to security
administrator

Central antivirus
signature update
engine

Push updated
signatures to
all servers and
workstations

Fails to
provide
adequate,
timely
protection
against
malware

Central
server
goes
down

Individual
Network is
node’s antivirus infected with
software is not malware
updated

Central
server can
be infected
and/or
infect other
systems

Heartbeat
status check
sent to central
console,
and e-mail
to network
administrator

Fire suppression
water pipes

Suppress fire
in building
1 in 5 zones

Fails to

close

Water
in pipes
freezes

None

Fire
suppression
system pipes
break

Suppression
sensors tied
directly into
fire system
central console

Etc.
Table 2-2 How an FMEA Can Be Carried Out and Documented

Building 1
has no
suppression
agent
available

System

Failure
Detection
Method

Fault Tree Analysis
While FMEA is most useful as a survey method to identify major failure modes in a
given system, the method is not as useful in discovering complex failure modes that may
be involved in multiple systems or subsystems. A fault tree analysis usually proves to be
a more useful approach to identifying failures that can take place within more complex
environments and systems. First, an undesired effect is taken as the root or top

event of
a tree of logic. Then, each situation that has the potential to cause that effect is added to
the tree as a series of logic expressions. Fault trees are then labeled with actual numbers
pertaining to failure probabilities. This is typically done by using computer programs
that can calculate the failure probabilities from a fault tree.
Figure 2-3 shows a simplistic fault tree and the different logic symbols used to represent
what must take place for a specific fault event to occur.
When setting up the tree, you must accurately list all the threats or faults that can occur
within a system. The branches of the tree can be divided into general categories, such
as physical threats, network threats, software threats, Internet threats, and component
failure threats. Then, once all possible general categories are in place, you can trim
them and effectively prune from the tree the branches that won’t apply to the system in
question. In general, if a system is not connected to the Internet by any means, remove
that general branch from the tree.

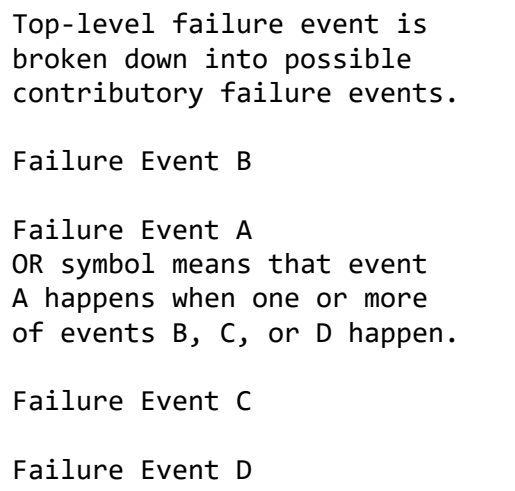


Figure 2-3 Fault tree and logic components

PART I

FMEA is used in assurance risk management because of the level of detail, variables, and

complexity that continues to rise as corporations understand risk at more granular levels.
This methodical way of identifying potential pitfalls is coming into play more as the need for risk awareness—down to the tactical and operational levels—continues to expand.

Some of the most common software failure events that can be explored through a fault tree analysis are the following:

- False alarms
- Insufficient error handling
- Sequencing or order
- Incorrect timing outputs
- Valid but unexpected outputs

Of course, because of the complexity of software and heterogeneous environments, this is a very small sample list.
EXAM TIP A risk assessment is used to gather data. A risk analysis examines the gathered data to produce results that can be acted upon.

Risk Analysis Approaches
So up to this point, we have accomplished the following items:

- Developed a risk management policy
- Developed a risk management team
- Identified organizational assets to be assessed
- Calculated the value of each asset
- Identified the vulnerabilities and threats that can affect the identified assets
- Chosen a risk assessment methodology that best fits our needs

The next thing we need to figure out is if our risk analysis approach should be quantitative or qualitative in nature. A quantitative risk analysis is used to assign monetary and numeric values to all elements of the risk analysis process. Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks. It is more of a scientific or mathematical approach (objective) to risk analysis compared to qualitative. A qualitative risk analysis uses a “softer” approach to the data elements of a risk analysis. It does not quantify that data, which means that it does not assign numeric values to the data so that it can be used in equations. As an example, the results of a quantitative risk analysis could be that the organization is at risk of losing $100,000 if a buffer

overflow were
exploited on a web server, $25,000 if a database were compromised, and $10,000 if a
file server were compromised. A qualitative risk analysis would not present these findings
in monetary values, but would assign ratings to the risks, as in Red, Yellow, and Green.
A quantitative analysis uses risk calculations that attempt to predict the level of
monetary losses and the probability for each type of threat. Qualitative analysis does not

Automated Risk Analysis Methods
Collecting all the necessary data that needs to be plugged into risk analysis equations
and properly interpreting the results can be overwhelming if done manually. Several
automated risk analysis tools on the market can make this task much less painful and,
hopefully, more accurate. The gathered data can be reused, greatly reducing the time
required to perform subsequent analyses. The risk analysis team can also print reports
and comprehensive graphs to present to management.
EXAM TIP Remember that vulnerability assessments are different from risk assessments. A vulnerability assessment just finds the vulnerabilities (the holes). A risk assessment calculates the probability of the vulnerabilities being exploited and the associated business impact.

The objective of these tools is to reduce the manual effort of these tasks, perform
calculations quickly, estimate future expected losses, and determine the effectiveness and
benefits of the security countermeasures chosen. Most automatic risk analysis products
port information into a database and run several types of scenarios with different
parameters to give a panoramic view of what the outcome will be if different threats
come to bear. For example, after such a tool has all the necessary information inputted,
it can be rerun several times with different parameters to compute the potential outcome
if a large fire were to take place; the potential losses if a virus were to damage 40 percent
of the data on the main file server; how much the organization would lose if an attacker
were to steal all the customer credit card information held in three databases; and so on.
Running through the different risk possibilities gives an organization a more

detailed
understanding of which risks are more critical than others, and thus which ones to
address first.

Steps of a Quantitative Risk Analysis
If we choose to carry out a quantitative risk analysis, then we are going to use mathematical equations for our data interpretation process. The most common equations used for
this purpose are the single loss expectancy (SLE) and the annualized loss expectancy (ALE).
The SLE is a monetary value that is assigned to a single event that represents the organization's potential loss amount if a specific threat were to take place. The equation is laid
out as follows:
Asset Value × Exposure Factor (EF) = SLE

use calculations. Instead, it is more opinion and scenario based (subjective) and uses a
rating system to relay the risk criticality levels.
Quantitative and qualitative approaches have their own pros and cons, and each applies
more appropriately to some situations than others. An organization's management and
risk analysis team, and the tools they decide to use, will determine which approach is best.
In the following sections we will dig into the depths of quantitative analysis and then
revisit the qualitative approach. We will then compare and contrast their attributes.

The exposure factor (EF) represents the percentage of loss a realized threat could have
on a certain asset. For example, if a data warehouse has the asset value of $150,000, it can
be estimated that if a fire were to occur, 25 percent of the warehouse would be damaged,
in which case the SLE would be $37,500:
Asset Value ($150,000) × Exposure Factor (25%) = $37,500
This tells us that the organization could potentially lose $37,500 if a fire were to take
place. But we need to know what our annual potential loss is, since we develop and use
our security budgets on an annual basis. This is where the ALE equation comes into play.
The ALE equation is as follows:
SLE × Annualized Rate of Occurrence (ARO) = ALE
The annualized rate of occurrence (ARO) is the value that represents the estimated

frequency of a specific threat taking place within a 12-month timeframe. The range can be from 0.0 (never) to 1.0 (once a year) to greater than 1 (several times a year), and anywhere in between. For example, if the probability of a fire taking place and damaging our data warehouse is once every 10 years, the ARO value is 0.1.

So, if a fire within an organization's data warehouse facility can cause $37,500 in damages, and the frequency (or ARO) of a fire taking place has an ARO value of 0.1 (indicating once in 10 years), then the ALE value is $3,750 ($37,500 × 0.1 = $3,750).

The ALE value tells the organization that if it wants to put in controls to protect the asset (warehouse) from this threat (fire), it can sensibly spend $3,750 or less per year to provide the necessary level of protection. Knowing the real possibility of a threat and how much damage, in monetary terms, the threat can cause is important in determining how much should be spent to try and protect against that threat in the first place. It would not make good business sense for the organization to spend more than $3,750 per year to protect itself from this threat.

Clearly, this example is overly simplistic in focusing strictly on the structural losses. In the real world, we should include other related impacts such as loss of revenue due to the disruption, potential fines if the fire was caused by a violation of local fire codes, and injuries to employees that would require medical care. The number of factors to consider can be pretty large and, to some of us, not obvious. This is why you want to have a diverse risk assessment team that can think of all the myriad impacts that a simple event might have.

Uncertainty

In risk analysis, uncertainty refers to the degree to which you lack confidence in an estimate. This is expressed as a percentage, from 0 to 100 percent. If you have a 30 percent confidence level in something, then it could be said you have a 70 percent uncertainty level. Capturing the degree of uncertainty when carrying out a risk analysis is important, because it indicates the level of confidence the team and management should have in the resulting figures.

Threat

Single Loss Expectancy (SLE)

Annualized Rate of Occurrence (ARO)

Annualized Loss Expectancy (ALE)

Facility

Fire

$230,000

0.1

$23,000

Trade secret

Stolen

$40,000

0.01

$400

File server

Failed

$11,500

0.1

$1,150

Business data

Ransomware

$283,000

0.1

$28,300

Customer credit card info

Stolen

$300,000

3.0

$900,000

Table 2-3 Breaking Down How SLE and ALE Values Are Used

Now that we have all these numbers, what do we do with them? Let’s look at the example in Table 2-3, which shows the outcome of a quantitative risk analysis. With this data, the organization can make intelligent decisions on what threats must be addressed first because of the severity of the threat, the likelihood of it happening, and how much could be lost if the threat were realized. The organization now also knows how much money it should spend to protect against each threat. This will result in good business decisions, instead of just buying protection here and there without a clear understanding of the big picture. Because the organization’s risk from a ransomware incident is $28,300, it would be justified in spending up to this amount providing ransomware preventive measures such as offline file backups, phishing awareness training, malware detection and prevention, or insurance.

When carrying out a quantitative analysis, some people mistakenly think that the process is purely objective and scientific because data is being presented in numeric values. But a purely quantitative analysis is hard to achieve because there is still some subjectivity when it comes to the data. How do we know that a fire will only take place once every 10 years? How do we know that the damage from a fire will be 25 percent of the value of the asset? We don’t know these values exactly, but instead of just pulling them out of thin air, they should be based upon historical data and industry experience.

In quantitative risk analysis, we can do our best to provide all the correct information, and by doing so we will come close to the risk values, but we cannot predict the future and how much future incidents will cost us or the organization.

Results of a Quantitative Risk Analysis

The risk analysis team should have clearly defined goals. The following is a short list of what generally is expected from the results of a risk analysis:

• Monetary values assigned to assets
• Comprehensive list of all significant threats
• Probability of the occurrence rate of each threat
• Loss potential the organization can endure per threat in a 12-month time span
• Recommended controls

PART I

Asset

Although this list looks short, there is usually an incredible amount of detail under each bullet item. This report will be presented to senior management, which will be concerned with possible monetary losses and the necessary costs to mitigate these risks. Although the report should be as detailed as possible, it should also include an executive summary so that senior management can quickly understand the overall findings of the analysis.

Qualitative Risk Analysis
Another method of risk analysis is qualitative, which does not assign numbers and monetary values to components and losses. Instead, qualitative methods walk through different scenarios of risk possibilities and rank the seriousness of the threats and the validity of the different possible countermeasures based on opinions. (A wide-sweeping analysis can include hundreds of scenarios.) Qualitative analysis techniques include judgment, best practices, intuition, and experience. Examples of qualitative techniques to gather data are Delphi, brainstorming, storyboarding, focus groups, surveys, questionnaires, checklists, one-on-one meetings, and interviews. The risk analysis team will determine the best technique for the threats that need to be assessed, as well as the culture of the organization and individuals involved with the analysis.
The team that is performing the risk analysis gathers personnel who have knowledge of the threats being evaluated. When this group is presented with a scenario that describes threats and loss potential, each member responds with their gut feeling and experience on the likelihood of the threat and the extent of damage that may result. This group explores a scenario of each identified vulnerability and how it would be exploited. The "expert" in the group, who is most familiar with this type of threat, should review the

scenario to ensure it reflects how an actual threat would be carried out. Safeguards that
would diminish the damage of this threat are then evaluated, and the scenario is played
out for each safeguard. The exposure possibility and loss possibility can be ranked as
high, medium, or low on a scale of 1 to 5 or 1 to 10.
A common qualitative risk matrix is shown in Figure 2-4. Once the selected personnel
rank the likelihood of a threat happening, the loss potential, and the advantages of each
Consequences
Likelihood

Insignificant

Minor

Moderate

Major

Severe

Almost certain

M

H

H

E

E

Likely

M

M

H

H

E

Possible

L

M

M

H

E

Unlikely

L

M

M

M

H

Rare

L

L

M

M

H

Figure 2-4 Qualitative risk matrix: likelihood vs. consequences (impact)

The Delphi technique is a group decision method used to ensure that each member gives an honest opinion of what he or she thinks the result of a particular threat will be. This avoids a group of individuals feeling pressured to go along with others' thought processes and enables them to participate in an independent and anonymous way. Each member of the group provides his or her opinion of a certain threat and turns it in to the team that is performing the analysis. The results are compiled and distributed to the group members, who then write down their comments anonymously and return them to the analysis group. The comments are compiled and redistributed for more comments until a consensus is formed. This method is used to obtain an agreement on cost, loss values, and probabilities of occurrence without individuals having to agree verbally.

safeguard, this information is compiled into a report and presented to

management to
help it make better decisions on how best to implement safeguards into the environment.
The benefits of this type of analysis are that communication must happen among team
members to rank the risks, evaluate the safeguard strengths, and identify weaknesses, and
the people who know these subjects the best provide their opinions to management.
Let’s look at a simple example of a qualitative risk analysis.
The risk analysis team presents a scenario explaining the threat of a hacker accessing
confidential information held on the five file servers within the organization. The risk
analysis team then distributes the scenario in a written format to a team of five people
(the IT manager, database administrator, application programmer, system operator,
and operational manager), who are also given a sheet to rank the threat’s severity, loss
potential, and each safeguard’s effectiveness, with a rating of 1 to 5, 1 being the least
severe, effective, or probable. Table 2-4 shows the results.

Threat = Hacker Accessing Confidential Information	Effectiveness of Firewall	Effectiveness of Intrusion Detection System	Effectiveness of Honeypot
4	4	3	2
4	4	3	4

1

2

3

3

4

2

1

System
operator

3

4

3

4

2

1

Operational
manager

5

4

4

4

4

2

Results

3.6

3.4

3.6

3.8

3

1.4

Severity
of Threat

Probability
of Threat
Taking Place

Potential
Loss to the
Organization

IT manager

4

2

Database
administrator

4

Application
programmer

Table 2-4 Example of a Qualitative Analysis

This data is compiled and inserted into a report and presented to management. When
management is presented with this information, it will see that its staff (or a chosen set)
feels that purchasing a firewall will protect the organization from this threat more than
purchasing an intrusion detection system (IDS) or setting up a honeypot system. This is the result of looking at only one threat, and management will view the severity,
probability, and loss potential of each threat so it knows which threats cause the greatest
risk and should be addressed first.

Quantitative vs. Qualitative
Each method has its advantages and disadvantages, some of which are outlined in

Table 2-5 for purposes of comparison.
The risk analysis team, management, risk analysis tools, and culture of the organization will dictate which approach—quantitative or qualitative—should be used. The goal of either method is to estimate an organization's real risk and to rank the severity of the threats so the correct countermeasures can be put into place within a practical budget.
Table 2-5 refers to some of the positive aspects of the quantitative and qualitative approaches. However, not everything is always easy. In deciding to use either a quantitative or qualitative approach, the following points might need to be considered.
Quantitative Cons:

- Calculations can be complex. Can management understand how these values were derived?
- Without automated tools, this process is extremely laborious.
- More preliminary work is needed to gather detailed information about the environment.
- Standards are not available. Each vendor has its own way of interpreting the processes and their results.

Attribute	Quantitative	Qualitative
Requires no calculations		X
Requires more complex calculations	X	
Involves high degree of guesswork		X
Provides general areas and indications of risk		X
Is easier to automate and evaluate	X	
Used in risk management performance tracking	X	
Allows for cost/benefit analysis	X	

Uses independently verifiable and objective metrics

X

Provides the opinions of the individuals who know the processes best
Shows clear-cut losses that can be accrued within one year’s time
Table 2-5 Quantitative vs. Qualitative Characteristics

X
X

Qualitative Cons:

NOTE Since a purely quantitative assessment is close to impossible and a purely qualitative process does not provide enough statistical data for financial decisions, these two risk analysis approaches can be used in a hybrid approach. Quantitative evaluation can be used for tangible assets (monetary values), and a qualitative assessment can be used for intangible assets (priority values).

Responding to Risks
Once an organization knows the amount of total and residual risk it is faced with, it must decide how to handle it. Risk can be dealt with in four basic ways: transfer it, avoid it, reduce it, or accept it.
Many types of insurance are available to organizations to protect their assets. If an organization decides the total risk is too high to gamble with, it can purchase insurance, which would transfer the risk to the insurance company.
If an organization decides to terminate the activity that is introducing the risk, this is known as risk avoidance. For example, if a company allows employees to use instant messaging (IM), there are many risks surrounding this technology. The company could decide not to allow any IM activity by employees because there is not a strong enough business need for its continued use. Discontinuing this service is an example of risk avoidance.
Another approach is risk mitigation, where the risk is reduced to a level considered acceptable enough to continue conducting business. The implementation of firewalls, training, and intrusion/detection protection systems or other control types represent types of risk mitigation efforts.
The last approach is to accept the risk, which means the organization

understands the
level of risk it is faced with, as well as the potential cost of damage, and decides to just
live with it and not implement the countermeasure. Many organizations will accept risk
when the cost/benefit ratio indicates that the cost of the countermeasure outweighs the
potential loss value.
A crucial issue with risk acceptance is understanding why this is the best approach
for a specific situation. Unfortunately, today many people in organizations are accepting
risk and not understanding fully what they are accepting. This usually has to do with
the relative newness of risk management in the security field and the lack of education
and experience in those personnel who make risk decisions. When business managers are
charged with the responsibility of dealing with risk in their department, most of the time

PART I

• The assessments and results are subjective and opinion based.
• Eliminates the opportunity to create a dollar value for cost/benefit discussions.
• Developing a security budget from the results is difficult because monetary values
are not used.
• Standards are not available. Each vendor has its own way of interpreting the processes and their results.

they will accept whatever risk is put in front of them because their real goals pertain to
getting a project finished and out the door. They don’t want to be bogged down by this
silly and irritating security stuff.
Risk acceptance should be based on several factors. For example, is the potential loss
lower than the countermeasure? Can the organization deal with the “pain” that will come
with accepting this risk? This second consideration is not purely a cost decision, but may
entail noncost issues surrounding the decision. For example, if we accept this risk, we
must add three more steps in our production process. Does that make sense for us? Or
if we accept this risk, more security incidents may arise from it, and are we prepared to
handle those?
The individual or group accepting risk must also understand the potential

visibility
of this decision. Let’s say a company has determined that it is not legally required
to protect customers’ first names, but that it does have to protect other items like
Social Security numbers, account numbers, and so on. So, the company ensures that
its current activities are in compliance with the regulations and laws, but what if its
customers find out that it is not protecting their full names and they associate this with
identity fraud because of their lack of education on the matter? The company may not
be able to handle this potential reputation hit, even if it is doing all it is supposed to be
doing. Perceptions of a company’s customer base are not always rooted in fact, but the
possibility that customers will move their business to another company is a potential
fact your company must comprehend.
Figure 2-5 shows how a risk management program can be set up, which ties together
many of the concepts covered thus far in this chapter.

PLAN
1. Identify team
2. Identify scope
3. Identify method
4. Identify tools
5. Understand acceptable
risk level

COLLECT INFORMATION
1. Identify assets
2. Assign value to assets
3. Identify vulnerabilities and threats
4. Calculate risks
5. Cost/benefit analysis
6. Uncertainty analysis

DEFINE
RECOMMENDATIONS
1. Risk mitigation
2. Risk transference
3. Risk acceptance
4. Risk avoidance

MANAGEMENT
RISK MITIGATION

RISK AVOIDANCE

Control selection
Implementation
Monitoring

Discontinue activity

RISK TRANSFERENCE

RISK ACCEPTANCE

Purchase insurance

Do nothing

Figure 2-5 How a risk management program can be set up

Total Risk vs. Residual Risk

threats × vulnerability × asset value = total risk
(threats × vulnerability × asset value) × controls gap = residual risk
You may also see these concepts illustrated as the following:
total risk – countermeasures = residual risk
NOTE The previous formulas are not constructs you can actually plug numbers into. They are instead used to illustrate the relation of the different items that make up risk in a conceptual manner. This means no multiplication or mathematical functions actually take place. It is a means of understanding what items are involved when defining either total or residual risk.

During a risk assessment, the threats and vulnerabilities are identified. The possibility of a vulnerability being exploited is multiplied by the value of the assets being assessed, which results in the total risk. Once the controls gap (protection the control cannot provide) is factored in, the result is the residual risk. Implementing countermeasures is a way of mitigating risks. Because no organization can remove all threats, there will always be some residual risk. The question is what level of risk the organization is willing to accept.

Countermeasure Selection and Implementation
Countermeasures are the means by which we reduce specific risks to acceptable levels.
This section addresses identifying and choosing the right countermeasures for computer systems. It gives the best attributes to look for and the different cost scenarios to investigate when comparing different types of countermeasures. The end product of the analysis of choices should demonstrate why the selected control is the most advantageous to the organization.

The reason an organization implements countermeasures is to reduce its overall risk to an acceptable level. As stated earlier, no system or environment is 100 percent secure, which means there is always some risk left over to deal with. This is called residual risk.
Residual risk is different from total risk, which is the risk an organization faces if it chooses not to implement any type of safeguard. An organization may choose to take on total risk if the cost/benefit analysis results indicate this is the best course of action. For example, if there is a small likelihood that an organization's web servers can be compromised and the necessary safeguards to provide a higher level of protection cost more than the potential loss in the first place, the organization will choose not to implement the safeguard, choosing to deal with the total risk.
There is an important difference between total risk and residual risk and which type of risk an organization is willing to accept. The following are conceptual formulas:

NOTE The terms control, countermeasure, safeguard, security mechanism, and protection mechanism are synonymous in the context of information systems security. We use them interchangeably.

Control Selection
A security control must make good business sense, meaning it is cost-effective (its benefit outweighs its cost). This requires another type of analysis: a cost/benefit analysis. A commonly used cost/benefit calculation for a given safeguard (control) is
(ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the organization
For example, if the ALE of the threat of a hacker bringing down a web server is $12,000 prior to implementing the suggested safeguard, and the ALE is $3,000 after implementing the safeguard, while the annual cost of maintenance and operation of the safeguard is $650, then the value of this safeguard to the organization is $8,350 each year.
Recall that the ALE has two factors, the single loss expectancy and the annual rate of occurrence, so safeguards can decrease either or both. The countermeasure referenced in the previous example could aim to reduce the costs associated with restoring the web server, or make it less likely that it is brought down, or both. All too often,

we focus our
attention on making the threat less likely, while, in some cases, it might be less expensive
to make it easier to recover.
The cost of a countermeasure is more than just the amount filled out on the purchase
order. The following items should be considered and evaluated when deriving the full
cost of a countermeasure:

- Product costs
- Design/planning costs
- Implementation costs
- Environment modifications (both physical and logical)
- Compatibility with other countermeasures
- Maintenance requirements
- Testing requirements
- Repair, replacement, or update costs
- Operating and support costs
- Effects on productivity
- Subscription costs
- Extra staff-hours for monitoring and responding to alerts

Types of Controls
In our examples so far, we've focused on countermeasures like firewalls and IDSs, but
there are many more options. Controls come in three main categories: administrative,
technical, and physical. Administrative controls are commonly referred to as
"soft controls" because they are more management oriented. Examples of administrative controls
are security documentation, risk management, personnel security, and training. Technical
controls (also called logical controls) are software or hardware components, as in firewalls,
IDS, encryption, and identification and authentication mechanisms. And physical controls

Many organizations have gone through the pain of purchasing new security products
without understanding that they will need the staff to maintain those products. Although
tools automate tasks, many organizations were not even carrying out these tasks before,
so they do not save on staff-hours, but many times require more hours. For example,
Company A decides that to protect many of its resources, purchasing an intrusion
detection system is warranted. So, the company pays $5,500 for an IDS. Is that

the
total cost? Nope. This software should be tested in an environment that is segmented
from the production environment to uncover any unexpected activity. After this testing
is complete and the security group feels it is safe to insert the IDS into its production
environment, the security group must install the monitoring management software, install the sensors, and properly direct the communication paths from the sensors to
the management console. The security group may also need to reconfigure the routers
to redirect traffic flow, and it definitely needs to ensure that users cannot access the IDS
management console. Finally, the security group should configure a database to hold all
attack signatures and then run simulations.
Costs associated with an IDS alert response should most definitely be considered.
Now that Company A has an IDS in place, security administrators may need additional
alerting equipment such as smartphones. And then there are the time costs associated
with a response to an IDS event.
Anyone who has worked in an IT group knows that some adverse reaction almost always takes place in this type of scenario. Network performance can take an unacceptable
hit after installing a product if it is an inline or proactive product. Users may no longer
be able to access a server for some mysterious reason. The IDS vendor may not have
explained that two more service patches are necessary for the whole thing to work
correctly. Staff time will need to be allocated for training and to respond to all of the
alerts (true or false) the new IDS sends out.
So, for example, the cost of this countermeasure could be $23,500 for the product
and licenses; $2,500 for training; $3,400 for testing; $2,600 for the loss in user
productivity once the product is introduced into production; and $4,000 in labor for
router reconfiguration, product installation, troubleshooting, and installation of the two
service patches. The real cost of this countermeasure is $36,000. If our total potential
loss was calculated at $9,000, we went over budget by 300 percent when applying this
countermeasure for the identified risk. Some of these costs may be hard or impossible to
identify before they are incurred, but an experienced risk analyst would account for many
of these possibilities.

are items put into place to protect facilities, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting. These control categories need to be put into place to provide defense-in-depth, which
is the coordinated use of multiple security controls in a layered approach, as shown
in Figure 2-6. A multilayered defense system minimizes the probability of successful
penetration and compromise because an attacker would have to get through several different types of protection mechanisms before she gained access to the critical assets.
For example, Company A can have the following physical controls in place that work in
a layered model:

- Fence
- Locked external doors
- Closed-circuit TV (CCTV)
- Security guard
- Locked internal doors
- Locked server room
- Physically secured computers (cable locks)

Potential threat

Virus scanners
Patch management
Rule-based access control
Account management
Secure architecture

Asset
Demilitarized zones (DMZs)
Firewalls
Virtual private networks (VPNs)
Policies and procedures
Physical security

Figure 2-6 Defense-in-depth

- Firewalls
- Intrusion detection system
- Intrusion prevention system
- Antimalware
- Access control
- Encryption

The types of controls that are actually implemented must map to the threats the

organization faces, and the number of layers that are put into place must map to the sensitivity of the asset. The rule of thumb is the more sensitive the asset, the more layers of protection that must be put into place.

So the different categories of controls that can be used are administrative, technical, and physical. But what do these controls actually do for us? We need to understand what the different control types can provide us in our quest to secure our environments.

The different types of security controls are preventive, detective, corrective, deterrent, recovery, and compensating. By having a better understanding of the different control types, you will be able to make more informed decisions about what controls will be best used in specific situations. The six different control types are as follows:

- Preventive Intended to avoid an incident from occurring
- Detective Helps identify an incident's activities and potentially an intruder
- Corrective Fixes components or systems after an incident has occurred
- Deterrent Intended to discourage a potential attacker
- Recovery Intended to bring the environment back to regular operations
- Compensating Provides an alternative measure of control

Once you understand fully what the different controls do, you can use them in the right locations for specific risks.

When looking at a security structure of an environment, it is most productive to use a preventive model and then use detective, corrective, and recovery mechanisms to help support this model. Basically, you want to stop any trouble before it starts, but you must be able to quickly react and combat trouble if it does find you. It is not feasible to prevent everything; therefore, what you cannot prevent, you should be able to quickly detect.

That's why preventive and detective controls should always be implemented together and should complement each other. To take this concept further: what you can't prevent, you should be able to detect, and if you detect something, it means you weren't able to prevent it, and therefore you should take corrective action to make sure it is indeed prevented the next time around. Therefore, all three types work together: preventive, detective, and corrective.

PART I

Technical controls that are commonly put into place to provide this type of layered

approach are

The control types described next (administrative, physical, and technical) are preventive in nature. These are important to understand when developing an enterprisewide security program. Obviously, these are only provided as illustrative examples.

Keep in mind as you go over them that a specific control may fall within multiple classifications. For example, most security cameras could be considered preventive (since they may dissuade criminals from breaking in if they are highly visible), detective (if there is a person monitoring them live), and corrective (if they are used to track a criminal that breached your physical perimeter).

Preventive: Administrative

- Policies and procedures
- Effective hiring practices
- Pre-employment background checks
- Controlled termination processes
- Data classification and labeling
- Security awareness

Preventive: Physical

- Badges, swipe cards
- Guards, dogs
- Fences, locks, mantraps

Preventive: Technical

- Passwords, biometrics, smart cards
- Encryption, secure protocols, call-back systems, database views, constrained user interfaces
- Antimalware software, access control lists, firewalls, IPS

Table 2-6 shows how these types of control mechanisms perform different security functions. Many students get themselves wrapped around the axle when trying to get their mind around which control provides which functionality. This is how this train of thought usually takes place: “A security camera system is a detective control, but if an attacker sees its cameras, it could be a deterrent.” Let’s stop right here. Do not make this any harder than it has to be. When trying to map the functionality requirement to a control, think of the main reason that control would be put into place. A firewall tries to prevent something bad from taking place, so it is a preventive control. Auditing logs is done after an event took place, so it is detective. A data backup system is

developed so
that data can be recovered; thus, this is a recovery control. Computer images are created
so that if software gets corrupted, they can be reloaded; thus, this is a corrective control.
Note that some controls can serve different functions. Security guards can deter would-be attackers, but if they don’t deter all of them, they can also stop (prevent)

Control Type:	Preventive	Detective	Corrective	Deterrent	Compensating
PART I					
Recovery					
Controls by Category:					
Physical					
Fences				X	
Locks	X				
Badge system		X			
Security guard			X		
Mantrap doors	X				

X

X

Lighting

X
X

Motion
detectors

X

Closed-circuit
TVs

X

Offsite facility
Administrative
Security policy

X

Monitoring and
supervising
Separation of
duties

X

X

X

X

Investigations
Security
awareness
training

X

X

Job rotation
Information
classification

X

X

X

Technical
ACLs

X

Encryption

X

Audit logs

X

IDS

X

Antimalware
software

X

X

Workstation
images
Smart cards

X
X

Data backup
Table 2-6 Control Categories and Types

X

the ones that try to get into a facility. Perhaps the attacker was particularly sneaky and
he managed to get into an office building, in which case the security guards can be
detective controls as they make the rounds and even corrective controls when they find
the intruder, call law enforcement, and escort the attacker out of the building and into
the backseat of a police car. When taking the CISSP exam, look for clues in the question
to determine which functionality is most relevant.
One control functionality that some people struggle with is a compensating control.

Let’s look at some examples of compensating controls to best explain their function.
If your organization needed to implement strong physical security, you might suggest to management that they employ security guards. But after calculating all the costs of security guards, your organization might decide to use a compensating (alternative) control that provides similar protection but is more affordable—as in a fence. In another example, let’s say you are a security administrator and you are in charge of maintaining the organization’s firewalls. Management tells you that a certain protocol that you know is vulnerable to exploitation has to be allowed through the firewall for business reasons.
The network needs to be protected by a compensating (alternative) control pertaining to this protocol, which may be setting up a proxy server for that specific traffic type to ensure that it is properly inspected and controlled. So a compensating control is just an alternative control that provides similar protection as the original control but has to be used because it is more affordable or allows specifically required business functionality.
Several types of security controls exist, and they all need to work together. The complexity of the controls and of the environment they are in can cause the controls to contradict each other or leave gaps in security. This can introduce unforeseen holes in the organization’s protection that are not fully understood by the implementers. An organization may have very strict technical access controls in place and all the necessary administrative controls up to snuff, but if any person is allowed to physically access any system in the facility, then clear security dangers are present within the environment.
Together, these controls should work in harmony to provide a healthy, safe, and productive environment.
The risk assessment team must evaluate the security controls’ functionality and effectiveness. When selecting a security control, some attributes are more favorable than others. Table 2-7 lists and describes attributes that should be considered before purchasing and committing to a security control.
Security controls can provide deterrence attributes if they are highly visible. This tells potential evildoers that adequate protection is in place and that they should move on to an easier target. Although the control may be highly visible, attackers should not be able to discover the way it works, thus enabling them to attempt to modify it, or

know how
to get around the protection mechanism. If users know how to disable the antimalware
program that is taking up CPU cycles or know how to bypass a proxy server to get to the
Internet without restrictions, they will do so.

Control Assessments
Once you select the administrative, technical, and physical controls that you think will
reduce your risks to acceptable levels, you have to ensure that this is actually the case.

Description	
Modular	The control can be installed or removed from an environment without adversely affecting other mechanisms.
Provides uniform protection	A security level is applied in a standardized method to all mechanisms the control is designed to protect.
Provides override functionality	An administrator can override the restriction if necessary.
Defaults to least privilege	When installed, the control defaults to a lack of permissions and rights instead of installing with everyone having full control.
Independence of control and the asset it is protecting	The given control can protect multiple assets, and a given asset can be protected by multiple controls.
Flexibility and security	The more security the control provides, the better. This functionality should come with flexibility, which enables you to choose different functions instead of all or none.
Usability	The control does not needlessly interfere with users' work.

Asset protection

The asset is still protected even if the countermeasure needs to be reset.

Easily upgraded

Software continues to evolve, and updates should be able to happen painlessly.

Auditing functionality

The control includes a mechanism that provides auditing at various levels of verbosity.

Minimizes dependence on other components

The control should be flexible and not have strict requirements about the environment into which it will be installed.

Must produce output in usable and understandable format

The control should present important information in a format easy for humans to understand and use for trend analysis.

Testable

The control should be able to be tested in different environments under different situations.

Does not introduce other compromises

The control should not provide any covert channels or back doors.

System and user performance

System and user performance should not be greatly affected by the control.

Proper alerting

The control should have the capability for thresholds to be set as to when to alert personnel of a security breach, and this type of alert should be acceptable.

Does not affect assets

The assets in the environment should not be adversely affected by the control.

Table 2-7 Characteristics to Consider When Assessing Security Controls

A control assessment is an evaluation of one or more controls to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome. Let’s look at each of those test elements in turn using anonymized examples from the real world.

PART I

Characteristic

You may have chosen the right control for a given risk, but you also need verification that the manner in which it is implemented is correct too. Let’s suppose you decide to upgrade a firewall to mitigate a number of risks you’ve identified. You invest a ton of money in the latest and greatest firewall and apply a bunch of rules to filter out the good from the bad. And yet, you forget to change the administrator’s default password, and an attacker is able to log into your firewall, lock out the security team by changing the password, and then change the rules to allow malicious traffic through. The technical control was good, it just wasn’t implemented correctly. You avoid this by developing a thorough set of tests that look at every aspect of the implementation and ensure no steps were skipped or done wrong.

Another aspect of verification is to ensure that the controls are operating as intended. You may have implemented the control correctly, but there are many reasons why it may not work as you expected it would. For example, suppose you implement a policy that all personnel in a facility must wear identification badges. Employees, contractors, and visitors each get their own unique badge design to differentiate them. The policy is implemented, and all staff are trained on it, but after a few weeks people get complacent and stop noticing whether they (or others) are wearing badges. The administrative control was properly implemented but is not working as intended. The control assessment should include operational checks, such as having different people (perhaps some who are well

known in the organization and some who are not part of it) walk through the facility
with no badges and see whether they are challenged or reported.
Finally, we want validation that the controls are producing the desired outcomes.
Controls are selected for the purpose of reducing risk…so are they? Suppose you install
temperature sensors in your data center that generate alarms whenever they get too hot.
You are trying to reduce the risk of hardware failures due to high temperatures. These
physical controls are properly installed and work as intended. In fact, they generate alarms
every day during peak usage hours. Are they reducing the risk? Unless you upgrade the
underpowered air conditioning unit, all these alarms will do nothing to help you avoid
outages. Any assessment of your controls must explicitly test whether the risk for which
they were selected is actually being reduced.
EXAM TIP An easy way to differentiate verification and validation is that verification answers the question “did we implement the control right?” while validation answers the question “did we implement the right control?”

Security and Privacy
Security effectiveness deals with metrics such as meeting service level agreement (SLA)
requirements, achieving returns on investment (ROIs), meeting set baselines, and providing management with a dashboard or balanced scorecard system. These are ways
to determine how useful the current security solutions and architecture as a whole are
performing.
Another side to assessing security controls is ensuring that they do not violate our
privacy policies and regulations. It does us no good to implement the best security
controls if they require gross violations of people’s right to keep certain information

Monitoring Risks
We really can’t just build a risk management program (or any program, for that matter),
call it good, and go home. We need a way to assess the effectiveness of our work, identify
deficiencies, and prioritize the things that still need work. We need a way to facilitate
decision making, performance improvement, and accountability through collection, analysis, and reporting of the necessary information. More importantly, we need to be

able to identify changes in the environment and be able to understand their impacts on
our risk posture. All this needs to be based on facts and metrics. As the saying goes, “You
can’t manage something you can’t measure.”
Risk monitoring is the ongoing process of adding new risks, reevaluating existing
ones, removing moot ones, and continuously assessing the effectiveness of our controls
at mitigating all risks to tolerable levels. Risk monitoring activities should be focused
on three key areas: effectiveness, change, and compliance. The risk management team
should continually look for improvement opportunities, periodically analyze the data
gathered from each key area, and report its findings to senior management. Let’s take a
closer look at how we might go about monitoring and measuring each area.

Effectiveness Monitoring
There are many reasons why the effectiveness of our security controls decreases.
Technical controls may not adapt quickly to changing threat actor behaviors. Employees may
lose awareness of (or interest in) administrative controls. Physical controls may not keep
up with changing behaviors as people move in and through our facilities. How do we
measure this decline in the effectiveness of our controls and, more importantly, the rising
risks to our organizations? This is the crux of effectiveness monitoring.
One approach is to keep track of the number of security incidents by severity.
Let’s say that we implemented controls to reduce the risk of ransomware attacks. We
redesigned our security awareness training, deployed a new endpoint detection and

about themselves from being known or used in inappropriate ways. For example, an
organization could have a policy that allows employees to use the organization’s assets
for personal purposes while they are on breaks. The same organization has implemented
Transport Layer Security (TLS) proxies that decrypt all network traffic in order to conduct
deep packet analysis and mitigate the risk that a threat actor is using encryption to hide
her malicious deeds. Normally, the process is fully automated and no other staff members
look at the decrypted communications. Periodically, however, security staff manually
check the system to ensure everything is working properly. Now, suppose an employee
reveals some very private health information to a friend over her personal

webmail and
that traffic is monitored and observed by a security staffer. That breach of privacy could
cause a multitude of ethical, regulatory, and even legal problems for the organization.
When implementing security controls, it is critical to consider their privacy implications.
If your organization has a chief privacy officer (or other privacy professional), that person
should be part of the process of selecting and implementing security controls to ensure
they don’t unduly (or even illegally) violate employee privacy.

response (EDR) solution, and implemented an automated offline backup system.
Subsequently, the number of ransomware-related incidents sharply declined across all
severity categories. While we still see a handful of localized cases here and there, no
data is lost, nobody is forced offline, and business is humming. However, recently we
are noticing that the number of low-severity incidents has started to increase. These are
cases where the ransomware makes it onto a workstation but is stopped as it attempts
to encrypt files. If we’re not paying attention to this trend, we may miss the fact that
the malware is evolving and becoming more effective at evading our EDR solution.
We’d be giving the adversary a huge advantage by letting them experiment and improve
while we do nothing about it. This is why effectiveness monitoring is important, and
why it has to be tied to specific metrics that can be quantified and analyzed over time.
In the previous example, the metric was the number of incidents related to ransomware
in our environment. There are many other metrics you could use, depending on the
control in question. You could use a red team and measure the number of times it
is successful at compromising various assets. You could use the number of suspected
phishing attacks reported by alert employees. Whatever your approach, you should
determine the effectiveness metrics you’ll use to monitor controls when you decide to use
those controls. Then, you really need to track those metrics over time to identify trends.
Failure to do so will result, almost inevitably, in the gradual (or perhaps sudden) increase
in risk until, one sad day, it is realized.
NOTE The Center for Internet Security (CIS) publishes a helpful (and free) document titled “CIS Controls Measures and Metrics,” currently in its seventh version. It provides specific measures for each control as well as goals for their values in your organization.

A good way to enable effectiveness monitoring is to establish a standing group that periodically checks known threats and the controls that are meant to mitigate them.
An example of this is a threat working group (TWG), which consists of members of all major parts of the organization, meeting regularly (say, monthly) to review the list of risks (sometimes called a risk registry) and ensure that threats and controls remain valid.
The TWG assigns owners to each risk and ensures those persons or groups are keeping up their responsibilities. The TWG can also be the focal point for scheduling security assessments, be they internal or external, to verify and validate the controls.

Change Monitoring
Even if you keep track of known threats and the risks they pose, it is likely that changes in your organization's environment will introduce new risks. There are two major sources of change that impact your overall risk: information systems and business. The first is perhaps the most obvious to cybersecurity professionals. A new system is introduced, an old one retired, or an existing one updated or reconfigured. Any of these changes can produce new risks or change those you are already tracking. Another source of changes that introduce risks is the business itself. Over time, your organization will embark on new ventures, change internal processes, or perhaps merge with or acquire another organization.

- Number of unauthorized changes
- Average time to implement a change
- Number of failed changes
- Number of security incidents attributable to changes

NOTE We will discuss change management in more detail in Chapter 19.

Compliance Monitoring
Something else that could change in your organization and affect your risk are legal, regulatory, and policy requirements. Compliance monitoring is a bit easier than effectiveness monitoring and change monitoring, because compliance tends to change fairly infrequently. Laws and external regulations usually take years to change, while internal regulations and policies should be part of the change management process we discussed previously. Though the frequency of compliance changes is fairly low, these changes can

have significant impacts in the organization. A great example of this is the General Data Protection Regulation (GDPR) that came into effect in May 2018. It was years in the making, but it has had huge effects on any organization that stores or processes data belonging to a person from the European Union (EU).

Another aspect of compliance monitoring is responding to audit findings. Whether it is an external or internal audit, any findings dealing with compliance need to be addressed. If the audit reveals risks that are improperly mitigated, the risk team needs to respond to them. Failure to do so could result in significant fines or even criminal charges.

So, what can we measure to monitor our compliance? It varies among organizations, but here are some common metrics to consider:

- Number of audit findings
- Ratio of internal (i.e., self-discovered) to external (i.e., audit) inquiries
- Average time to close an inquiry
- Number of internal disciplinary actions related to compliance

All these changes need to be carefully analyzed to ensure an accurate understanding of their effects on the overall risk posture.

Monitoring changes to your environment and dealing with the risks they could introduce is part of a good change management process. Typically, organizations will have a change advisory board (CAB) or a similarly named standing group that reviews and approves any changes such as the development of new policies, systems, and business processes. The CAB measures changes through a variety of metrics that also are used to monitor risks, such as the following:

No organization is perfectly compliant all the time, so there is always an element of compliance risk. These risks, however, increase dramatically if there is no formal process for searching for and dealing with issues that violate policies, regulations, or laws.

Risk Reporting

Risk reporting is an essential component of risk management in general and risk monitoring in particular. (Recall that risk management encompasses framing, assessing,

responding to, and monitoring the risks.) Reporting enables organizational decisionmaking, security governance, and day-to-day operations. It is also important for compliance purposes.

So, how should we report risks? There is no set formula for reporting, but there are a couple of guiding principles. The first one is to understand the audience. There are at least three groups at which you may target risk reports: executives (and board members), managers, and risk owners. Each requires a different approach.

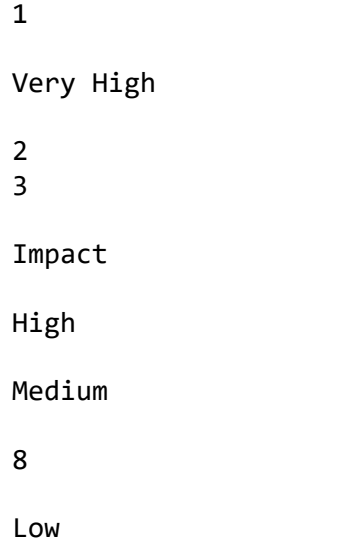
Executives and Board Members

Senior leaders in an organization are generally not interested in the details, nor should they be. Their role is to set and monitor the strategic direction, not to run day-to-day operations. These leaders want to know whether risks can be properly mitigated or require change to the organizational strategy. They will be interested in the biggest risks to the organization and will want to know what is being done to address them. Executives and board members should also be briefed on risks that have been "accepted" and what their potential impacts could be.

When dealing with senior decision makers, risk heat maps, such as illustrated in Figure 2-7, are typically used rather than verbose descriptions. This is to ensure that these leaders can get the information they need at a glance in order to decide whether strategic adjustments may be needed. In Figure 2-7, board members likely would be interested in

Risk

Figure 2-7
Sample risk
heat map



11

7
5

4

6

10
9

Very Low

12
13
15

14

Very
Low

Low

Medium

High

Very
high

↟Chapter 2: Risk Management

95

Managers
Managers across the organization will need much more detailed reports because they are
responsible for, well, managing the risks. They will want to know current risks and how
they've been trending over time. Are risks decreasing or increasing? Either way, why?
Where does progress seem to be stuck? These are some of the questions managers will
want the report to answer. They will also want to be able to drill into specific items of
interest to get into the details, such as who owns the risk, how we are responding to the
risk, and why the current approach may not be working.
Many organizations rely on risk management dashboards for this level of reporting.
These dashboards may be part of a risk management tool, in which case they'd be
interactive and allow drilling into specific items in the report. Organizations

without
these automated tools typically use spreadsheets to generate graphs (showing trends over
time) or even manually developed slides. Whatever the approach, the idea is to present
actionable information allowing business unit managers to track their progress over time
with respect to risks.

Risk Owners
This is the internal audience that needs the most detailed reporting, because the risk
owners are the staff members responsible for managing individual risks. They take direction from management as they respond to specific risks. For example, if the organization
decides to transfer a given risk, the risk owner will be responsible for ensuring the insurance policy is developed and acquired effectively. This will include performance indicators, such as cost, coverage, and responsiveness. Cybersecurity insurance companies often
require that certain controls be in place in order to provide coverage, so the risk owner
must also ensure that these conditions are met so that the premiums are not being paid
in vain.

Continuous Improvement
Only by reassessing the risks on a periodic basis can the risk management team's statements on security control performance be trusted. If the risk has not changed and the
safeguards implemented are functioning in good order, then it can be said that the risk is
being properly mitigated. Regular risk management monitoring will support the information security risk ratings.
Vulnerability analysis and continued asset identification and valuation are also important tasks of risk management monitoring and performance. The cycle of continued risk analysis is a very important part of determining whether the safeguard
controls that have been put in place are appropriate and necessary to safeguard the assets
and environment.
Continuous improvement is the practice of identifying opportunities, mitigating threats, improving quality, and reducing waste as an ongoing effort. It is the hallmark of
mature and effective organizations.

PART I

discussing risk item #7 first since it is particularly significant. That is the point of a heat
map: it allows senior-level audiences to home in on the important topics for discussion.

Level	Maturity	Characteristics
1	Initial	Risk activities are ad hoc, reactive, and poorly controlled.
2	Repeatable	Procedures are documented and (mostly) followed.
3	Defined	Standard procedures, tools, and methods are applied consistently.
4	Managed	Quantitative methods are applied both to risk management and to the program.
5	Optimizing	Data-driven innovation occurs across the entire organization.

Table 2-8 Typical Maturity Model

Risk Maturity Modeling

Maturity models are tools that allow us to determine the ability of our organizations for continuous improvement. We generally assess the maturity of an organization's risk management on a scale of 1 to 5, as shown in Table 2-8. There is actually a level 0, which is where the organization is not managing risk at all.

While it may be tempting to think that we should all strive to achieve the highest level of maturity with regard to risk management, the reality is that we should reach the right level of maturity given our resources, strategies, and business environment. It would make little sense for a very small retail company to strive for level 5, because

doing so
would require a level of resource investment that is not realistic. Conversely, it would be a
very bad idea for a large enterprise in the defense industry to be satisfied with a maturity
level 1, because the risks it faces are substantial. Ultimately, the level of maturity that
makes sense is a business decision, not a cybersecurity one.

Supply Chain Risk Management
Many organizations fail to consider their supply chain when managing risk, despite the
fact that it often presents a convenient and easier back door to an attacker. So what is a
supply chain anyway? A supply chain is a sequence of suppliers involved in delivering
some product. If your company manufactures laptops, your supply chain will include
the vendor that supplies your video cards. It will also include whoever makes the integrated circuits that go on those cards, as well as the supplier of the raw chemicals that are
involved in that process. The supply chain also includes suppliers of services, such as the
company that maintains the heating, ventilation, and air conditioning (HVAC) systems
needed to keep your assembly lines running.
The various organizations that make up your supply chain will have a different outlook
on security than you do. For one thing, their threat modeling will include different
threats than yours. Why would a criminal looking to steal credit card information target
an HVAC service provider? This is exactly what happened in 2013 when Target had over
40 million credit cards compromised. Target had done a reasonable job at securing its
perimeter, but not its internal networks. The attacker, unable (or maybe just unwilling)
to penetrate Target’s outer shell head-on, decided to exploit the vulnerable network of
one of Target’s HVAC service providers and steal its credentials. Armed with these, the

Figure 2-8
Simplified supply
chain

Materials
Supplier

Components
Manufacturer

10
10101
010

Software
Developer

Security
Provider

Distributor
Your Company

Customers

thieves were able to gain access to the point of sale terminals and, from there, the credit card information.

The basic processes you'll need to implement to manage risk in your supply chain are the same ones you use in the rest of your risk management program. The differences are mainly in what you look at (that is, the scope of your assessments) and what you can do about it (legally and contractually). A good resource to help integrate supply chain risk into your risk management program is NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

One of the first things you'll need to do is to create a supply chain map for your organization. This is essentially a network diagram of who supplies what to whom, down to your ultimate customers. Figure 2-8 depicts a simplified systems integrator company ("Your Company"). It has a hardware components manufacturer that supplies it hardware and is, in turn, supplied by a materials producer. Your Company receives software from a developer and receives managed security from an external service provider. The hardware and software components are integrated and configured into Your Company's product, which is then shipped to its distributor and on to its customers. In this example, the company has four suppliers on which to base its supply chain risk assessment. It is also considered a supplier to its distributor.

Now, suppose the software developer in Figure 2-8 is attacked and the threat actors

insert malicious code into the developer’s software product. Anyone who receives that
application from Your Company, or perhaps through an otherwise legitimate software
update, also gets a very stealthy piece of malware that “phones home” to these actors,
telling them where the malware is and what its host network looks like. These are
sophisticated, nation-state spies intent on remaining undetected while they penetrate
some very specific targets. If an infected organization is of interest to them, they’ll deliver
the next stage of malware with which to quietly explore and steal files. Otherwise, they’ll

tell the malware to go dormant, making their actions extremely difficult to detect. This
is a high-level description of a cyber campaign discovered in late 2020 that exploited the
Orion software developed by U.S.-based firm SolarWinds. The magnitude of this series
of attacks underscores the importance of managing risk introduced by your suppliers.

Upstream and Downstream Suppliers
Suppliers are “upstream” from your company if they supply materials, goods, or services
to your company and your company uses those in turn to provide whatever it is that it
supplies to others. The core vulnerability that exists in these supply arrangements is that
you could allow untrusted hardware, software, or services into your organization
or products, where they could cause security problems. The Greeks used this to their advantage
against the Trojans.
Conversely, your company may be upstream from others in the same supply chain.
These would be your company’s downstream suppliers. While it may be tempting to
think that you should be concerned only about supply chain security upstream, those
who follow your company in the supply chain may have their own set of upstream
requirements for your firm. Furthermore, your customers may not care that a security
issue was caused by your downstream distributor; your brand name could be damaged
all the same.

Risks Associated with Hardware, Software, and Services
While we explore risks inherent in any hardware, software, and services later in this book,
for now let’s consider those risks that are specifically tied to supply chains. That is to say,

what risks do you face when you acquire something (or someone's service) and insert it into your information systems?

Hardware

One of the major supply chain risks is the addition of hardware Trojans to electronic components. A hardware Trojan is an electronic circuit that is added to an existing device in order to compromise its security or provide unauthorized functionality. Depending on the attacker's access, these mechanisms can be inserted at any stage of the hardware development process (specification, design, fabrication, testing, assembly, or packaging).

It is also possible to add them after the hardware is packaged by intercepting shipments in the supply chain. In this case, the Trojan may be noticeable if the device is opened and visually inspected. The earlier in the supply chain that hardware Trojans are inserted, the more difficult they are to detect.

Another supply chain risk to hardware is the substitution of counterfeit components. The problems with these clones are many, but from a security perspective one of the most important is that they don't go through the same quality controls that the real ones do. This leads to lower reliability and abnormal behavior. It could also lead to undetected hardware Trojans (perhaps inserted by the illicit manufacturers themselves). Obviously, using counterfeits could have legal implications and will definitely be a problem when you need customer support from the manufacturer.

Software

Services

More organizations are outsourcing services to allow them to focus on their core business functions. Organizations use hosting companies to maintain websites and e-mail servers, service providers for various telecommunication connections, disaster recovery companies for co-location capabilities, cloud computing providers for infrastructure or application services, developers for software creation, and security companies to carry out vulnerability management. It is important to realize that while you can outsource functionality, you cannot outsource risk. When your organization is using these third-party

service providers, it can still be ultimately responsible if something like a data breach
takes place. The following are some things an organization should do to reduce its risk
when outsourcing:

- Review the service provider's security program
- Conduct onsite inspection and interviews
- Review contracts to ensure security and protection levels are agreed upon
- Ensure service level agreements are in place
- Review internal and external audit reports and third-party reviews
- Review references and communicate with former and existing customers
- Review Better Business Bureau reports
- Ensure the service provider has a business continuity plan (BCP) in place
- Implement a nondisclosure agreement (NDA)
- Understand the provider's legal and regulatory requirements

Service outsourcing is prevalent within organizations today but is commonly forgotten
about when it comes to security and compliance requirements. It may be economical to
outsource certain functionalities, but if this allows security breaches to take place, it can
turn out to be a very costly decision.

Other Third-Party Risks
An organization's supply chain is not its only source of third-party risks. There are many
other ways in which organizations may be dependent on each other that don't really fit the

Like hardware, third-party software can be Trojaned by an adversary in your supply
chain, particularly if it is custom-made for your organization. This could happen if your
supplier reuses components (like libraries) developed elsewhere and to which the attacker
has access. It can also be done by a malicious insider working for the supplier or by a
remote attacker who has gained access to the supplier's software repositories. Failing all
that, the software could be intercepted in transit to you, modified, and then sent on its
way. This last approach could be made more difficult for the adversary by using code
signing or hashes, but it is still possible.

supplier–consumer model. For example, many companies have a network of channel
partners that help them directly or indirectly sell products. Others engage in general or limited

partnerships for specific projects, and these relationships require sharing some resources
and risks. Most organizations nowadays have a complex web of (sometimes not so obvious)
third parties on whom they rely to some extent and who, therefore, introduce risks.

Minimum Security Requirements
The key to effectively mitigating risks to an organization introduced by its suppliers is
to clearly state each party's requirements in the contract or agreement that governs their
relationship. In terms of cybersecurity, this includes whatever measures are needed to
protect sensitive data at rest, in transit, and in use. It also includes the actions the supplier
shall perform should the data become compromised, as well as the means through which
the purchasing organization may proactively verify compliance. In summary, the critical
classes of requirements that should be included in a contractual agreement are as follows.

• Data protection Proactive cybersecurity measures
• Incident response Reactive cybersecurity measures
• Verification means Ways in which the customer may verify the preceding requirements
If any requirements are missing, ambiguously stated, or otherwise vitiated, the supplier
agreement can become void, voidable, or unenforceable. So, how do you verify that your
supplier is complying with all contractual requirements dealing with risk? Third-party
assessments are considered best practice and may be required for compliance (e.g., with
PCI DSS). The following are some examples of external evaluations that would indicate
a supplier's ability to comply with its contractual obligations:

• ISO 27001 certification
• U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC)
• Payment Card Industry Digital Security Standard (PCI DSS) certification
• Service Organization Control 1 (SOC1) or 2 (SOC2) report
• U.S. Federal Risk and Authorization Management Program (FedRAMP) authorization
NOTE We will discuss these third-party evaluations in subsequent chapters.

Other third-party evaluations, such as vulnerability assessments and penetration tests, are helpful in establishing a baseline of security in the organization. However, by
themselves, these limited-scope tests are insufficient to verify that the supplier is able to
fulfill its contractual obligations.

Service Level Agreements

Business Continuity
Though we strive to drive down the risks of negative effects in our organizations, we can be sure that sooner or later an event will slip through and cause negative impacts. Ideally, the losses are contained and won't affect the major business efforts. However, as security professionals we need to have plans in place for when the unthinkable happens. Under those extreme (and sometimes unpredictable) conditions, we need to ensure that our organizations continue to operate at some minimum acceptable threshold capacity and quickly bounce back to full productivity.
Business continuity (BC) is an organization's ability to maintain business functions or quickly resume them in the event that risks are realized and result in disruptions.
The events can be pretty mundane, such as a temporary power outage, loss of network connectivity, or a critical employee (such as a systems administrator) suddenly becoming ill. These events could also be major disasters, such as an earthquake, explosion, or energy grid failure. Disaster recovery (DR), by contrast to BC, is the process of minimizing the effects of a disaster or major disruption. It means taking the necessary steps to ensure that the resources, personnel, and business processes are safe and able to resume operation in a timely manner. So, DR is part of BC and the disaster recovery plan (DRP) covers a subset of events compared to the broader business continuity plan (BCP).
EXAM TIP A business continuity plan (BCP) and a disaster recovery plan (DRP) are related but different. The DRP is a subset of the BCP and is focused on the immediate aftermath of a disaster. The BCP is much broader and covers any disruption including (but not limited to) disasters.
NOTE We discuss disaster recovery plans in detail in Chapter 23.

A BCP can include getting critical systems to another environment while repair of the original facilities is underway, getting the right people to the right places during this time, and performing business in a different mode until regular conditions are back in place. A BCP also involves dealing with customers, partners, and shareholders through different channels until everything returns to normal. So, disaster recovery

deals with,

PART I

A service level agreement (SLA) is a contractual agreement that states that a service provider guarantees a certain level of service. If the service is not delivered at the agreed-upon
level (or better), then there are consequences (typically financial) for the service provider.
SLAs provide a mechanism to mitigate some of the risk from service providers in the
supply chain. For example, an Internet service provider (ISP) may sign an SLA of 99.999
percent (commonly called “five nines”) uptime to the Internet backbone. That means
that the ISP guarantees less than 26 seconds of downtime per month.

“Oh my goodness, the sky is falling,” and continuity planning deals with, “Okay, the
sky fell. Now, how do we stay in business until someone can put the sky back where it
belongs?”
Business Continuity
Planning
Senior
management
IT Disaster Recovery
Planning

Business lines

Application availability

Data confidentiality and integrity
Telecommunications and network
Property management

While disaster recovery and business continuity planning are directed at the development of plans, business continuity management (BCM) is the holistic management
process that should cover both of them. BCM provides a framework for integrating resilience with the capability for effective responses in a manner that protects the
interests of an organization’s key stakeholders. The main objective of BCM is to allow
the organization to continue to perform business operations under various conditions.
Business Continuity Management

Issues
Addressed