Another complexity that comes into play when an organization is attempting to work with organizations in other parts of the world is import and export laws. Each country has its own specifications when it comes to what is allowed in its borders and what is allowed out. For example, the Wassenaar Arrangement implements export controls for “Conventional Arms and Dual-Use Goods and Technologies.” It is currently made up of 42 countries and lays out rules on how the following items can be exported from country to country:

- Category 1
- Category 2
- Category 3
- Category 4
- Category 5
- Category 5
- Category 6
- Category 7
- Category 8
- Category 9

Special Materials and Related Equipment
Material Processing
Electronics
Computers
Part 1: Telecommunications
Part 2: Information Security
Sensors and Lasers
Navigation and Avionics
Marine
Aerospace and Propulsion

The main goal of the Wassenaar Arrangement is to prevent the buildup of military capabilities that could threaten regional and international security and stability. So, everyone is keeping an eye on each other to make sure no one country’s weapons can take everyone else out. The idea is to try and make sure everyone has similar offensive and defensive military capabilities with the hope that we won’t end up blowing each other up.
One item the agreement deals with is cryptography, which is considered a dual-use good because it can be used for both military and civilian purposes. The agreement recognizes the danger of exporting products with cryptographic functionality to countries that are in the “offensive” column, meaning that they are thought to have friendly ties with terrorist organizations and/or want to take over the world through the use of weapons of

mass destruction. If the “good” countries allow the “bad” countries to use cryptography, then the “good” countries cannot snoop and keep tabs on what the “bad” countries are up to.

The specifications of the Wassenaar Arrangement are complex and always changing. Which countries fall within the “good” and “bad” categories changes, and what can be exported to whom and how changes. In some cases, no products that contain

Again, you do not need to know all these international laws to become a CISSP. However, you need to be aware that they exist and may impact your business and cybersecurity even if you didn’t know your organization had interests in those countries.

It is best to consult your organization’s legal or compliance team to determine which laws apply to your own team.

cryptographic functions can be exported to a specific country; some countries are allowed to import only products with limited cryptographic functions; some countries require certain licenses to be granted; and other countries (the “good” countries) have no restrictions.

While the Wassenaar Arrangement deals mainly with the exportation of items, some countries (China, Russia, Iran, etc.) have cryptographic import restrictions that have to be understood and followed. These countries do not allow their citizens to use cryptography because they believe that the ability to monitor many aspects of a citizen’s online activities is essential to effectively governing people. This obviously gets very complex for companies who sell products that use integrated cryptographic functionality. One version of the product may be sold to China if it has no cryptographic functionality. Another version may be sold to Russia if a certain international license is in place. A fully functioning product can be sold to Canada, because who are they ever going to hurt?

It is important to understand the import and export requirements your organization must meet when interacting with entities in other parts of the world. You could inadvertently break a country’s law or an international treaty if you do not get the right type of lawyers involved in the beginning and follow the approved processes.

Transborder Data Flow

While import and export controls apply to products, a much more common asset that constantly moves in and out of every country is data, and, as you might imagine at this point, there are laws, regulations, and processes that address what data can be moved where, when, why, how, and by whom. A transborder data flow (TDF) is the movement of machine-readable data across a political boundary such a country’s border. This data is generated or acquired in one country but may be stored and processed in other countries as a result of TDFs. In a modern, connected world, this happens all the time. For example, just imagine all the places your personal data will go when you make an airline reservation to travel overseas, especially if you have a layover along the way.

NOTE Transborder data flows are sometimes called cross-border data flows.

Some governments control transborder data flows by enacting data localization laws that require certain types of data to be stored and processed within the borders of their respective country, sometimes exclusively. There are many reasons for these laws, but they pretty much boil down to protecting their citizens, either by ensuring a higher standard of privacy protection or by allowing easier monitoring of their actions (typically the things citizens try to do overseas). Data localization can increase the cost of doing business in some countries because your organization may have to provision (and protect) information systems in that country that it otherwise wouldn’t.

Ironically, the very technology trend that initially fueled data localization concerns, cloud computing services, ultimately became an important tool to address those concerns

Privacy

Privacy is becoming more threatened as the world increasingly relies on computing technology. There are several approaches to addressing privacy, including the generic approach and regulation by industry. The generic approach is horizontal enactment—rules that stretch across all industry boundaries. It affects all industries, including government. Regulation by industry is vertical enactment. It defines requirements for specific verticals, such as the financial sector and health care. In both cases, the overall objective is twofold. First, the initiatives seek to protect citizens' personally identifiable information.

Second, the initiatives seek to balance the needs of government and businesses to collect and use PII with consideration of security issues.

In response, countries have enacted privacy laws. For example, although the United States already had the Federal Privacy Act of 1974, it has enacted new laws, such as the Gramm-Leach-Bliley Act of 1999 and HIPAA, in response to an increased need to protect personal privacy information. These are examples of a vertical approach to addressing privacy, whereas the EU's GDPR, Canada's Personal Information Protection and Electronic Documents Act, and New Zealand's Privacy Act of 1993 are horizontal approaches. Most countries nowadays have some sort of privacy requirements in their laws and regulations, so we need to be aware of their impact on our information systems and their security to avoid nasty legal surprises.

Licensing and Intellectual Property Requirements

Another way to get into trouble, whether domestically or internationally, is to run afoul of intellectual property laws. As previously introduced, intellectual property (IP) is a type of property created by human intellect. It consists of ideas, inventions, and expressions that are uniquely created by a person and can be protected from unauthorized use by others. Examples are song lyrics, inventions, logos, and secret recipes. IP laws do not necessarily look at who is right or wrong, but rather how an organization or individual can protect what it rightfully owns from unauthorized duplication or use and what it can do if these laws are violated.

So who designates what constitutes authorized use? The owner of the IP does this by granting licenses. A license is an agreement between an IP owner (the licensor) and somebody else (the licensee), granting that party the right to use the IP in very specific ways. For example, the licensee can only use the IP for a year unless they renew the license (presumably after paying a subscription fee). A license can also be, and frequently is, nontransferable, meaning only the licensees, and not their family members or friends, can use it. Another common provision in the agreement is whether or not the license will be exclusive to the licensee.

in a cost-effective manner. At their onset, cloud computing services promised affordable access to resources around the globe, sometimes by shifting loads and storage from one region to another. In recent years, the major cloud service providers have adapted to localization laws by offering an increasing number of regions (sometimes down to individual countries) where the data is guaranteed to remain.

Licenses can become moot if the IP is not properly protected by the licensor. An organization must implement safeguards to protect resources that it claims to be intellectual property and must show that it exercised due care (reasonable acts of protection) in its efforts to protect those resources. For example, if an employee sends a file to a friend and the company terminates the employee based on the activity of illegally sharing IP, then in a wrongful termination case brought by the employee, the company must show the court why this file is so important to the company, what type of damage could be or has been caused as a result of the file being shared, and, most important, what the company had done to protect that file. If the company did not secure the file and tell its employees that they were not allowed to copy and share that file, then the company will most likely lose the case. However, if the company implemented safeguards to protect that file and had an acceptable use policy in its employee manual that explained that copying and sharing the information within the file was prohibited and that the punishment for doing so could be termination, then the company could not be found liable of wrongfully terminating the employee.

Intellectual property can be protected by different legal mechanisms, depending upon the type of resource it is. As a CISSP, you should be knowledgeable of four types of IP laws: trade secrets, copyrights, trademarks, and patents. These topics are addressed in depth in the following sections, followed by tips on protecting IP internally and combating software piracy.

Trade Secret

Trade secret law protects certain types of information or resources from unauthorized use or disclosure. For a company to have its resource qualify as a trade secret, the resource must provide the company with some type of competitive value or advantage. A trade secret can be protected by law if developing it requires special skill, ingenuity, and/or expenditure of money and effort. This means that a company cannot say the sky is blue and call it a trade secret.

A trade secret is something that is proprietary to a company and important for its survival and profitability. An example of a trade secret is the formula used for a soft drink, such as Coke or Pepsi. The resource that is claimed to be a trade secret must be confidential and protected with certain security precautions and actions. A trade secret could also be a new form of mathematics, the source code of a program, a method of making the perfect jelly bean, or ingredients for a special secret sauce. A trade secret has no expiration date unless the information is no longer secret or no longer provides economic benefit to the company.

Many companies require their employees to sign a nondisclosure agreement (NDA), confirming that they understand its contents and promise not to share the company’s trade secrets with competitors or any unauthorized individuals. Companies require an NDA both to inform the employees of the importance of keeping certain information secret and to deter them from sharing this information. Having employees sign the NDA also gives the company the right to fire an employee or bring charges if the employee discloses a trade secret.

Copyright

In the United States, copyright law protects the right of the creator of an original work to control the public distribution, reproduction, display, and adaptation of that original work. The law covers many categories of work: pictorial, graphic, musical, dramatic, literary, pantomime, motion picture, sculptural, sound recording, and architectural. Copyright law does not cover the specific resource, as does trade secret law. It protects the expression of the idea of the resource instead of the resource itself. A copyright is usually used to protect an author’s writings, an artist’s drawings, a programmer’s source code, or specific rhythms and structures of a musician's creation. Computer programs and manuals are just two examples of items protected under the Federal Copyright Act. The program or manual is covered under copyright law once it has been written. Although including a warning and the copyright symbol (©) is not required, doing so is encouraged so others cannot claim innocence after copying another's work.

Copyright protection does not extend to any method of operations, process, concept, or procedure, but it does protect against unauthorized copying and distribution of a protected work. It protects the form of expression rather than the subject matter. A patent deals more with the subject matter of an invention; copyright deals with how that invention is represented. In that respect, copyright is weaker than patent protection, but the duration of copyright protection is longer. Copyright protection exists for the life of the creator plus 70 years. If the work was created jointly by multiple authors, the 70 years start counting after the death of the last surviving one.

Computer programs can be protected under the copyright law as literary works. The law protects both the source code and object code, which can be an operating system, application, or database. In some instances, the law can protect not only the code but also the structure, sequence, and organization. The user interface is part of the definition of a software application structure; therefore, one vendor cannot copy the exact composition of another vendor's user interface.

Copyright infringement cases have exploded in numbers since the rise of "warez" sites that use the common BitTorrent protocol. BitTorrent is a peer-to-peer file sharing protocol and is one of the most common protocols for transferring large files. Warez is a term that refers to copyrighted works distributed or traded without fees or royalties, in general violation of the copyright law. The term generally refers to unauthorized releases by groups, as opposed to file sharing between friends.

PART I

A low-level engineer working at Intel took trade secret information that was valued by Intel at $1 billion when he left his position at the company and went to work at his new employer, rival chipmaker Advanced Micro Devices (AMD). Intel discovered that this person still had access to Intel's most confidential information even after starting work at AMD. He even used the laptop that Intel provided to him to download 13 critical documents that contained extensive information about the company’s new processor developments and product releases. Unfortunately, these stories are not rare, and companies are constantly dealing with challenges of protecting the very data that keeps them in business.

Once a warez site posts copyrighted material, it is very difficult to have it removed because law enforcement is commonly overwhelmed with larger criminal cases and does not have the bandwidth to go after these “small fish.” Another issue with warez sites is that the actual servers may reside in another country; thus, legal jurisdiction makes things more difficult and the country that the server resides within may not even have a copyright law. Film and music recording companies have had the most success in going after these types of offenders because they have the funds and vested interest to do so.

Trademark

A trademark is slightly different from a copyright in that it is used to protect a word, name, symbol, sound, shape, color, or combination of these. The reason a company would trademark one of these, or a combination, is that it represents the company (brand identity) to a group of people or to the world. Companies have marketing departments that work very hard to create something new that will cause the company to be noticed and stand out in a crowd of competitors, and trademarking the result of this work with a government registrar is a way of properly protecting it and ensuring others cannot copy and use it.

Companies cannot trademark a number or common word. This is why companies create new names—for example, Intel’s Pentium and Apple’s iPhone. However, unique colors can be trademarked, as well as identifiable packaging, which is referred to as “trade dress.” Thus, Novell Red and UPS Brown are trademarked, as are some candy wrappers.

Registered trademarks are generally protected for ten years, but can be renewed for another ten years indefinitely. In the United States, you must file paperwork with the U.S. Patent and Trademark Office (USPTO) between the fifth and sixth years showing that you are actually using the trademark. This means that you can’t just create a trademark you don’t ever use and still keep others from using it. You have to file another “Declaration of Use” between the ninth and tenth year, and then every nine to ten years thereafter.

NOTE In 1883, international harmonization of trademark laws began with the Paris Convention, which in turn prompted the Madrid Agreement of 1891. Today, international trademark law efforts and international registration are overseen by the World Intellectual Property Organization (WIPO), an agency of the United Nations. The United States is a party to this agreement.

There have been many interesting trademark legal battles over the years. In one case a person named Paul Specht started a company named “Android Data” and had his company’s trademark approved in 2002. Specht’s company failed, and although he attempted to sell it and the trademark, he had no buyers. When Google announced that it was going to release a new mobile operating system called Android, Specht built a new website using his old company’s name to try and prove that he was indeed still using this trademark. Specht took Google to court and asked for $94 million in trademark infringement damages. The court ruled in Google’s favor and found that Google was not liable for damages.

Patent

EXAM TIP

A patent is the strongest form of intellectual property protection.

The amount of patent litigation in the technology world is remarkable. In October 2020, Centripetal Networks won a $1.9 billion award against Cisco Systems involving network threat detection technologies. In April of the same year, Apple and Broadcom were ordered to pay Caltech $1.1 billion because they infringed multiple Caltech patents pertaining to wireless error correction codes. Even though the amounts of these awards are certainly eye-popping, they are not the only notable ones. It turns out that 2020 was a pretty rough year for Apple, because it was also ordered to pay $506 million to PanOptis and another $109 million to WiLAN in two other infringement cases.

This is just a brief list of recent patent litigation. These patent cases are like watching 100 Ping-Pong matches going on all at the same time, each containing its own characters and dramas, and involving millions and billions of dollars.

PART I

Patents are given to individuals or organizations to grant them legal ownership of, and enable them to exclude others from using or copying, the invention covered by the patent. The invention must be novel, useful, and not obvious—which means, for example, that a company could not patent air. Thank goodness. If a company figured out how to patent air, we would have to pay for each and every breath we took!

After the inventor completes an application for a patent and it is approved, the patent grants a limited property right to exclude others from making, using, or selling the invention for a specific period of time. For example, when a pharmaceutical company develops a specific drug and acquires a patent for it, that company is the only one that can manufacture and sell this drug until the stated year in which the patent is up (usually 20 years from the date of approval). After that, the information is in the public domain, enabling all companies to manufacture and sell this product, which is why the price of a drug drops substantially after its patent expires and generic versions hit the market.

The patent process also applies to algorithms. If an inventor of an algorithm acquires a patent, she has full control over who can use the algorithm in their products. If the inventor lets a vendor incorporate the algorithm, she will most likely get a fee and possibly a license fee on each instance of the product that is sold.

Patents are ways of providing economic incentives to individuals and organizations to continue research and development efforts that will most likely benefit society in some fashion. Patent infringement is huge within the technology world today. Large and small product vendors seem to be suing each other constantly with claims of patent infringement. The problem is that many patents are written at a very high level. For example, if Inge developed a technology that accomplishes functionality A, B, and C, you could actually develop your own technology in your own way that also accomplished A, B, and C. You might not even know that Inge’s method or patent existed; you just developed this solution on your own. Yet if Inge did this type of work first and obtained the patent, then she could go after you legally for infringement.

Figure 3-4 Defendants added to litigation campaigns by year (Data provided by RPX Corporation on 12/14/20. © 2020 RPX Corporation)

While the various vendors are fighting for market share in their respective industries, another reason for the increase in patent litigation is the emergence of nonpracticing entities (NPEs), also known as patent trolls. NPE (or patent troll) is a term used to describe a person or company who obtains patents, not to protect their invention, but to aggressively and opportunistically go after another entity that tries to create something based upon them. A patent troll has no intention of manufacturing an item based upon their patent, but wants to get licensing fees from an entity that does manufacture the item.

For example, let’s say that Donald has ten new ideas for ten different technologies. He puts them through the patent process and gets them approved, but he has no intention of putting in all the money and risk it takes to actually create these technologies and attempt to bring them to market. He is going to wait until you do this and then he is going to sue you for infringing upon his patent. If he wins the court case, you have to pay him licensing fees for the product you developed and brought to market.

It is important to do a patent search before putting effort into developing a new methodology, technology, or business method. As you can see in Figure 3-4, there is a lot of litigation due to patent infringement, and thousands of new defendants are being added to the party each year. These cases are very costly but can oftentimes be avoided with a bit of homework.

Internal Protection of Intellectual Property

Ensuring that specific resources are protected by the previously mentioned laws is very important, but other measures must be taken internally to make sure the resources that are confidential in nature are properly identified and protected.

The resources protected by one of the previously mentioned laws need to be identified and integrated into the organization’s data classification scheme. This should be directed by management and carried out by the IT staff. The identified resources should have the necessary level of access control protection, auditing enabled, and a proper

Software Piracy

Software piracy occurs when the intellectual or creative work of an author is used or duplicated without permission or compensation to the author. It is an act of infringement on ownership rights, and if the pirate is caught, he could be sued civilly for damages, be criminally prosecuted, or both.

When a vendor develops an application, it usually licenses the program rather than sells it outright. The license agreement contains provisions relating to the approved use of the software and the corresponding manuals. If an individual or organization fails to observe and abide by those requirements, the license may be terminated and, depending on the actions, criminal charges may be leveled. The risk to the vendor that develops and licenses the software is the loss of profits it would have earned.

There are four categories of software licensing. Freeware is software that is publicly available free of charge and can be used, copied, studied, modified, and redistributed without restriction. Shareware, or trialware, is used by vendors to market their software. Users obtain a free, trial version of the software. Once the user tries out the program, the user is asked to purchase a copy of it. Commercial software is, quite simply, software that is sold for or serves commercial purposes. And, finally, academic software is software that is provided for academic purposes at a reduced cost. It can be open source, freeware, or commercial software.

Some software vendors sell bulk licenses, which enable several users to use the product simultaneously. These master agreements define proper use of the software along with restrictions, such as whether corporate software can also be used by employees on their home machines. One other prevalent form of software licensing is the End User

License Agreement (EULA). It specifies more granular conditions and restrictions than a master agreement. Other vendors incorporate third-party license-metering software that keeps track of software usability to ensure that the customer stays within the license limit and otherwise complies with the software licensing agreement.

The information security officer should be aware of all these types of contractual commitments required by software companies. This person needs to be educated on the restrictions the organization is under and make sure proper enforcement mechanisms are in place. If an organization is found guilty of illegally copying software or using

storage environment. If a resource is deemed secret, then not everyone in the organization should be able to access it. Once the individuals who are allowed to have access are identified, their level of access and interaction with the resource should be defined in a granular method. Attempts to access and manipulate the resource should be properly audited, and the resource should be stored on a protected system with the necessary security mechanisms.

Employees must be informed of the level of secrecy or confidentiality of the resource and of their expected behavior pertaining to that resource.

If an organization fails in one or all of these steps, it may not be covered by the laws described previously, because it may have failed to practice due care and properly protect the resource that it has claimed to be so important to the survival and competitiveness of the organization.

more copies than its license permits, the security officer in charge of this task may be primarily responsible.

Thanks to easy access to high-speed Internet, employees’ ability—if not the temptation—to download and use pirated software has greatly increased. The June 2018 BSA Global Software Survey, a study conducted by the Business Software Alliance (BSA) and International Data Corporation (IDC), found that 37 percent of the software installed on personal computers globally was not properly licensed. This means that for every two dollars’ worth of legal software that is purchased, one dollar’s worth is pirated.

Software developers often use these numbers to calculate losses resulting from pirated copies. The assumption is that if the pirated copy had not been available, then everyone who is using a pirated copy would have instead purchased it legally.

Not every country recognizes software piracy as a crime, but several international organizations have made strides in curbing the practice. The Federation Against Software Theft (FAST) and the Business Software Alliance (author of the Global Software Survey) are organizations that promote the enforcement of proprietary rights of software. This is a huge issue for companies that develop and produce software, because a majority of their revenue comes from licensing fees. The study also estimates that the total economic damage experienced by the industry was $46.3 billion in losses in 2018.

One of the offenses an individual or organization can commit is to decompile vendor object code. This is usually done to figure out how the application works by obtaining the original source code, which is confidential, and perhaps to reverse-engineer it in the hope of understanding the intricate details of its functionality. Another purpose of reverse-engineering products is to detect security flaws within the code that can later be exploited. This is how some buffer overflow vulnerabilities are discovered.

Many times, an individual decompiles the object code into source code and either finds security holes to exploit or alters the source code to produce some type of functionality that the original vendor did not intend. In one example, an individual decompiled a program that protects and displays e-books and publications. The vendor did not want anyone to be able to copy the e-publications its product displayed and thus inserted an encoder within the object code of its product that enforced this limitation. The individual decompiled the object code and figured out how to create a decoder that would overcome this restriction and enable users to make copies of the e-publications, which infringed upon those authors’ and publishers’ copyrights. The individual was arrested and prosecuted under the Digital Millennium Copyright Act (DMCA), which makes it illegal to create products that circumvent copyright protection mechanisms. Interestingly enough, many computer-oriented individuals protested this person’s arrest, and the company prosecuting (Adobe) quickly decided to drop all charges.

DMCA is a U.S. copyright law that criminalizes the production and dissemination of technology, devices, or services that circumvent access control measures that are put into place to protect copyright material. So if you figure out a way to “unlock” the proprietary way that Barnes & Noble protects its e-books, you can be charged under this act. Even if you don’t share the actual copyright-protected books with someone, you still broke this specific law and can be found guilty.

Compliance Requirements

While it is important to know which specific laws and regulations your organization needs to be compliant with, it is also important to know how to ensure that compliance is being met and how to properly convey that to the necessary stakeholders. If it hasn’t already done so, your organization should develop a compliance program that outlines what needs to be put into place to be compliant with the necessary internal and external drivers. Then, an audit team should periodically assess how well the organization is doing to meet the identified requirements.

The first step is to identify which laws and regulations your organization needs to be compliant with (e.g., GDPR, HIPAA, PCI DSS, etc.). This will give you the specific requirements that the laws and regulations impose on your organization. The requirements, in turn, inform your risk assessment and allow you to select the appropriate controls to ensure compliance. Once this is all done and tested, the auditors have stuff to audit. These auditors can be internal or external to the organization and will have long checklists of items that correspond with the legal, regulatory, and policy requirements the organization must meet.

NOTE

Audits and auditors will be covered in detail in Chapter 18.

It is common for organizations to develop governance, risk, and compliance (GRC) programs, which allow for the integration and alignment of the activities that take place in each one of these silos of a security program. If the same key performance indicators (KPIs) are used in the governance, risk, and compliance auditing activities, then the resulting reports can effectively illustrate the overlap and integration of these different concepts. For example, if a healthcare organization is not compliant with various HIPAA requirements, this is a type of risk that management must be aware of so that it can ensure the right activities and controls are put into place. Also, how does executive management carry out security governance if it does not understand the risks the organization is facing and the outstanding compliance issues? It is important for all of these things to be understood by the decision makers in a holistic manner so that they can make the best decisions pertaining to protecting the organization as a whole. The agreed-upon KPI values are commonly provided to executive management in dashboards or scorecard formats, which allow management to quickly understand the health of the organization from a GRC point of view.

NOTE The European Union passed a similar law called the Copyright Directive.

Contractual, Legal, Industry Standards, and Regulatory Requirements

Regulations in computer and information security cover many areas for many different reasons. We’ve already covered some of these areas, such as data privacy, computer misuse, software copyright, data protection, and controls on cryptography. These regulations can be implemented in various arenas, such as government and private sectors, for reasons dealing with environmental protection, intellectual property, national security, personal privacy, public order, health and safety, and prevention of fraudulent activities.

Security professionals have so much to keep up with these days, from understanding how the latest ransomware attacks work and how to properly protect against them, to inventorying sensitive data and ensuring it only exists in approved places with the right protections. Professionals also need to follow which new security products are released and how they compare to the existing products. This is followed up by keeping track of new technologies, service patches, hotfixes, encryption methods, access control mechanisms, telecommunications security issues, social engineering, and physical security. Laws and regulations have been ascending the list of things that security professionals also need to be aware of. This is because organizations must be compliant with more and more laws and regulations, both domestically and internationally, and noncompliance can result in a fine or a company going out of business, and in some cases certain executive management individuals ending up in jail.

Laws, regulations, and directives developed by governments or appointed agencies do not usually provide detailed instructions to follow to properly protect computers and company assets. Each environment is too diverse in topology, technology, infrastructure, requirements, functionality, and personnel. Because technology changes at such a fast pace, these laws and regulations could never successfully represent reality if they were too detailed. Instead, they state high-level requirements that commonly puzzle organizations about how to be compliant with them. This is where the security professional comes to the rescue.

In the past, security professionals were expected to know how to carry out penetration tests, configure firewalls, and deal only with the technology issues of security. Today, security professionals are being pulled out of the server rooms and asked to be more involved in business-oriented issues. As a security professional, you need to understand the laws and regulations that your organization must comply with and what controls must be put in place to accomplish compliance. This means the security professional now must have a foot in both the technical world and the business world.

But it’s not just laws and regulations you need to be aware of. Your organization may also need to be compliant with certain standards in order to be competitive (or even do business) in certain sectors. If your organization processes credit cards, then it has to comply with the Payment Card Industry Data Security Standard (PCI DSS). This is not a law or even a government regulation; instead, it is an example of a mandatory industry standard. If your organization is a financial institution that is considered part of the critical national infrastructure of the United Kingdom, then it may have to comply with the CBEST standard even though any reputable organization in that

If You Are Not a Lawyer, You Are Not a Lawyer

Many times organizations ask their security professionals to help them figure out how to be compliant with the necessary laws and regulations. While you might be aware of and have experience with some of these laws and regulations, there is a high likelihood that you are not aware of all the necessary federal and state laws, regulations, and international requirements your organization must meet. These laws, regulations, and directives morph over time and new ones are added, and while you may think you are interpreting them correctly, you may be wrong. It is critical that an organization get its legal department involved with compliancy issues. Many security professionals have been in this situation over many years. At many organizations, the legal staff does not know enough about all of these issues to ensure the organization is properly protected. In this situation, advise the organization to contact outside counsel to help them with these issues.

Organizations look to security professionals to have all the answers, especially in consulting situations. You will be brought in as the expert. But if you are not a lawyer, you are not a lawyer and should advise your customer properly in obtaining legal help to ensure proper compliance in all matters. The increasing use of cloud computing is adding an incredible amount of legal and regulatory compliance confusion to current situations.

It is a good idea to have a clause in any type of consulting agreement you use that explicitly outlines these issues so that if and when the organization gets hauled to court after a computer breach, your involvement will be understood and previously documented.

sector is expected to do so voluntarily. And, finally, if your organization wants to sell cloud services to the U.S. government, it won’t even be considered unless it is Federal Risk and Authorization Management Program (FedRAMP) certified. So, compliance is not just about laws and regulations. There are many other standards that may be critical to the success of your organization.

Another compliance requirement that is sometimes missed by cybersecurity professionals is related to contracts and other legally binding agreements. In the course of doing business, your organization may enter into agreements that may have security requirements. For example, your organization may partner with another organization and thereby gain access to its sensitive data. The partnering agreement may have a clause requiring both organizations to ensure that they have certain controls in place to protect that data. If these protections are not already part of your own security architecture and you fail to implement them (or even become aware of them), you would not be in compliance with the contractual obligations, which could make your organization liable in the event of a breach. The point is that we need to have open lines of communication with our legal and business colleagues to ensure we are made aware of any security clauses before we enter into a contract.

Over time, the CISSP exam has become more global in nature and less U.S.-centric. Specific questions on U.S. laws and regulations have been taken out of the test, so you do not need to spend a lot of time learning them and their specifics. Be familiar with why laws are developed and put in place and their overall goals, instead of memorizing specific laws and dates.

Privacy Requirements

Privacy compliance requirements stem from the various data protection laws and regulations we’ve already covered in this chapter (for example, CCPA, GDPR, and HIPAA). The hard part is ensuring you are aware of all the localities within which your organization gathers, stores, and processes various types of private data. The good news is that, at their core, these laws are not all that different from one another in terms of the security controls they require. In almost every case, the controls are reasonable things we would want to have anyway. So, most of the work you’ll require to remain compliant is pretty straightforward.

Where things get a bit murkier is when we consider what data is covered and when we are required to notify someone. For example, the GDPR covers PII on EU persons and HIPAA covers PHI on any patient treated by a U.S. healthcare provider. So, if you suffer a data breach affecting the PHI of a German national who received care in your U.S. facilities, you will most likely have to follow both reporting procedures in these two laws. Under the GDPR, you’d have 72 hours from the time of discovery, while under HIPAA, you could have up to 60 days. The notified parties, in addition to the individual whose information was compromised, vary in each case, which further complicates things.

The best approach is collaborate with your business and legal colleague to develop detailed notification procedures that cover each potential breach. Once you’re satisfied that your organization can comply with the notification requirements, you should exercise different scenarios to test the procedures and ensure everyone is trained on how to execute them. A breach will ruin your day all by itself, so there’s no sense in adding the need to figure out compliance requirements at the point of crisis to make it worse. Furthermore, having procedures that are periodically exercised can help prove to any investigators that you were doing the right things all along.

Liability and Its Ramifications

Executives may be held responsible and liable under various laws and regulations. They could be sued by stockholders and customers if they do not practice due diligence and due care. Due diligence can be defined as doing everything within one’s power to prevent a bad thing from happening. Examples of this would be setting appropriate policies, researching the threats and incorporating them into a risk management plan, and ensuring audits happen at the right times. Due care, on the other hand, means taking the precautions that a reasonable and competent person would take in the same situation. For example, someone who ignores a security warning and clicks through to a malicious website would fail to exercise due care.

Before you can figure out how to properly protect yourself, you need to find out what it is you are protecting yourself against. This is what due diligence is all about— researching and assessing the current level of vulnerabilities so the true risk level is understood. Only after these steps and assessments take place can effective controls and safeguards be identified and implemented.

Due Care vs. Due Diligence

Due diligence is the act of gathering the necessary information so the best decisionmaking activities can take place. Before a company purchases another company, it should carry out due diligence activities so that the purchasing company does not have any “surprises” down the road. The purchasing company should investigate all relevant aspects of the past, present, and predictable future of the business of the target company. If this does not take place and the purchase of the new company hurts the original company financially or legally, the decision makers could be found liable (responsible) and negligent by the shareholders.

In information security, similar data gathering should take place so that there are no “surprises” down the road and the risks are fully understood before they are accepted. If a financial company is going to provide online banking functionality to its customers, the company needs to fully understand all the risks this service entails for the company. Website hacking attempts will increase, account fraud attempts will increase, database attacks will increase, social engineering attacks will increase, and so forth. While this company is offering its customers a new service, it is also making itself a juicier target for attackers and lawyers. The company needs to carry out due diligence to understand all these risks before offering this new service so that the company can make the best business decisions. If it doesn’t implement proper countermeasures, the company opens itself up to potential criminal charges, civil suits, regulatory fines, loss of market share, and more.

Due care pertains to acting responsibly and “doing the right thing.” It is a legal term that defines the standards of performance that can be expected, either by contract or by implication, in the execution of a particular task. Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.

If an organization does not have sufficient security policies, necessary countermeasures, and proper security awareness training in place, it is not practicing due care and can be found negligent. If a financial institution that offers online banking does not implement TLS for account transactions, for example, it is not practicing due care.

Many times due diligence (data gathering) has to be performed so that proper due care (prudent actions) can take place.

PART I

EXAM TIP Due diligence is normally associated with leaders, laws, and regulations. Due care is normally applicable to everyone, and failure to exercise it could be used to show negligence.

Senior management has an obligation to protect the organization from a long list of activities that can negatively affect it, including protection from malicious code, natural disasters, privacy violations, infractions of the law, and more. The costs and benefits of this protection should be evaluated in monetary and nonmonetary terms to ensure that the cost of security does not outweigh the expected benefits. Security should be proportional to potential loss estimates pertaining to the severity, likelihood, and extent of potential damage.

As Figure 3-5 shows, there are many costs to consider when it comes to security breaches: loss of business, response activities, customer and partner notification, and detection and escalation measures. These types of costs need to be understood so that the organization can practice proper due care by implementing the necessary controls to reduce the risks and these costs. Security mechanisms should be employed to reduce the frequency and severity of security-related losses. A sound security program is a smart business practice.

Senior management needs to decide upon the amount of risk it is willing to take pertaining to computer and information security, and implement security in an economical and responsible manner. These risks do not always stop at the boundaries of the organization.

Many organizations work with third parties, with whom they must share sensitive data. The main organization is still liable for the protection of this sensitive data that it owns, even if the data is on another organization’s network. This is why more and more regulations are requiring organizations to evaluate their third-party security measures.

If one of the organizations does not provide the necessary level of protection and its negligence affects a partner it is working with, the affected organization can sue the upstream organization. For example, let’s say Company A and Company B have constructed an extranet. Company A does not put in controls to detect and deal with viruses. Company A

6,061

30%

1,845

6,025

30%
1,833

4,826

34%
1,621

4,587

37%
1,703

4,557
3,608
40%
1,430

65%
3,936

2013

65%
3,924

61%
2,928

57%
2,610

2014
NPE

2015
2016
Operating Company

54%
1,957

3,375
47%
1,599

48%
1,608

3,603
39%

1,396

54%
1,961

2017
2018
2019
Pure Design Patent Litigation

Figure 3-5 Data breach costs (Source: Ponemon Institute and IBM Security)

42%
1,926

21%
981
36%
1,636
2020 YTD

EXAM TIP Responsibility generally refers to the obligations and expected actions and behaviors of a particular party. An obligation may have a defined set of specific actions that are required, or a more general and open approach, which enables the party to decide how it will fulfill the particular obligation. Accountability refers to the ability to hold a party responsible for certain actions or inaction.

Each company has different requirements when it comes to its list of due care responsibilities. If these steps are not taken, the company may be charged with negligence if damage arises out of its failure to follow these steps. To prove negligence in court, the plaintiff must establish that the defendant had a legally recognized obligation, or duty, to protect the plaintiff from unreasonable risks and that the defendant’s failure to protect the plaintiff from an unreasonable risk (breach of duty) was the proximate cause of the plaintiff ’s damages. Penalties for negligence can be either civil or criminal, ranging from actions resulting in compensation for the plaintiff to jail time for violation of the law.

EXAM TIP Proximate cause is an act or omission that naturally and directly produces a consequence. It is the superficial or obvious cause for an occurrence. It refers to a cause that leads directly, or in an unbroken sequence, to a particular result. It can be seen as an element of negligence in a court of law.

Requirements for Investigations

Investigations are launched for a multitude of specific reasons. Maybe you suspect an employee is using your servers to mine bitcoin after hours, which in most places would be a violation of acceptable use policies. Maybe you think civil litigation is reasonably foreseeable or you uncover evidence of crime on your systems. Sometimes, we are the targets of investigation and not the investigators, such as when a government regulator suspects we are not in compliance. Though the investigative process is similar regardless of the reason, it is important to differentiate the types of investigations you are likely to come across.

Administrative

An administrative investigation is one that is focused on policy violations. These represent the least impactful (to the organization) type of investigation and will likely result in administrative action if the investigation supports the allegations. For instance, violations of voluntary industry standards (such as PCI DSS) could result in

gets infected with a destructive virus and it is spread to Company B through the extranet. The virus corrupts critical data and causes a massive disruption to Company B’s production. Therefore, Company B can sue Company A for being negligent. Both companies need to make sure they are doing their part to ensure that their activities, or the lack of them, will not negatively affect another company, which is referred to as downstream liability.

an administrative investigation, particularly if the violation resulted in some loss or bad press for the organization. In the worst case, someone can get fired. Typically, however, someone is counseled not to do something again and that is that. Either way, you want to keep your human resources (HR) staff involved as you proceed.

Criminal

A seemingly administrative affair, however, can quickly get stickier. Suppose you start investigating someone for a possible policy violation and along the way discover that person was involved in what is likely criminal activity. A criminal investigation is one that is aimed at determining whether there is cause to believe beyond a reasonable doubt that someone committed a crime. The most important thing to consider is that we, as information systems security professionals, are not qualified to determine whether or not someone broke the law; that is the job of law enforcement agencies (LEAs). Our job, once we have reason to believe that a crime may have taken place, is to preserve evidence, ensure the designated people in our organizations contact the appropriate LEA, and assist them in any way that is appropriate.

Civil

Not all statutes are criminal, however, so it is possible to have an alleged violation of a law result in something other than a criminal investigation. The two likeliest ways to encounter this is regarding possible violations of civil law or government regulations. A civil investigation is typically triggered when a lawsuit is imminent or ongoing. It is similar to a criminal investigation, except that instead of working with an LEA you will probably be working with attorneys from both sides (the plaintiff is the party suing and the defendant is the one being sued). Another key difference in civil (versus criminal) investigations is that the standard of proof is much lower; instead of proving beyond a reasonable doubt, the plaintiff just has to show that the preponderance of the evidence supports the allegation.

Regulatory

Somewhere between the previous three (administrative, criminal, and civil investigations) lies the fourth kind you should know. A regulatory investigation is initiated by a government regulator when there is reason to believe that the organization is not in compliance. These vary significantly in scope and could look like any of the other three types of investigation depending on the severity of the allegations. As with criminal investigations, the key thing to remember is that your job is to preserve evidence and assist the regulator’s investigators as appropriate.

Chapter Review

The fact that the Internet is a global medium does not negate the power of governments to establish and enforce laws that govern what can be done by whom on networks within each country. This can create challenges for cybersecurity professionals whose organizations have clients, partners, or activities in multiple jurisdictions. The most important thing you can do as a CISSP is develop a good relationship with your legal team and use that to ensure you are aware of all the legal and regulatory requirements that may pertain to cybersecurity. Then, after you implement the necessary controls,

Quick Review

- Law is a system of rules (written or otherwise), created by a government, that apply equally to everyone in the country.
- Regulations are written rules issued by an executive body, covering specific issues, and apply only to the specific entities that fall under the authority of the agency that issues them.
- Civil law system:
  - Uses prewritten rules and is not based on precedent.
  - Is different from civil (tort) laws, which work under a common law system.
- Common law system:
  - Made up of criminal, civil, and administrative laws.
- Customary law system:
  - Addresses mainly personal conduct and uses regional traditions and customs as the foundations of the laws.
  - Is usually mixed with another type of listed legal system rather than being the sole legal system used in a region.
- Religious law system:
  - Laws are derived from religious beliefs and address an individual’s religious responsibilities; commonly used in Muslim countries or regions.
- Mixed law system:
  - Uses two or more legal systems.
- Criminal law deals with an individual’s conduct that violates government laws developed to protect the public.
- Civil law deals with wrongs committed against individuals or organizations that result in injury or damages. Civil law does not use prison time as a punishment, but usually requires financial restitution.
- Administrative, or regulatory, law covers standards of performance or conduct expected by government agencies from companies, industries, and certain officials.
- Many attacks cross international borders, which make them harder to prosecute because doing so requires deconflicting the laws of the various countries involved; attackers use this to their advantage.

check with your lawyer friends again to ensure you’ve exercised due diligence. Keep checking, because laws and regulations do change over time, particularly if you are operating in multiple countries.

- Island-hopping attacks are those in which an attacker compromises an easier target that has a trusted connection to the ultimate target.
- An advanced persistent threat (APT) is a sophisticated threat actor that has the means and the will to devote extraordinary resources to compromising a specific target and remaining undetected for extended periods of time.
- A data breach is a security event that results in the actual or potential compromise of the confidentiality or integrity of protected information by unauthorized actors.
- Personally identifiable information (PII) is data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
- Each country has specific rules that control what can be legally imported and exported. This applies particularly to some cryptographic tools and techniques.
- A transborder data flow (TDF) is the movement of machine-readable data across a political boundary such as a country’s border.
- Data localization laws require that certain types of data be stored and processed in that country, sometimes exclusively.
- Intellectual property (IP) is a type of property created by human intellect that consists of ideas, inventions, and expressions that are uniquely created by a person and can be protected from unauthorized use by others.
- A license is an agreement between an intellectual property (IP) owner (the licensor) and somebody else (the licensee), granting that party the right to use the IP in very specific ways.
- Trade secrets are deemed proprietary to a company and often include information that provides a competitive edge. The information is protected as long as the owner takes the necessary protective actions.
- Copyright protects the expression of ideas rather than the ideas themselves.
- Trademarks protect words, names, product shapes, symbols, colors, or a combination of these used to identify products or a company. These items are used to distinguish products from the competitors’ products.
- A patent grants ownership and enables that owner to legally enforce his rights to exclude others from using the invention covered by the patent.
- Due diligence can be defined as doing everything within one’s power to prevent a bad thing from happening. It is normally associated with leaders,

laws, and regulations.

- Due care means taking the precautions that a reasonable and competent person would take in the same situation. It is normally applicable to everyone, and its absence could be used to show negligence.
- Administrative investigations are focused on policy violations.

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. When can executives be charged with negligence?
A. If they follow the transborder laws
B. If they do not properly report and prosecute attackers
C. If they properly inform users that they may be monitored
D. If they do not practice due care when protecting resources

2. To better deal with computer crime, several legislative bodies have taken what steps in their strategy?
A. Expanded several privacy laws
B. Broadened the definition of property to include data
C. Required corporations to have computer crime insurance
D. Redefined transborder issues

3. Which of the following is true about data breaches?
A. They are exceptionally rare.
B. They always involve personally identifiable information (PII).
C. They may trigger legal or regulatory requirements.
D. The United States has no laws pertaining to data breaches.

Use the following scenario to answer Questions 4–6. Business is good and your company is expanding operations into Europe. Because your company will be dealing with personal information of European Union (EU) citizens, you know that it will be subject to the EU’s General Data Protection Regulation (GDPR). You have a mature security program that is certified by the International Organization for Standardization (ISO), so you are confident you can meet any new requirements.

- Criminal investigations are aimed at determining whether there is cause to believe that someone committed a crime.
- A civil investigation is typically triggered when a lawsuit is imminent or ongoing, and is similar to a criminal investigation, except that instead of working with law enforcement agencies you will probably be working with attorneys from both sides.
- A regulatory investigation is initiated by a government regulator when there is reason to believe that the organization is not in compliance.

4. Upon learning of your company’s plans to expand into Europe, what should be one of the first things you do?
A. Consult your legal team
B. Appoint a Data Protection Officer (DPO)
C. Label data belonging to EU persons
D. Nothing, because your ISO certification should cover all new requirements

5. You have determined all the new GDPR requirements and estimate that you will need an additional $250,000 to meet them. How can you best justify this investment to your senior business leaders?
A. It is the right thing to do.
B. You are legally required to provide that money.
C. You’ll make way more profits than that in the new market.
D. The cost of noncompliance could easily exceed the additional budget request.

6. Your Security Operations Center (SOC) chief notifies you of a data breach in which your organization’s entire customer list may have been compromised. As the data controller, what are your notification requirements?
A. No later than 72 hours after you contain the breach
B. Within 30 days of the breach
C. As soon as possible, but within 60 days of becoming aware of the breach
D. No later than 72 hours after becoming aware of the breach

Use the following scenario to answer Questions 7–9. Faced with a lawsuit alleging patent infringement, your CEO stands up a working group to look at licensing and intellectual property (IP) issues across the company. The intent is to ensure that the company is doing everything within its power to enforce IP rights, both its own rights and others’ rights. The CEO asks you to lead an effort to look internally and externally for any indication that your company is violating the IP rights of others or that your own IP is being used by unauthorized parties.

7. Which term best describes what the CEO is practicing?
A. Due care

B. Due diligence
C. Compliance
D. Downstream liability

A. Do nothing; the blogs are not particularly valuable, and you have bigger problems
B. Contact the webmasters directly and ask them to take the blogs down
C. Have the legal team send a cease-and-desist order to the offending organization
D. Report your findings to the CEO

9. You discover dozens of workstations running unlicensed productivity software in a virtual network that is isolated from the Internet. Why is this a problem?
A. Users should not be able to install their own applications.
B. It is not a problem as long as the virtual machines are not connected to the Internet.
C. Software piracy can have significant financial and even criminal repercussions.
D. There is no way to register the licenses if the devices cannot access the Internet.
10. Which of the following would you use to control the public distribution, reproduction, display, and adaptation of an original white paper written by your staff?
A. Copyright
B. Trademark
C. Patent
D. Trade secret
11. Many privacy laws dictate which of the following rules?
A. Individuals have a right to remove any data they do not want others to know.
B. Agencies do not need to ensure that the data is accurate.
C. Agencies need to allow all government agencies access to the data.
D. Agencies cannot use collected data for a purpose different from what they collected it for.
12. Which of the following has an incorrect definition mapping?
i. Civil (code) law: Based on previous interpretations of laws
ii. Common law: Rule-based law, not precedent-based
iii. Customary law: Deals mainly with personal conduct and patterns of behavior
iv. Religious law: Based on religious beliefs of the region
A. i, iii
B. i, ii, iii
C. i, ii
D. iv

8. You discover that another organization is publishing some of your company's copyrighted blogs on its website as if they were its own. What is your best course

of action?

Answers

1. D. Executives are held to a certain standard and are expected to act responsibly when running and protecting an organization. These standards and expectations equate to the due care concept under the law. Due care means to carry out activities that a reasonable person would be expected to carry out in the same situation. If an executive acts irresponsibly in any way, she can be seen as not practicing due care and be held negligent.
2. B. Many times, what is corrupted, compromised, or taken from a computer is data, so current laws have been updated to include the protection of intangible assets, as in data. Over the years, data and information have become many organizations' most valuable asset, which must be protected by the laws.
3. C. Organizations experiencing a data breach may be required by laws or regulations to take certain actions. For instance, many countries have disclosure requirements that require notification to affected parties and/or regulatory bodies within a specific timeframe.
4. A. Your best bet when facing a new legal or regulatory environment or issue is to consult with your legal team. It is their job to tell you what you're required to do, and your job to get it done. Your will almost certainly need to appoint a Data Protection Officer (DPO), and you will probably need to label or otherwise categorize data belonging to EU persons, but you still need to check with your attorneys first.
5. D. Fines for noncompliance with the GDPR can range from up to €20 million (approximately $22.5 million) to 4 percent of a company's annual global revenue—whichever is greater. While it is true that this is the right thing to do, that answer is not as compelling to business leaders whose job is to create value for their shareholders.
6. D. The GDPR has the strictest breach notification requirements of any data protection law in the world. Your organization is required to notify the supervisory authority of the EU member state involved within 72 hours of becoming aware of the breach. Examples of supervisory authorities are the Data Protection Commission in Ireland, the Hellenic Data Protection Authority in Greece, and the Agencia Española de Protección de Datos in Spain.
7. B. Due diligence is doing everything within one's power to prevent a bad thing from happening and is normally associated with an organization's leaders. Given the CEO's intent, this is the best answer. Compliance could be an answer but is not the best one since the scope of the effort appears to be very broad and there is no mention of specific laws or regulations with which the CEO wants to comply.
8. C. A company must protect resources that it claims to be intellectual property

such as copyrighted material and must show that it exercised due care (reasonable acts of protection) in its efforts to protect those resources. If you ignore this apparent violation, it may be much more difficult to enforce your rights later when more valuable IP is involved. You should never attempt to do this on your own. That’s why you have a legal team!

9. C. Whether or not the computers on which unlicensed software runs can reach the Internet is irrelevant. The fact is that your company is using a software product that it is not authorized to use, which is considered software piracy.
10. A. A copyright fits the situation precisely. A patent could be used to protect a novel invention described in the paper, but the question did not imply that this was the case. A trade secret cannot be publicly disseminated, so it does not apply. Finally, a trademark protects only a word, symbol, sound, shape, color, or combination of these.
11. D. The Federal Privacy Act of 1974 and the General Data Protection Regulation (GDPR) were created to protect personal data. These acts have many stipulations, including that the information can only be used for the reason for which it was collected.
12. C. The following has the proper definition mappings:
i. Civil (code) law: Rule-based law, not precedent-based
ii. Common law: Based on previous interpretations of laws
iii. Customary law: Deals mainly with personal conduct and patterns of behavior
iv. Religious law: Based on religious beliefs of the region

⬆This page intentionally left blank

⬆CHAPTER

Frameworks

This chapter presents the following:

- Overview of frameworks
- Risk frameworks
- Information security frameworks
- Enterprise architecture frameworks
- Other frameworks

You can’t build a great building on a weak foundation.
—Gordon B. Hinckley

The previous chapters have covered a lot of material dealing with governance, risk, and compliance. By now, you may be asking yourself, “How does this all fit together into an actionable process?” This is where frameworks come to the rescue. You can think of a framework as a strong foundation on which to build whatever it is you’re trying to build, whether it’s a risk management program or security controls. A framework gives you just enough rigidity to keep your effort from collapsing under its own weight, but still gives you a lot of leeway so that you can customize the framework to your particular situation.

While it is possible (though very difficult) to build successful programs all by yourself, why reinvent the wheel when you can leverage the hard-earned lessons of other experts in the field?

In this chapter, we will discuss a variety of frameworks that you are likely to encounter both in your job and when taking the CISSP exam. We divide them into three groups: risk frameworks, information security frameworks, and enterprise architecture frameworks.

Risk management enables any successful information security program, so we’ll tackle those two groups in that order, followed by enterprise architecture frameworks. We’ll then round out our discussion with the other frameworks and concepts that you should know.

Overview of Frameworks

A framework is a basic structure underlying a system, concept, or text. So the purpose of frameworks in IT and cybersecurity is to provide structure to the ways in which we manage risks, develop enterprise architectures, and secure all our assets. Think of frameworks as the consensus of many great minds on how we should approach these issues.

As you will see in the following sections, various for-profit and nonprofit organizations have developed their own frameworks for risk management, security programs, security controls, process management, and enterprise development. We will examine their similarities and differences and illustrate where each is used within the industry. The following is a basic breakdown.

Risk:

- NIST RMF The Risk Management Framework, developed by the National Institute of Standards and Technology, is composed of three interrelated NIST Special Publications (SPs): 800-39, 800-37, and 800-30.

- ISO/IEC 27005 Focused on risk treatment, this joint International Organization for Standardization/International Electrotechnical Commission framework is best used in conjunction with ISO/IEC 27000 series standards.
- OCTAVE The Operationally Critical Threat, Asset, and Vulnerability Evaluation framework, developed at Carnegie Mellon University, is focused on risk assessment.
- FAIR The FAIR Institute’s Factor Analysis of Information Risk framework focuses on more precisely measuring the probabilities of incidents and their impacts.

Security Program:

- ISO/IEC 27000 series This is a series of international standards on how to develop and maintain an information security management system (ISMS), developed by ISO and IEC.
- NIST Cybersecurity Framework Driven by the need to secure government systems, NIST developed this widely used and comprehensive framework for risk-driven information security.

Security Controls:

- NIST SP 800-53 This NIST publication provides a catalog of controls and a process for selecting them in order to protect U.S. federal systems.
- CIS Controls The Center for Internet Security (CIS) Controls framework is one of the simplest approaches for companies of all sizes to select and implement the right controls.
- COBIT 2019 This is a business framework to allow for IT enterprise management and governance that was developed by ISACA.

Enterprise Architecture:

- Zachman Framework This is a model for the development of enterprise architectures, developed by John Zachman.
- TOGAF The Open Group Architecture Framework is a model and methodology for the development of enterprise architectures.

NOTE

Chapter 1 already discussed the SABSA model.

Risk Frameworks

By combining the definition of a framework in the previous section with our definition of risk management in Chapter 2, we can define a risk management framework (RMF) as a structured process that allows an organization to identify and assess risk, reduce it to an acceptable level, and ensure that it remains at that level. In essence, an RMF is a structured approach to risk management.

As you might imagine, there is no shortage of RMFs out there. What is important to you as a security professional is to ensure your organization has an RMF that works for you. That being said, there are some frameworks that have enjoyed widespread success and acceptance. You should at least be aware of these, and ideally adopt (and perhaps modify) one of them to fit your organization’s particular needs. We’ll cover the NIST RMF in more detail, mostly to familiarize you with the components of this framework, but also because it is the one you are most likely to encounter in your career.

NIST RMF

The NIST Risk Management Framework (RMF) is described in three core interrelated Special Publications (there are other key publications specific to individual steps of the RMF):

- SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations
- SP 800-39, Managing Information Security Risk
- SP 800-30, Revision 1, Guide for Conducting Risk Assessments

This framework incorporates the key elements of risk management that you should know as a security professional. It is important to keep in mind, however, that it is geared toward federal government entities and may have to be modified to fit your own needs.

The NIST RMF outlines the seven-step process shown in Figure 4-1, each of which will be addressed in turn in the following sections. It is important to note that this is a never-ending cycle because our information systems are constantly changing. Each change needs to be analyzed to determine whether it should trigger another trip around the loop.

- DoDAF The U.S. Department of Defense Architecture Framework was developed to ensure interoperability of systems to meet military mission goals.
- SABSA The Sherwood Applied Business Security Architecture model and methodology for the development of information security enterprise architectures was developed by the SABSA Institute.

Figure 4-1 The NIST Risk Management Framework process

CATEGORIZE

MONITOR

SELECT
PREPARE
Process initiation

AUTHORIZE

IMPLEMENT

ASSESS

Prepare
The first step is to ensure that the top executives and the senior leaders (at both the strategic and operational levels) are in sync across the organization. This includes agreeing on roles, priorities, constraints, and risk tolerance. Another key activity during the prepare step is to conduct an organizational risk assessment that provides a common point of reference for the entire team to communicate about strategic risks. One of the outcomes of this assessment is the identification of high-value assets, on which the entire effort will be focused.

Categorize
The next step is to categorize your information systems based on criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. The idea is to create categories for your systems based on how important they are so that you can prioritize your defensive resources. All U.S. government agencies are required to use the following NIST SP 800-60 documents for this purpose: Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories and Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.
NIST SP 800-60 applies sensitivity and criticality to each security objective (confidentiality, integrity, and availability) to determine a system’s criticality. For example, suppose you have a customer relationship management (CRM) system. If its confidentiality were to be compromised, this would cause significant harm to your company, particularly if the information fell into the hands of your competitors. The system’s integrity and availability, on the other hand, would probably not be as critical to your business, so they would be classified as relatively low. The format for describing the security category (SC) of this CRM would be as follows:
SCCRM = {(confidentiality, high),(integrity, low),(availability, low)}

SP 800-60 uses three SCs: low impact, moderate impact, and high impact. A lowimpact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is one in which at least one of the security

Select

Once you have categorized your systems, it is time to select, and quite possibly tailor, the controls you will use to protect them. The NIST RMF defines three types of security controls: common, system-specific, and hybrid. A common control is one that applies to multiple systems and exists outside of their individual boundaries. Following our CRM example, if you placed a web application firewall (WAF) in front of the CRM (and in front of all your other web applications), that would be an example of a common control. The WAF is outside the system boundary of the CRM and protects it and other systems.

System-specific controls, on the other hand, are implemented within the system boundary and, obviously, protect only that specific system. The system owner, and not the broader organization, is responsible for these. An example would be a login page on the CRM that forces the use of Transport Layer Security (TLS) to encrypt the user credentials. If the authentication subsystem was an integral part of the CRM, then this would be an example of an application-specific control.

Wouldn’t it be wonderful if everything was black or white, true or false? Alas, the real world is much messier than that. Oftentimes, controls blur the line between common and system-specific and become something else. A hybrid control, according to the NIST RMF, is one that is partly common and partly system-specific. Continuing our CRM example, a hybrid control could be security awareness training. There would be a common aspect to the training (e.g., don’t share your password) but also some systemspecific content (e.g., don’t save your customers’ information and e-mail it to your personal account so that you can reach out to them while you’re on vacation).

The specific controls required to mitigate risks to acceptable levels are documented in the NIST control catalog, NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations. We’ll discuss this publication later in this chapter, but for now it is worth noting that it provides a mapping between the impact categories we assigned to information systems in the categorize step of this RMF and specific controls that mitigate risks to those systems.

Implement

There are two key tasks in this step: implementation and documentation. The first part is very straightforward. For example, if you determined in the previous step that you need to add a rule to your WAF to filter out attacks like Structured Query Language (SQL) injection, you implement that rule. Simple. The part with which many of us struggle is the documentation of this change.

The documentation is important for two obvious reasons. First, it allows everyone to understand what controls exist, where, and why. Have you ever inherited a system that is configured in a seemingly nonsensical way? You try to understand why certain parameters

objectives is moderate and no security objective is greater than moderate. Finally, a high-impact system is an information system in which at least one security objective is high. This method of categorization is referred to as the “high water mark” because it uses the highest security objective category to determine the overall category of the system. In our example, the SC of the CRM system would be high because at least one objective (confidentiality) is rated high.

or rules exist but hesitate to change them because the system might fail. Likely, this was the result of either improper documentation or (even worse) a successful attack. The second reason why documentation is important is that it allows us to fully integrate the controls into the overall assessment and monitoring plan. Failing to do this invites having controls that quietly become obsolete and ineffective over time and result in undocumented risks.

Assess

The security controls we implement are useful to our overall risk management

effort
only insofar as we can assess them. It is absolutely essential to our organizations to have
a comprehensive plan that assesses all security controls (common, hybrid, and systemspecific) with regard to the risks they are meant to address. This plan must be reviewed
and approved by the appropriate official(s), and it must be exercised.
To execute an assessment plan, you will, ideally, identify an assessor who is both
competent and independent from the team that implemented the controls. This person
must act as an honest broker that not only assesses the effectiveness of the controls but
also ensures the documentation is appropriate for the task. For this reason, it is important
to include all necessary assessment materials in the plan.
The assessment determines whether or not the controls are effective. If they are, then
the results are documented in the report so that they are available as references for the
next assessment. If the controls are not effective, then the report documents the results,
the remediation actions that were taken to address the shortcomings, and the outcome
of the reassessment. Finally, the appropriate security plans are updated to include the
findings and recommendations of the assessment.
NOTE An assessment of security controls is also called an audit. We discuss audits in detail in Chapter 18.

Authorize

As we already discussed, no system is ever 100 percent risk-free. At this stage in the RMF,
we present the results of both our risk and controls assessments to the appropriate decisionmaker in order to get approval to connect our information system into our broader architecture and operate it. This person (or group) is legally responsible and accountable for the
system while it is operating, and therefore must make a true risk-based decision to allow
the system to operate. This person determines whether the risk exposure is acceptable to
the organization. This normally requires a review of a plan of action that addresses how
and when the organization will deal with the remaining weaknesses and deficiencies in the
information system. In many organizations this authorization is given for a set period of
time, which is usually specified in a plan of action and milestones (POAM or POA&M).

Monitor

These milestones we just mentioned are a key component of the monitoring or continuous improvement stage of the RMF. At a minimum, we must periodically look at all our controls and determine whether they are still effective. Has the threat changed its tactics, techniques, and procedures (TTPs)? Have new vulnerabilities been discovered? Has an

ISO/IEC 27005

ISO/IEC 27005, updated in 2018, is another widely used information security risk management framework. Similar to the NIST RMF we just discussed, ISO/IEC 27005 provides guidelines for information security risk management in an organization but does not dictate a specific approach for implementing it. In other words, the framework tells us what sorts of things we ought to do, but not how to do them. Similarly to how the NIST RMF can be paired with the security controls in NIST SP 800-53, ISO/IEC 27005 is best used in conjunction with ISO/IEC 27001, which, as we'll see shortly, provides a lot more structure to information security program development.

The risk management process defined by ISO/IEC 27005 is illustrated in Figure 4-2.

It all starts with establishing the context in which the risks exist. This is similar to the

Figure 4-2
ISO/IEC 27005
risk management
process

CONTEXT ESTABLISHMENT
RISK ASSESSMENT
RISK ANALYSIS

RISK ESTIMATION

RISK EVALUATION

RISK DECISION POINT 1
Assessment satisfactory

No
Yes

RISK TREATMENT

RISK DECISION POINT 2
Treatment satisfactory

No
Yes

RISK ACCEPTANCE

END OF FIRST OR SUBSEQUENT ITERATIONS

RISK MONITORING AND REVIEW

RISK COMMUNICATION

RISK IDENTIFICATION

undocumented or unapproved change to our configuration altered our risk equations?

These are only some of the issues that we address through ongoing monitoring and continuous improvement.

business impact analysis (BIA) we discussed in Chapter 2, but it adds new elements, such as evaluation criteria for risks as well as the organizational risk appetite. The risk assessment box in the middle of the figure should look familiar, since we also discussed this process (albeit with slightly different terms) in Chapter 2.

The risk treatment step is similar to the NIST RMF steps of selecting and implementing controls but is broader in scope. Rather than focusing on controls to mitigate the risks, ISO/IEC 27005 outlines four ways in which the risk can be treated:

- Mitigate the risk by implementing controls that bring it to acceptable levels.
- Accept the risk and hope it doesn’t realize, which assumes that the impact of this risk is less than the cost of treating it.
- Transfer the risk to another entity such as an insurance company or a business partner.
- Avoid the risk by not implementing the information system that brings it, or by changing business practices so the risk is no longer present or is reduced to acceptable levels.

NOTE The NIST RMF also briefly touches on these treatments in the authorize step of its process.

Risk acceptance in ISO/IEC 27005 is very similar to the authorize step in the NIST RMF, and the risk monitoring steps in both are very similar. A notable difference between these two RMFs, on the other hand, is that ISO/IEC 27005 explicitly identifies risk communication as an important process. This is an essential component of any risk management methodology, since we cannot enlist the help of senior executives, partners, or other stakeholders if we cannot effectively convey our message to a variety of audiences. Just because this communication is not explicitly called out in the NIST RMF or any other RMF, however, doesn’t decrease its importance.

As you can see, this framework doesn’t really introduce anything new to the risk conversation we’ve been having over the last two chapters; it just rearranges things a bit. Of course, despite these high-level similarities, the two risk-based frameworks we’ve discussed differ in how they are implemented. For best results, you should combine ISO/IEC 27005 risk management with an ISO/IEC 27001 security program.

OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is not really a framework per se. Rather, it is a methodology for risk assessments developed at Carnegie Mellon University. So, while it falls short of a framework, it is fairly commonly used in the private sector. As a cybersecurity professional, you really should be aware of it and know when it might come in handy.

OCTAVE is self-directed, meaning that it uses a small team of representatives of IT and the business sides of the organization to conduct the analysis. This promotes

FAIR

If you want to apply a more rigorous, quantitative approach to managing risk, you may want to read up on the Factor Analysis of Information Risk (FAIR), which is a proprietary framework for understanding, analyzing, and measuring information risk. In fact, if you want a quantitative approach, this is pretty much the only international standard framework you can use. Recall that a quantitative approach is one in which risks are reduced to numbers (typically monetary quantities), while a qualitative approach uses categories of risks such as low, medium, and high.

The main premise of FAIR is that we should focus not on possible threats but on probable threats. Thus, its quantitative nature makes a lot of sense. In this framework, risk is defined as the “probable frequency and probable magnitude of future loss,” where loss can be quantified as lost productivity, costs of replacement or response, fines, or competitive advantage. Note that each of these can be reduced (perhaps with a bit of work) to monetary quantities. If this approach appeals to you, consider it in conjunction with the discussion of quantitative risk assessment in Chapter 2.

Information Security Frameworks

Armed with the knowledge gained from the risk management frameworks, we are now ready to properly secure our information systems. After all, our main goal is to develop costeffective defenses that enable our organizations to thrive despite the risks they face. For this reason, most information security frameworks have an explicit tie-in to risk management.

Broadly speaking, information security frameworks can be divided into two categories: those that look holistically at the entire security program, and those that are focused on controls. These are not mutually exclusive, by the way. As we will see, the NIST Cybersecurity Framework is compatible with the NIST SP 800-53 controls. Nor do information security frameworks have to be implemented in a wholesale manner. This is, after all, the beauty of frameworks: we get to pick and choose the parts that make the most sense to us and then tailor those to our specific organizational needs.

collaboration on identifying risks and facilitates communication with business leaders on those risks. It also follows the approach of focusing on the most critical assets in risk analysis to prioritize areas of attention. OCTAVE follows the 80/20 Pareto principle, which states that 80 percent of the consequences come from 20 percent of the causes.

This highlights one of the key benefits of this methodology, which is its focus on speed based on the fact that, for most businesses, time is money.

This risk assessment methodology is divided into three phases. The first is an organizational view, in which the analysis team defines threat profiles based on assets that are critical to the business. The second phase then looks at the organization’s technology infrastructure to identify vulnerabilities that might be exploited by those threats. Finally, in the third phase, the team analyses and classifies individual risks as high, medium, or low and then develops mitigation strategies for each. This classification scheme belies one of the advantages or drawbacks (depending on your perspective) of OCTAVE: it is fundamentally a qualitative approach to assessing risks.

Security Program Frameworks

Let’s start at the top. A security program is made up of many components: logical, administrative, and physical protection mechanisms (i.e., controls); procedures; business processes; and people. These components all work together to provide a protection level for an environment. Each has an important place in the framework, and if one is missing or incomplete, the whole framework may be affected. The program should work in layers: each layer provides support for the layer above it and protection for the layer below it. Because a security program is a framework, organizations are free to plug in different types of technologies, methods, and procedures to accomplish the necessary protection level for their environment.

A security program based upon a flexible framework sounds great, but how do we build one? Before a fortress is built, the structure is laid out in blueprints by an architect. We need a detailed plan to follow to properly build our security program. Thank goodness industry standards have been developed just for this purpose. Let’s take a closer look at two of the most popular information security program frameworks: the ISO/IEC 27000 series and the NIST Cybersecurity Framework.

ISO/IEC 27000 Series

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27000 series serves as industry best practices for the management of security controls in a holistic manner within organizations around the world.

The list of standards that makes up this series grows each year. Collectively, these standards describe an information security management system (ISMS), but each standard has a specific focus (such as metrics, governance, auditing, and so on). The currently published ISO/IEC 27000 series of standards (with a bunch of them omitted) include the following:

- ISO/IEC 27000
- ISO/IEC 27001
- ISO/IEC 27002
- ISO/IEC 27003
- ISO/IEC 27004
- ISO/IEC 27005
- ISO/IEC 27007
- ISO/IEC 27014
- ISO/IEC 27017
- ISO/IEC 27019
- ISO/IEC 27031
- ISO/IEC 27033

- ISO/IEC 27034
- ISO/IEC 27035

Overview and vocabulary
ISMS requirements
Code of practice for information security controls
ISMS implementation guidance
ISMS monitoring, measurement, analysis, and evaluation
Information security risk management
ISMS auditing guidelines
Information security governance
Security controls for cloud services
Security for process control in the energy industry
Business continuity
Network security
Application security
Incident management

It is common for organizations to seek an ISO/IEC 27001 certification by an accredited third party. The third party assesses the organization against the ISMS requirements laid out in ISO/IEC 27001 and attests to the organization's compliance level. Just as (ISC)2 attests to information security professionals' knowledge once they pass the CISSP exam, the third party attests to the security practices within the boundaries of the organization it evaluates.
It is useful to understand the differences between the ISO/IEC 27000 series of standards and how they relate to each other. Figure 4-3 illustrates the differences between general requirements, general guidelines, and sector-specific guidelines.
EXAM TIP You don't have to memorize the entire ISO/IEC 27000 series of standards. You just need to be aware of them.

As you probably realize, ISO 27001 is the most important of these standards for most organizations. It is not enough to simply purchase the document and implement it in your environment; you actually need an external party (called a Certification Body) to audit you and certify that you are in compliance with the standard. This ISO 27001 certification is useful to demonstrate to your customers and partners that you are not a security risk to them, which in some cases can be a contractual obligation. Additionally,
Figure 4-3
How ISO/IEC

27000 standards
relate to each
other

27001
ISMS Requirements

General Requirements

What is an ISMS?
What must it do?

27002
Code of Practice

General Guidelines

How should an ISMS
provide information
security?
27011
ISMS Guidelines for
Telecommunications
Organizations
How should an ISMS
provide information security
in a telecommunications
sector organization?

SectorSpecific
Guidelines

27799
Health Informatics ISMS in Health
How should an ISMS
provide information
security in a health
services organization?

- ISO/IEC 27037 Digital evidence collection and preservation
- ISO/IEC 27050 Electronic discovery
- ISO/IEC 27799 Health organizations

this certification can help avoid regulatory fines by proving that the organization practices due diligence in protecting its information systems. The certification process can take a year or longer (depending on how mature your security program is), but for many medium and large business, it is worth the investment.

NIST Cybersecurity Framework

On February 12, 2013, U.S. President Barack Obama signed Executive Order 13636, calling for the development of a voluntary cybersecurity framework for organizations that are part of the critical infrastructure. The goal of this construct was for it to be flexible, repeatable, and cost-effective so that it could be prioritized for better alignment with business processes and goals. A year to the day later, NIST published the “Framework for Improving Critical Infrastructure Cybersecurity,” commonly called the Cybersecurity Framework, which was the result of a collaborative process with members of the government, industry, and academia. The Cybersecurity Framework is divided into three main components:

- Framework Core Consists of the various activities, outcomes, and references common to all organizations. These are broken down into five functions, 22 categories, and 98 subcategories.
- Implementation Tiers Categorize the degree of rigor and sophistication of cybersecurity practices, which can be Partial (tier 1), Risk Informed (tier 2), Repeatable (tier 3), or Adaptive (tier 4). The goal is not to force an organization to move to a higher tier, but rather to inform its decisions so that it can do so if it makes business sense.
- Framework Profile Describes the state of an organization with regard to the Cybersecurity Framework categories and subcategories. A Framework Profile enables decision-makers to compare the “as-is” situation to one or more “to-be” possibilities, so that they can align cybersecurity and business priorities and processes in ways that make sense to that particular organization. An organization’s Framework Profile is tailorable based on the requirements of the industry segment within which it operates and the organization’s needs.

The Framework Core practices organize cybersecurity activities into five higher-level functions with which you should be familiar. Everything we do can be aligned with one of these:

- Identify Understand your organization’s business context, resources, and risks.
- Protect Develop appropriate controls to mitigate risk in ways that make sense.
- Detect Discover in a timely manner anything that threatens your security.
- Respond Quickly contain the effects of anything that threatens your security.
- Recover Return to a secure state that enables business activities after an incident.

Security Control Frameworks

Up to now we have reviewed the ISO/IEC 27000 series and the NIST CSF, both of which outline the necessary components of an organizational security program. Now we are going to get more focused and look at the objectives of the controls we are going to put into place to accomplish the goals outlined in our security program and enterprise architecture. This is where security control frameworks come in handy. This section presents three popular frameworks: NIST SP 800-53, CIS Controls, and COBIT.

NIST SP 800-53

One of the standards that NIST has been responsible for developing is SP 800-53, Security and Privacy Controls for Information Systems and Organizations, currently in its fifth revision (Rev. 5). It outlines controls that agencies need to put into place to be compliant with the Federal Information Processing Standards (FIPS). It is worth noting that, although this publication is aimed at federal government organizations, many other organizations have voluntarily adopted it to help them better secure their systems.

Basically, SP 800-53 provides specific guidance on how to select security controls. It prescribes a four-step process for applying controls:

1. Select the appropriate security control baselines.
2. Tailor the baselines.
3. Document the security control selection process.
4. Apply the controls.

The first step assumes that you have already determined the security categories (SCs) of your information systems based on criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. SP 800-53 uses three SCs: low impact, moderate impact, and high impact. If this sounds familiar, that’s because we discussed this categorization earlier in this chapter when we covered the NIST RMF and SP 800-60.

This exercise in categorizing your information systems is important because it enables you to prioritize your work. It also determines which of the more than 1,000 controls listed in SP 800-53 you need to apply to it. These controls are broken down into 20 families. Table 4-1 outlines the control categories that are addressed in SP 800-53, Rev. 5.

Let’s circle back to the example of the customer relationship management system we used when discussing the NIST RMF. Recall that we determined that the CRM’s SC was high because the impact of a loss of confidentiality was high. We can go through the entire catalog of controls and see which of them apply to this hypothetical CRM. In the

EXAM TIP For the exam, you should remember the five functions of the NIST Cybersecurity Framework and the fact that it is voluntary.

ID	Family	ID	Family
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security