinary actions.

Culture

At the end of the day, the best way to test the security awareness of an organization may
be by assessing its security culture. Do we have the kind of environment in which users

feel safe self-reporting? Are they well incentivized to do so? Do they actively seek information and guidance when encountering a strange or suspicious situation? Self-reports
and requests for information by users provide a good indicator of whether the organizational culture is helping or hindering us in securing our systems.

Most organizations cannot afford to be incapable of performing their business processes
for very long. Depending on the specific organization, the acceptable downtime can be
measured in minutes, hours, or, in some noncritical sectors, maybe days. Consequently,
we all need to have procedures in place for ensuring we can go on working regardless of
what happens around or to us. As introduced in Chapter 2, business continuity is the term
used to describe the processes enacted by an organization to ensure that its vital business
processes remain unaffected or can be quickly restored following a serious incident. Business continuity looks holistically at the entire organization. A subset of this effort, called
disaster recovery, focuses on restoring the information systems after a disastrous event.
Like any other business process, these processes must be periodically assessed to ensure
they are still effective.

Often, the initial response to an emergency affects the ultimate outcome. Emergency
response procedures are the prepared actions that are developed to help people in a crisis
situation better cope with the disruption. These procedures are the first line of defense
when dealing with a crisis situation. People who are up to date on their knowledge of
these procedures will perform the best, which is why training and drills are very important.
Emergencies are unpredictable, and no one knows when they will be called upon to perform their disaster recovery duties.
Protection of life is of the utmost importance and should be dealt with first before
attempting to save material objects. Emergency procedures should show the people in
charge how to evacuate personnel safely (see Table 19-1). All personnel should know
their designated emergency exits and destinations. Emergency gathering spots should

take into consideration the effects of seasonal weather. One person in each designated group is often responsible for making sure all people are accounted for. One person in particular should be responsible for notifying the appropriate authorities: the police department, security guards, fire department, emergency rescue, and management. With proper training, employees will be better equipped to handle emergencies and avoid the reflex to just run to the exit.

EXAM TIP Protection of human life is always the top priority in situations where it is threatened.

If the situation is not life threatening, designated staff should shut down systems in an orderly fashion, and remove critical data files or resources during evacuation for safekeeping. There is a reason for the order of activities. As with all processes, there are

Procedure: Personnel Evacuation Description	Location	Names of Staff Trained to Carry Out Procedure	Comments:
Each floor within the building must have two individuals who will ensure that all personnel have been evacuated from the building after a disaster. These individuals are responsible for performing employee head count, communicating with the business continuity plan (BCP) coordinator, and assessing emergency response needs for their employees.	West wing parking lot	David Miller Michelle Lester	These individuals are responsible for maintaining an up-to-date listing of employees on their specific floor. These individuals must have a company-issued walkie-talkie and proper training for this function.

Table 19-1 Sample Emergency Response Procedure

Date Last
Carried Out

Drills were
carried out on
May 4, 2021.

dependencies with everything we do. Deciding to skip steps or add steps could in fact
cause more harm than good.

Once things have approached a reasonable plateau of activity, one or more people will
most likely be required to interface with external entities, such as the press, customers,
shareholders, and civic officials. One or more people should be prepped in their reaction
and response to the recent disaster so a uniform and reasonable response is given to explain
the circumstances, how the organization is dealing with the disaster, and what customers
and others should now expect from the organization. The organization should quickly
present this information instead of allowing others to come to their own conclusions and
start false rumors. At least one person should be available to the press to ensure proper
messages are being reported and sent out.

Another unfortunate issue needs to be addressed prior to an emergency: potential
looting, vandalism, and fraud opportunities from both a physical perspective and a
logical perspective. After an organization is hit with a large disturbance or disaster, it
is usually at its most vulnerable, and others may take advantage of this vulnerability.

Careful thought and planning, such as provision of sufficient security personnel on site,
enable the organization to deal with these issues properly and provide the necessary and
expected level of protection at all times.

Ideally, we collect most of the data we need for assessing our disaster recovery and
business continuity processes before any real emergencies arise. This allows us to ensure
we are prepared and to improve the effectiveness of our organizational responses to these
unforeseen events. Still, the best data is captured during an actual emergency situation.

After any real or training events, it is imperative that we have a debriefing immediately
after it. This event, sometimes called a hot wash, must happen while memories

are still
fresh. It is an ad hoc discussion of what happened, how we dealt with it, what went well,
and how we can do better in the future. Ideally, it is followed by a more deliberate afteraction review (AAR) that takes place later, once the stakeholders have had a chance to
think through the events and responses and analyze them in more detail. Hot wash notes
and AAR reports are excellent sources of security process data for disaster recovery and
business continuity.

For many security professionals, report writing is perhaps one of the least favorite activities, and yet it is often one of the most critical tasks for our organizations. While we all
thrive on putting hands on keyboards and patch panels when it comes to securing our
networks, we often cringe at the thought of putting in writing what it is that we've done
and what it means to the organization. This is probably the task that best distinguishes
the true security professional from the security practitioner: the professional understands
the role of information systems security within the broader context of the business and is
able to communicate this to both technical and nontechnical audiences alike.
It seems that many of us have no difficulty (though perhaps a bit of reluctance) describing the technical details of a plan we are proposing, a control we have implemented,
or an audit we have conducted. It may be a bit tedious, but we've all done this at some

point in our careers. The problem with these technical reports, important though they
are, is that they are written by and for technical personnel. If your CEO is a technical
person running a technical company, this may work fine. However, sooner or later most
of us will work with decision-makers that are not inherently technical. These leaders
will probably not be as excited about the details of an obscure vulnerability you just
discovered as they will be about its impact on the business. If you want your report to
have a business impact, it must be both technically sound and written in the language of
the business.

Analyzing Results

Before you start typing that report, however, you probably want to take some time to review the outputs, ensure you understand them, and then infer what they mean to your organization. Only after analyzing the results can you provide insights and recommendations that will help maintain or improve your organization's security. The goal of this analysis process is to move logically from facts to actionable information.

A list of vulnerabilities and policy violations is of little value to business leaders unless it is placed in context. Once you have analyzed all the results in this manner, you'll be ready to start writing the official report.

You can think of analyzing results as a three-step process to determine the following:

What?, So what?, and Now what? First you gather all your data, organize it, and study it carefully. You find out what is going on. This is where you establish the relevant and interesting facts. For example, you may have determined the fact that 12 of your servers are not running on the latest software release. Worse yet, you may have found that three of those servers have vulnerabilities that are being exploited in the wild. The instinctive reaction of many would be to say this is a big deal that needs to be corrected immediately.

But wait.

The second step in your analysis is to determine the business impact of those facts. This is the so what? Though we tend to focus on the technology and security aspects of our environments, we have a responsibility to consider facts in a broader organizational context. Continuing with the previous example, you may find that those 12 servers provide a critical business function and cannot be updated in the near term for perfectly legitimate operations reasons. You may also discover that you already have compensatory administrative or technical controls that mitigate the risk they pose. So maybe it's not that big of a deal after all.

The third step is to figure out the now what? The whole point of measuring security is to ensure it is sufficient or to improve it so that it is sufficient. The analysis process leads to results, and these are only valuable if they are actionable. They must point to one or more sound recommendations that address the broader organizational needs. In our example, you clearly don't want to leave those servers as they are indefinitely.

Maybe you have considered two courses of action: either leave things as they are but reassess every 30 days or update the servers immediately despite the resulting business impact. You evaluate the alternatives using risk and business impact as decision criteria and ultimately decide that keeping an extra-close eye on the unpatched servers for a few more weeks is the better course of action. You put down a date for the next decision point and go from there. The point is that your decision is based on a sound analysis of the facts.

Remediation

Most assessments uncover vulnerabilities. While many cybersecurity practitioners think of vulnerabilities in terms of software defects to be patched, the reality is that most vulnerabilities in the average organization tend to come from misconfigured systems, inadequate policies, unsound business processes, or unaware staff. Correcting most of these vulnerabilities requires engagement by more than just the IT or security teams.

Even the more mundane system patches need to be carefully coordinated with all affected departments within the organization. Vulnerability remediation should include all stakeholders, especially those who don’t have the word “security” anywhere in their job titles.

The fact that you’re leveraging a multifunctional extended team to remediate vulnerabilities highlights the need for the sound analyses described in the previous section.

You’ll need the support of everyone from the very top of the organization on down, which is why you want to educate them on your findings, why they are impacted, and what you must all do about them. It is likely that remediation will impact the business, so it is also critical to have contingency plans and be able to handle exceptional cases.

Exception Handling

Sometimes, vulnerabilities simply can’t be patched (at least, not in any reasonable amount of time). Some of us have dealt with very big and expensive medical devices that require Food and Drug Administration accreditations that preclude their patching without putting them through an expensive and time-consuming recertification process.

The solution is to implement compensatory controls around the problem, document the exception, and revisit the vulnerability over time to see if can be

remediated directly at some
point in the future. For example, a medical device may be micro-segmented in its own
VLAN behind a firewall that would only allow one other device to communicate with it,
and then using only a specific port and protocol.

The Language of Your Audience
PART VI

You cannot be an effective communicator if you don’t know your audience. Learning to speak the language(s) of those you are trying to inform, advise, or lead is absolutely critical. It has been said that accounting is the language of business, which
means you can generally do well communicating in terms of the financial impacts of
your findings. The fact that risks are expressed as the probability of a certain amount
of loss should make this fairly easy as long as you have some sort of risk management program in place.
Still, in order to up your game, you want to be able to communicate in the language of the various disciplines that make up a business. Human resource leaders will care most about issues like staff turnover and organizational culture.
Your marketing (or public affairs) team will be focused on what external parties think about your organization. Product managers will be very reluctant to support
proposals that can slow down their delivery tempo. We could go on, but the point is that, while the facts and analyses must be unassailable, you should always try to
communicate them in the language of…whoever it is you’re trying to persuade.

Ethical Disclosure
Occasionally, security assessments lead to discoveries of vulnerabilities that were not
known and which affect other organizations. Perhaps you were performing a code review on one of the products your company sells and you discovered a vulnerability, or maybe your pentesting team was conducting a pen test on a system your
organization bought from one of its vendors and they found a previously unknown way to exploit the system. However you discover the vulnerability, you have an ethical obligation to properly disclose it to the appropriate parties. If the vulnerability
is in your own product, you need to notify your customers and partners as soon as
possible. If it is in someone else’s product, you need to notify the vendor or manufacturer immediately so they can fix it. The goal of ethical disclosure is to inform
anyone who might be affected as soon as feasible, so a patch can be developed before
any threat actors become aware of the vulnerability.

More commonly, exception handling is required because something crashed while we were attempting to patch a system. Though we should always test patches in a sandbox environment before pushing them out to production systems, we can never be 100 percent certain that something won't go wrong. In those cases, particularly if the system is mission-critical, we roll back the patch, get the system back online as quickly and securely as we can, document the exception, and move on with remediation of other systems. We circle back, of course, but exception handling is typically a time-intensive effort that should not delay the larger remediation effort.

Writing Technical Reports

After analyzing the assessment results, the next step is to document. A technical report should be much more than the output of an automated scanning tool or a generic checklist with yes and no boxes. There are way too many so-called auditors that simply push the start button on a scanning tool, wait for it to do its job, and then print a report with absolutely none of the analysis we just discussed.

A good technical report tells a story that is interesting and compelling for its intended audience. It is very difficult to write one without a fair amount of knowledge about its readers, at least the most influential ones. Your goal, after all, is to persuade them to take whatever actions are needed to balance risks and business functions for the betterment of the organization. Simultaneously, you want to anticipate likely objections that could undermine the conversation. Above all else, you must be absolutely truthful and draw all conclusions directly from empirical facts. To improve your credibility, you should always provide in an appendix the relevant raw data, technical details, and automated reports.

The following are key elements of a good technical audit report:

• Executive Summary We'll get into the weeds of this in the next section, but you should always consider that some readers may not be able to devote more than a few minutes to your report. Preface it with a hard-hitting summary of key take-aways.

• Background Explain why you conducted the experiment/test/assessment/audit in the first place. Describe the scope of the event, which should be tied to the reason for doing it in the first place. This is a good place to list any

relevant
references such as policies, industry standards, regulations, or statutes.
• Methodology As most of us learned in our science classes, experiments (and audits) must be repeatable. Describe the process by which you conducted the study. This is also a good section in which to list the personnel who participated,
dates, times, locations, and any parts of the system that were excluded (and why).
• Findings You should group your findings to make them easier to search and read for your audience. If the readers are mostly senior managers, you may want to group your findings by business impact. Technologists may prefer groupings by class of system. Each finding should include the answer to “so what?” from your analysis.
• Recommendations This section should mirror the organization of your findings and provide the “now what?” from your analysis. This is the actionable part of the report, so you should make it compelling. When writing it, you should
consider how each key reader will react to your recommendations. For instance, if
you know the CFO is reluctant to make new capital investments, then you could frame expensive recommendations in terms of operational costs instead.
• Appendices You should include as much raw data as possible, but you certainly want to include enough to justify your recommendations. Pay attention to how you organize the appendices so that readers can easily find whatever data they may be looking for.
If you are on the receiving end of this process, always be wary of reports that look
auto-generated, which usually points to an ineffective auditing team. Also be careful
about reports that, having failed to find any significant vulnerabilities, overemphasize the
importance of less important flaws. If the security posture of the organization is good,
then the auditors should not shy away from saying so.

Getting into the technical weeds with an audit report is wonderful for techies, but it
doesn’t do the business folks any good. The next step in writing impactful reports is to
translate the key findings and recommendations into language that is approachable and
meaningful to the senior leadership of your organization. After all, it is their support that
will allow you to implement the necessary changes. They will provide both the authority
and resources that you will need.
Typically, technical reports (among others) include an executive summary of no more
than a page or two, which highlights what senior leaders need to know from the report.
The goal is to get their attention and effect the desired change. One way to get a business
leader’s attention is to explain the audit findings in terms of risk exposure. Security is

almost always perceived as a cost center for the business. A good way to show return on
investment (ROI) for a department that doesn’t generate profits is by quantifying how
much money a recommended change could potentially save the company.

PART VI

Executive Summaries

One way to quantify risk is to express it in monetary terms. We could say that the risk
(in dollars) is the value of an asset multiplied by the probability of the loss of that asset. In
other words, if our customer’s data is worth $1 million and there is a 10 percent chance
that this data will be breached, then our risk for this data breach would be $100,000.
How can we come up with these values? There are different ways in which accountants
valuate other assets, but the most common are the following.

• The cost approach simply looks at the cost of acquiring or replacing the asset. This
is the approach we oftentimes take to valuating our IT assets (minus information,
of course). How might it be applied to information? Well, if an information asset
is a file containing a threat intelligence report that cost the organization $10,000,
then the cost approach would attach that value to this asset.
• The income approach considers the expected contribution of the asset to the firm’s revenue stream. The general formula is value equals expected (or potential)
income divided by capitalization rate. The capitalization rate is the actual net income divided by the value of the asset. So, for instance, if that $10,000 threat intelligence report brought in $1,000 in net income last year (so the capitalization rate is 0.10) and our projections are that it will bring in $2,000
this year, then its present value would be $2,000 ÷ 0.10, or $20,000. As you should be able to see, the advantage of this approach is that it takes into account
the past and expected business conditions.
• The market approach is based on determining how much other firms are paying for a similar asset in the marketplace. It requires a fair amount of transparency
in terms of what other organizations are doing. For instance, if we have no way of knowing how much others paid for that threat intelligence report, then we couldn’t use a market approach to valuating it. If, on the other hand, we were able to find out that the going rate for the report is actually $12,000, then we can

use that value for our report (asset) and celebrate that we got a really good deal.
So, as long as the life-cycle costs of implementing our proposed controls (say, $180,000) are less than the risks they mitigate (say, $1,000,000), it should be obvious
that we should implement the control, right? Not quite. The controls, after all, are not
perfect. They will not be able to eliminate the risk altogether, and will sometimes fail.
This means that we need to know the likelihood that the control will be effective at
thwarting an attack. Let’s say that we are considering a solution that has been shown to
be effective about 80 percent of the time and costs $180,000. We know that we have a
10 percent chance of being attacked and, if we are, that we have a 20 percent chance
of our control failing to protect us. This means that the residual risk is 2 percent of
$1,000,000, or $20,000. This is then added to the cost of our control ($180,000) to give
us the total effective cost of $200,000.
This is the sort of content that is impactful when dealing with senior leaders. They
want to know the answers to questions such as these: How likely is this control to work?
How much will it save us? How much will it cost? The technical details are directly

important to the ISMS team and only indirectly important to the business leaders. Keep
that in mind the next time you package an audit report for executive-level consumption.

Management Review and Approval

Plan

Figure 19-4
The Plan-DoCheck-Act loop

Act

Do
Check

A management review is a formal meeting of senior organizational leaders to determine
whether the management systems are effectively accomplishing their goals. In the

context of the CISSP, we are particularly interested in the performance of the ISMS. While
we restrict our discussion here to the ISMS, you should be aware that the management
review is typically much broader in scope.
While management reviews have been around for a very long time, the modern use of the term is perhaps best grounded in quality standards such as the ISO 9000 series.
These standards define a Plan-Do-Check-Act loop, depicted in Figure 19-4. This cycle
of continuous improvement elegantly captures the essence of most topics we cover in this
book. The Plan phase is the foundation of everything else we do in an ISMS, because
it determines our goals and drives our policies. The Do phase of the loop is the focal
point of Part VII of this book (“Security Operations”). The Check phase is the main
topic of this chapter and the previous one. Lastly, the Act phase is what we formally
do in the management review. We take all the information derived from the preceding
stages and decide whether we need to adjust our goals, standards, or policies in order to
continuously improve our posture.
The management review, unsurprisingly, looks at the big picture in order to help set
the strategy moving forward. For this reason, a well-run review will not be drawn into
detailed discussions on very specific technical topics. Instead, it takes a holistic view of
the organization and makes strategic decisions, which is the primary reason why the
management review must include all the key decision makers in the organization. This
top-level involvement is what gives our ISMS legitimacy and power.
When communicating with senior executives, it is important to speak the language of the business and to do so in a succinct manner. We already discussed this style of
communication when we covered reports in the previous section, but it bears repeating
here. If we are not able to clearly and quickly get the point across to senior leaders on the
first try, we may not get another chance to do so.

Before the Management Review
The management review should happen periodically. The more immature the management system and/or the organization, the more frequent these reviews should take place.
Obviously, the availability of the key leaders will be a limiting factor during

scheduling.
This periodicity helps ensure that the entire organization is able to develop an operational rhythm that feeds the senior-level decision-making process. Absent this regularity,
the reviews risk becoming reactive rather than proactive.
The frequency of the meetings should also be synchronized with the length of time
required to implement the decisions of the preceding review. If, for instance, the leaders
decided to implement sweeping changes that will take a year to develop, integrate, and
measure, then having a review before the year is up may not be particularly effective. This
is not to say that enough time must lapse to allow every single change to yield measurable
results, but if these reviews are conducted too frequently, management won't be able to
make decisions that are informed by the results of the previous set of actions.

Reviewing Inputs
The inputs to the management review come from a variety of sources. A key input is
the results of relevant audits, both external and internal. These are, in part, the reports
described earlier in the chapter. In addition to making the audit reports available for
review, it is also necessary to produce executive summaries that describe the key findings,
the impact to the organization, and the recommended changes (if any). Remember to
write these summaries in business language.
Another important input to the review is the list of open issues and action items from
the previous management review. Ideally, all these issues have been addressed and all
actions have been completed and verified. If that is not the case, it is important to highlight
whatever issues (e.g., resources, regulations, changes in the landscape) prevented them
from being closed. Senior leaders normally don't like surprises (particularly unpleasant
ones), so it might be wise to warn them of any unfinished business before the review is
formally convened.
In addition to the feedback from auditors and action officers, customer feedback is an important input to the management review. Virtually every organization has customers, and they are normally the reason for the organization to exist in the first place.
Their satisfaction, or lack thereof, is crucial to the organization's success. Chapter 18
mentioned real user monitoring (RUM) as one way of measuring their interactions with
our information systems. Organizations are also increasingly relying on social media

analysis to measure customer sentiments with regard to the organization in general and specific issues. Finally, we can use questionnaires or surveys, although these tend to have a number of challenges, including very low response rates and negative bias among respondents.

The final inputs to the management review are the recommendations for improvement based on all the other inputs. This is really the crux of the review. (While it is technically possible for a review to include no substantive change recommendations, it would be extremely unusual since it would mean that the ISMS team cannot think of any way to

improve the organizational posture.) The ISMS team presents proposed high-level changes that require the approval and/or support of the senior leaders. This is not the place to discuss low-level tactical changes; we can take care of those ourselves. Instead, we would want to ask for changes to key policies or additional resources. These recommendations must logically follow from the other inputs that have been presented to the review panel.

In setting the stage for the senior leaders' decision-making process, it is often useful to present them with a range of options. Many security professionals typically offer three to five choices, depending on the complexity of the issues. For instance, one option could be "do nothing," which describes what happens if no changes are made. At the other end of the spectrum, we could state an option that amounts to the solid-gold approach in which we pull out all the stops and make bold and perhaps costly changes that are all but guaranteed to take care of the problems. In between, we would offer one to three other choices with various levels of risk, resource requirements, and business appeal.

When we present the options, we should also present objective evaluative criteria for management to consider. A criterion that is almost always required in the presentation is the monetary cost of the change. This factor should be the life-cycle cost of the option, not just the cost of implementation. It is a common mistake to overlook the maintenance costs over the life of the system/process, disregarding the fact that these costs are often

much greater than the acquisition price tag. Other factors you may want to consider
presenting are risk, impact on existing systems or processes, training requirements, and
complexity. But whatever evaluative factors you choose, you should apply them to each
of the options in order to assess which is the best one.

Management Approval

Chapter Review
Whereas the focus of Chapter 18 was assessing and testing technical controls, this chapter discussed administrative controls, analyzing results, and communicating them effectively. We also introduced a couple of tools that will make this effort a whole lot easier
(and more effective) for you: security metrics, KPIs, and KRIs. Together with the topics

PART VI

The senior leadership considers all the inputs; typically asks some pretty pointed questions; and then decides to approve, reject, or defer the recommendations. The amount of
debate or discussion at this point is typically an indicator of how effective the ISMS team
was at presenting sound arguments for changes that are well nested within (and supportive of) the business processes. Obviously, the leadership’s decisions are the ultimate
testament to how convincing the ISMS team’s arguments were.
Typically, senior management will decide to either approve the recommendation in its
entirety, approve it with specific changes, reject the recommendation, or send the ISMS
team back to either get more supporting data or redesign the options. Regardless of the
outcome, there will likely be a list of deliverables for the next management review that will
have to be addressed. It is a good idea to conclude the management review with a review
of open and action items, who will address them, and when each is due. These all become
inputs to the next management review in a cycle that continues indefinitely.

discussed in the previous chapter, we hope to have given you useful insights into how to
measure and improve your ISMS, particularly when improvements depend on your ability to persuade other leaders in your organization to support your efforts. This all sets the
stage for the next part of this book: “Security Operations.”

Quick Review

• A factor is an attribute of an ISMS that has a value that can change over time.
• A measurement is a quantitative observation of a factor at a particular point in time.
• A baseline is a value for a factor that provides a point of reference or denotes that some condition is met by achieving some threshold value.
• A metric is a derived value that is generated by comparing multiple measurements against each other or against a baseline.
• Good metrics are relevant, quantifiable, actionable, robust, simple, and comparative.
• An indicator is a particularly important metric that describes a key element of the effectiveness of an ISMS.
• A key performance indicator (KPI) is an indicator that is particularly significant in showing the performance of an ISMS compared to its stated goals.
• Key risk indicators (KRIs) measure the risk inherent in performing a given action or set of actions.
• Privileged user accounts pose significant risk to the organization and should be carefully managed and controlled.
• User accounts should be promptly suspended whenever the user departs the organization permanently or for an extended period.
• Data backups should not be considered reliable unless they have been verified to be usable to restore data.
• Business continuity is the term used to describe the processes enacted by an organization to ensure that its vital business processes remain unaffected or can be quickly restored following a serious incident.
• Disaster recovery focuses on restoring the information systems after a disastrous event and is a subset of business continuity.
• Security training is the process of teaching a skill or set of skills that enables people to perform specific functions better.
• Security awareness training is the process of exposing people to security issues so that they are able to recognize and respond to them better.
• Social engineering, in the context of information security, is the process of manipulating individuals so that they perform actions that violate security protocols.
• Phishing is social engineering conducted through a digital communication.

• A drive-by download is an automatic attack that is triggered simply by visiting a malicious website.
• Disaster recovery and business continuity processes both need to be evaluated

regularly to ensure they remain effective in the face of environmental changes in
and around the organization.
• Reports must be written with a specific audience in mind if they are to be effective.
• A management review is a formal meeting in which senior organizational leaders determine whether the information security management systems are effectively accomplishing their goals.

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. What is a key performance indicator (KPI)?
A. A value for a factor that denotes that some condition is met
B. The result of comparing multiple measurements
C. A significant indicator that shows the performance of an ISMS
D. A quantitative observation of a factor of an ISMS at a point in time

2. Which of the following is true about key risk indicators (KRIs)?
A. They tell managers where an organization stands with regard to its goals.
B. They are inputs to the calculation of single loss expectancy (SLE).
C. They tell managers where an organization stands with regard to its risk appetite.
D. They represent an interpretation of one or more metrics that describes the
PART VI

effectiveness of the ISMS.
3. All of the following are normally legitimate reasons to suspend rather than delete
user accounts except
A. Regulatory compliance
B. Protection of the user’s privacy
C. Investigation of a subsequently discovered event
D. Data retention policy
4. Data backup verification efforts should
A. Have the smallest scope possible
B. Be based on the threats to the organization
C. Maximize impact on business
D. Focus on user data

5. What is the difference between security training and security awareness training?
A. Security training is focused on skills, while security awareness training is

focused on recognizing and responding to issues.

B. Security training must be performed, while security awareness training is an aspirational goal.
C. Security awareness training is focused on security personnel, while security training is geared toward all users.
D. There is no difference. These terms refer to the same process.
6. Which of the following is not a form of social engineering?
A. Pretexting
B. Fishing
C. Whaling
D. Blackmailing
7. When assessing the performance of your organization during a disaster recovery drill, which is the highest priority?
A. Safeguarding sensitive assets
B. Notifying the appropriate authorities
C. Preventing looting and vandalism
D. Protection of life
8. Which of the following is true about vulnerability remediation after an organizational security assessment?
A. All vulnerabilities uncovered must be remediated as soon as possible.
B. It entails applying patches to all vulnerable software systems.
C. Properly done, it should never impact the business.
D. It requires the support of everyone from the very top of the organization.
9. Which of the following is true of management reviews?
A. They happen periodically and include results of audits as a key input.
B. They happen in an ad hoc manner as the needs of the organization dictate.
C. They are normally conducted by mid-level managers, but their reports are presented to the key business leaders.
D. They are focused on assessing the management of the information systems.

↟Chapter 19: Measuring Security

Answers
1. C. Key performance indicators (KPIs) are indicators that are particularly significant in showing the performance of an ISMS compared to its stated goals. Because every KPI is a metric, answer B (the partial definition of a metric) would also be correct but would not be the best answer since it leaves out the significance and purpose of the metric.
2. C. Key risk indicators (KRIs) allow managers to understand when specific activities of the organization are moving it toward a higher level of risk. They are useful to understanding changes and managing the overall risk.
3. B. If the organization was intentionally attempting to protect the privacy of its user, suspension of the account would be a poor privacy measure compared to outright deletion.
4. B. The verification of data backups should focus on assessing the organization’s ability to respond to the threats identified during the threat modeling and risk management processes. If the organization can’t respond to these threats, then its backups may be useless.

5. A. Security training is the process of teaching a skill or set of skills that will
enable people to perform specific functions better. Security awareness training, on the other hand, is the process of exposing people to security issues so that they
are able to recognize and respond to them better. Security training is typically provided to security personnel, while security awareness training should be provided to every member of the organization.
6. B. The correct term for social engineering conducted over digital communications
means is phishing, not fishing.
7. D. In any situation where loss or harm to human lives is a possible outcome, protection of life is the top priority. The other options are all part of a disaster
recovery process, but are never the top priority.

9. A. Management reviews work best when they are regularly scheduled events involving the key organizational leaders, because this allows the subordinate leaders to plan and conduct the assessments, such as audits that provide inputs to the review.

PART VI

8. D. Because most remediations will have some impact on the business, they require
the support of everyone. This is particularly true of organizational (as opposed to system-specific) assessments because not all vulnerabilities will involve just a
software patch.

↟This page intentionally left blank

↟PART VII

Security Operations
Chapter 20
Chapter 21
Chapter 22
Chapter 23

Managing Security Operations
Security Operations
Security Incidents
Disasters

↟This page intentionally left blank

↟20

CHAPTER

Managing Security
Operations
This chapter presents the following:

• Foundational security operations concepts
• Change management processes
• Configuration management
• Resource protection
• Patch and vulnerability management
• Physical security management
• Personnel safety and security

Management is keeping the trains running on time.
—Andy Dunn

Security operations is a broad field, but the image that comes to many of our minds when we hear the term is a security operations center (SOC) where analysts, threat hunters, and incident responders fight off cyberthreats day in and day out. That is, in fact, an important aspect of security operations, but it isn't the complete scope. A lot of other work goes into ensuring our spaces are protected, our systems are optimized, and our people are doing the right things. This chapter covers many of the issues that we, as security leaders, must tackle to create a secure operational environment for our organizations. Security operations is the business of managing security. It may not be as exciting as hunting down a threat actor in real time, but it is just as important.

Foundational Security Operations Concepts

Security operations revolves around people much more than around computers and networks. A good chunk of our jobs as CISSPs is to lead security teams who prevent teams of attackers from causing us harm; our computers and networks are just the battlefields

on which these groups fight each other. Sometimes, it is our own teammates who can become the enemy, either deliberately or through carelessness. So, we can't really manage security operations without first understanding the roles we need our teammates to fill and the ways in which we keep the people filling those roles honest.

Table 20-1 shows some of the common IT and security roles within organizations and their corresponding job definitions. Each role needs to have a completed and welldefined job description. Security personnel should use these job descriptions when assigning access rights and permissions in order to ensure that individuals have access only to those resources needed to carry out their tasks.

Table 20-1 contains just a few roles with a few tasks per role. Organizations

should
create a complete list of roles used within their environment, with each role's associated
tasks and responsibilities. This should then be used by data owners and security personnel
when determining who should have access to specific resources and the type of access. A
clear and unambiguous understanding of roles and responsibilities across the organization
is critical to managing security. Without it, ensuring that everyone has the right access
they need for their jobs, and no more, becomes very difficult. In the sections that follow
we look at other foundational concepts we all need to be able to apply to our security
operations.

Organizational Role	Core Responsibilities
Cybersecurity Analyst	Monitors the organization's IT infrastructure and identifies and evaluates threats that could result in security incidents
Help Desk/Support	Resolves end-user and system technical or operations problems
Incident Responder	Investigates, analyzes, and responds to cyber incidents within the organization
IT Engineer	Performs the day-to-day operational duties on systems and applications
Network Administrator	Installs and maintains the local area network/wide area network (LAN/WAN) environment
Security Architect	Assesses security controls and recommends and implements enhancements
Security Director	Develops and enforces security policies and processes to maintain the security and safety of all organizational assets

Security Manager

Implements security policies and monitors security operations

Software Developer

Develops and maintains production software

System Administrator

Installs and maintains specific systems (e.g., database, e-mail)

Threat Hunter

Proactively finds cybersecurity threats and mitigates them before they compromise the organization

Table 20-1 Roles and Associated Tasks

SecOps

In many organizations the security and IT operations teams become misaligned because their responsibilities have different (and oftentimes conflicting) focuses.

The operations staff is responsible for ensuring systems are operational, highly available, performing well, and providing users with the functionality they need. As new technology becomes available, they come under pressure by business leaders to deploy it as soon as possible to improve the organization's competitiveness. But many times this focus on operations and user functionality comes at the cost of security. Security mechanisms commonly decrease performance, delay provisioning, and reduce the functionality available to the users.

The conflicts between the priorities and incentives of the IT operations and security teams can become dysfunctional in many organizations. Many of us have witnessed the finger pointing and even outright hostility that can crop up when things go wrong. A solution that is catching on is SecOps (Security + Operations), which is the integration of security and IT operations people, technology, and processes to reduce risks while improving business agility. The goal is to create a culture in which security is baked into the entire life cycle of every system and process in the organization. This is accomplished by building multifunctional teams where, for instance, a cloud system administrator and a cloud security engineer work together under the leadership of a manager who is responsible for delivering agile and secure functionality to the organization.

Accountability

PART VII

Users’ access to resources must be limited and properly controlled to ensure that excessive privileges do not provide the opportunity to cause damage to an organization and its resources. Users’ access attempts and activities while using a resource need to be properly monitored, audited, and logged. The individual user ID needs to be included in the audit logs to enforce individual responsibility. Each user should understand his responsibility when using organizational resources and be accountable for his actions.
Capturing and monitoring audit logs helps determine if a violation has actually occurred or if system and software reconfiguration is needed to better capture only the activities that fall outside of established boundaries. If user activities were not captured and reviewed, it would be very hard to determine if users have excessive privileges or if there has been unauthorized access.
Auditing needs to take place in a routine manner. Also, security analysts and managers need to review audit and log events. If no one routinely looks at the output, there really is no reason to create logs. Audit and function logs often contain too much cryptic or mundane information to be interpreted manually. This is why products and services are available that parse logs for organizations and report important findings. Logs should be monitored and reviewed, through either manual or automatic methods, to uncover suspicious activity and to identify an environment that is shifting away from its original

baselines. This is how administrators can be warned of many problems before they become too big and out of control.
When reviewing events, administrators need to ask certain questions that pertain to the users, their actions, and the current level of security and access:

- Are users accessing information and performing tasks that are not necessary for their job description? The answer indicates whether users’ rights and permissions need to be reevaluated and possibly modified.
- Are repetitive mistakes being made? The answer indicates whether users need to have further training.
- Do too many users have rights and privileges to sensitive or restricted data or resources?
The answer indicates whether access rights to the data and resources need to

be reevaluated, whether the number of individuals accessing them needs to be reduced, and/or whether the extent of their access rights should be modified.

Need-to-Know/Least Privilege

Least privilege (one of the secure design principles introduced in Chapter 9) means an individual should have just enough permissions and rights to fulfill her role in the organization and no more. If an individual has excessive permissions and rights, it could open the door to abuse of access and put the organization at more risk than is necessary. For example, if Dusty is a technical writer for a company, he does not necessarily need to have access to the company's source code. So, the mechanisms that control Dusty's access to resources should not let him access source code.

Another way to protect resources is enforcing need to know, which means we must first establish that an individual has a legitimate, job role–related need for a given resource.

Least privilege and need to know have a symbiotic relationship. Each user should have a need to know about the resources that she is allowed to access. If Mikela does not have a need to know how much the company paid last year in taxes, then her system rights should not include access to these files, which would be an example of exercising least privilege. The use of identity management software that combines traditional directories; access control systems; and user provisioning within servers, applications, and systems is becoming the norm within organizations. This software provides the capabilities to ensure that only specific access privileges are granted to specific users, and it often includes advanced audit functions that can be used to verify compliance with legal and regulatory directives.

Separation of Duties and Responsibilities

The objective of separation of duties (another of the secure design principles introduced in Chapter 9) is to ensure that one person acting alone cannot compromise the organization's security in any way. High-risk activities should be broken up into different parts and distributed to different individuals or departments. That way, the organization does not need to put a dangerously high level of trust in certain individuals. For fraud to take place, collusion would need to be committed, meaning more than one person would have to be

involved in the fraudulent activity. Separation of duties, therefore, is a preventive measure that requires collusion to occur for someone to commit an act that is against policy.

Separation of duties helps prevent mistakes and minimize conflicts of interest that can take place if one person is performing a task from beginning to end. For instance, a programmer should not be the only one to test her own code. Another person with a different job and agenda should perform functionality and integrity testing on the programmer's code, because the programmer may have a focused view of what the program is supposed to accomplish and thus may test only certain functions and input values, and only in certain environments.

Another example of separation of duties is the difference between the functions of a computer user and the functions of a security administrator. There must be clearcut lines drawn between system administrator duties and computer user duties. These will vary from environment to environment and will depend on the level of security required within the environment. System and security administrators usually have the responsibility of installing and configuring software, performing backups and recovery procedures, setting permissions, adding and removing users, and developing user profiles.

The computer user, on the other hand, may set or change passwords, create/edit/delete files, alter desktop configurations, and modify certain system parameters. The user should not be able to modify her own security profile, add and remove users globally, or make critical access decisions pertaining to network resources. This would breach the concept of separation of duties.

Privileged Account Management

Separation of duties also points to the need for privileged account management processes that formally enforce the principle of least privilege. A privileged account is one with elevated rights. When we hear this term, we usually think of system administrators, but it is important to consider that privileges often are gradually attached to user accounts for legitimate reasons but never reviewed again to see if they're still needed. In some cases, regular users end up racking up significant (and risky) permissions without anyone being aware of it (known as authorization creep).

More commonly, you will hear this concept under the label of privileged account management (PAM) because many organizations have very granular, role-based access controls. PAM consists of the policies and technologies used by an organization to control elevated (or privileged) access to any asset. It consists of processes for addressing the needs for individual elevated privileges, periodically reviewing those needs, reducing them to least privilege when appropriate, and documenting the whole thing.

Job rotation means that, over time, more than one person fulfills the tasks of one position within the organization. This enables the organization to have more than one person who understands the tasks and responsibilities of a specific job title, which provides backup and redundancy if a person leaves the organization or is absent. Job rotation also helps identify fraudulent activities, and therefore can be considered a detective type

PART VII

Job Rotation

of control. If Keith has performed David's position, Keith knows the regular tasks and routines that must be completed to fulfill the responsibilities of that job. Thus, Keith is better able to identify whether David does something out of the ordinary and suspicious.

A related practice is mandatory vacations. Chapter 1 touched on reasons to make sure employees take their vacations. Reasons include being able to identify fraudulent activities and enabling job rotation to take place. If an accounting employee has been performing a "salami attack" by shaving off pennies from multiple accounts and putting the money into his own account, the employee's company would have a better chance of figuring this out if that employee is required to take a vacation for a week or longer. When the employee is on vacation, another employee has to fill in. She might uncover questionable documents and clues of previous activities, or the company may see a change in certain patterns once the employee who is committing fraud is gone for a week or two. It is best for auditing purposes if the employee takes two contiguous weeks off from

work, which allows more time for fraudulent evidence to appear. Again, the idea behind
mandatory vacations is that, traditionally, those employees who have committed fraud
are usually the ones who have resisted going on vacation because of their fear of being
found out while away.

Service Level Agreements

As we discussed briefly in Chapter 2, a service level agreement (SLA) is a contractual
agreement that states that a service provider guarantees a certain level of service. For
example, a web server will be down for no more than 52 minutes per year (which is
approximately a 99.99 percent availability). SLAs help service providers, whether they
are an internal IT operation or an outsourcer, decide what type of availability
technology is appropriate. From this determination, the price of a service or the budget of the
IT operation can be set. Most frequently, organizations use SLAs with external service
providers to guarantee specific performance and, if it is not delivered, to penalize (usually
monetarily) the vendor.

The process of developing an internal SLA (that is, one between the IT operations
team and one or more internal departments) can also be beneficial to an organization. For
starters, it drives a deeper conversation between IT and whoever is requesting the service.
This alone can help both sides get a clearer understanding of the opportunities and threats
the service brings with it. The requestor will then better understand the tradeoffs between
service levels and costs and be able to negotiate the most cost-effective service with the
IT team. The IT team can then use this dialogue to justify resources such as budget or
staffing. Finally, internal SLAs allow all parties to know what “right” looks like.

Whether the SLA is internal or external, the organization must collect metrics to
determine whether or not it is being met. After all, if nobody measures the service,
what’s the point of requiring a certain level of it? Identifying these metrics, in and
of itself, allows the organization to determine whether a particular requirement is
important or not. If both parties are having a hard time figuring out how much
scheduled downtime is acceptable, that requirement probably doesn’t need to be
included in the SLA.

Change Management

The Greek philosopher Heraclitus said that “the only constant in life is change,” and most of us would agree with him, especially when it comes to IT and security operations in our organizations. Change is needed to remain relevant and competitive, but it can bring risks that we must carefully manage. Change management, from an IT perspective, is the practice of minimizing the risks associated with the addition, modification, or removal of anything that could have an effect on IT services. This includes obvious IT actions like adding new software applications, segmenting LANs, and retiring network services. But it also includes changes to policies, procedures, staffing, and even facilities. Consequently, any change to security controls or practices probably falls under the umbrella of change management.

Change Management Practices

Well-structured change management practices are essential to minimizing the risks of changes to an environment. The process of devising these practices should include representatives for all stakeholders, so it shouldn’t just be limited to IT and security staff.

Most organizations that follow this process formally establish a group that is responsible for approving changes and overseeing the activities of changes that take place within the organization. This group can go by one of many names, but for this discussion we will refer to it as the change advisory board (CAB).

The CAB and change management practices should be laid out in the change management policy. Although the types of changes vary, a standard list of procedures can help keep the process under control and ensure it is carried out in a predictable manner.

The following steps are examples of the types of procedures that should be part of any change management policy:

• Request for a change to take place The individual requesting the change must do so in writing, justify the reasons, clearly show the benefits and possible pitfalls of (that is, risk introduced by) the change. The Request for Change (RFC) is the standard document for doing this and contains all information required to approve a change.

• Evaluate the change The CAB reviews the RFC and analyzes its potential

impacts across the entire organization. Sometimes the requester is asked to conduct more research and provide more information before the change is approved. The CAB then completes a change evaluation report and designates the individual or team responsible for planning and implementing the change.
• Plan the change Once the change is approved, the team responsible for implementing it gets to work planning the change. This includes figuring out all the details of how the change interfaces with other systems or processes, developing
a timeline, and identifying specific actions to minimize the risks. The change must
also be fully tested to uncover any unforeseen results. Regardless of how well we test,
there is always a chance that the change will cause an unacceptable loss or outage, so
every change request should also have a rollback plan that restores the system to the
last known-good configuration.

• Implementation Once the change is planned and fully tested, it is implemented and integrated into any other affected processes and systems. This may include reconfiguring other systems, changing or developing policies and procedures, and providing training for affected staff. These steps should be fully documented and
progress should be monitored.
• Review the change Once the change is implemented, it is brought back to the CAB for a final review. During this step, the CAB verifies that the change was implemented as planned, that any unanticipated consequences have been properly addressed, and that the risks remain within tolerable parameters.
• Close or sustain Once the change is implemented and reviewed, it should be entered into a change log. A full report summarizing the change may also be submitted to management, particularly for changes with large effects across the organization.
These steps, of course, usually apply to large changes that take place within an organization. These types of changes are typically expensive and can have lasting effects
on an organization. However, smaller changes should also go through some type of change control process. If a server needs to have a patch applied, it is not good practice
to have an engineer just apply it without properly testing it on a nonproduction server,
without having the approval of the IT department manager or network administrator, and
without having backup and backout plans in place in case the patch causes some negative
effect on the production server. Of course, these changes still need to be documented.
For this reason, ITIL 4 (introduced in Chapter 4) specifies three types of changes that
follow the same basic process but tailored for specific situations:

• Standard changes Preauthorized, low-risk changes that follow a well-known

procedure. Examples include patching a server or adding memory or storage to it.
• Emergency changes Changes that must be implemented immediately.
Examples include implementing a security patch for a zero-day exploit or
isolating the network from a DDoS attack.
• Normal changes All other changes that are not standard changes or
emergency changes. Examples include adding a server that will provide new
functionality or introducing a new application to (or removing a legacy one
from) the golden image.
Regardless of the type of change, it is critical that the operations department
create
approved backout plans before implementing changes to systems or the network. It
is
very common for changes to cause problems that were not properly identified
before the
implementation process began. Many network engineers have experienced the
headaches
of applying poorly developed “fixes” or patches that end up breaking something
else in
the system. Developing a backout plan ensures productivity is not negatively
affected by
these issues. This plan describes how the team will restore the system to its
original state
before the change was implemented.

Change Management Documentation
Failing to document changes to systems and networks is only asking for trouble,
because
no one will remember, for example, what was done to that one server in the
demilitarized
zone (DMZ) six months ago or how the main router was fixed when it was acting up
last year. Changes to software configurations and network devices take place
pretty often
in most environments, and keeping all of these details properly organized is
impossible,
unless someone maintains a log of this type of activity.
Numerous changes can take place in an organization, some of which are as
follows:

• New computers installed
• New applications installed
• Different configurations implemented
• Patches and updates installed
• New technologies integrated
• Policies, procedures, and standards updated
• New regulations and requirements implemented
• Network or system problems identified and fixes implemented
• Different network configurations implemented
• New networking devices integrated into the network
• Company acquired by, or merged with, another company
The list could go on and on and could be general or detailed. Many organizations

have
experienced some major problem that affects the network and employee
productivity.
The IT department may run around trying to figure out the issue and go through
hours
or days of trial-and-error exercises to find and apply the necessary fix. If no
one properly
documents the incident and what was done to fix the issue, the organization may
be
doomed to repeat the same scramble six months to a year down the road.

Configuration Management
PART VII

At every point in the O&M part of assets' life cycles (which we discussed in
Chapter 5),
we need to also ensure that we get (and keep) a handle on how these assets are
configured. Sadly, most default configurations are woefully insecure. This means
that if we do
not configure security when we provision new hardware or software, we are
virtually
guaranteeing successful attacks on our systems. Configuration management (CM) is
the
process of establishing and maintaining consistent configurations on all our
systems to
meet organizational requirements.
Configuration management processes vary among organizations but have certain
elements in common. Virtually everyone that practices it starts off by defining
and
establishing organization-wide agreement on the required configurations for all
systems
in the scope of the effort. At a minimum, this should include the users'
workstations

and all business-critical systems. These configurations are then applied to all
systems.
There will be exceptions, of course, and special requirements that lead to
nonstandard
configurations, which need to be approved by the appropriate individuals and
documented. There will also be changes over time, which should be dealt with
through
the change management practices defined in the previous section. Finally,
configurations
need to be periodically audited to ensure continued compliance with them.

Baselining
A baseline is the configuration of a system at a point in time as agreed upon by
the appropriate decision makers. For a typical user workstation, a baseline
defines the software
that is installed (both operating system and applications), policies that are
applied (e.g.,

disabling USB thumb drives), and any other configuration setting such as the domain name, DNS server address, and many others. Baselining allows us to build a system once, put it through a battery of tests to ensure it works as expected, and then provision it out consistently across the organization.

In a perfect world, all systems that provide the same functionality are configured identically. This makes it easier to manage them throughout their life cycles. As we all know, however, there are plenty of exceptions in the real world. System configuration exceptions often have perfectly legitimate business reasons, so we can't just say "no" to exception requests and keep our lives simple. The system baseline allows us to narrow down what makes these exceptional systems different. Rather than document every single configuration parameter again (which could introduce errors and omissions), all we have to do is document what is different from a given baseline.

Baselines do more than simply tell us what systems (should) look like at a given point in time; they also document earlier configuration states for those systems. We want to keep old baselines around because they tell the story of how a system evolved. Properly annotated, baselines tell us not only the "what" but also the "why" of configurations over time.

A related concept to baselining is the golden image, which is a preconfigured, standard template from which all user workstations are provisioned. A golden image is known by many other names including gold master, clone image, master image, and base image. Whatever name you use, it saves time when provisioning systems because all you have to do is clone the image onto a device, enter a handful of parameters unique to the system (such as the hostname), and it's ready for use. Golden images also improve security by consistently applying security controls to every cloned system. Another advantage is a reduction in configuration errors, which also means a lower risk of inadvertently introduced vulnerabilities.

Provisioning

We already addressed secure provisioning in Chapter 5 but the topic bears revisiting in the context of configuration management. Recall that provisioning is the set of all activities required to provide one or more new information services to a