

CHAPTER 5

Information Security Management

© Antishock/Shutterstock

EXECUTIVES AT THE EASY WORX COMPANY DECIDED THAT maintaining corporate data centers and infrastructure was too expensive. They had heard the marketing pitches about the cloud at trade shows and computer conferences they attended, so the executive team mandated that by the end of the year, they would be “completely in the cloud” and would have committed all their data centers to sales and leases by then. The technical teams worked diligently to make the top-down driven date and in the process took shortcuts, such as doing “lift and shift” of existing applications to achieve the deadline, rather than building cloud native applications to begin with, or re-architecting the existing ones for the cloud. They made the transition on schedule, but soon after, things broke, including several crucial cybersecurity countermeasures.

To further complicate matters, they had no fallback contingency plan because all their data centers were “gone!” The company spent a fortune to try to patch and retrofit reactively on the fly. They outsourced work to consultants, and they used every means available to try to compensate for lost time and money. Meanwhile, coinciding with these issues, the executives found that many of the fixed costs they were used to with their own data centers suddenly were variable costs with extreme spikes in expenses. Worse, because of the way they had deployed the systems in the cloud to their respective virtual private cloud subnets, the available tools were blind to how much individual departments were spending, for example, on virtual instances and on-demand service functions. Rather, they were only able to obtain aggregate cost reports, so they also had to build new tools just for cost accounting purposes. It became so expensive and unpredictable that the company ran into financial problems, and they laid off many of the employees who had worked so hard to fulfill the mandate.

Have you ever been adversely affected by a top-down decision that was mandated and was poorly planned?

Chapter 5 Topics

This chapter covers the following topics and concepts:

- Discuss the importance of strategy in information security decisions.
- Delve into the information security management life cycle (ISML) and DevSecOps.
- Take a look at some of the frameworks that can be useful in information security planning and management.

Chapter 5 Learning Objectives

When you finish this chapter, you should:

- ☐ Know what the information security management life cycle (ISML) is and why it is important.
- ☐ Explain the concepts of strategy and tactics, how to go about them, and how they relate to the information security management life cycle.
- ☐ Become familiar with governance frameworks, at a high-level, and explain these frameworks in relation to the role of technology manager.
- ☐ Start thinking about broader aspects of ISML and DevSecOps, including risk assessments and risk management.

5.1 Managing Information Security

Managing information and cybersecurity has often been an afterthought. Methods such as **DevSecOps** have strived to better integrate the security processes into the continuous integration and continuous deployment (CI/CD) loop. It's a good first step, but integrating information security management into the entirety of the planning and design processes is also needed, both at the strategic and tactical levels. The **information security management life cycle (ISML)** is another important set of processes to help ensure security integration. Managing information and cybersecurity begins with analyzing the security problems. Part of this involves doing risk assessments and establishing appropriate risk management procedures; we will cover these in greater detail after we examine threats and vulnerabilities. First, let's start by focusing on the planning, architecture, and design aspects of information security management in the ISML.

The last several decades have seen an unprecedented increase in the power of technologies, along with the power of new security tools. Yet along with these new technologies come new vulnerabilities. Tools for version management, requirements management, design and analysis, defect tracking, and automated testing have helped security professionals, software developers, and administrators to better manage the complexity of thousands of requirements and hundreds of thousands of lines of code. However, as the productivity of the software development environment has increased along with using **Agile** methods, it has also become easier to exploit weaknesses because of the sheer volume of code and files that can now be generated, including **Infrastructure as Code (IaC)**. As a result, security breaches continue to outpace security countermeasures installed to prevent them.

The rapid pace of software development and/or service implementations are not always compatible with the efforts needed to understand and to satisfy the simultaneous demands for functionality and security needs, because of deadlines and schedule pressures. Teams often spend too little effort in terms of understanding the real security problems; frequently too little is known about the needs of the users and other stakeholders in relation to security. There is often information overload relative to the technological and human resources environments in most companies to effectively keep up with security threats while maintaining business competitiveness.

Too often, managers and their teams tend to forge ahead without enough knowledge of any single aspect of these problems, sometimes providing technological solutions based on an inadequate understanding of the issues. The resulting systems, solutions, and procedures do not fit the needs of the users or stakeholders, do not provide adequate security for the most part, and deliver less than might reasonably be expected as functional solutions. The consequences of these mismatches are often seen in the inadequacy of security solutions for the customers and for solution providers. DevSecOps and the ISML is then should be are designed to help mitigate these issues by outlining processes and guidelines for the problem analysis and to define specific goals and designs for information security.

IaC	Infrastructure as Code refers to the use of automation with scripting and declarations in text-based configuration files such as JSON or YAML to provision infrastructure, whether bare metal or virtual. Tools such as Puppet® and Ansible® are often used for this.
DevSecOps	DevSecOps is a full-stack method for implementing security checks and features into the DevOps CI/CD pipeline.
ISML	The information security management life cycle (ISML) is a software development life cycle (SDLC) to incorporate information security processes into the overall information security management function, from conception to deployment of a system or service.

5.1.1 ISML and Strategy

The first step in the ISML involves defining the information technology and security strategy and tactics to achieve company goals. From these, we can develop the information and security architecture, followed by logical and physical security designs. Here we will cover a little bit about strategy and tactics in general before we dive deeper specifically into information and cybersecurity strategy and tactics. First, however, let's discuss information architecture.

The notion of information architecture helps technology managers to conceptualize the areas where information and systems are applied, and where these divide into strata, and where the security touchpoints are located. The horizontal strata include the business architecture, data architecture, and communications architecture. The horizontal strata serve the entire organization and include all the information needs. The vertical strata include the flows of the information through the lines of business at the operational, managerial, and strategic levels. Some of the information is used in primary activities, which are those that go directly toward the production and delivery of the product or service, and the support activities, which are those that involve overhead costs and technological infrastructure to carry out the primary activities. All of these layers as well as their connection points are of concern for information, cybersecurity, and technology management (**Figure 5.1**).

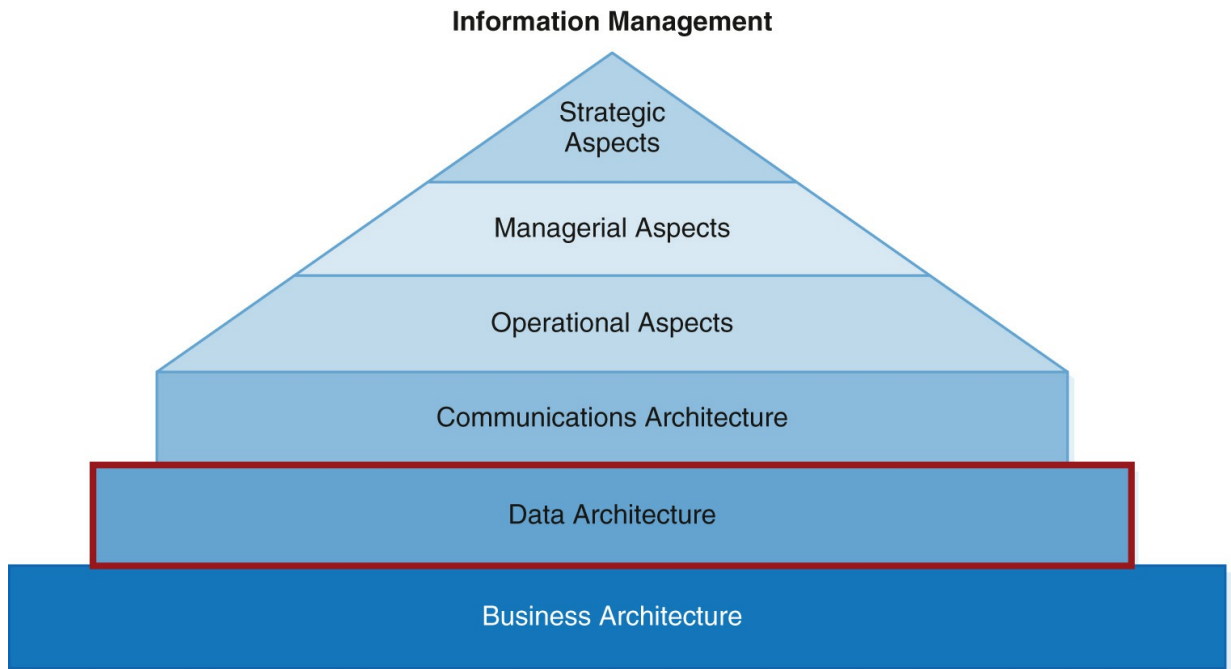


FIGURE 5-1 Information Architecture Strata

5.1.1.1 Strategy and Five Forces Model

To survive, let alone thrive, an organization must create a competitive advantage. A competitive advantage is a product or service that an organization's customers place a greater value on than similar offerings from a competitor. Unfortunately, competitive advantages are often only temporary because competitors tend to seek ways to duplicate the competitive advantage. In turn, organizations must continuously adopt new strategies. When an organization is the first into market with a competitive advantage, it gains what is called a **first-mover advantage**. The first-mover advantage occurs when an organization can significantly impact its market by being the first with a useful novelty. This can create a "name brand."

In Focus

A disruptive technology is one that has sufficient inertia to change a paradigm. That is, it can force new ways of finding new markets, or economically mining out assets from existing markets that have been forsaken as lost causes or sunk costs.

As an example, FedEx created a first-mover advantage many years ago when it developed its customer self-service software allowing people and organizations to request a package pickup, print mailing slips, and track packages online. Other parcel delivery services such as UPS quickly followed with their own versions of the software. Today,

customer self-service on the Internet is a standard for doing business in the parcel delivery industry. As organizations develop their competitive advantages, they must pay close attention to their competition through **environmental scanning** processes. Environmental scanning involves determining the competitive landscape and analyses of events and trends in the situations external to the organization.

In Focus

Environmental scanning is not only used in strategy, but it is used in threat assessments, as we shall see.

Information technology has the opportunity to play an important role in environmental scanning. For instance, PepsiCo/Frito-Lay, a premier provider of snack foods such as Cracker Jacks and Cheetos, does not just send its representatives into grocery stores to stock shelves—they carry handheld computers and record the product offerings, inventory, and even product locations of competitors. Frito-Lay uses this information to gain business intelligence on everything from how well competing products are selling to the strategic placement of its own products on shelves and rows. In assessing a strategy, whether commercial, operational, or relative to cybersecurity, we find Michael Porter's Five Forces Model useful.^{1, 2} The Five Forces Model helps us determine the relative attractiveness or aversion toward various strategic decisions based on the following categories and criteria:

- Buyer power
- Supplier power
- Threat of substitute products or services
- Threat of new entrants
- Rivalry among existing competitors

Buyer power in the Five Forces Model is high when buyers have many choices regarding vendors and low when buyers' choices are too few. To reduce buyer power (and create a competitive advantage), an organization must make it more attractive for customers to buy from it rather than from its competition. One of the best examples is the "loyalty program" that many organizations offer. Loyalty programs reward customers based on the amount of business they do with a particular organization. The travel industry is famous for its loyalty programs such as frequent-flyer programs for airlines and frequent-stayer programs for hotels. Relative to ISML, buying power is important to picking security tools and approaches. As a consumer, if my buying power is low, I might be locked into a single vendor's toolkit. What if those tools end up being inadequate? For example, what if I chose an enterprise cybermonitoring technology and later began deploying containers and discovered that the tools could not monitor containerized applications? How difficult would it be to switch

vendors along with the effort to reconfigure and deploy new tools and exit the contractual or licensing agreement?

In Focus

Importantly, knowing about strategy lends to understanding strategic technology, as opposed to operational or tactical technologies.

Supplier power in the Five Forces Model is high when buyers have few purchase choices. A supplier organization in a market will want buyer power to be low. A supply chain consists of all parties involved, directly or indirectly, in the procurement of a product or raw material. As a buyer, the organization can create a competitive advantage by locating alternative supply sources. IT-enabled business-to-business (B2B) marketplaces can help. A B2B marketplace is an Internet-based service that brings buyers and sellers together. One important variation of the B2B marketplace is a private exchange, which is a B2B marketplace in which a single buyer posts its needs and then opens the bidding to any supplier who would bid. There are proprietary suppliers and open-source suppliers. Proprietary suppliers strive to lock their customers into their solution by making it difficult for customers to switch vendors, either by means of the investment to implement the technology or by contractual agreements, or both. Open-source vendors typically build on standard frameworks that make moving to other technologies simpler, but they often lack many features that proprietary vendors supply. Open-source organizations often do not provide technical support for their products, or if they do, it's through third-party contractors. Some vendors have free or open-source community versions and proprietary versions, with the free or open-source version lacking valuable features. Managers should evaluate the features versus the cost of switching vendors when making security technology decisions (**Figure 5.2**).



FIGURE 5-2 Michael Porter's Concept of Strategy

© Peepo/E+/Getty Images.

The threat of substitute products or services in the Five Forces Model is high when there are many alternatives to a product or service and low when there are few alternatives. Switching costs are those that can make customers reluctant to switch to another product or service. The switching cost may not be monetary. Amazon.com is an example. If you purchase products at Amazon, over time Amazon develops a unique profile of your buying habits. When a customer visits Amazon repeatedly, Amazon can begin to offer products tailored to that particular customer based on the customer's profile. These preferences are a form of intellectual currency, which in fact is sold to undisclosed other parties by Amazon, as is done essentially by all such service providers. The other two forces, threat of new entrants and rivalry among existing competitors, are more important to business positioning and less important in the ISML, although managers should keep an eye on what security technologies are emerging in the marketplace that might be useful and be on the lookout for which ones in use might become obsolete or discontinued in a short time frame.

In Focus

If a social media company you use, such as Facebook, Twitter, or LinkedIn, does not sell a product, it is likely you are the product.

5.1.1.2 Strategy and Tactics

As we noted earlier, strategy is not well defined, either as a process or a concept. Technology managers need to determine what **technology strategy** means within our organizations, and then we must ensure that it is incorporated into the ISML. Some organizations conduct strategic planning with the assumption that a strategy can be engineered. Other organizations use brainstorming or “visioning” sessions to try to qualify and organize the strategic mission and vision (**Figure 5.3**). The processes range from a science to an art and skills-based to talent-based. In other words, if strategy is a science, there will be preplanned steps, contingencies, and action plans. If it is an art, then strategy will be organic, agile, and emergent as the environment changes. If it is skills based, then strategy will lean on structured and quantitative measures such as **Six Sigma®** but if it is talent-based, then strategy will lean on “outside-the-box” and creative thinkers and loose criteria such as **CMM®, CMMI®**, or the like.

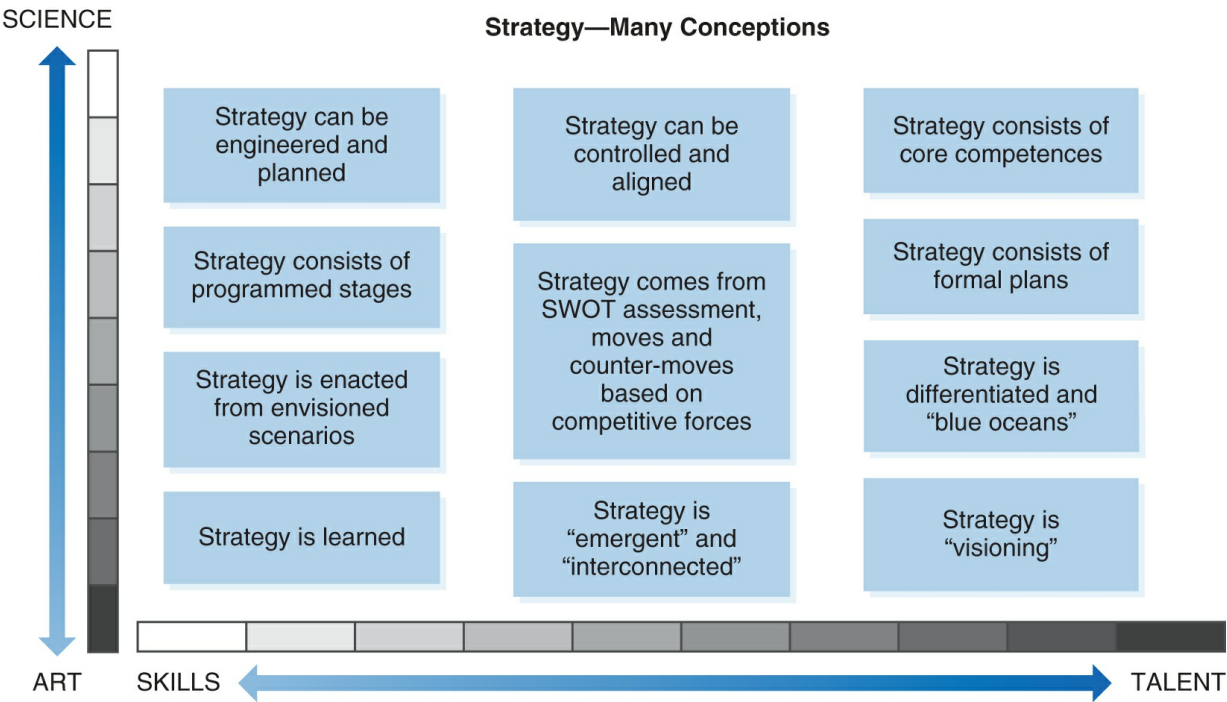


FIGURE 5-3 Strategy Conceptions

Technology Strategy	Technology strategy is a concept and process that determines the overarching goals of the organization and is important in the ISML. In addition, technology strategy informs strategic security initiatives.
Technology Tactics	Technology tactics are the moves made within a strategy and are important in DevSecOps. Technology tactics also inform tactical security initiatives.
Technology Operations	Technology operations is the execution of both technology strategy and technology tactics. Moreover, technology operations incorporate both ISML and DevSecOps.
Six Sigma	Consists of techniques and tools to measure and implement processes and process and quality improvements. It is fundamentally prescriptive in outlining what must be done and how to do it.
CMM /	The Capability Maturity Model (CMM) consists of a set of criteria that define the maturity of

CMMI organizational processes. It is primarily descriptive rather than prescriptive. CMMI builds on CMM to include integration criteria. Specialized organizations such as the CMMI Institute® provide cybersecurity-specific CMMI criteria, training, and auditing.

Tactics are generally the steps taken to achieve a strategy. Using the chess analogy, a strategy might be to use the king's bishop to control two diagonals where it can attack the central square, or to use a pawn to open up pathways for the pieces to advance from the back and into the fight for the central squares. Tactics are the moves according to the rules, such as a piece that can move horizontally, or a tactic might be to move the bishop to an active square. **Technology operations** incorporates both the **strategy** and the **tactics** to ensure that systems security and functionality are sustained (**Figure 5.4**).



FIGURE 5-4 Strategy, Tactics, and Operations

© Domin_domin/E+/Getty Images.

Organizations have primary activities and support activities. Primary activities include inbound logistics (inputs), operations (processing), outbound logistics (distribution), marketing and sales, and service. This is sometimes referred to as the value chain. Support activities are those that facilitate the primary business activities. For instance, a hospital's main function is to treat patients, but the health information systems are necessary to support that function. Thus, primary activities are supported by the technological infrastructure. Defining the technology strategy encompasses the business and security processes across the value chain. The functions of business and security are mutually supportive. Security is useless if systems are not operational, indeed, a class of attacks that include denial of service specifically aim at disrupting business. Likewise, a business cannot

function effectively without good security. The idea behind defining the technology strategy holistically as part of ISML is because of these mutually supportive and interdependent functions.

One method for formulating strategy is to utilize a principles framework. Principles guide the strategy, which determine the tactics. There are many ways to categorize principles, but three of the most common are management principles, vendor principles, and system principles (**Figure 5.5**). Management principles include the degree of risk the leadership in the organization is willing to accept, for example, deciding to delay security patching to maintain productivity would reflect a high risk-taking management approach. The importance of time to market compared to developing quality and rich features in a product has a bearing on the effort put into testing and security processes. Whether management is focused on cost savings to deliver low-cost goods or services compared to producing or delivering something unique may determine decisions such as the extent to which cybersecurity is baked into their cost of doing business.

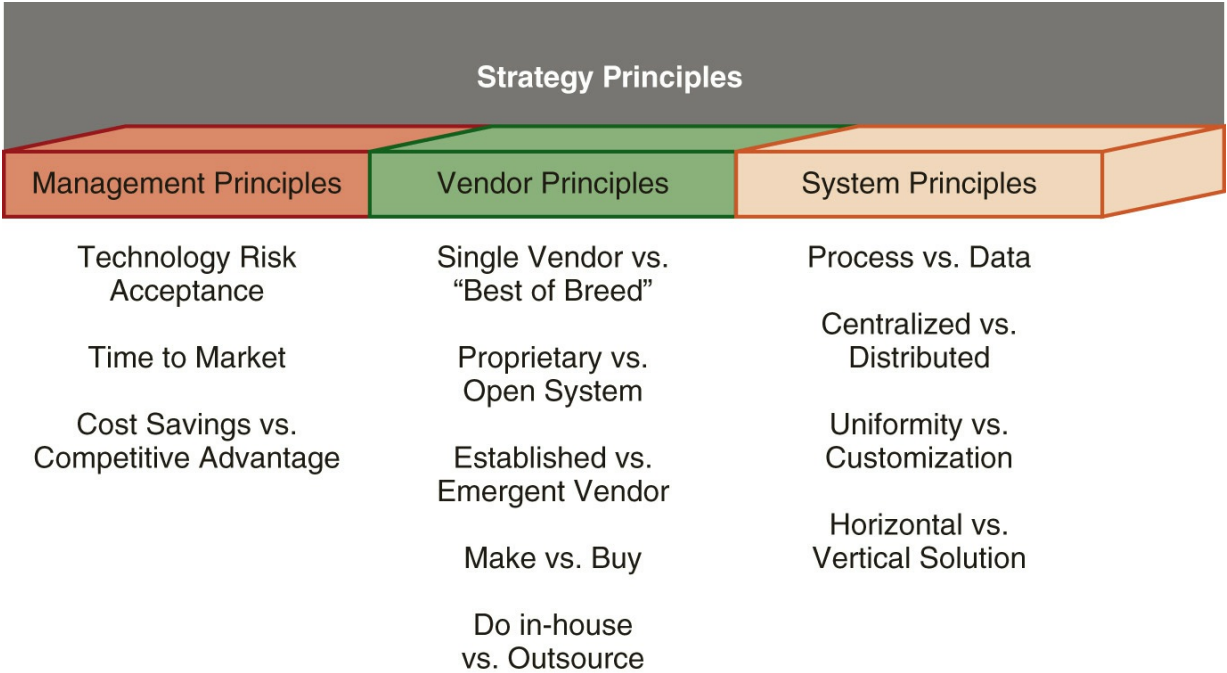


FIGURE 5-5 Principles Framework

Vendor principles include whether to leverage a single vendor or acquire technologies that are the best in their categories even though it may involve many vendors. Similarly, a company may try to leverage technologies that are feature rich with good technical support that tend to be proprietary, versus selecting open-source technologies that may require substantial inhouse development and support. Vendor principles also include whether or not to work with small emergent vendors who may be more innovative than larger, more established vendors, but may carry greater risk, or pick one that has been in business for a long time. They also include whether to build the technologies, or buy them commercially

off-the-shelf (COTS).

System principles include whether to design systems around processes or the data, whether to produce centralized or distributed solutions, whether to build or buy a technology that is general purpose and uniform, or whether it should be highly customized or customizable. Finally, a system principle would include whether the solution fits horizontally across an organization and its value chain, or whether it serves a particular vertical, such as a department or business function. Here, the concept of **cloud native** is important. Cloud native is a term used to describe container-based environments, which can be migrated easily between on-premise systems and the cloud.

To determine the working principles for our technology selections, a survey may be distributed to the stakeholders. The survey would use a Likert scale of, say, 1 to 7 points, with competing principles arranged on polar ends of the survey, such as to the question: “Should we leverage proprietary vendor solutions for volume discounts and feature richness” on pole 1, and “Should we leverage open-source technologies to keep from being locked into a vendor” on pole 7, such as seen in **Figure 5.6**.

Q1: It is most important to leverage:

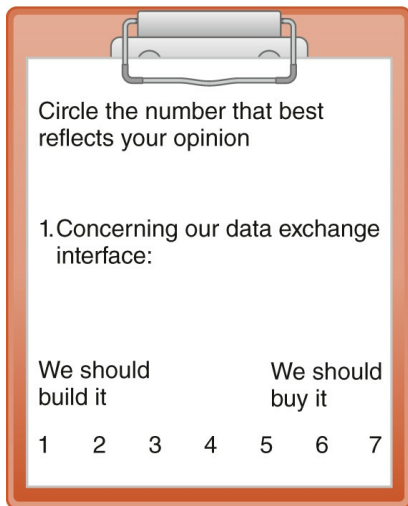
Open Systems::	1	2	3	4	5	6	7
::Proprietary Systems							

Q2: It is most important to buy from:

Established Vendors::	1	2	3	4	5	6	7
::Emerging Vendors							

FIGURE 5-6 Sample Survey Question Format

After we collect the surveys and analyze them, we start with the mean score from all the stakeholder responses, which indicates the average on where stakeholders lean on that particular principle. For example, a mean score of 6 on the question of whether to build (= 1) or buy (= 7) indicates the stakeholders strongly lean toward buying the technology. When we evaluate a technology, we should weight purchasing greater than building. Hence, given two equally appealing technology proposals, one proposed to build in-house, the other to acquire, we would lean heavily toward purchasing, but if we are the decision-maker, we might still choose to build it, but we had best be prepared to justify the decision. The standard deviation tells us how much the stakeholders agree or disagree. If there is a large standard deviation, we will want to get the stakeholders together to discuss it and iron out the principle to gain better consensus (**Figure 5.7**).



Circle the number that best reflects your opinion

1. Concerning our data exchange interface:

We should build it				We should buy it		
1	2	3	4	5	6	7



© Fizkes/Shutterstock.

Mean

- What the average is
- Ex: $M = 6.25$

Standard Deviation

- How much stakeholders agree or disagree
- Ex: $SD = 0.02$

FIGURE 5-7 Principles Survey

5.1.2 ISML and Governance Frameworks

Once the information strategy has been defined, ISML incorporates requirements from applicable governance frameworks. There are many regulations and governance frameworks that we will cover in greater detail later; for now, we'll just discuss a few examples. Ultimately, regulatory and governance requirements end up as implementable tasks during the DevSecOps process and are used by both the Operations and Compliance departments for conformance testing and auditing.

Regulatory and governance frameworks have expanded in recent years. Because of mismanagement and carelessness with important information, including information related to or managed by government entities, there are growing legislative actions and increasing regulatory controls enacted for the governance of organizations, especially those that are or deal with government agencies. Some of the regulations have targeted the protection of privacy in response to cases that have ranged from criminal front operations that were able to steal information from credit bureaus, to the loss of laptop computers that contained sensitive and unprotected employee and military data.³ Governance therefore is in essence the processes by which organizations are managed according to some criteria. In its most formal sense, governance typically means conforming to regulations and/or requirements set for an agency, industry, or organization.

When many employees in the United States are asked about workplace governance, they refer to the activities of the Department of Labor and the **Occupational Safety and Health Administration (OSHA)**. While these are among most visible governance bodies, there are many lesser-known but equally important agencies and regulatory bodies of which managers need to be aware. Two major areas where managers need to acquaint themselves involve standards by which regulators hold certain organizations responsible for taking or preventing certain actions and those that pertain to the development and enforcement of personnel policies. One example is the **Sarbanes–Oxley Act of 2002 (SOX)**

that was passed by Congress in response to several highly public corporate failures. In this legislation, all companies listed on a U.S. stock exchange must provide an assessment of their internal financial controls in their annual report. Like most regulations, there have been several updates to SOX over the years, which keeps the compliance teams busy. While SOX specifically applies only to companies listed on a U.S. stock exchange, the United Kingdom implemented similar provisions in the **Combined Code on Corporate Governance**, and in the European Union, similar actions were taken with the **Basel II**, which also recommended the implementation of internal controls.

The implications of these regulations for information systems are that controls must be in place for systems that handle company financial information, which requires companies to pay increased attention to the information systems that store, process, and transmit that information. While this represents a significant undertaking for private companies, the U.S. government is particularly affected. For example, the Office of Management and Budget (OMB) revised Circular A-123 requires federal agencies to implement internal controls similar to those found in SOX, and the Government Information Security Reform section of the National Defense Authorization of 2001 helped coordinate federal information policy with respect to information security.

In addition to laws covering financial controls, several pieces of privacy legislation have been enacted in the United States, United Kingdom, and European Union. Among these are the **U.S. Gramm–Bliley–Leach Act (GBLA)**, also called the Gramm–Leach–Bliley Act, which requires financial institutions to disclose to their customers their data-sharing policies and prohibits those institutions from selling customer information, and the **U.S. Fair and Accurate Credit Transactions Act (FACTA)** that requires safeguards to help prevent identity theft. The UK's **Data Protection Act**, the EU's many privacy protection laws, and Canada's **Personal Information Protection and Electronic Documents Act (PIPEDA)** all contain requirements that affect the collection, storage, and transmission of personal information.⁴ There are many other regulations and governance frameworks we will encounter further down the road.

In Focus

Treaties are important to international regulatory enforcement. A treaty is a written agreement between nation states or international agencies that is designed to establish a relationship governed by a public international law. A multilateral treaty has several parties, whereas a bilateral treaty has two.⁵

5.2 Technology Management and Governance

As indicated, there are a variety of national and international regulations along with various regulatory agencies. Later, we will go into some detail about how these fit into the information security management processes (risk assessment and risk management, specifically), along with criteria used to help managers comply with regulations and laws—as well as to help us ensure a well-managed organization from a security standpoint. At this stage, we will try to bridge between those two aspects for managing securely by briefly discussing management and governance.

Earlier, we defined governance, and previously we gave a summary of organizational and managerial rights and duties. Putting these two concepts together, we might say that management and governance means using policies, processes, and procedures to ensure that the organization conforms and performs according to the criteria defined for—and by—the organization to maintain organizational and security effectiveness. Knowing how laws and regulations as these relate to governance is important to managers in organizations where information systems are used.⁶ Beyond the administrative features we have addressed thus far, also important are elements such as responsible, efficient, and effective managing of human resources and knowledge capital. In other words, management and governance strive to meet (or stay within) controls laid down as regulations, laws, guidelines, best practices, and ethical advice given by stakeholders.⁷

Technology management needs to address some categories of activities to both govern and be governed well. Among these are performing risk assessments; developing risk management strategies and plans; conducting audits regarding assets, policies, and procedures; doing background checks on new employees and performance evaluations of current ones; producing performance plans and communicating expectations; providing or funding training and development; conducting system and network testing and evaluation; developing contingency and remediation plans; and ensuring proper handling and reporting of incidents and continuity of operations, among other activities.⁸

5.2.1 Governance and Security Programs

Earlier, we mentioned a few regulations and frameworks used to govern actions about various aspects of information such as employee and/or customer privacy. There are many others we will discuss later. In actuality, security criteria by themselves are inert. They become active when management enacts programs to ensure compliance with the criteria (which includes regulations and laws). To highlight this point, the Federal Information Security Management Act (FISMA) was an attempt in the United States to consolidate laws and regulations for a variety of security issues.⁵ For the most part, FISMA officially applies to U.S. government agencies and their suppliers and contractors, but in fact, while security criteria may differ, the processes and procedures such as performing risk assessments, conducting audits, doing background checks, providing security training, and so forth, can be very applicable and helpful to most organizations.

Even though it may not be required for an organization, using one or more, or a blend, of security criteria and management programs might help to improve information security.

While laws and regulations cannot be ignored and compliance is mandatory, oversight of nonregulated security programs should similarly undergo a security design, implementation, and inspection in the information security management life cycle. For example, the life cycle might include an iterative process of evaluating business needs, resolving business needs with business processes, distilling those processes into categories in which security is one, and within the security category, determining risks/vulnerabilities, determining countermeasures, including their costs and cost-to-benefit metrics, implementing security controls, assessing whether the controls were effective, and then ascertaining approvals and authorizations, then the process is repeated. The steps are as follows:

1. Develop relevant criteria for governance.
2. Perform risk assessments.
3. Conduct random periodic audits of assets, policies, and procedures.
4. Consistently do background checks on new employees.
5. Consistently do performance evaluations of current employees.
6. Regularly do performance plans and communicate expectations.
7. Provide or adequately fund training and development on security and relevant regulations.
8. Conduct random periodic system and network testing and evaluation.
9. Develop and update contingency and remediation plans.
10. Review to ensure proper handling and reporting of incidents.
11. Prepare and audit business and operations continuity contingency plans.

While governance is essentially an administrative process, it requires extensive knowledge of the technological considerations. For the most part, a good administrative approach is useless unless there are technical approaches to follow and enforce them. Again, policies must be both enforceable and enforced. Enforceability is usually an administrative consideration, enforcement is often (but not always) a technical consideration.

5.2.2 Enacting Security Programs

After the preliminary steps have been completed in the ISML, ongoing assessments, including risk assessments and risk management, take place. Because there are so many

risks and because they are so complex, managers usually begin by assigning them to a quadrant in a risk matrix, for example, consisting of low, medium, or high risk on an x-axis, against low, medium, or high on a likelihood (or exposure) y-axis. This yields an “impact” assessment. The procedure, while clearly far from complete in showing the range and degrees of risk and impact, can at least help managers to prioritize which of their many security tasks they should attend to first. In relation to the problem analysis part of this process, there are several important objectives to consider, as follows:

- Problem analysis is the process of understanding real-world problems and users’ needs and proposing solutions to meet those needs.
- The goal of problem analysis is to gain a better understanding, before development of solutions begins, for the target problem to be solved.
- Eventually, but not immediately, the root cause—or the problem behind the problem—needs to be determined for a final solution.

As an example, a low impact incident might be the potential loss of confidential information. To highlight this in a tangible way, although the fairly recent Snowden and WikiLeaks disclosures of U.S. National Security Agency spying technologies may be embarrassing to the U.S. government, but that specific disclosure was perhaps not catastrophic. Enemies of the United States already knew about these programs. Similarly, if an employee posted on his or her social media site a company assessment of a rival’s technical strengths and weaknesses, this would be troubling for sure, but likewise not catastrophic even if the posting was defamatory in nature. Of more moderate concern to a corporation might be the public disclosure of a company’s network topology. On the surface, this may seem benign, but in actuality, it would save an astute hacker time and energy (and possible detection) to “footprint” a target site. High impact might be a case where a hacker breaches a loosely protected database in a HIPAA-regulated company and retrieves patient histories and insurance information, or in the actual case where a state actor was able to steal all of the security clearance background information from the U.S. Office of Personnel Management (see 2014 OPM security breach). The state actor could then map and identify every U.S. intelligence asset around the world. That was catastrophic!

Security programs therefore need to incorporate measured and hierarchically proportionate countermeasures. The Federal Information Processing Standards (FIPS) recommends conducting risk assessments and analyses using structured methods; implementing access controls; offering security awareness and technical training; conducting audits and resolving these to the accountable manager; implementing configuration control systems; performing contingency planning; using technologies that can perform identification, authentication, and authorization; having an incident reporting and response plan; and having in place (among other things) an escalation procedure for security breaches.

5.3 Control Frameworks

Once the preliminary and foundational steps have been taken to develop strategies and determine applicable regulatory and governance criteria, we need a framework, or set of frameworks, to help guide the activities throughout the ISML. There is an abundance of control frameworks; we will introduce a few of the more common ones here. Some of the prominent control framework acronyms that we will expand on as we go along are ITIL, ITSM, BS15000, and ISO2000x. For example, the *IT Infrastructure Library (ITIL)* is a set of management best practices that was developed in the United Kingdom for information systems technology and has broad support throughout Europe and Canada. *Information Technology Service Management (ITSM)* is an IT management framework that implements the components of ITIL.

The main goal of ITIL/ITSM, in terms of most management frameworks, is to enable an organization to establish and manage its IT infrastructure in the most effective and efficient manner possible. The British Standard *BS 15000/ISO 2000x* takes these processes and divides them over the five areas that are entitled: Release Processes, Control Processes, Resolution Processes, Relationship Processes, and Service Delivery Processes. These areas are then implemented and managed to improve IT delivery efficiency and effectiveness in much the same way as in ITSM. Let's take a look at these more closely.

In Focus

Many configuration frameworks are known as “checklists” in the security literature because they tend to list steps that are to be taken, and then security auditors check them off as they go down the lists to see if an organization is compliant.

5.3.1 ITIL / ITSM

ITIL/ITSM is unique in that it focuses on the provision of information technology as a service. While previous versions of ITIL aggregated IT processes into one of two broad areas—service delivery, which is responsible for the management of services, and service support, which relates to the effective delivery of services—versions 3 and 4 have at their core service strategy, with service design, service transition, service operation, and continuous service improvement defining the remainder of the service life cycle, as follows:

1. **Service strategy**—Defines who will receive what services and how the provision of those services will be measured. In addition, this area includes defining the value of the services offered, identifying the critical success factors associated with enacting the service strategy, and developing an understanding of the roles and responsibilities of

individuals who are executing the strategy.

2. **Service design**—Specifies the architecture, processes, and policies that will be used to implement the service strategy. This includes the catalog of services to be offered and the specification of the level, or quality, of those services, the specification of capacity and availability required to meet those service levels, and the required continuity and security management specifications. Also included in service design is a clear specification of supplier requirements. The design is pulled together into a Service Design Package (SDP).
3. **Service transition**—Provides the resources required to implement the SDP. This includes managing change, configuration, product release control, and knowledge management to ensure that operations provide a known and standard level of service.
4. **Service operations**—Provides the agreed-upon levels of service and handles the routine events as well as the unexpected incidents and problems. Service operations also includes the service desk function, which provides centralized customer service and serves as a focal point for collecting and managing information related to the current state of operations.
5. **Continual service improvement**—Evaluates current operations in an effort to find ways to improve them. This consists of defining what can and should be measured, collecting and analyzing data to identify variation from standards or opportunities for improvement, and planning and implementing appropriate change, and this is an ongoing process.

5.3.2 COBIT

Another popular framework is the ***Control Objectives for Information and related Technology (COBIT)***. Like ITIL, COBIT defines, identifies, organizes, and links IT activities and resource to business processes to ensure that the IT assets are secure, verifiable, and in COBIT's case in particular, auditable. The framework contains 34 processes, which are organized into the four major areas: planning, building, running, and monitoring, as follows:

1. **Planning**—Covers the processes that distill down from strategic plans to tactical plans. For instance, it suggests strengths, weaknesses, opportunities, and threats (SWOT) analyses, risk assessments, and contingency planning.
2. **Building**—Incorporates the security process life cycle—specifically the ISML, along with materials and requirements planning, requisitions and acquisitions, implementation and rollouts or deployments.

3. **Running**—Is as indicated—covers the operations and business processing, service and/or product delivery, and support.
4. **Monitoring**—Covers measuring critical success factors (CSFs), collecting business alignment metrics, problem detection and incident reporting, and includes a feedback loop.

COBIT provides criteria and guidance for each of these areas. Additionally, COBIT separates the framework components into control objectives with audit guidelines and control practices, activity goals for efficiency and effectiveness, and specific metrics that indicate maturity, performance, and goal attainment.

In Focus

While ITIL and COBIT are the most popular management frameworks, other frameworks do exist. The U.S. Government Accountability Office created the IT Investment Management Framework, which is a five-stage maturity model. The Software Engineering Institute at Carnegie Mellon University released the Capability Maturity Model Integration (CMMI) framework for process improvement. While the maturity model is probably best known in relation to software engineering, there are corollaries for security management as well.

5.3.3 ISO 27K IT Security Control Selection

Within the broader context of IT management, there are specific frameworks for IT security that enhance the generalities and, together, tend to be synergistic. The most popular among these security frameworks is the ISO 27000: 27001/27002 (17799), the de facto series of standards for information system security internationally. The ISO 27000 (ISO27K) family of standards provides guidelines that explain how to structure the information security management system (ISMS), analyze risks to identify suitable information security controls, and measure and improve the ISMS thereafter. It does not go into detail on implementing specific controls, but it does provide general guidance by reference to the standards.

In Focus

If you are actively implementing the ISO27K standards, you are welcome to join the ISO27k Implementers' Forum to discuss the practicalities with others doing the same thing. The community of forum members will be pleased to advise you in relation to implementation, giving you the benefit of their collective experience in this field (www.ISO27001certificates.com).

The Information Technology Code of Practice for Information Security Management (ISO 27002) gives specific guidance in the “how” of information system security and is divided into 11 sections that broadly address information security and provide guidelines and best practices for ensuring the security of all information assets, as seen here:

1. **Security policy**—The security policy section objective is to provide management direction and support for information security.
2. **Organizing information security**—The organizational security objectives include managing information security within the organization and maintaining the security of organizational information processing facilities and information assets accessed by third parties.
3. **Asset management**—The asset management objectives include assigning responsibility for assets and establishing their classification related to the requirements of the organization.
4. **Human resource security**—The human resource security objectives address responsibilities before, during, and at the end of employment.
5. **Physical and environmental security**—The physical and environmental objectives address issues related to physical areas and equipment.
6. **Communications and operations management**—The communications and operations management objectives address a variety of areas, including operational procedures, contracted service delivery, system planning and acceptance, protection against malicious code, backups, network security, media handling, exchange of information, E-commerce, and monitoring.
7. **Access control**—The access control objectives include determining business requirements for access, managing users, specifying user responsibilities, controlling access on networks, operating systems, and applications, as well as addressing issues related to telecommuting.
8. **System acquisition, development, and maintenance**—The system acquisition, development and maintenance objectives include the specification of security requirements early in the acquisition or development process, ensuring the correct functional requirements of applications, cryptographic controls, file security, and technical vulnerability management.
9. **Incident management**—The incident management objective specifies requirements related to reporting and management of incidents.
10. **Business continuity management**—The business continuity management objectives

deal specifically with issues related to interruption of business activities.

11. **Compliance**—The compliance objectives include ensuring the compliance with legal requirements, following security policies and standards, and addressing the IT security audit process.⁹

While ISO 27702 provides the controls, ISO 27001 Information Security Management System Requirements provide an approach to managing security in a well-defined and systematic way. Additionally, it provides a means for an organization to certify their adherence to the security standard.

5.3.4 NIST 800-53

Another popular framework is the Recommended Security Controls for Federal Information Systems (RSCFIS), which is also known as the *U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53*. The framework offers specific guidance in information system security management and control selection. NIST SP 800-53 outlines security controls that are based on the Federal Information Processing Standard (FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems. It was designed to give guidance for organizations implementing FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. NIST 800-53 organizes security controls into 3 classes and 17 associated families and provides guidance for establishing different groups of controls. Examples are seen in **Table 5.1**.¹⁰

TABLE 5-1 NIST 800-53 Classes and Families		
CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

NIST 800-53 outlines two baseline groups of controls that are to be implemented on all information systems in an organization or unit. It also specifies system controls unique to an individual system. The partitioning of controls in this manner is designed to be cost efficient, as well as to provide a central and standardized means of deployment and security assurance. The establishment of security control baselines designed to meet the organization's specific policy requirements enhances this process. In addition to establishing the baseline framework, the publication also provides guidance on the process of selecting and specifying security controls to manage risk through a nine-step process, as follows:

1. Categorize the information assets.
2. Select baseline controls.
3. Adjust the controls based on organizational factors.
4. Document the final set of controls.
5. Implement the controls.
6. Assess the implementation and impact of the controls.
7. Determine the risk associated with the information system.
8. Authorize system use if the risk is determined to be acceptable.
9. Monitor the controls and system for effectiveness.

Mini-Case Activity: What Went Wrong?

The following scenario involves a curious neighbor, who escalates a passive surveillance into an active attack. What do you think went wrong, and what should be done in the future to try to prevent a similar situation from happening?

Episode: Your neighbor, named Bob, was sitting at home working on his laptop, and with a right mouse button click, he noticed wireless networks were available, and one was unsecured! So, he attempted a connection. Of course, most wireless networks are secured, and trying to connect to them will be difficult even if using a weak WEP or WPA protocol (although some password crackers can break these). Further still, many of them will have firewalls that will block his attempt—but there are the occasions when one will find an unsecured network, and that probably means a poorly protected system as well.