DOWNLOAD PDF CHAPTER 1: INFORMATION SECURITY GOVERNANCE

Chapter 1 : Information Security: Principles and Practices, 2nd Edition

Start studying CISM Information Security Governance Chapter 1. Learn vocabulary, terms, and more with flashcards, games, and other study tools.

Deliver, Service, and Support Monitor, Evaluate, and Assess As you may notice, these four domains apply very well to system development processes, which is helpful. Policies may need to be developed for a system as it goes through the stages of development. The four domains are meant to be done in sequence, each building on the work of the previous domain. Align, Plan, and Organize First Domain Moving ahead to page 6, the author begins a discussion of the first domain: Align, Plan, and Organize. Note in the graphic on page 6 that this domain is the only one that provides input to more than one successor. The Align, Plan, and Organize domain is where we learn about the user requirements, the needs of the organization, and the goals of the organization. The text stresses SLAs. These are agreements about the services we will receive, and about the services we will provide. In either case, the agreement should specify: The text recounts a few details about the Target data breach of Read the article on Mr. This points out the necessity of having proper controls, and making sure they are being used. This phase includes identifying the threats, vulnerabilities, and risks associated with this organization and its activities. This knowledge is handed off to the people who conduct the next phase. Build, Acquire, and Implement Second Domain This domain assumes we have obtained the requirements for our system in the previous phase. The word build might be better understood as design and create. The text points out that creating policies and controls cannot be done without proper input from the previous phase. This phase also is concerned with changes to existing systems, adding new systems, and managing the changes that will take place. The people working on this phase need to plan for and manage the changes that will take place for the systems and the people who use them. The text lists several outputs for this phase: The text tells us that this phase makes changes to any controls, policies, procedures, contracts, and SLAs that are not working, based on observations, reports, and data on operations. This assumes that you can still make changes in contracts and SLAs. Some environments would not have those options once such agreements are in place. Testing takes place on the entire environment. We determine whether the controls are serving the big picture goals business requirements, strategic goals of the organization. The system is assessed and audited several ways: IA is concerned with protecting information that is being processed or being used. Why do we care about that subset? The text makes it a bit clearer by listing the "five pillars of the IA model". You will recognize most of them: There seems to be agreement on lots of web sites, including the Department of Defense , that IA does embrace these five concepts. So, what about the two new ones? The text continues with a longer disscussion on each of the five points. As the text explains, a good governance process will examine the rules that it enforces and recommend changes to them when they do not, should not, or should no longer apply to the requests that are being turned down. A typical governance process will consist of several layers, attempting to coordinate requests with the operational and strategic needs of various elements of the organization. It is often true that a request will have to go through several layers of approval before it runs into a need that creates a conflict. Examiners on committees at each level need to have an understanding of the big picture, and of the needs of their specific organizational areas. Governance is especially important when processes are examined by government auditors, and can show that an organization is making the best effort possible to comply with laws and regulations. Policies I think the author started on the wrong track this time. A policy is not a document, or even a series of them, although a policy is often stored that way. A policy is a rule, or a set of rules, that affects how we want our organization and its employees to function. As the text states, the idea behind a policy may start with a principle, which is often a broad, general statement of what we believe to be right, true, or beneficial. A policy is more detailed, and more specific about what we expect our people to do. The list on page 16 shows us a hierarchy of related concepts: Note that the items near the top of the list are more general, and they become more focused and specific as we move down through the first four bullets. The text spends several pages telling us why policies and the other items in a policy framework are important and needed. They are the first line of defense from internal and external attacks. They control and

manage changes to our systems. They provide a statement about who does what in an emergency. They reduce the cost of wasted or counterproductive efforts. They provide a means to comply with laws and regulations. The text warns us that simply making a policy does not guarantee it is a good policy. Policies should be reviewed before and after they are put in place. New policies or revisions may be needed when processes are changed, when systems are changed, when "improvements" are made, and when problems are being resolved. Chapter 2 Chapter 2 begins with discussion of business drivers, The most obvious one is money. The chapter presents some examples of data breaches that caused companies to spend millions of dollars in reparations to customers whose personal data were exposed. In a case like that, there is also the loss of good will and customer loyalty to be considered, which will affect future earnings for the company. When a breach is the result of improper or missing precautions, the company may be subject to fines from the government as well. So, what do we do? As the text has already explained, we need useful security policies. We also need security policy compliance: People are not always thinking about security, so we need to create security controls which can be devices, procedures, or policies that are meant to increase security for an enterprise. Increasing security can also be described as decreasing risk. The text begins by saying that we could classify security controls as one of three types: Physical controls - These include any physical barrier, like a locked door or a fence, as well as security cameras and guards Administrative controls - These include the procedures to create security policies and the security policies themselves. Technical controls - Actions that are performed by devices technical solutions , such as firewalls denying packets. The author goes on to explain that all three types of controls have the same subtypes. Deterrent and Compensating controls are not listed in this text. Deterrent controls - used to discourage attacks; applied before an attack; example: People will be lost if there are too many to remember, and they will have little chance of complying if the the policies and controls are too hard to follow. Make fewer policies, and make controls easy to use to get better compliance. The text tells us that we will benefit from a security awareness program for our employees. Employees whose daily jobs do not address security issues need to be reminded about the rules we need them to follow. The text offers a list of principles that apply to employee training and awareness programs: Repetition - reminding users about security issues from time to time helps them stay aware of them Onboarding - new hires should be made aware of security policies when they start their jobs Support - policies should be supported from all levels of the organization, starting at the top Relevance - tell employees why we have rules, not just that we have them Metrics - measure your success by asking employees what they know or have learned The text explains that a reduction in risk will occur with a successful security awareness program. The text spends some pages talking about various kinds of assets to protect. We should assume we want to protect all of them. We are told that a business liability happens when a business cannot meet its obligations. These obligations come in two types: Legal obligations are, of course, things the organization is required to do by law. Promised commitments are related to explicit or implicit contracts, such as failing to provide a promised product or service. The text tells us we should have policies to protect the company from the actions of employees that may create a liability. There are five recommended steps on page 46 that support this concept: Policy - Have clearly stated policies about customer information that inform our employees of their responsibilities. Enforce - The text says to "express strong disapproval when policy is not followed". Respond - Incidents that cause a breach of security require a quick and effective response to limit damage, and to correct problems when they arise. Analyze - Determine the cause of problems, and resolve those causes. Educate - Train employees in their duties, and in security concepts that affect their jobs. One of the critical policies you should have is an Acceptable Use Policy, which tells employees what they are and are not allowed to do with the assets of the organization, such as telephones, cameras, computers, and links to the Internet. The chapter ends with some thoughts about operational consistency. There should be policies that address doing things well and doing them the same way every time assuming we have the kind of operation that needs such a policy. Manage - Manage how processes are done, and respond to deviations from processes Measure - Measure our outputs, such as volume, consistency, quality, waste, production cost Review - Assess processes and products to make sure both are acceptable Track - Report, analyze, and record defects, errors, and incidents Improve - Make changes to policies and procedures as needed Chapter 3 The text discusses a few laws that are relevant to information

system security. Be aware that there are many others. Gramm-Leach-Bliley Act GLBA, - also called the Financial Services Modernization Act; deregulated banks and financial services, allowing each institution to offer banking, investments, and insurance services Included three rules that affect privacy. The Financial Privacy Rule allows people to opt out of having their data shared with partner companies, but it is usually implemented so that it is easier to allow the sharing. The Safeguards Rule requires that companies have data security plans. The Pretexting Rule tells institutions to implement procedures to keep from releasing information to people who are trying to gain information under false pretenses pretexting. They had to be told to do that?

DOWNLOAD PDF CHAPTER 1: INFORMATION SECURITY GOVERNANCE

Chapter 2 : Chapter 1, Introduction to the Management of Information Security

CHAPTER 1 Information Security Governance and Risk Management This domain includes questions from the following topics: â€¢ Security terminology and principles â€¢ Protection control types â€¢ Security frameworks, models, standards, and best practices.

Physical and environmental security A. System acquisition, development and maintenance A. Information security incident management A. Strategy Resource The Information Security manager must be aware of: Action Plan to Implement Strategy - Implementing an information strategy requires one or more projects or initiatives. Practice Question Which of the following is the MOST important reason to provide effective communication about information security? It makes information security more palatable to resistant employees. It mitigates the weakest link in the information security landscape. It informs business units about the information security strategy. It helps the organization conform to regulatory information security requirements. Practice Question Which of the following approaches BEST helps the information security manager achieves compliance with various regulatory requirements? Rely on corporate counsel to advise which regulations are the most relevant. Stay current with all relevant regulations and request legal interpretation. Ignore many of the regulations that have no penalties. Practice Question Which of the following MOST helps ensure that assignment of roles and responsibilities is effective? Senior management is in support of the assignments. The assignments are mapped to required skill. The assignments are given on a voluntary basis. Maintaining appropriate regulatory compliance b. Ensuring disruptions are within acceptable levels c. Prioritizing allocation of remedial resources d.

Chapter 3 : Answer CCNA Security Chapter 1 Test â€“ CCNAS v â€¢ Invisible Algorithm

CISSP Chapter 1 Security Governance study guide by ka3byz includes 86 questions covering vocabulary, terms and more. Quizlet flashcards, activities and games help you improve your grades.

Chapter 4 : CISM Lecture Guide Chapter1: Information Security Governance - 24%

The first area of CISM study we will examine is the area of Information Security Governance. The goal of this domain is to establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.

Chapter 5 : Chapter 1 - Security Governance Through Principles and Policies - Stuvia

Security Governance The IT Governance Institute in its Board Briefing on IT Governance, 2 nd Edition, defines Security governance as follows: "Security governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved.