Policies & Procedures

Now, when I discuss policies and procedures, I'm not talking specifically about technical controls necessarily but instead, I'm focusing a lot on administrative controls. Policies are one part of a larger concept known as IT governance. IT governance is used to provide us a comprehensive security management framework for the organization to build upon. We do this by using Policies, Standards, Baselines, Guidelines, Procedures, and Information classification and even an entire lifecycle approach to our information technology systems. Policies are used to define the role of security inside of an organization and it establishes the desired end state for that security program.

Policies tend to be very broad and they provide the basic foundation upon which the Standards, Baselines, Guidelines, and Procedures are going to be built. Security policies are built to fill in one of three levels. They can be Organizational, System-specific, or Issue-specific.

Organizational Policies

Organizational security policies are going to provide direction and goals. They're going to give you a framework to meet the business goals and define the roles, responsibilities, and terms associated with it.

System-specific Policies

System-specific policies are going to address the security of a specific technology, application, network, or computer system. These system-specific policies tend to be much more technical and they focus on protecting a certain piece of the system or a certain piece of technology.

Issue-specific Policies

Finally, we have Issue-Specific Policies and these are built to address a specific security issue such as email privacy, employee termination procedures, or other specific issues. Now, in addition to those three areas, our policies can be further sep

Now, in addition to those three areas, our policies can be further separated down into one of three categories inside of information security. They're regulatory, advisory, or informative.

Regulatory Policies

When I talk about regulatory policies, I'm talking about things that address mandatory standards and laws that are going to affect the organization.

Advisory Policies

Advisory policies are going to provide us guidance on what is and what is not considered an acceptable activity. The most common example of this type of policy is known as the acceptable use policy or AUP. And this is something that companies provide to their employees to tell them what they can and can't do on the network.

Informative Policies

The third type is an Informative policy. Now, an Informative Policy is going to focus on a certain topic and it's designed to be educational in nature.

Standard

So, as we move beyond the policy, we then go into Standards. And Standards are used to implement a policy in an organization. These are going to include things like mandatory actions, steps, or rules that are needed to achieve the desired level of security.

Baseline

Beyond that, we have Baselines. And Baselines are created as reference points. And these are used to document any kind of system so, you can later go back and compare it for later analysis. We talked about Baselines in terms of security earlier and we also talked about Baselines of the network, where you know what the network pattern is and then you can decide if something is above that Baseline or below that Baseline which becomes an anomaly.

Guidelines

Now, guidelines are not required actions but instead, these are the recommended ones. Guidelines tend to be flexible in nature. They allow for exceptions and allowances when in a unique situation occurs.
So, for example, let's say I have a guideline that every employee gets one terabyte of storage on our cloud servers. That might be fine for most people and if we have secretaries or accountants or somebody who does a lot of contract work, those are fairly small files and so, one terabyte is plenty of information and plenty of storage. But my video editor might come up and say you know what, one terabyte is not sufficient for me, I need five terabytes because I'm dealing with these large video files all the time. Well, because it's a guideline, we can make an exception in an allowance for that person, we could say you know what, normally, we give one terabyte but because of your specific job role we're going to break that and we're going to go beyond that and give you more storage and break that guideline that we normally have.

Procedures

And Procedures are our detailed step-by-step instructions that are created to ensure personnel can perform a given action. These procedures are where those high-level policies are transferred all the way down through those standards and guidelines into actionable steps.

Tips

Now, further the Security+ exam, the big concept from this lesson that I want you to remember is the idea of a policy and a procedure. Remember that a policy is something that gives you generic guidance to the organization. For example, your password policy might say that all passwords have to be long, strong, complex, and be changed every 90 days. Then, we have a procedure which is very specific. And if I had a password procedure, that might detail exactly how to configure that password policy on a Windows 2016 server. Or, I might have a password procedure that's going to tell the user how they can change their password every 90 days by going into Windows and following steps one through five.

Data Classifications

Data classification is based on the value to the organization and the sensitivity of that information if it's going to be disclosed. The person that decides the level of data classification is the data owner. Now, what exactly would we consider sensitive data or information? Well, sensitive data is any information that can result in the loss of security or loss of advantage to a company, especially if it's accessed by unauthorized persons. Now, basically, this is the data that we need to be protecting. Anything that is sensitive, we want to make sure there is protection around it.

There are two different classification schemes that are normally used by organizations. And the way you choose yours is based on whether you're a commercial business, or a governmental organization.

Commercial Business

So, if you're a commercial business like we are, you're going to use one of four common classification levels. And these go from lowest to highest as:

1. public
2. sensitive
3. private
4. confidential

Governmental Organization

Now, if you work in a military or government sector, you're going to have five different classification levels going from lowest to highest. These are probably what you hear inside movies all the time. Things like:

1. Unclassified
2. Sensitive but unclassified
3. Confidential
4. Secret
5. Top secret

Data Ownership

Now, when we talk about data ownership, this is the process of identifying the person responsible for the confidentiality, integrity, availability, and privacy of the information assets. Now, you might think that the data owner is the person who created that file,

but that's not what we're talking about. In an enterprise environment, there are different roles that fall under this idea of data ownership. These include things like the data owner themselves, the data steward, the data custodian, and the privacy officer.

Data owner

This is going to be a senior executive role, and they have the ultimate responsibility for maintaining the confidentiality, integrity, and availability of the information asset. So, what is their real role here as the data owner? It's not the person who created the file. It's the senior executive, and this data owner is going to be responsible for labeling the asset and ensuring that it's protected with the appropriate controls.

Data steward

Now, the data steward is a role that’s focused on the quality of the data and the associated metadata. This data steward is going to be somebody who is working for the data owner. They're going to be involved with making sure that the data is appropriately labeled and classified. So, we said that all financial data should be labeled financial data, and it should be taken care of this way. That's going to be the role of the data steward to make sure that's actually done.

Data custodian

This is a role that’s responsible for handling the management of the system on which the data assets are stored. So, who might be a data custodian? Well, a system administrator. These are the people responsible for enforcing the access control, the encryption, and the backup and recovery measures that protect this data based on the requirements set forth by that data owner.

Privacy officer

Now, this is a role that’s responsible for the oversight of any kind of privacy-related data, things like PII, SPI, or PHI. Any of those things that are managed by the company fall under the realm of the privacy officer. This is the person who's going to really be on the hook if you have a data breach because, normally, when you have a data breach, what people are concerned about is the private user data that has been expelled. And so, that is going to be what they're focused on.

PII and PH

One of the largest privacy concerns inside most organizations today is how you're going to collect, process, and store PII, known as personally identifiable information.

Now, the first step in protecting PII is to understand what constitutes this class of information. If a piece of data can be used either by itself or in combination with some other piece of data to identify a singular person, then it's considered PII.

Well, this is things like your full name, your driver's license number, you social security number, your date of birth, your place of birth, digital versions of your biometric features like your fingerprints or your retina scans, financial account numbers, your addresses, your email addresses, and even your social media usernames.

Federal Privacy Act of 1974

The first one is Federal Privacy Act of 1974. This affects any U.S. government computer system that collects, stores, uses, or disseminates personally identifiable information. If you work for the government or one of its contractors, then this law is going to apply to your organization.

HIPPA

HIPAA is the Health Insurance Portability and Accountability Act and it affects health care providers, facilities, insurance companies, and other medical data clearinghouses. If your organization is processing or storing medical data, you're likely going to be affected by HIPAA. It's enforced by the Department of Health and Human Services in the United States and it provides you with the standards and procedures that have to be used, at a minimum, for storing, using, and transmitting medical information and healthcare data.

SOX

The third law you should know is Sarbanes-Oxley or SOX, as it's also known. This was originally enacted by Congress back in 2002 as the Public Company Accounting Reform and Investor Protection Act of 2002, but you're almost always going to hear it referred to as SOX or Sarbanes-Oxley. If your organization is a publicly-traded U.S. corporation, it's affected by this regulation and it has to follow certain accounting methods and financial reporting requirements. Now, the important thing to keep in

mind with Sarbanes-Oxley is that if you fail to follow it, your senior leadership, like your CEO, can actually receive jail time for it.

GLBA

The next regulation we're going to talk about is known as GLBA or the Gramm-Leach-Bliley Act of 1999. Now, this affects banks, mortgage companies, loan offices, insurance companies, investment companies, and credit card providers. Basically, if you work for a financial institution, this is going to affect you. GLBA directly affects the security of personal identifiable information and it prohibits sharing of financial information with any third parties and it also provides guidelines for securing that financial information.

FISMA

Another law that affects you if you're working for the federal government is the Federal Information System Security Management Act of 2002, also known as FISMA. Now, FISMA requires each agency in the government to develop, document, and implement an agency-wide information systems security program to help protect their data. Basically, FISMA is all about cybersecurity. The goal here is to create more secure networks across the entire U.S. government.

PCI DSS

Now, the final thing we're going to talk about here is a standard, not an actual law or regulation. But it's one that affects you if you take credit card payments. It's known as PCI DSS or the Payment Card Industry Data Security Standard. This is an agreement that any organization who collects, stores, or processes credit card information for a customer has to follow. Again, this isn't a law or regulation, but it is a contractual obligation or agreement and it's a standard that must be followed if your organization wants to be able to handle credit card transactions.

HAVA

Now, another federal law that you should know about is known as HAVA, which is the Help America Vote Act of 2002, or HAVA. Now, it was designed to help replace the old punch card systems back in the voting machines that we used and it provides regulations that govern the security, confidentiality, and integrity of the personal information that's collected, stored, or processed during the election cycle and the voting process.

SB 1386

Now, the last law we're going to talk about is actually a California law, so it only affects businesses that operate in California as a California corporation. Now, why are we covering it then? Because this doesn't even apply to my company. Well, it's because a lot of IT companies out there do business in California or they're based out there and this makes them a California business under this law. This law is called the SB 1386, which is the number that was assigned to this regulation. Now, it was created in 2003 and requires any California business that stores computerized personal information to immediately disclose any breach of security that it becomes aware of.

Legal Requirements

When we talk about privacy, we're really talking about a data governance requirement that arises when you're collecting and processing personal data to ensure the rights of the subject's data. So, if I collect information from you when you sign up for my course, I get your name, your email, maybe your credit card information, I have to keep that information private. It doesn't necessarily mean that I have to have it encrypted in my database, although we do that, we just have to make sure that nobody else can get that data who doesn't have a need to know inside our organization. That's the idea of privacy.

GDPR

Now, one of the biggest requirements and one of the best requirements in terms of privacy is GDPR. This is the General Data Protection Regulation. And this says that personal data cannot be collected, processed, or retained without the individual's informed consent. Now, when I talk about informed consent, this means that the data must be collected and processed only for the stated purpose and that purpose must be clearly described to the user in plain language, not legalese.

So, if you go to a website and they say give us your name, your email, and your home address so that we can sell you this product and then deliver it to your house, that's the stated purpose. That doesn't mean that they can now send you mailers every single week to your home address to try and get you to buy more stuff unless that was part of their privacy policy that you accepted. So, GDPR says they have to be upfront with this.

Now, GDPR also provides the right for a user to withdraw consent at any time. It also gives them the ability to inspect, amend, or erase data that's held about them. We like to call this the right to be forgotten. If you're a resident and citizen of the

European Union, you can call up the company or fill out their form and say, I want you to forget everything you've ever known about me and they have to go into their database and scrub you out of it.
That is part of that law. It gives you a lot of protections if you're a European citizen.

Now, what happens if you have a data breach? Well, this depends again where you are and what laws you fall under. For instance, if you deal with GDPR, you have responsibilities. Within 72 hours, if you're doing business within Europe, you have to notify the regulators and the users that you had a data breach. So, once again, this is an area where the European citizens have better rights than the Americans do based on the laws that are in each of those countries at the time of this filming. Now, let me give you a quick word of warning. Data breaches can happen both accidentally and through malicious interference. Just because you had a data breach doesn't mean that some hacker got in.

Privacy Technologies

De-identification

When I'm talking about de-identification, this is the methods and technologies that remove identifying information from data before we distribute that data. Now, the real benefit of de-identification here is to be able to take data that may be protected by privacy. And once we do the de-identification, that data now becomes usable by us again for other purposes. Now, this doesn't violate anybody's privacy because we are de-identifying the data. Oftentimes, your de-identification is going to be implemented as part of your database design. Now, there are lots of different things that we have to talk about when we talk about de-identification. This includes things like data masking, tokenization, aggregation and banding, and re-identification.

Data Masking

Now, when we talk about data masking, this is where a de-identification method is used where a generic or placeholder label is substituted in for real data while preserving the structure or format of the original data. So, let's say you're going to give me all your credit cards. I take all your credit cards and I take away all of the information from your 16 digits and I put XXXX in front of all those 16 digits. That would mask the data. Nobody would be able to identify that credit card anymore as yours because we don't have the credit card. We just have XXXXX. That's a form of data masking.

Tokenization

The next one we have is what’s known as tokenization. Now, this is a de-identification method where a unique token is substituted in for real data. Now, when you do tokenization, one of the things you have to worry about is if you have the ability to go back and be reversible and usually with tokenization, it is. So, again, let's say I had your social security numbers. Instead of changing them all to one, I assign a random number to each of my students. That's now their student ID. That student ID is now substituted in for that social security number field. But I might have a master list in my safe that says this student ID matches this social security number. That's what we're talking about with tokenization.

Aggregation/Banding

Now, aggregation and banding is where you de-identify people by gathering the data and generalizing it to protect the individuals involved. So, if we were using aggregation and banding, we might take all of our subjects in a medical trial and instead of identifying them as the person or the subject number, we would say out of the 100 people who participated in this trial, 90% of them didn't have side effects. Now, that doesn't mean any of those 90 quickly identifies as you. It just means somebody didn't have a side effect. It's one of those 90. And if we knew that you didn't have side effects, well, you're just one of 90. We don't know you individually. And that's where we're able to protect your privacy.

Re-identification

Re-identification is an attack that combines de-identified data sets with other data sources, things that you know, to discover how secure the de-identification method is. And so, if we use that system in our company, that would not be secure.

Security Policies

Now, there are things that you legally must follow, and that's all those things we just talked about. But your organization will also create a lot of policies that they want their own employees to follow, as well. Now, these aren't legally binding or required, but they are used as part of a good, overarching security program by adding these administrative security controls to your security systems.

This **privacy policy** is going to govern the labeling of data to ensure that all employees understand what data they're looking at and handling happens to be personal information. And this will help prevent the mishandling of confidential information.

Next, we have what's known as the **AUP**, or the acceptable use policy. An acceptable use policy is used to define the rules and restrict how computer, network, or other system can be used. For example, your organization might have a policy that states you can't use the Internet to browse -- or gambling websites while you're at work.

Change management is our next policy. And change management is a structured way of changing the state of a computer system, network, or IT procedure. Back when we talked about creating a secure, known good baseline for the security of our systems, I mentioned that we want to control the configuration changes to be made to that secure baseline. And that's exactly what change management does for us. A good change management policy is designed to make sure that you're going to get the changes that you want in a secure and methodical manner.

Next, we have the **separation of duties**. Separation of duties is a preventative type of administrative control, and it's one that should be considered when you're drafting up your organizational authentication and authorization policies. Separation of duties is designed to prevent fraud and abuse by distributing various tasks and approval authorities across a number of different users.

Now, the next policy is to consider **job rotation**. Job rotation is a detective type of administrative control. And with job rotation, different users are trained to perform the tasks of the same position in order to help prevent and identify fraud that could occur if one employee had the job the entire time themself.

Another administrative control you need to consider is what are you going to do when you hire or fire somebody. We also call this **onboarding and offboarding**. When we consider this, we're talking specifically about information system security, and not the human resource part of this process. But you should consult your human resources team whenever you're developing this part of your security policy.

These aren’t necessarily policies, but they are concepts that you have to keep in mind when you're writing your policies.

Due diligence means that you’re ensuring the IT infrastructure risks are known and managed properly. To achieve due diligence, you need to ensure that you conduct proper risk assessment and conduct risk management activities to keep operations running smoothly over time.

Due care is the mitigation actions that an organization takes to defend itself against risks that have been identified during your due diligence. So, let's say I do due diligence, and I find that our company is not utilizing a modern operating system. And this represents a big vulnerability. So, maybe I find they're using XP still, for instance. Well, if I want to exercise due care, I would allocate money to upgrade the system from Windows XP all the way up to Windows 10.

Due process is a legal term, and it refers to how an organization must respect and safeguard personnel's rights. For example, if you're the federal government, you can't eavesdrop or wiretap on any US citizen you want. You can't just go and say, hey, I'm going to listen to Johnny's phone calls today. No, this is prohibited by the US constitution's fourth amendment, which protects us against illegal search and seizure.
Now, basically, when you hear due process in terms of the Security+ exam, I want you to think about the fact that due process is used to protect a person from the government, but it can also protect your organization from frivolous lawsuits.

User Education

Security Awareness Training

So, the first type of training is known as security awareness training, and it's used to reinforce the importance of having users help you secure the organization's valuable resources. This includes things like educating your end users on the current threats facing the organization, phishing campaigns, how to protect their passwords, as well as what to do in the event of an incident.

Security Training

Now, security training is our second category, and it's used to teach the organization's personnel the skills they need to perform their job in a more secure

manner. So, this training is usually going to be focused on IT staff and administrators, as well as other technical employees. For example, let's say I sent my system administrators down to get some training to learn the most secure way to set up a user account and create passwords, and this training would be a form of security training.

Vendor Relationships

Whenever you're dealing with vendors outside your organization, you're going to need to have some agreements and contracts in place. That's what we're going to talk about in this lesson. We're going to discuss NDAs, MOUs, SLAs, ISAs, and BPAs.

NDA

An NDA is a non-disclosure agreement, and it's an agreement between two parties that define what data is considered confidential and can't be shared outside of that relationship.

MOU

MOUs are a memorandum of understanding. And this is a non-binding agreement between two or more organizations to detail what common line of action they're intending to take. Now, essentially, this is a formal version of a gentleman's agreement because it's actually written down and signed by all parties. But it's pretty much like a handshake, right? If you and I agreed to go into business together and I understand you're going to do x, y, and z, and you understand that I'm going to do a, b, and c, that's what an MOU does. An MOU is often referred to as a letter of intent, and it's most often used within an organization by two of its smaller internal divisions.

SLA

Another business document to consider using is what's known as a service-level agreement or SLA. Now, this agreement is concerned with the ability to support and respond to problems within a given timeframe while providing the agreed-upon level of service to the user.

ISA

Next, let's talk about information sharing. Often, multiple organizations want to work together and that requires them to share information between their networks. An

agreement that focuses on connecting two systems from two different organizations is called an interconnection service agreement or ISA. An ISA is an agreement that allows the owners and operators of the two IT systems to document what technical requirements each organization has to meet. If your organization is planning to connect its network to another organization, it's a good idea to ensure you have an interconnection security agreement in place, detailing exactly what level of security each organization needs to meet.

BPA

Now, business partnership agreement is conducted between two business partners that establishes the conditions of their relationship. These include things like each person's responsibility, as well as the revenue, system, and data sharing details. One example of this is my company. We entered into a business partnership agreement with another company to produce an online training course on the CompTIA Advanced Security Practitioner or CASP+ Exam. Now, in our agreement, it clearly stated that I was responsible for writing all of the scripts and all of the videos, flying out to their studios to film it, but my partner was responsible for providing me travel expenses.

Disposal Policies

Asset disposal occurs whenever a system is no longer needed by an organization. And it doesn't mean it has to be some old worn out piece of junk computer. It may be that you have a new iPhone and you just got a brand new one three weeks later. What are you going to do with that one that was there three weeks earlier? Well, you're going to have to dispose of it somehow, and it can be reused, resold, or completely thrown away. This disposal might require the system to be destroyed, it could be that the assets can be reused for another purpose, or it's resold to get you some money back.

Now, in organizations that require a high level of security for their data, it's commonplace for data storage devices to be electronically or physically destroyed first.

If your organization is using hard drives for storage, these can be destroyed through a degaussing process. Degaussing exposes the hard drive to a powerful magnetic field, and this causes the previously-written data to be wiped from the drive, and the drive to become a blank slate once again.

Now, if all of that sounds a little too violent for you, that's okay, there's electronic mechanisms to do this too. This is known as purging. Purging, also known as sanitizing, is the act of removing data in such a way that it cannot be reconstructed using any known forensic techniques. This includes using special bit-by-bit erasing software that can allow you to rewrite the hard drive many times over with a series of ones and zeros. And if you do this at least seven times or even 35 times for real high-security applications, you can actually erase that drive and then reuse it again. Another technique you can use is to encrypt the drive, and if you destroy the encryption key, this again makes the data on it impossible to read, and this is another way to basically sanitize your drive.

Now, if you want to reuse that hard drive more easily, though, you would use a clearing technique. A clearing technique is the removal of data with a certain amount of assurance that it can't be reconstructed. For example, if you delete a file or a folder from your hard disk, and then you replace the area that was stored on it with a series of zeros, this would constitute clearing. This is also used to do a secure-erase function inside of some operating systems. Now, unfortunately, the data is actually recoverable with special techniques and forensic procedures, though. And so, if you want to conduct something like a low-level format of the hard disk, this would be categorized as clearing, as well. The bottom line, if you're working in a high-security environment, you shouldn't use clearing. Instead, you should opt for purging or physical destruction.

IT Security Frameworks

SABSA

First, we have the Sherwood Applied Business Security Architecture, also known as SABSA. SABSA is a risk-driven architecture, and it seeks to consider the security problem by thinking about the what, where, when, why, who, and how of a problem. And they think about this as it intersects with six different layers. The operational, component, physical, logical, conceptual, and contextual layers.

COBIT

Next, we'll consider COBIT. COBIT stands for the Control Objectives for Information and Related Technology. And it's a security controlled development framework that divides IT into four domains. Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. Each of these domains is then broken down into one of 34 other processes. And this is very similar to other service management frameworks like ITIL or ISO 27000.

NIST Special Publication 800-53

Next, let's take a quick look at the NIST Special Publication 800-53. This is a security control framework developed by the U.S. Department of Commerce. Each control is placed into one of three categories. It is technical, operational, or management. We talked about this back in our security controls lesson. Each of these classes contains numerous security controls, as well. And if you're working for a government agency, you're likely going to be using the framework that is the NIST Special Publication 800-53.

ITIL

ITIL is a framework that used to be known as the IT Infrastructure Library because it was very focused on service operations and security of your networks. But it has grown into something larger now, with the new ITIL 4. ITIL is still the de facto standard for IT service management. But now, it's being expanded to include all sorts of other service-based connections that we have with our organizations to provide value to our end users.

Exam Tips

Now, for the Security+ exam, you don't need to know ITIL in depth. But I would recommend checking out an ITIL 4 course because most employers rely heavily on ITIL for their operations. And being able to discuss ITIL, its processes, and its concepts is a great thing to have in your back pocket during a job interview. After all, ITIL is the language of IT operations, and as security professionals, we need to fit in to that system effectively. Now, in the Security+ exam, you're not going to be asked a lot of questions about frameworks. But you should know that there are frameworks that exist, such as SABSA, COBIT, the NIST Special Publications, ISO 27000, and ITIL. On the exam, the most I would expect you to see on the exam about frameworks is the fact that we use frameworks as a basis for our policies, our procedures, and our standards.

Key Frameworks

CIS

The Center for Internet Security creates a framework that's based on a consensus-developed secure configuration guidelines for hardening, these are known as benchmarks, as well as some prescriptive, prioritized, and simplified sets of cybersecurity best practices, these are known as configuration guides. Now, when

we look at benchmarks, this tells us what are the things that we should be using as we go through and make sure our systems are up to snuff. When we look at the configuration guides, this will be actually step by step instructions.

RMF

The next framework we're going to cover is known as the Risk Management Framework or RMF. Now, RMF is something that has become very popular in recent years. This is a process that integrates security and risk management activities into the system development lifecycle early on. This way, we can do this as an approach to security control selection and specification that considers the effectiveness, efficiency, and constraints due to the different laws, directives, executive orders, policies, standards, and regulations. You should just know that the Risk Management Framework is made by NIST and it's used in federal government systems.

CSF

The other one that's made by NIST is known as the Cybersecurity Framework or CSF. This is a set of industry standards and best practices that were created by NIST to help organizations manage their cybersecurity risks. Often, you will find that Risk Management Framework and the CSF work together inside of an organization. Again, it's not something you need to know in depth for the exam, but you should be aware that the CSF, the Cyber Security Framework, is made by NIST, and you should be aware of the five category functions that we have, identify, protect, detect, respond, and recover.

ISO 27001

The next framework we're going to talk about is an international one. This is known as ISO 27001. ISO is the International Organization for Standardization. And this is an international standard that details the requirements for establishing, implementing, maintaining, and continually improving an information security management system or ISMS. Now, when you hear ISO 27001, I just want you to think about the fact that this is a basic procedure for cybersecurity, and it is an international standard.

ISO 27002

The next one we have is ISO 27002. This again is an international standard and it provides best practice recommendations on information security controls for use for those responsible, for initiating, implementing, or maintaining information security management systems, ISMSs. So, again, you can see how 27001 and 27002 could work together. With 27001, we're talking about the requirements for establishing and

maintaining these systems. When we're talking about 27002, we're talking specifically about the controls that we're going to choose to protect those systems.

ISO 27701

Next, we have the ISO 27701. This, again, is an international standard and it acts as a privacy extension to the ISO 27001. It's used to enhance the existing ISMS with additional requirements in order to establish, implement, maintain, and continually improve privacy information management systems. So, if you have 27001, that's your information systems. If you have 27002, that's the controls to protect those systems. When you talk about 27701, you're talking about adding privacy on top of that.

ISO 31000

The final international standard we want to talk about is ISO 31000. This is an international standard for enterprise risk management, and it provides a universally-recognized paradigm for practitioners and companies to employ risk management processes to replace the myriad of existing standards, methodologies, and paradigms that differed between different industries, subject matters, and regions. So, essentially, if you think about risk management framework, the RMF, how it's used in the United States, the ISO 31000 was trying to do this globally. They're trying to figure out how we can make everybody use the exact same Risk Management Framework, and that's where ISO 31000 comes into play.

SOC

Now, the next framework we're going to talk about is System and Organization Controls, also known as SOC. Now, this is a suite of reports that are going to be produced during an audit. And this is going to be used by service organizations to issue validated reports of internal controls over those information systems to the users of those services. Now, if you're going to go ahead and get a SOC audit done, this is going to be something that is going to be used in conjunction with some of your other frameworks. So, if you're using NIST RMF or NIST Cybersecurity Framework, that tells you what controls you wanted to put in place. The SOC is going to do the audit of those controls and make sure you're in compliance. They mentioned the SOC 2 and they mentioned type II underneath this idea of a SOC. When we talk about SOC 2, this means it is a trusted services criteria. And this is basically when you go and look at the manual for SOC, it'll tell you what those requirements are as part of that audit. That's what the trusted services criteria is used for. Now, when I talk about the type II, this is going to address the operational effectiveness of the specified control over a given period of time. Normally, that's going to be 9 to 12 months. So, if I'm doing an audit and I'm looking to make sure you have multifactor authentication to prevent people from logging onto your

systems, I can then say how effective is your implementation of multifactor authentication over a 9 to 12 month period and I can put that into my report, as well, if I'm doing a SOC 2, type II report.

Cloud Control Matrix

The next framework we want to talk about comes from the Cloud Security Alliance. It is the Cloud Control Matrix. This is a framework that's designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a given cloud provider. So, if you're trying to decide are you going to go with Azure or AWS or Google cloud, you can run it through your Cloud Control Matrix to figure out which one is best going to meet your needs and provide you the best security.

Reference Architecture

Now, the final thing we want to talk about also comes from the Cloud Security Alliance and it's the Reference Architecture. This is a methodology and a set of tools that enable security architects, enterprise architects, and risk management professionals to leverage a common set of solutions that fulfill their common needs to be able to assess where their internal IT and their cloud providers are in terms of security capabilities, and to plan a roadmap to meet the security needs of their business. Essentially, when we talk about a reference architecture, we're saying, this is the thing we're going to build towards, this is how we want to build this thing to make sure it's secure. Now, once we do that over time, that may change and things go and deviate away from that reference architecture, that's when we go away from baseline, but what we designed as a reference architecture gives us the outline of what we want and how we want everything to match up so we can have the best security and we meet our roadmap to meet those needs.