Selecting Security Controls

Table of Contents

Selecting Security Controls

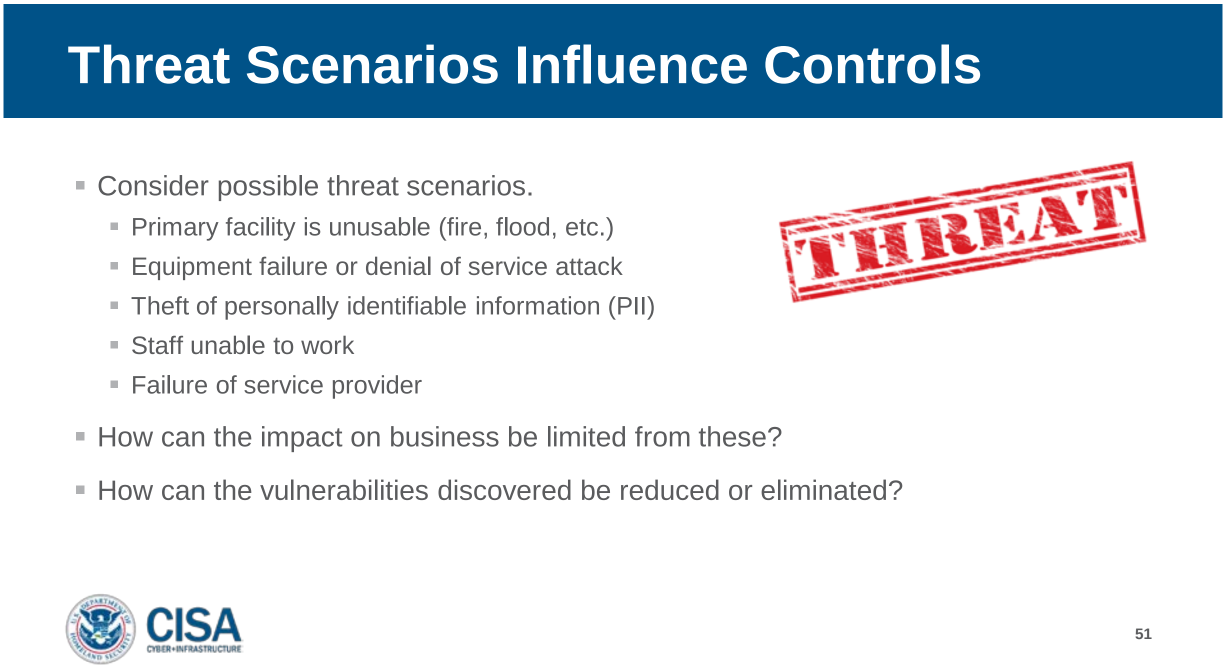
CISA
CYBER+INFRASTRUCTURE

Selecting Security Controls

50

**050 Instructor: For this particular presentation, we're going to talk about selecting security controls.

Threat Scenarios Influence Controls



Threat Scenarios Influence Controls

- Consider possible threat scenarios.
  - Primary facility is unusable (fire, flood, etc.)
  - Equipment failure or denial of service attack
  - Theft of personally identifiable information (PII)
  - Staff unable to work
  - Failure of service provider
- How can the impact on business be limited from these?
- How can the vulnerabilities discovered be reduced or eliminated?

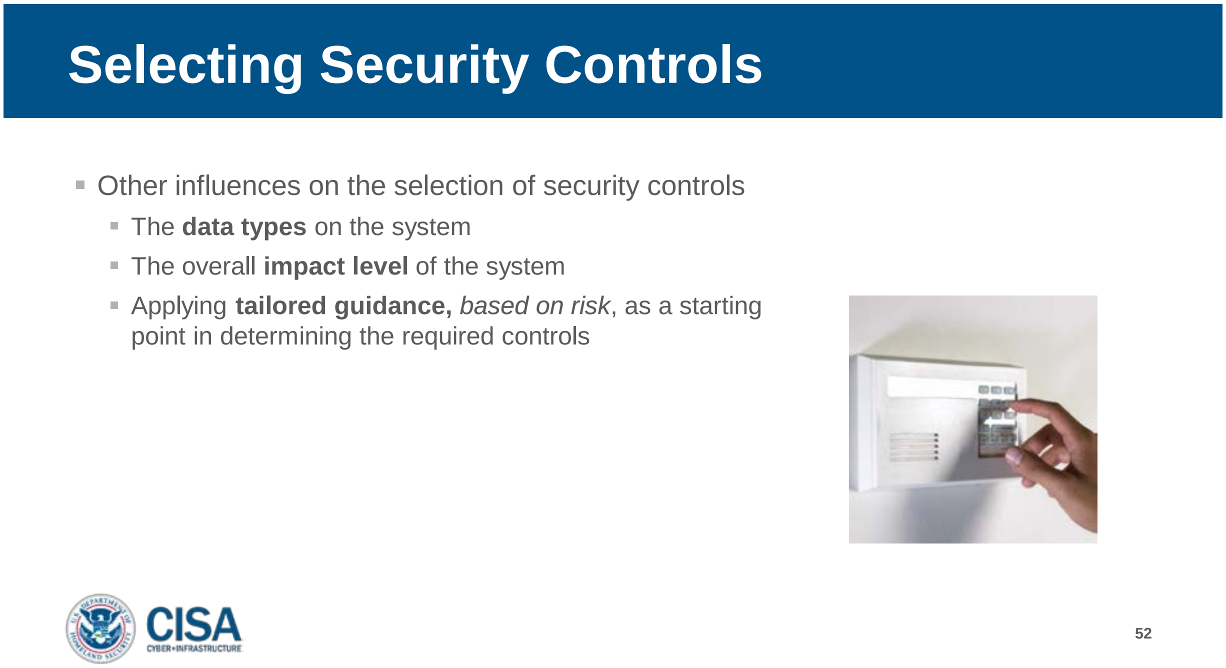
CISA CYBER+INFRASTRUCTURE

51

**051 We want to start by thinking about different threat scenarios that influence the controls. If we go back a second and we think about risk, remember that any good risk is going to be comprised of a threat actor, vulnerability, some level of uncertainty related to it, and impact that is related to that risk of basically how we'd feel the pain if the risk came true; and one way to think about selection of controls is we could start with coming up with different scenarios as to how we'd necessarily have these risks come about.

Some examples could include if we have lost a facility that we use. For example, we could have a fire or maybe a hurricane comes up the coast and takes it out. We could also have a critical equipment failure, or we could have theft of critical information and find it publicized on the internet. Whatever the scenario is, we really want to think about the impact on the business and what we can really get out of this is think about how we're going to actually manage that risk so it doesn't happen. We also want to think about the vulnerabilities that lead to it, and what are those vulnerabilities that could be reduced or eliminated such that the risk can be really limited.

Selecting Security Controls



Selecting Security Controls

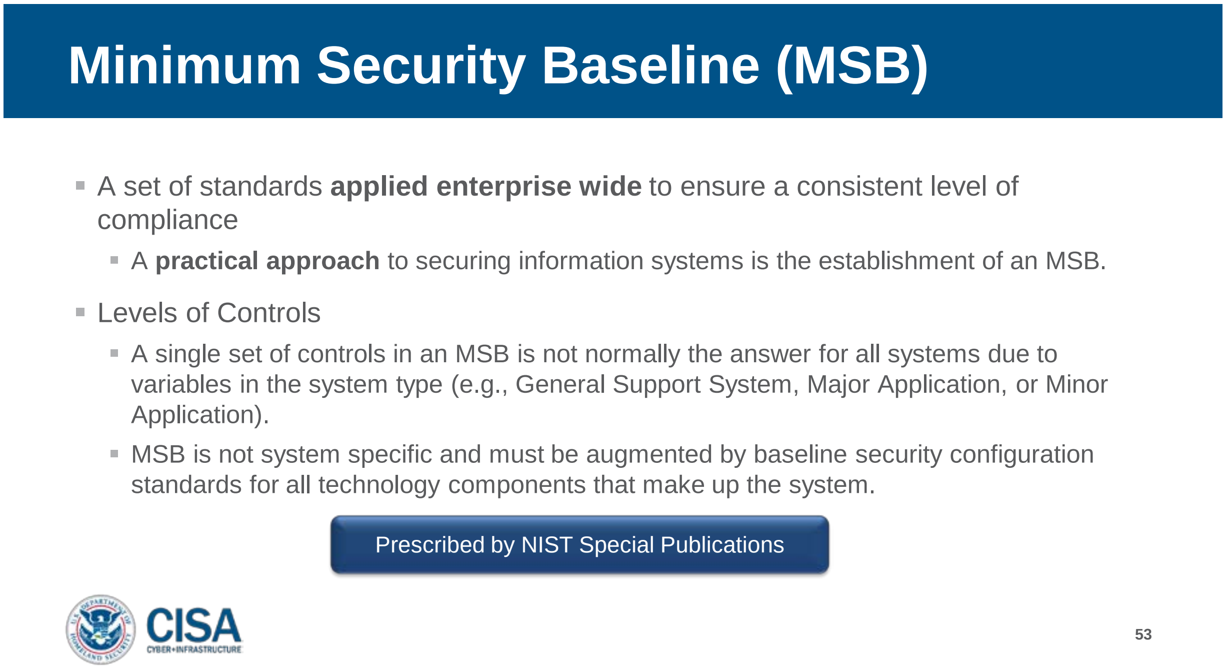
- Other influences on the selection of security controls
  - The **data types** on the system
  - The overall **impact level** of the system
  - Applying **tailored guidance,** *based on risk*, as a starting point in determining the required controls

CISA
CYBER+INFRASTRUCTURE

52

**052 So selecting these security controls, there are other things we want to think about too. For example, if our asset is data, we really want to think about the types of data that we have in the system, and even more important than that, we want to think about the information that we glean from that data and we want to talk more specifically about the impact to the organization would bring the organization to a halt. So what we want to do maybe is we could seek some additional guidance here to help us adjust our response in accordance with what that impact level would be related to that information.

Minimum Security Baseline (MSB)



Minimum Security Baseline (MSB)

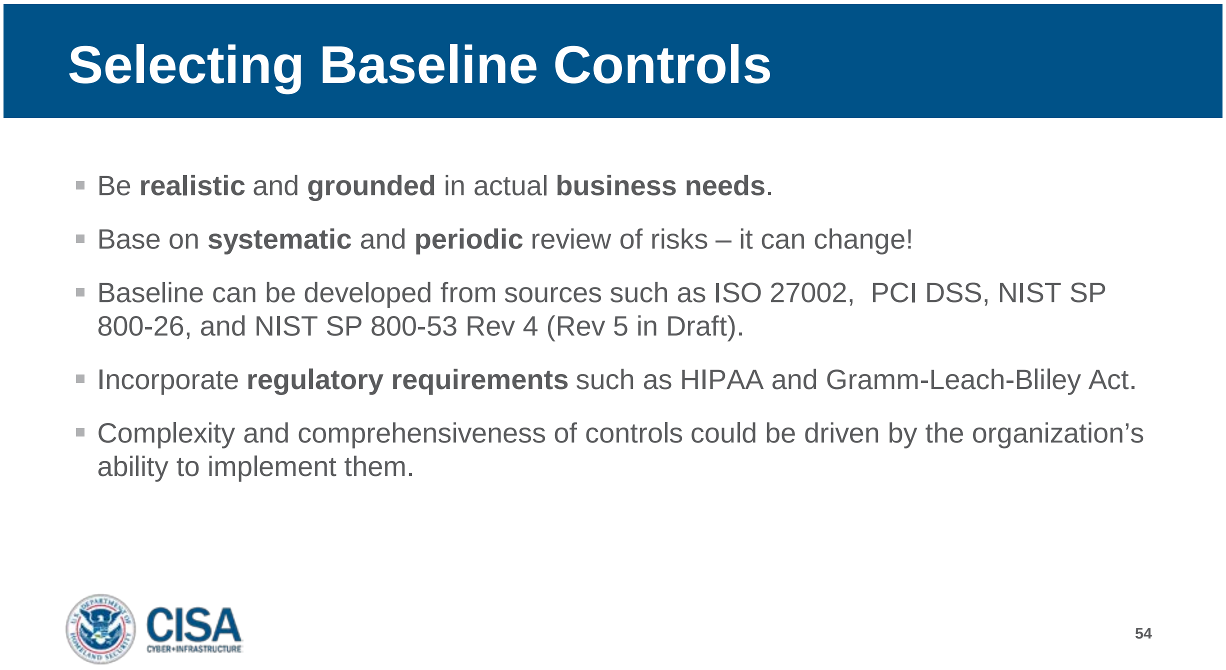
- A set of standards **applied enterprise wide** to ensure a consistent level of compliance
  - A **practical approach** to securing information systems is the establishment of an MSB.
- Levels of Controls
  - A single set of controls in an MSB is not normally the answer for all systems due to variables in the system type (e.g., General Support System, Major Application, or Minor Application).
  - MSB is not system specific and must be augmented by baseline security configuration standards for all technology components that make up the system.

Prescribed by NIST Special Publications

53

**053 So as you may recall, NIST has an 800 series that deals with cybersecurity. The document I'm thinking about is NIST 800-53. What you want to use that document for is selecting a baseline of controls, a set of controls that may be generally applicable to your organization. Now we understand that not every baseline is going to be absolutely perfect for your organization, but it's a good starting point. It will give you a good idea of what controls are most applicable to your organization given the priorities of risk that you have and the classification of the risks that you come up with in your risk register. It's not typically system-specific, but what it can do is provide you at least a good starting point of the technology components that make up your system and what you need to do to insulate them.

Selecting Baseline Controls



Selecting Baseline Controls

- Be **realistic** and **grounded** in actual **business needs**.
- Base on **systematic** and **periodic** review of risks – it can change!
- Baseline can be developed from sources such as ISO 27002, PCI DSS, NIST SP 800-26, and NIST SP 800-53 Rev 4 (Rev 5 in Draft).
- Incorporate **regulatory requirements** such as HIPAA and Gramm-Leach-Bliley Act.
- Complexity and comprehensiveness of controls could be driven by the organization’s ability to implement them.

54

**054 You want to keep your selection of these controls realistic, and you want to keep focusing on your strategic needs as much as your business needs, because remember the whole name of the game is to keep a resilient enterprise, to make sure that you can keep operating despite whatever risks may come to light or to fruition. You want to also look at how often you're going to be reviewing these risks and what kind of security controls you're going to be putting around it. How is it that you're going to measure the effectiveness of those controls that you have in place?

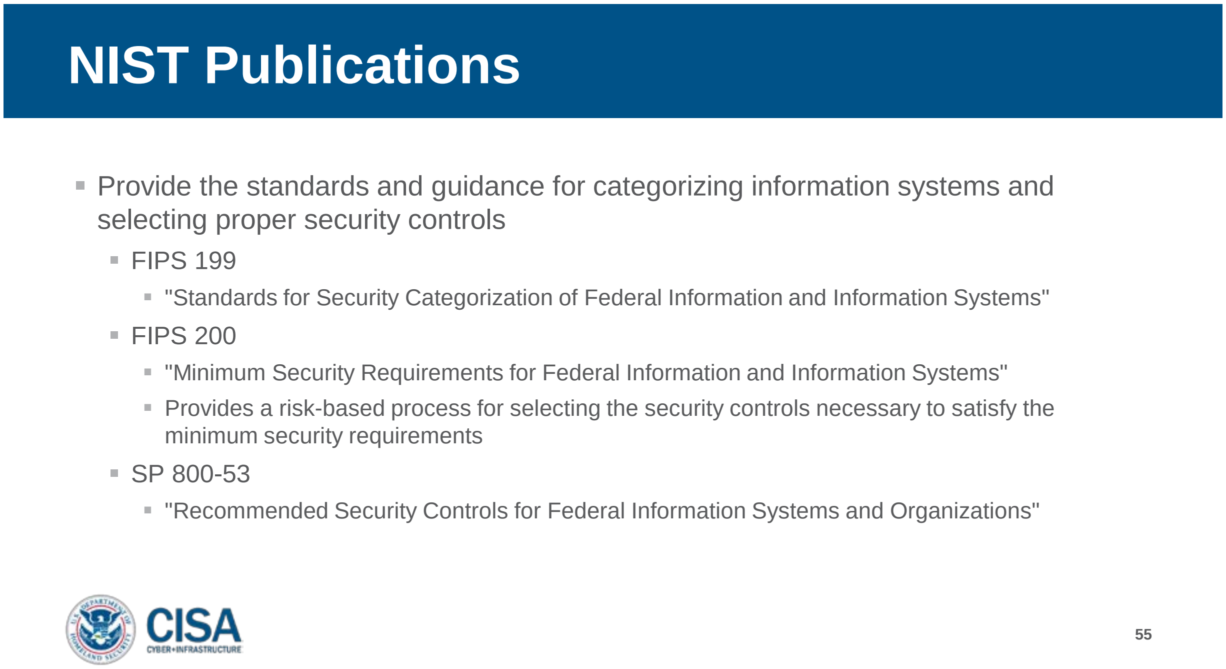
There's some additional standards here too. It's not just NIST 800-53. There are some others like ISO, and you can talk about-- if you work with credit information, there's PCI. There's also some additional 800 series. Another one here that I might want to add is NIST SP 800-171, which actually deals specifically with controls for the defense industrial base. It's also a good document to look at.

You may also think about regulatory requirements in your organization, especially if you're handling HIPAA data or other financial data where Gramm-Leach-Bliley may apply to your organization.

Clearly, there's going to be a consideration for how comprehensive you need these controls to be. We've talked in the past about defense-in-depth. Let's talk about that again for a moment. Imagine that I have a critical asset and imagine that I have a wall of a block of Swiss cheese, and on the other side is a threat actor. The threat actor needs to thread through all the holes of that block of Swiss cheese such that he can get to the other side in an unimpeded fashion.

Now, I could slice that block of cheese up and have a whole bunch of different slices and it'll have a whole bunch of different holes, and if I can change the configuration on each of those security elements, I can actually make it harder or more tortuous for that threat actor to get to my critical asset. We would call that notion or that whole idea defense-in-depth.

NIST Publications



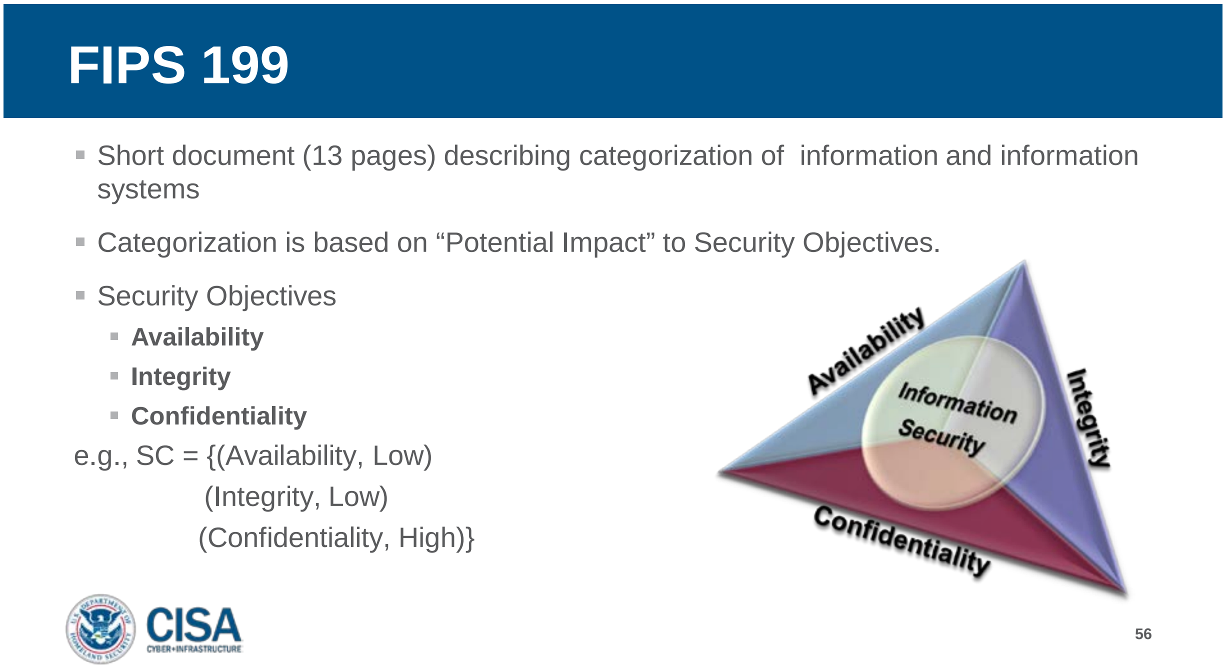
NIST Publications

- Provide the standards and guidance for categorizing information systems and selecting proper security controls
  - FIPS 199
    - "Standards for Security Categorization of Federal Information and Information Systems"
  - FIPS 200
    - "Minimum Security Requirements for Federal Information and Information Systems"
    - Provides a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements
  - SP 800-53
    - "Recommended Security Controls for Federal Information Systems and Organizations"

55

**055 Some other NIST publications you want to consider here are FIPS 199 and FIPS 200. FIPS 199 and 200 will really help you characterize your risk and provide you direction on how to assign levels of severity for those risks. Then you can turn around and go to 53, which provides a good set of matrices that you can align those levels of degree of severity for those risks with security controls that may help you best.

FIPS 199



FIPS 199

- Short document (13 pages) describing categorization of information and information systems
- Categorization is based on “Potential Impact” to Security Objectives.
- Security Objectives
  - **Availability**
  - **Integrity**
  - **Confidentiality**

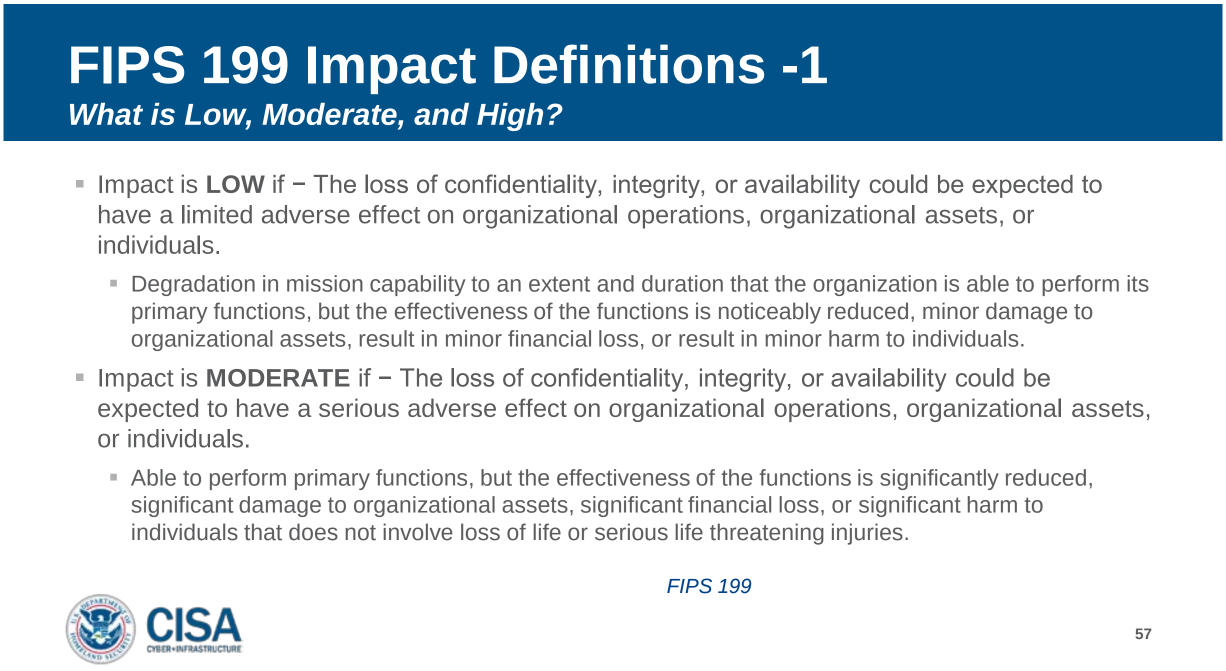
e.g., SC = {(Availability, Low)
(Integrity, Low)
(Confidentiality, High)}

Availability
Integrity
Information Security
Confidentiality
CISA
CYBER+INFRASTRUCTURE

56

**056 FIPS 199 provides you with the classification of information in your system based upon the impact on your security objectives. Remember, what we're trying to emphasize here is that our information and our data is available, that the integrity is maintained, and the confidentiality is maintained. I have an example here of how they actually use notation for those classifications.

FIPS 199 Impact Definitions -1 What is Low, Moderate, and High?



FIPS 199 Impact Definitions -1

What is Low, Moderate, and High?

- Impact is **LOW** if – The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
  - Degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced, minor damage to organizational assets, result in minor financial loss, or result in minor harm to individuals.
- Impact is **MODERATE** if – The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
  - Able to perform primary functions, but the effectiveness of the functions is significantly reduced, significant damage to organizational assets, significant financial loss, or significant harm to individuals that does not involve loss of life or serious life threatening injuries.

FIPS 199

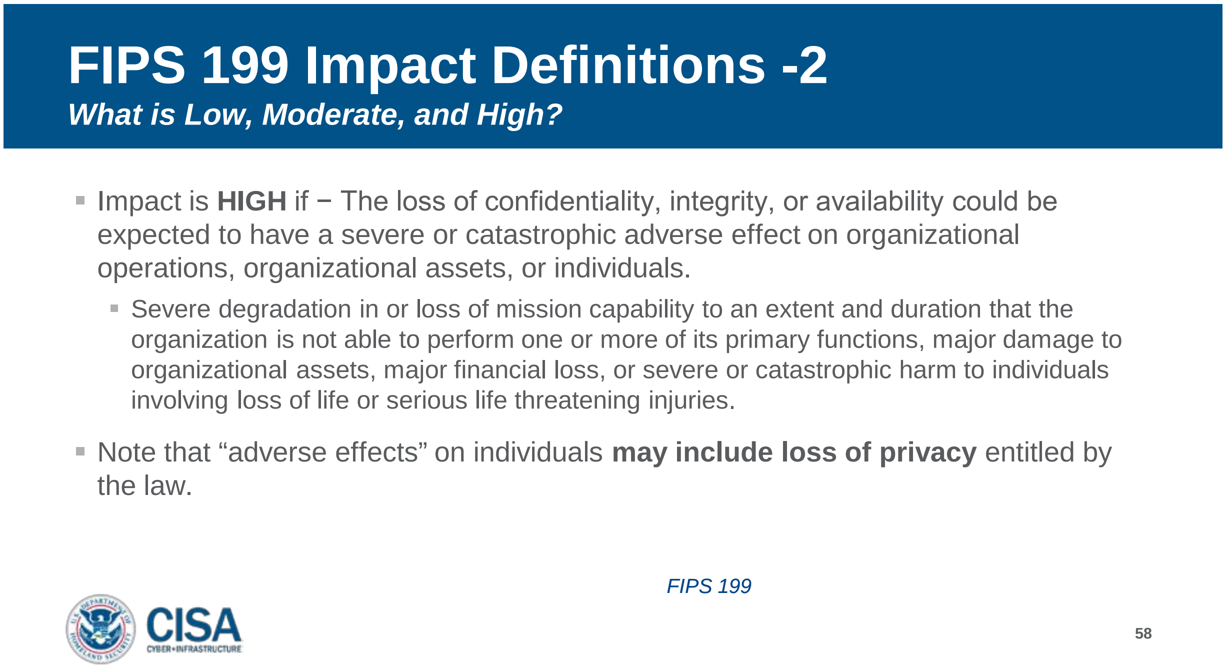
CISA CYBER+INFRASTRUCTURE

57

**057 Now, to be more specific-- and I encourage you go look at FIPS 199-- let's talk a little bit about the classification levels that they have. For example, if they say they have a low impact, that means that if you lose any of those elements of CIA-- the confidentiality, the integrity, the availability-- that you would have a limited adverse effect. You could probably carry on after this risk has come to light. Sure, your mission may be degraded somewhat and you may have some functions that are noticeably reduced, but you could still make it from one end of the field to the other.

This contrasts with moderate, where you lose CIA yet again, but it's going to have a more serious adverse effect. In this particular case, the effectiveness of the function may be reduced to a point where you're not going to accomplish your mission, or you may even realize a significant financial loss or have harmed individuals within your organization.

FIPS 199 Impact Definitions -2 What is Low, Moderate, and High?



FIPS 199 Impact Definitions -2

What is Low, Moderate, and High?

- Impact is **HIGH** if – The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
  - Severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions, major damage to organizational assets, major financial loss, or severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
- Note that “adverse effects” on individuals **may include loss of privacy** entitled by the law.

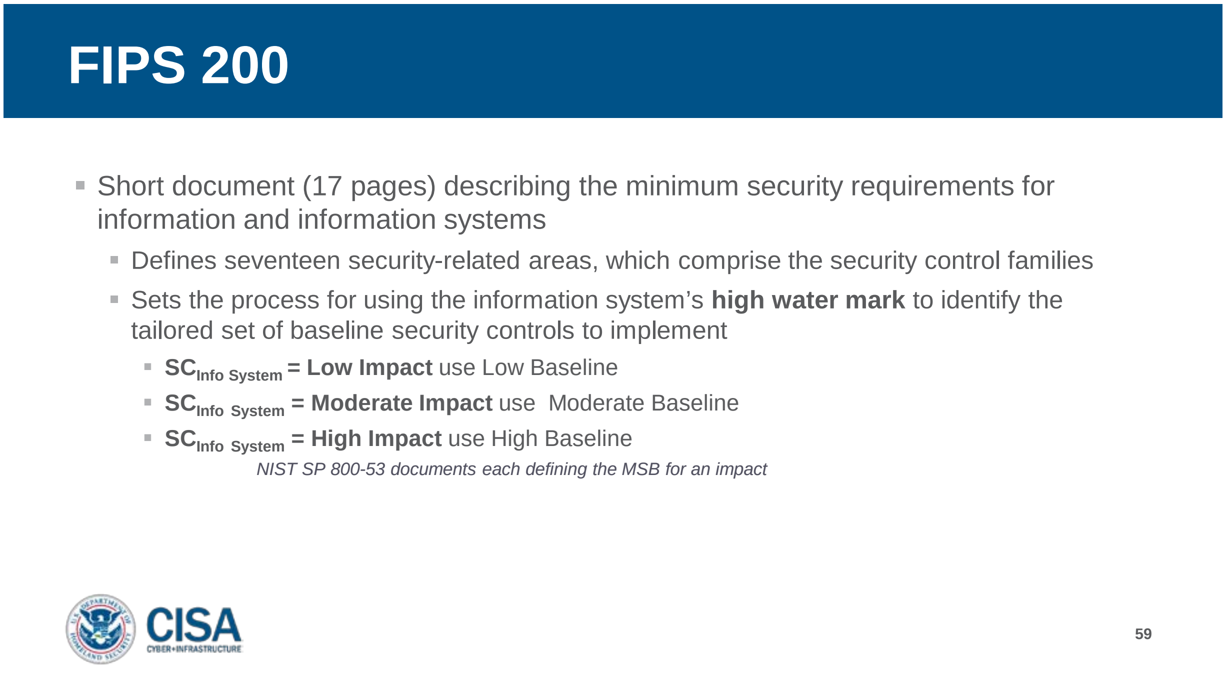
FIPS 199

CISA CYBER+INFRASTRUCTURE

58

**058 Worse still, you could have a high classification, where once again you've lost CIA to a point where it's severely degraded your mission. You may not even be able to complete it. You may have major damage that takes you out of your operations altogether, or you could have a financial loss similarly that could really destroy your organization.

FIPS 200



FIPS 200

- Short document (17 pages) describing the minimum security requirements for information and information systems
  - Defines seventeen security-related areas, which comprise the security control families
  - Sets the process for using the information system's **high water mark** to identify the tailored set of baseline security controls to implement
    - $\mathbf{SC}_{\textbf{Info System}}$ **= Low Impact** use Low Baseline
    - $\mathbf{SC}_{\textbf{Info System}}$ **= Moderate Impact** use Moderate Baseline
    - $\mathbf{SC}_{\textbf{Info System}}$ **= High Impact** use High Baseline

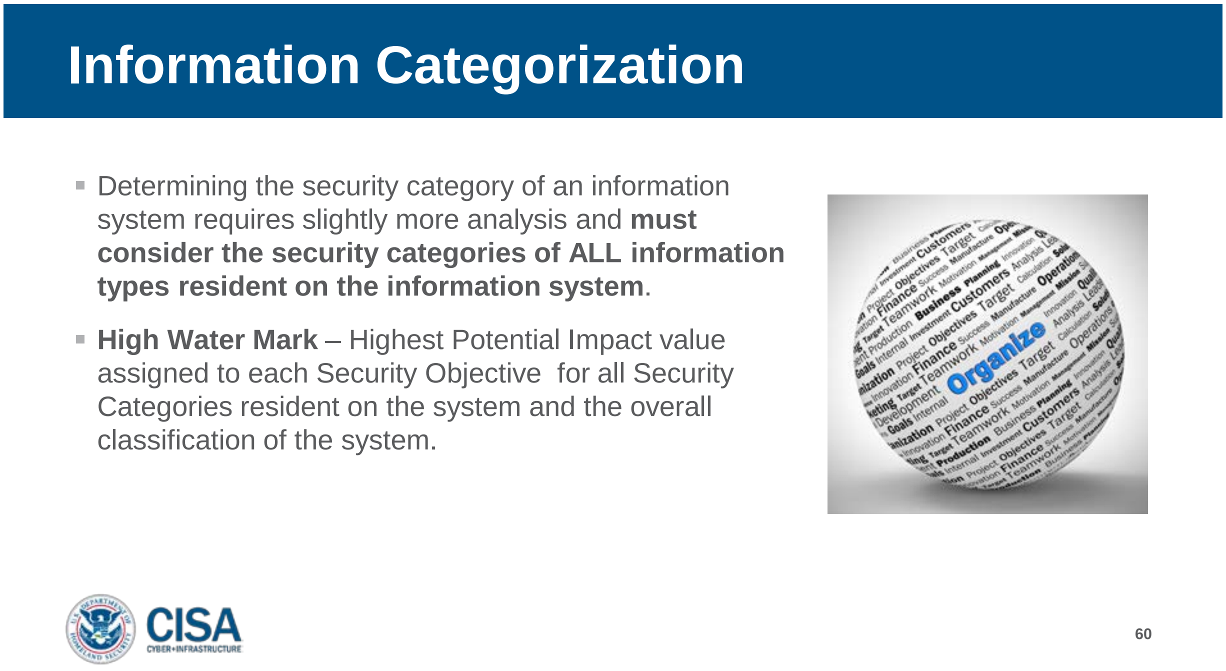
NIST SP 800-53 documents each defining the MSB for an impact

59

**059 However you classify it, what you want to do is you want to think about how to leverage those classifications now into selecting those security controls.

There's one more step to take here though. We got to look at FIPS 200. That's a relatively short document, and what it does is it gives you security-related areas that you can use to associate with each of those levels of classification that you've given.

Information Categorization



Information Categorization

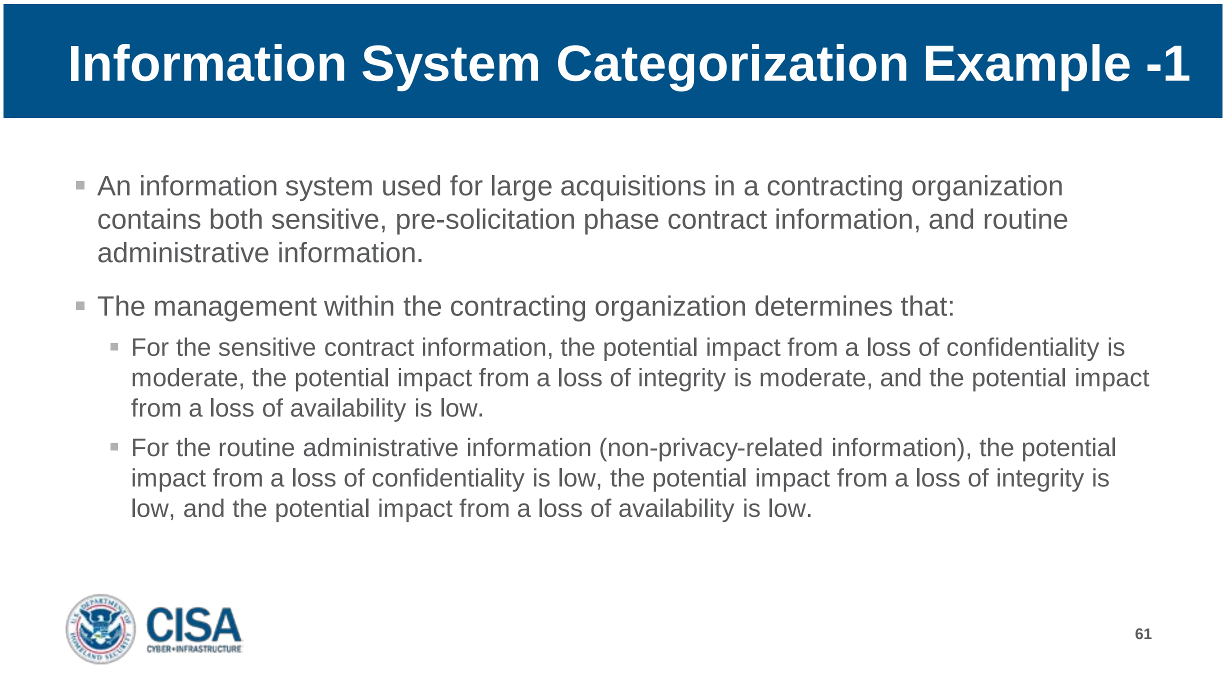
- Determining the security category of an information system requires slightly more analysis and **must consider the security categories of ALL information types resident on the information system**.
- **High Water Mark** – Highest Potential Impact value assigned to each Security Objective for all Security Categories resident on the system and the overall classification of the system.

CISA
CYBER+INFRASTRUCTURE

60

**060 But before we go to NIST SP 800-53, we have to go back and think about the characterizations that we gave in terms of CIA. Remember high, medium, and low? What we really want to focus upon here is finding what the high water mark is. So suppose I have confidentiality that is a medium rank and I have integrity and I have availability as low. The high water mark there is going to be that medium rank. It's the highest potential impact for that security objective.

Information System Categorization Example -1



Information System Categorization Example -1

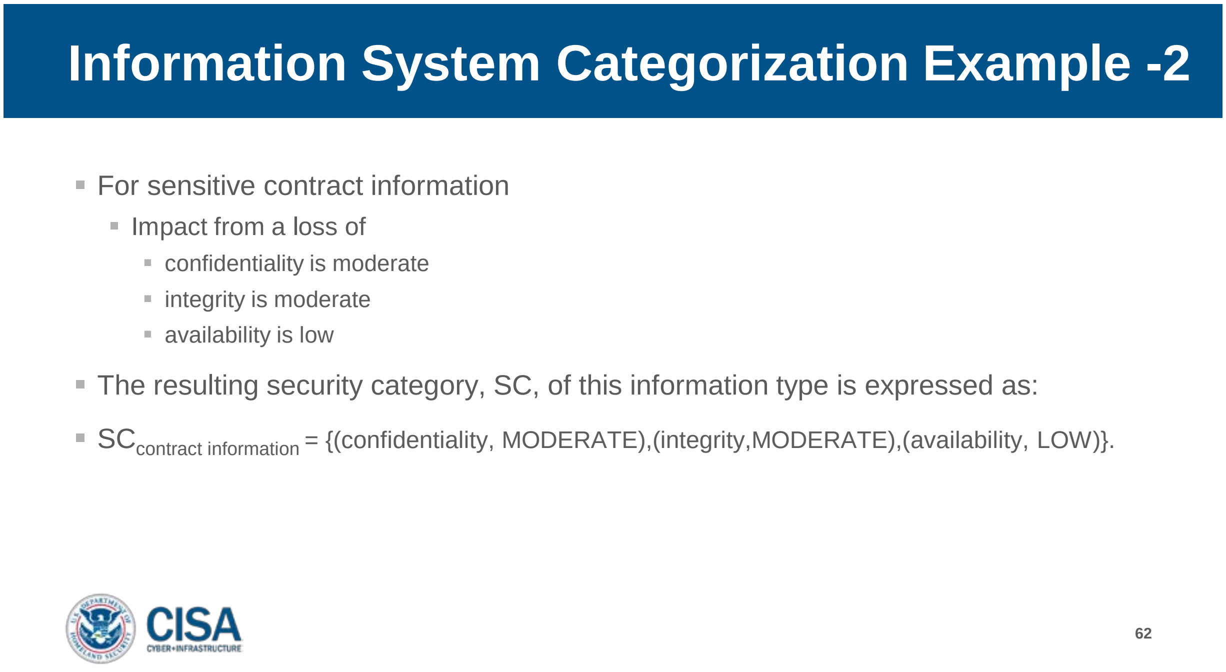
- An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information, and routine administrative information.
- The management within the contracting organization determines that:
  - For the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low.
  - For the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

61

**061 So now that we understand what the high water mark is, let's talk about some scenarios that we can apply these new categorizations to, and then we can talk about maybe the security control selection.

For these two scenarios, one we're going to have sensitive contract information, and we go through our analysis and we find out the potential impact for loss of confidentiality is moderate; we find out that the impact for loss of integrity is moderate; and we find out that the impact for loss of availability is actually low. Similarly, we have yet another scenario where we could just have routine administrative administration, nothing privacy related. Maybe it's something having to do with just day-to-day operations, like maybe a production schedule or something to that effect. And what we have there, we find after our analysis, is that we have a categorization of confidentiality impact being low, the loss of integrity is low, and the loss of availability is actually quite low as well.

Information System Categorization Example -2



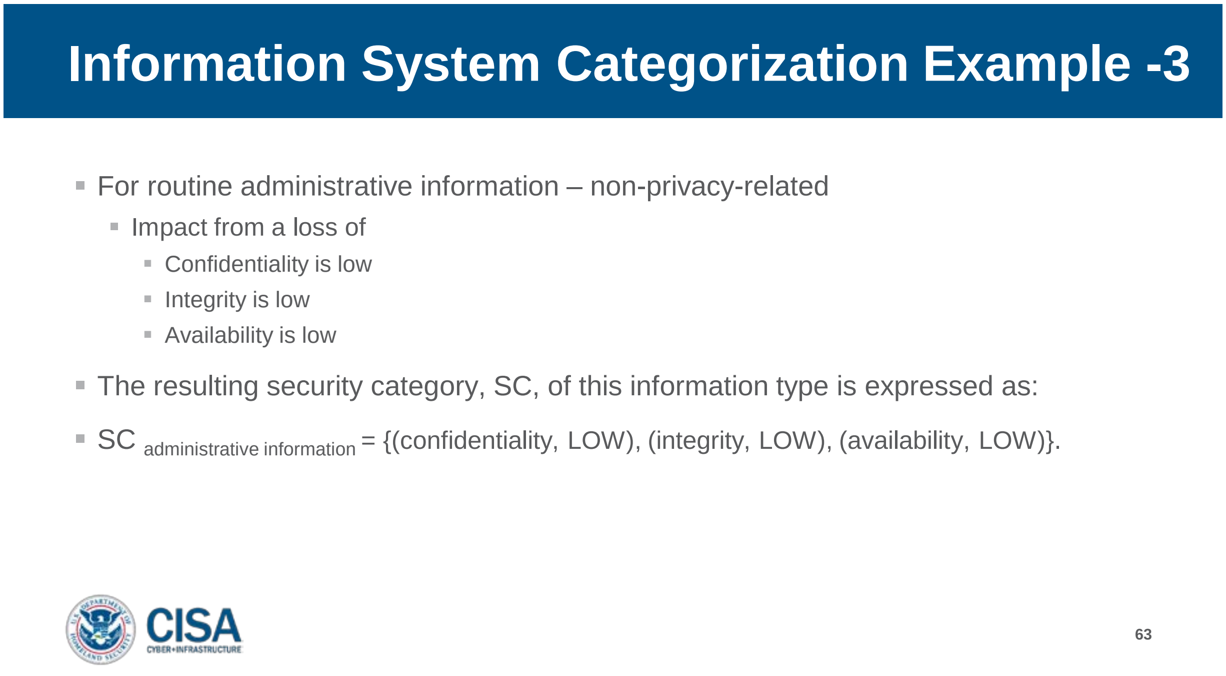
Information System Categorization Example -2

- For sensitive contract information
  - Impact from a loss of
    - confidentiality is moderate
    - integrity is moderate
    - availability is low
- The resulting security category, SC, of this information type is expressed as:
- $SC_{\text{contract information}}$ = {(confidentiality, MODERATE),(integrity,MODERATE),(availability, LOW)}.

CISA
CYBER+INFRASTRUCTURE
62

**062 So here's the annotation that we would use from FIPS for the categorization of that contract information. Notice once again it's moderate for confidentiality, moderate for integrity, low for availability.

Information System Categorization Example -3



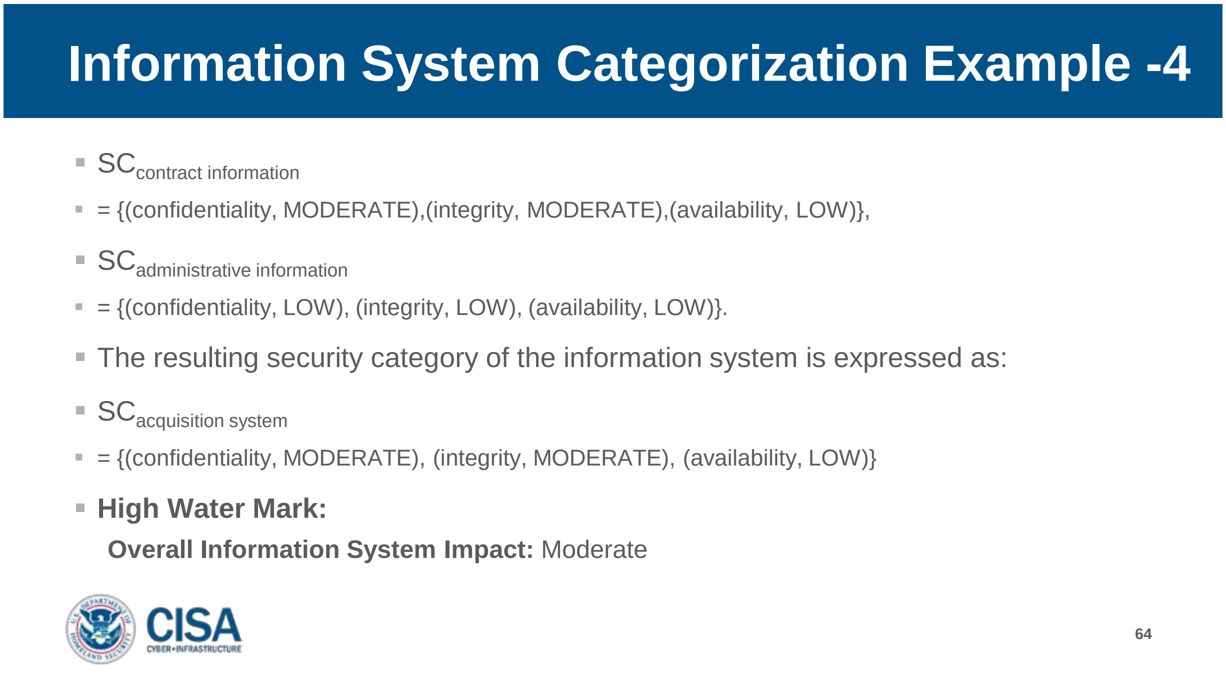
Information System Categorization Example -3

- For routine administrative information – non-privacy-related
  - Impact from a loss of
    - Confidentiality is low
    - Integrity is low
    - Availability is low
- The resulting security category, SC, of this information type is expressed as:
- $SC_{\text{administrative information}}$ = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

63

**063 And here's what it would look like for that routine administrative information. Once again, confidentiality low, integration low, availability low. So take a minute and think about this. What's my high water mark?

Information System Categorization Example -4



Information System Categorization Example -4

- $SC_{\text{contract information}}$
- = {(confidentiality, MODERATE),(integrity, MODERATE),(availability, LOW)},
- $SC_{\text{administrative information}}$
- = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.
- The resulting security category of the information system is expressed as:
- $SC_{\text{acquisition system}}$
- = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)}
- **High Water Mark:**

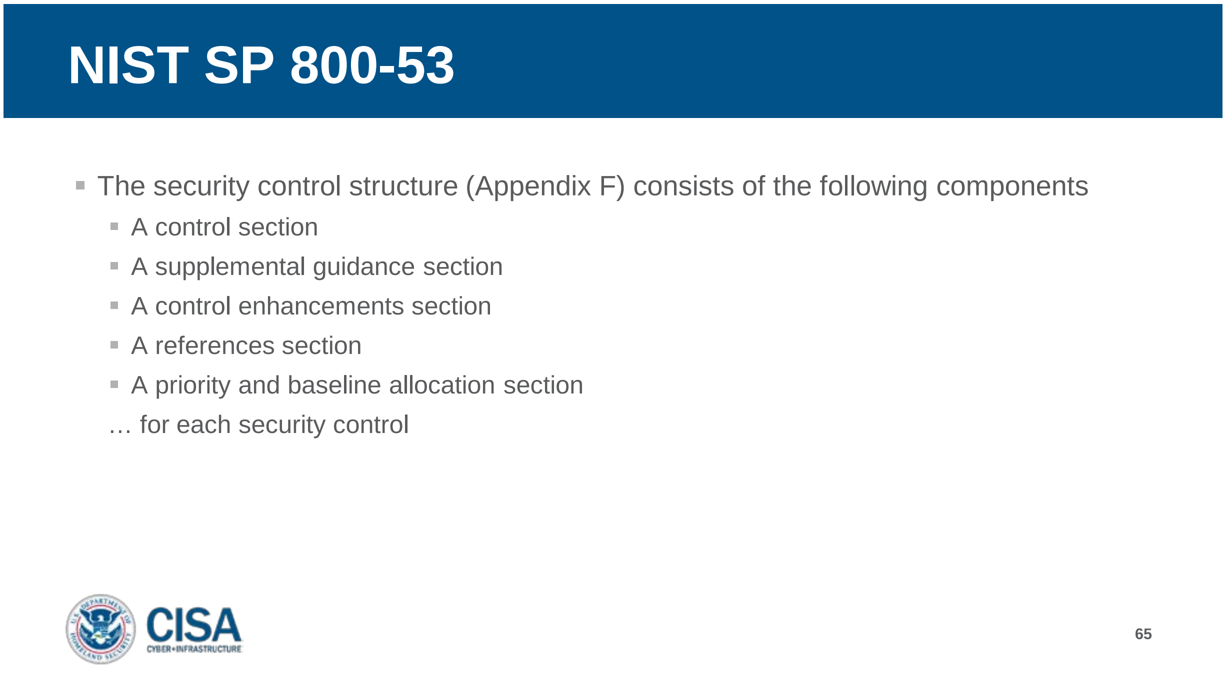
  Overall Information System Impact: Moderate

CISA
CYBER+INFRASTRUCTURE

64

**064 Well, if I look at these together in aggregate, I find out that my actual overall information system impact is moderate.

NIST SP 800-53



NIST SP 800-53

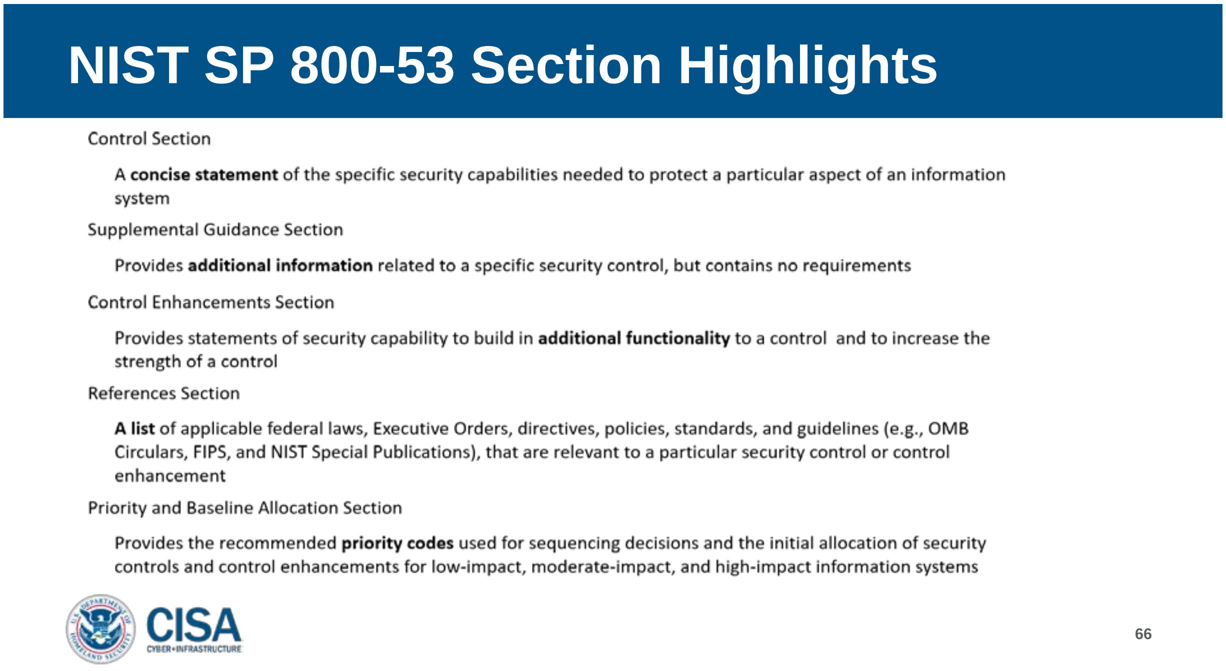
- The security control structure (Appendix F) consists of the following components
  - A control section
  - A supplemental guidance section
  - A control enhancements section
  - A references section
  - A priority and baseline allocation section

  … for each security control

65

**065 Now what I want to do is I want to turn to NIST SP 800-53, because this is where the rubber meets the road in terms of actually identifying the security controls I need, and what I'm going to do is I'm going to walk through a control section in Appendix Foxtrot, and it's going to provide me some guidance on how to pick these actual specific controls.

NIST SP 800-53 Section Highlights



NIST SP 800-53 Section Highlights

Control Section

A **concise statement** of the specific security capabilities needed to protect a particular aspect of an information system

Supplemental Guidance Section

Provides **additional information** related to a specific security control, but contains no requirements

Control Enhancements Section

Provides statements of security capability to build in **additional functionality** to a control and to increase the strength of a control

References Section

A list of applicable federal laws, Executive Orders, directives, policies, standards, and guidelines (e.g., OMB Circulars, FIPS, and NIST Special Publications), that are relevant to a particular security control or control enhancement

Priority and Baseline Allocation Section

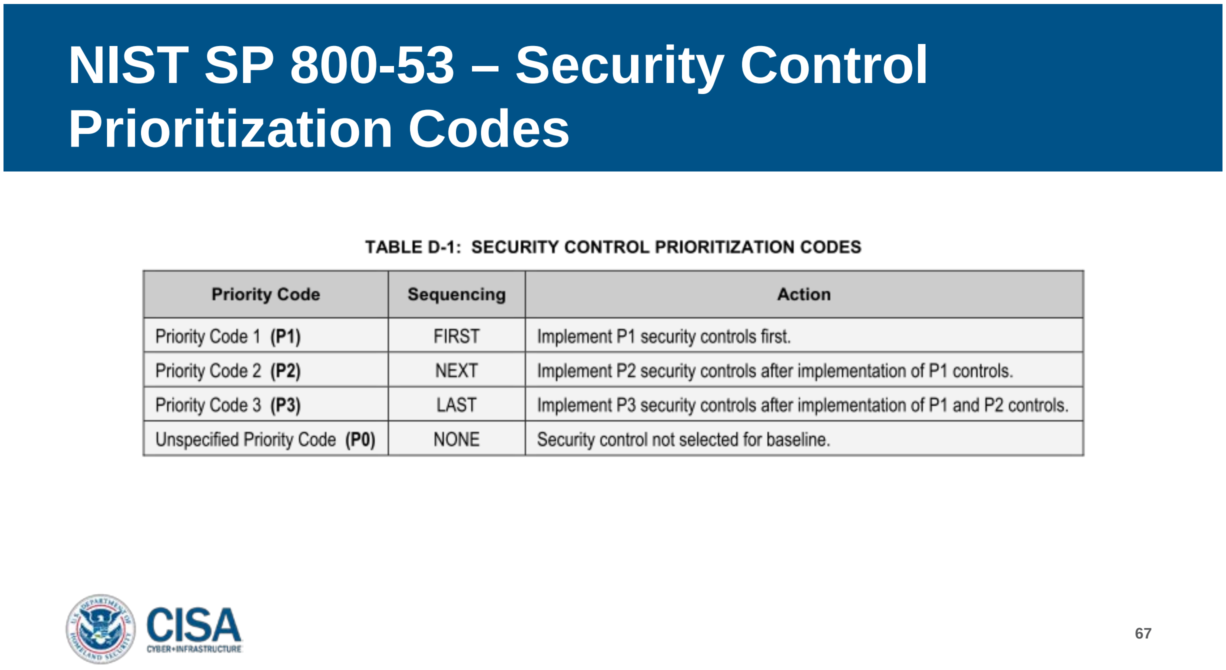
Provides the recommended **priority codes** used for sequencing decisions and the initial allocation of security controls and control enhancements for low-impact, moderate-impact, and high-impact information systems

66

**066 Now, when we do this, there's some things I want to point out in 53 that you want to think about as you actually go through this document. It is kind of meaty; I think it's something like 489 pages, or something crazy like that. Do not get frustrated, and do not feel like it's such a big elephant to eat. Rather, what you want to do is focus on the sections where you can get the most impact for your organization. Control selection, for example, may be a good first place to start. You want to think about having a concise statement that they provide you for specific security capabilities. It's in there. They also give you some supplemental guidance for each one too, which is just like a little bit more additional information about each control. They can also tell you about how you can actually go over the top.

Suppose you already have a control in place and you want to just enhance what you have. That's in there as well. And if anything, you can go to the reference section and you can read a list of all the applicable federal laws and regulations, some applicable executive orders. There's a lot of good information in there in that regard too.

NIST SP 800-53 – Security Control Prioritization Codes



NIST SP 800-53 – Security Control Prioritization Codes

TABLE D-1: SECURITY CONTROL PRIORITIZATION CODES

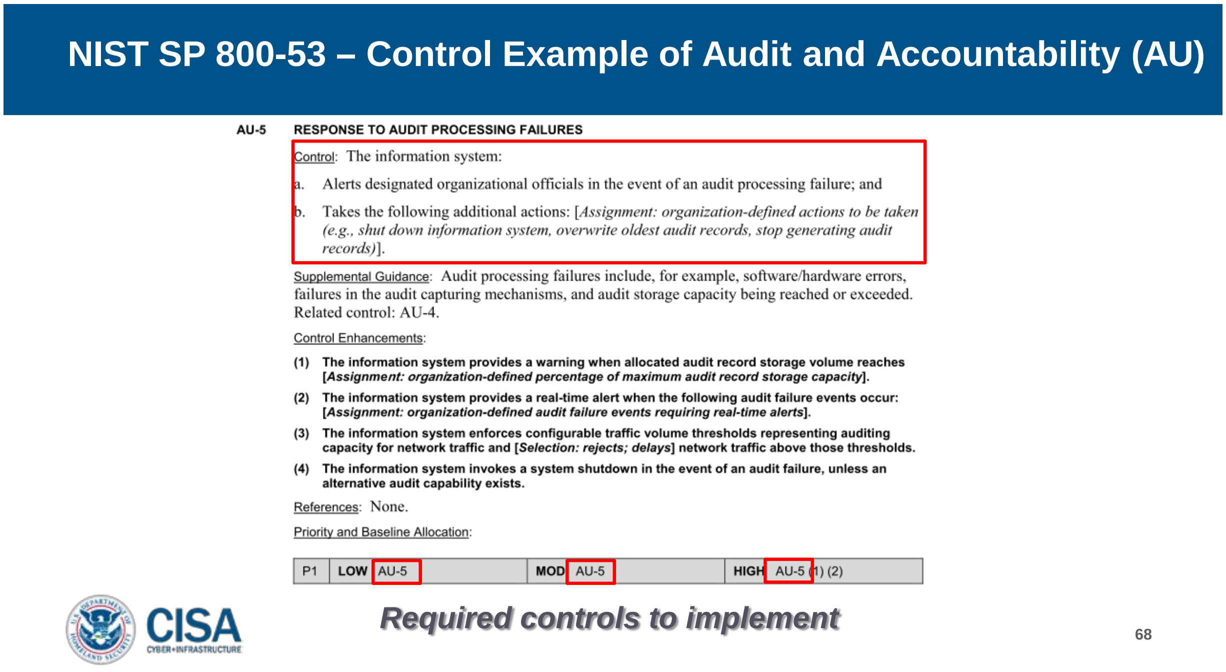
Priority Code	Sequencing	Action
Priority Code 1 **(P1)**	FIRST	Implement P1 security controls first.
Priority Code 2 **(P2)**	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 **(P3)**	LAST	Implement P3 security controls after implementation of P1 and P2 controls.
Unspecified Priority Code **(P0)**	NONE	Security control not selected for baseline.

67

**067 So, before you actually go out and start selecting controls, what you really want to think about is how you're going to prioritize them as well. SP 800-53 does that in Appendix Delta. So go look there and you'll find these priority codes. There's P1, P2, P3, and P0. And you want to think about this in terms of how am I going to sequence implementing these controls.

Remember, you don't have an infinite resource pool, so you're definitely going to want to start with a priority code of 1 first, working all the way through to priority code 3 if at all possible, if you can afford it. Clearly with P1, you're going to implement those security controls first, and then you do 2, and then subsequently 3 if you still have resources left.

NIST SP 800-53 – Control Example of Audit and Accountability (AU)



NIST SP 800-53 – Control Example of Audit and Accountability (AU)

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects; delays*] network traffic above those thresholds.

(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

References: None.

Priority and Baseline Allocation:

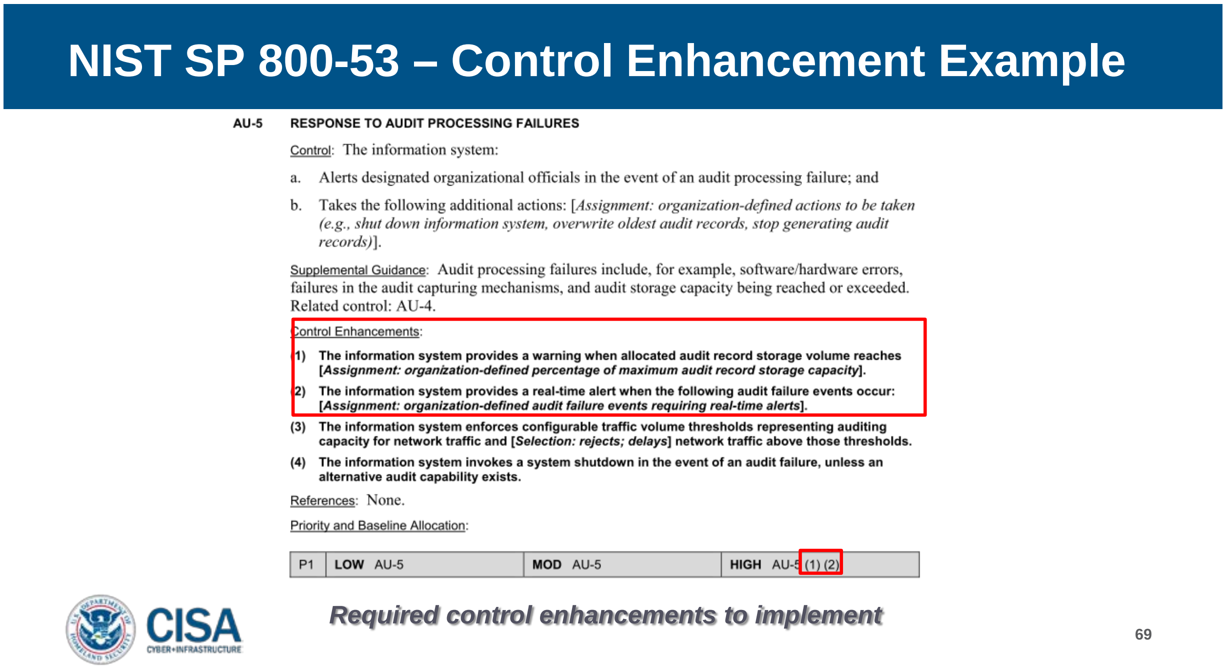
P1	LOW	AU-5	MOD	AU-5	HIGH	AU-5 (1) (2)

Required controls to implement

68

**068 Okay, so let's get more into the details. Now that we've identified a priority code, what we want to do is actually talk about an individual control. For example, let's talk about the audit and accountability control here for response to audit process and failure. Notice our priority codes are at the bottom of the page, and those are the required controls that you have to implement based on the priority code that you assign. The control at the top gives you the top-level idea of what you need to implement for that base set of controls.

NIST SP 800-53 – Control Enhancement Example



NIST SP 800-53 – Control Enhancement Example

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects; delays*] network traffic above those thresholds.

(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

References: None.

Priority and Baseline Allocation:

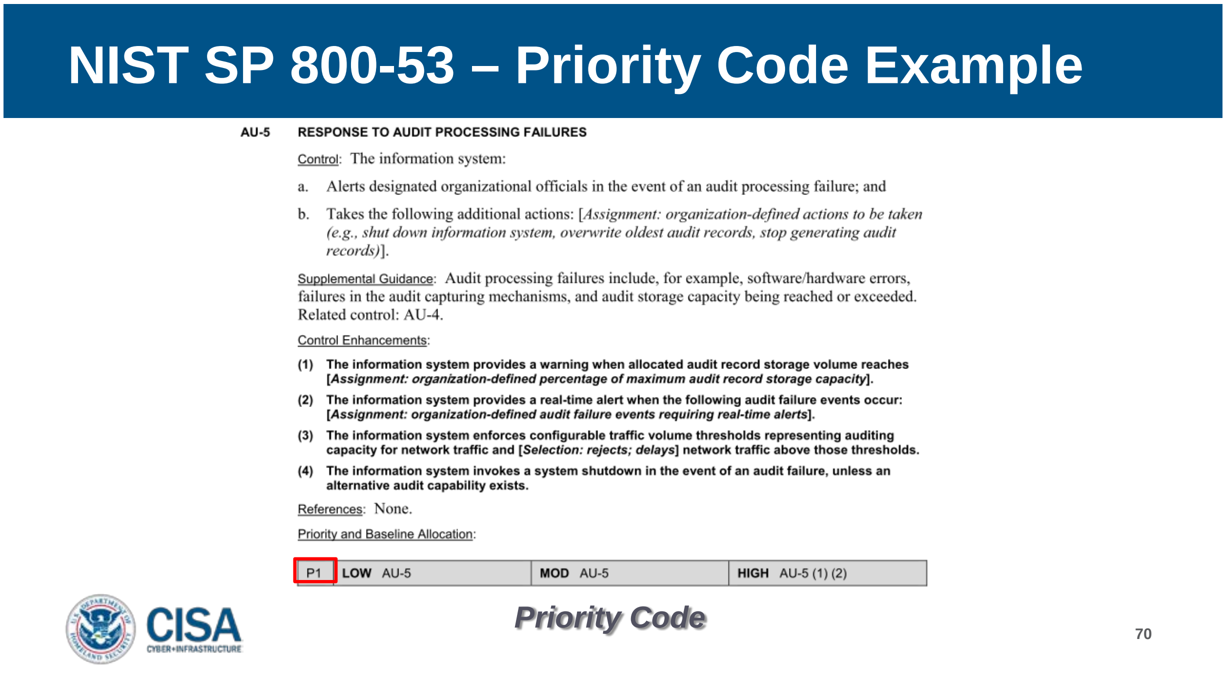
P1	**LOW** AU-5	**MOD** AU-5	**HIGH** AU-5 (1) (2)

Required control enhancements to implement

69

**069 Now, notice that as my P code or my priority goes up, the enhancements which were optional if my priority was low have now become required as I get to a high priority code.

NIST SP 800-53 – Priority Code Example



NIST SP 800-53 – Priority Code Example

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects; delays*] network traffic above those thresholds.

(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

References: None.

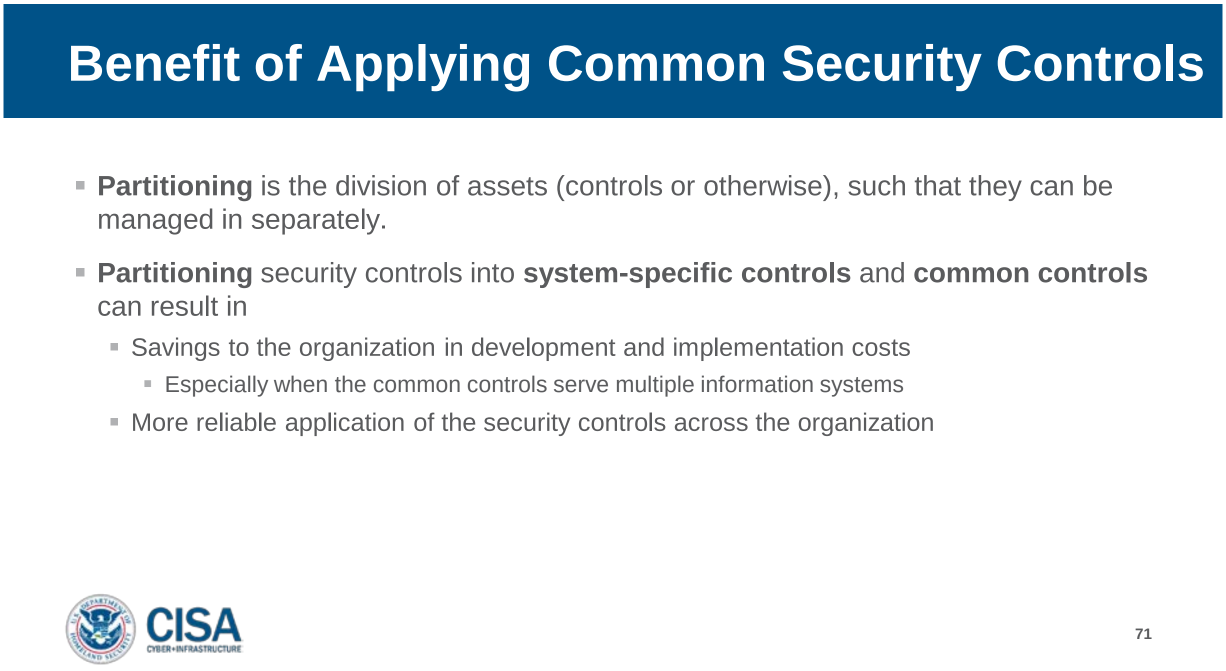
Priority and Baseline Allocation:

P1	**LOW** AU-5	**MOD** AU-5	**HIGH** AU-5 (1) (2)

Priority Code

**070 Once again I want to emphasize it's important to have that priority code so that you know specifically what baseline you're going to set with each of these controls that you're looking at.

Benefit of Applying Common Security Controls



Benefit of Applying Common Security Controls

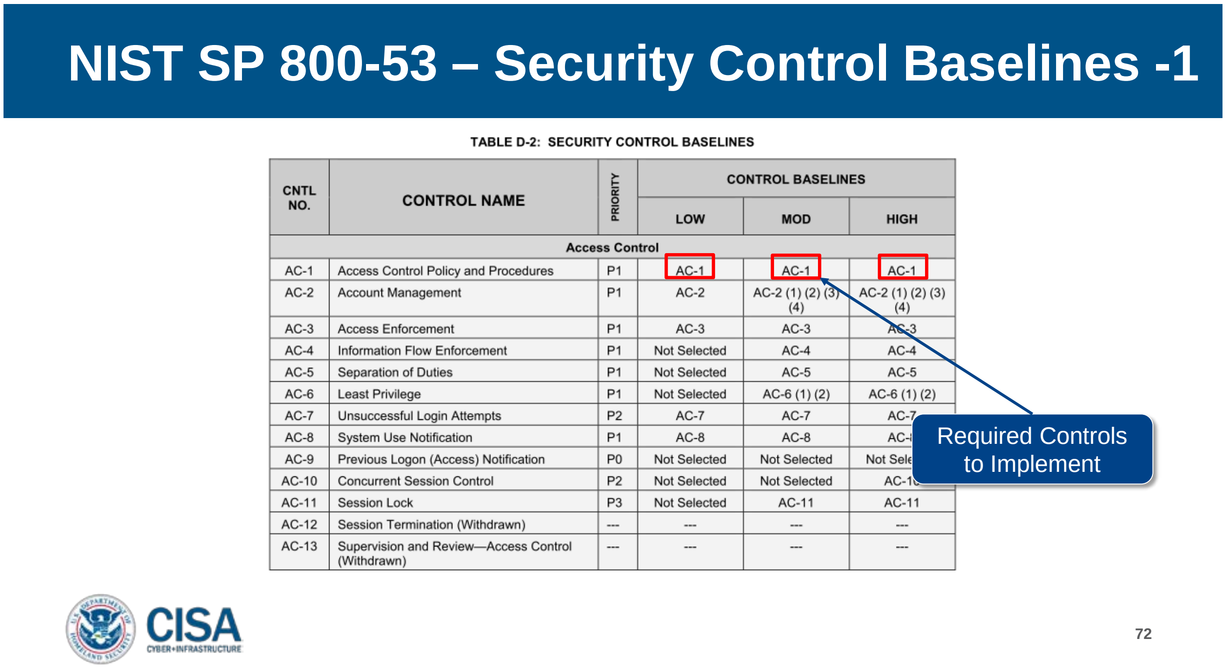
- **Partitioning** is the division of assets (controls or otherwise), such that they can be managed in separately.
- **Partitioning** security controls into **system-specific controls** and **common controls** can result in
  - Savings to the organization in development and implementation costs
    - Especially when the common controls serve multiple information systems
  - More reliable application of the security controls across the organization

71

**071 Now there are some benefits here too. Think about this: If I have some assets and what I want to do is I want to break them up, I can actually partition them, so that way I have security controls that I only assign to certain specific systems. I could also go the other way and have common controls and realize savings because I'm using one control for several systems. It depends on how you have designed your with and how you've designed your system. In all cases though, clearly, since we have that limited resource set, we want to focus on savings at times, this is a strategy that you can take in looking at the common controls lens for selecting your security controls.

One other benefit there that I want to mention is that you can have a more reliable application of your controls across the organization because they can become somewhat universal when you have common controls.

NIST SP 800-53 – Security Control Baselines -1



NIST SP 800-53 – Security Control Baselines -1

TABLE D-2: SECURITY CONTROL BASELINES

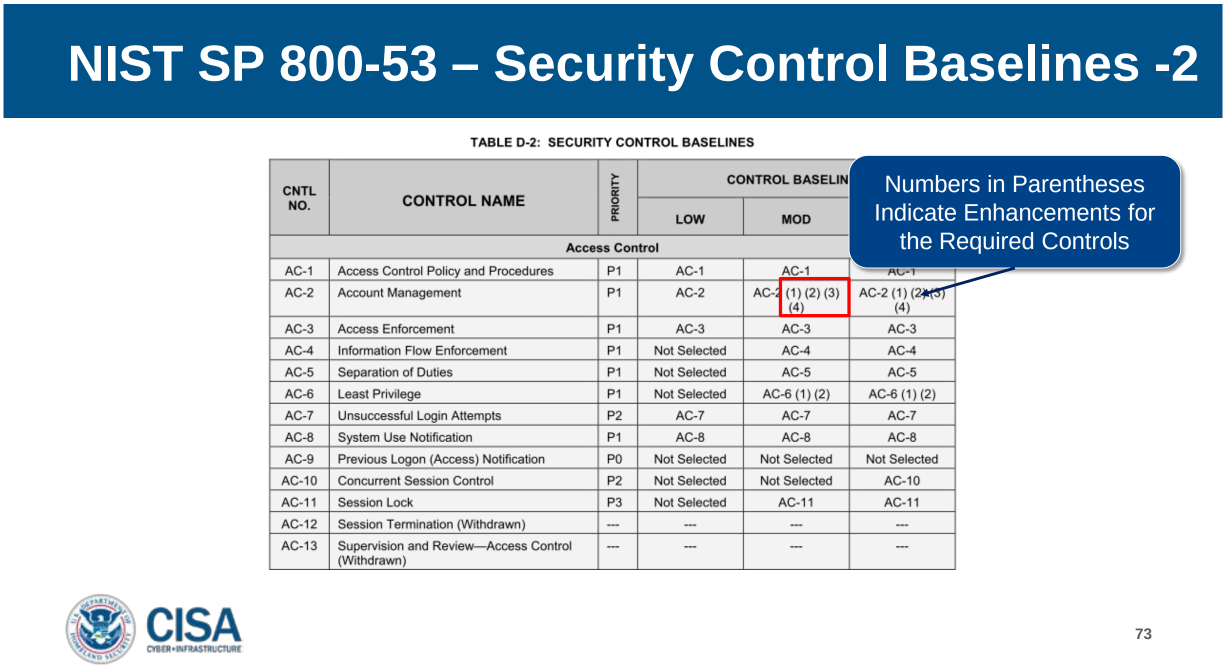
CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
	Access Control				
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2)	AC-6 (1) (2)
AC-7	Unsuccessful Login Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Sele
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-1
AC-11	Session Lock	P3	Not Selected	AC-11	AC-11
AC-12	Session Termination (Withdrawn)	---	---	---	---
AC-13	Supervision and Review—Access Control (Withdrawn)	---	---	---	---

Required Controls to Implement

72

**072 Now, when you set your security control baseline, if we go back and look at Table Delta 2, we can actually go find out if we have a moderate classification from our FIPS discussion, that we know that we need to implement this AC1 control. That's what's required for that baseline.

NIST SP 800-53 – Security Control Baselines -2



NIST SP 800-53 – Security Control Baselines -2

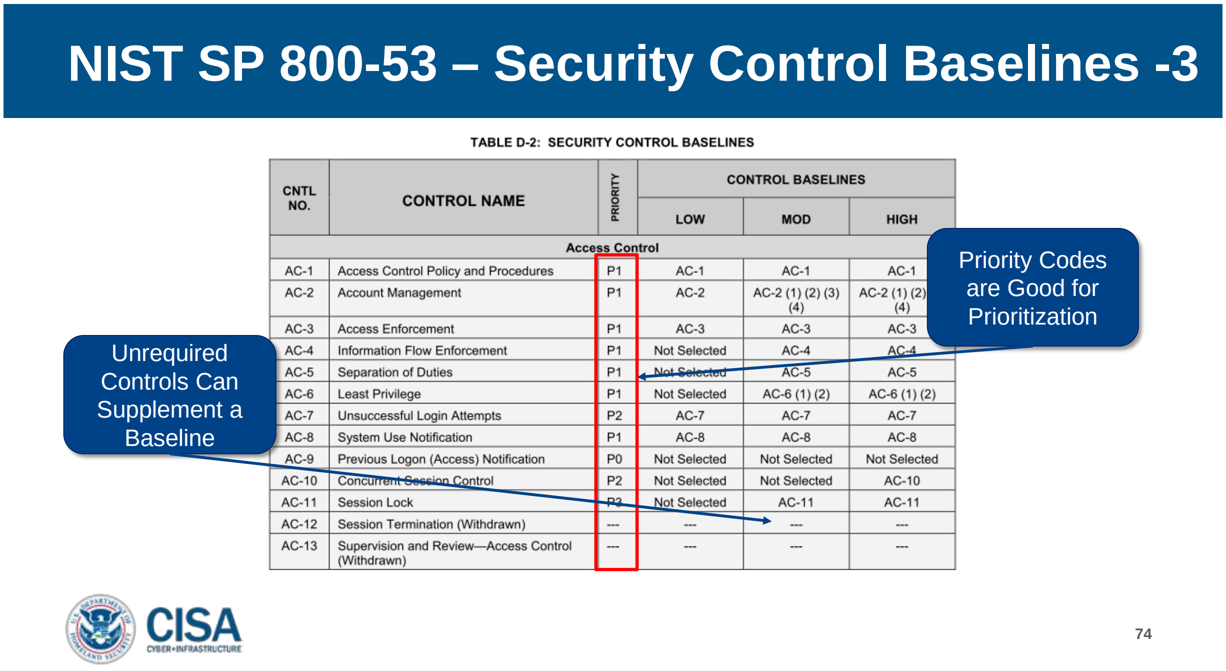
TABLE D-2: SECURITY CONTROL BASELINES

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELIN		
			LOW	MOD	
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2)	AC-6 (1) (2)
AC-7	Unsuccessful Login Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11	AC-11
AC-12	Session Termination (Withdrawn)	---	---	---	---
AC-13	Supervision and Review—Access Control (Withdrawn)	---	---	---	---

Numbers in Parentheses Indicate Enhancements for the Required Controls

**073 The numbers in parentheses following are enhancements for required controls. And remember, not only as our priority code goes up we have to add the enhancements, but in this particular case, this is in alignment with what baseline we've selected and our priority that we've established. In this case, if it were moderate, we actually want to instantiate the 1, 2, 3 and 4 enhancements on AC1 as well.

NIST SP 800-53 – Security Control Baselines -3



NIST SP 800-53 – Security Control Baselines -3

TABLE D-2: SECURITY CONTROL BASELINES

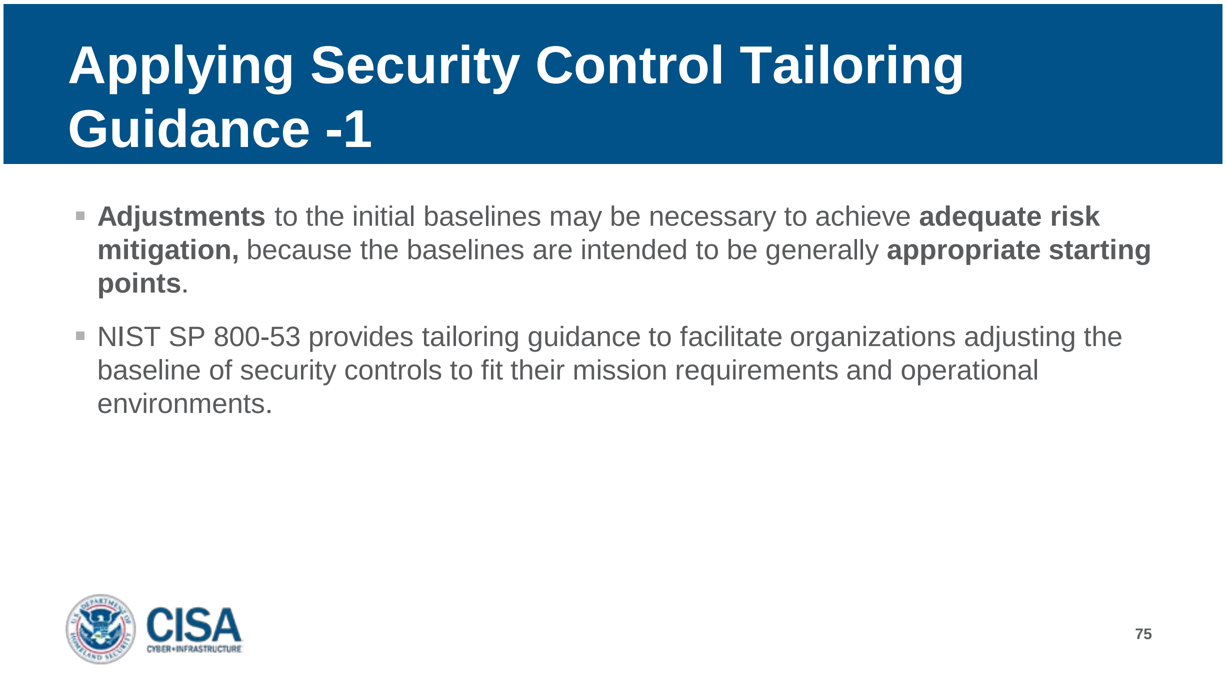
CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
	Access Control				
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (4)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2)	AC-6 (1) (2)
AC-7	Unsuccessful Login Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11	AC-11
AC-12	Session Termination (Withdrawn)	---	---	---	---
AC-13	Supervision and Review—Access Control (Withdrawn)	---	---	---	---

Priority Codes are Good for Prioritization

Unrequired Controls Can Supplement a Baseline

**074 Notice the P codes are to the left. We also want to make sure that we maintain which ones we're going to implement first before others. In this particular case, notice that we have a number of controls from AC1, all the way down to about AC6. At AC7, it becomes a P2, and then it goes back to P1 again. So how this is making out is you're going to have to implement AC8 before you go back and look at AC7. Notice too that you're going to have some control sets that actually have a dashed line. That means that that's not required for your baseline.

Applying Security Control Tailoring Guidance -1



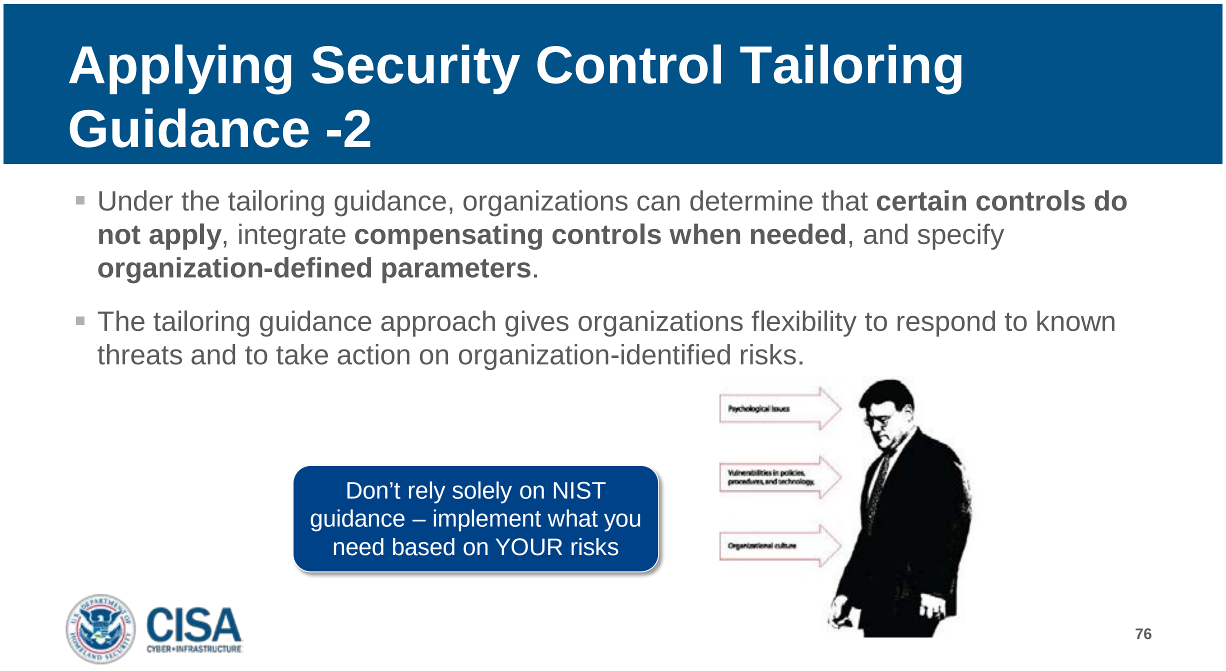
Applying Security Control Tailoring Guidance -1

- **Adjustments** to the initial baselines may be necessary to achieve **adequate risk mitigation,** because the baselines are intended to be generally **appropriate starting points**.
- NIST SP 800-53 provides tailoring guidance to facilitate organizations adjusting the baseline of security controls to fit their mission requirements and operational environments.

75

**075 So now what we want to do is we want to modify this baseline and make adjustments to it so that way it fits our risk profile. Now, remember that these baselines are good starting points, but your organization has its own specific needs. You have your own strategy. You have your own business objectives. You want to keep this in mind as you're going through and selecting these controls out of these baselines. Remember, in all cases, it's just a good start.

Applying Security Control Tailoring Guidance -2



Applying Security Control Tailoring Guidance -2

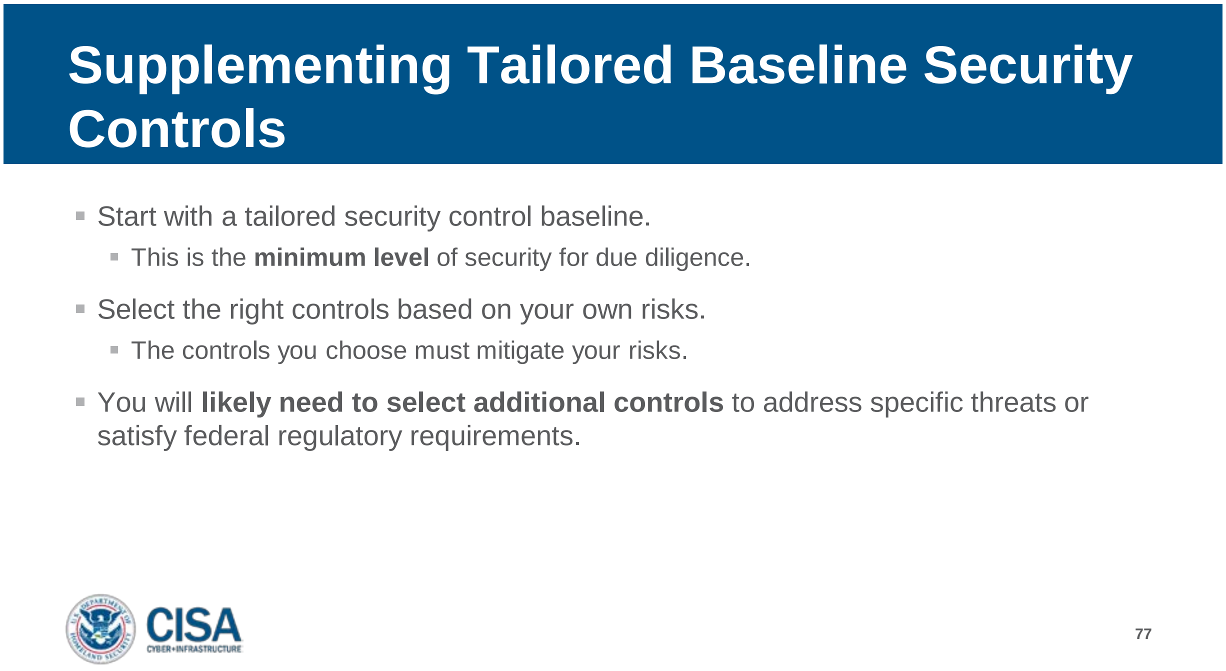
- Under the tailoring guidance, organizations can determine that **certain controls do not apply**, integrate **compensating controls when needed**, and specify **organization-defined parameters**.
- The tailoring guidance approach gives organizations flexibility to respond to known threats and to take action on organization-identified risks.

Don’t rely solely on NIST guidance – implement what you need based on YOUR risks

**076 So now that we've selected these control sets from a baseline, what we could do too is we could tailor and scope them so that they accommodate our organization better. For example, some controls may not apply altogether. Maybe we can have some controls that will compensate for each other. It all depends too on how the organizational boundaries are, or the parameters are set, and what our needs are.

In all cases, what I would encourage you to do is to not necessarily rely strictly on NIST guidance. You really want to implement what you need for your risks.

Supplementing Tailored Baseline Security Controls



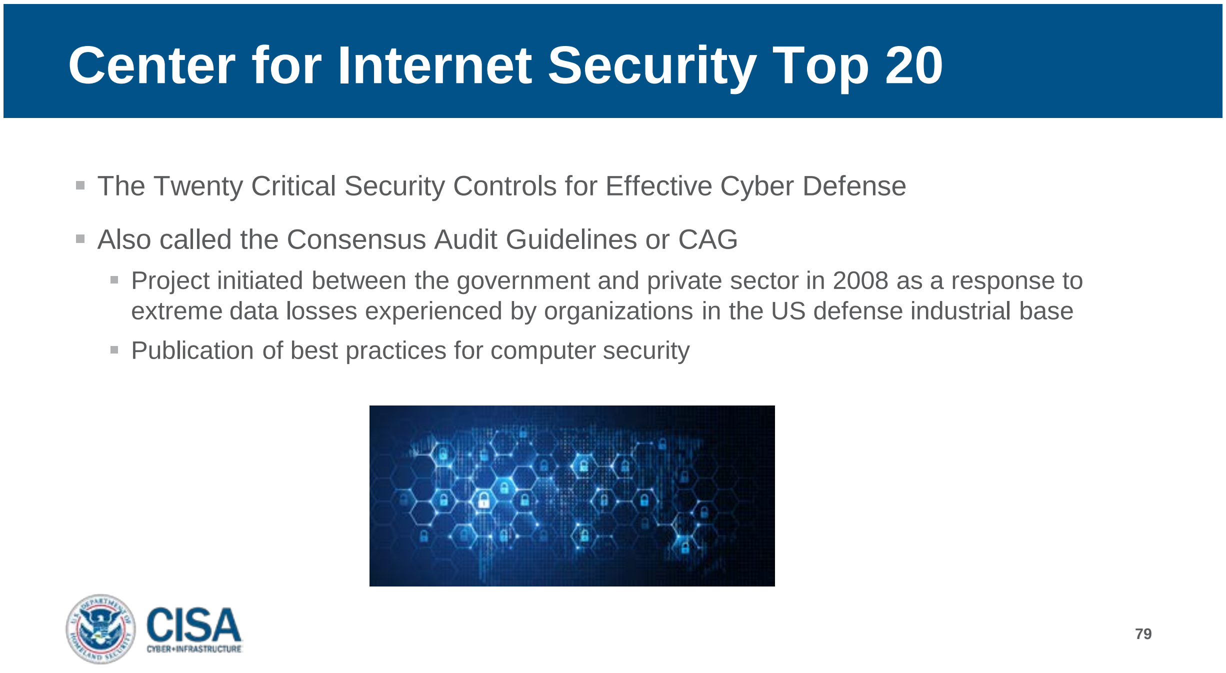
Supplementing Tailored Baseline Security Controls

- Start with a tailored security control baseline.
  - This is the **minimum level** of security for due diligence.
- Select the right controls based on your own risks.
  - The controls you choose must mitigate your risks.
- You will **likely need to select additional controls** to address specific threats or satisfy federal regulatory requirements.

77

**077 So now that we have this baseline established, what we can do is we have our minimum baseline that we've-- that assures us that our minimum level of security is met, and then what we may want to do too, if we have any additional resources left over, is select the right controls for our risk that we have. Remember, our risks may be specific to our organization, so we may need additional to mitigate those risks, or we may have a certain confidence that we want to achieve in meeting those risks. So that's where we would have to go and maybe select some of these additional controls. It's likely that you will need them depending on what your risk portfolio looks like.

Center for Internet Security Top 20

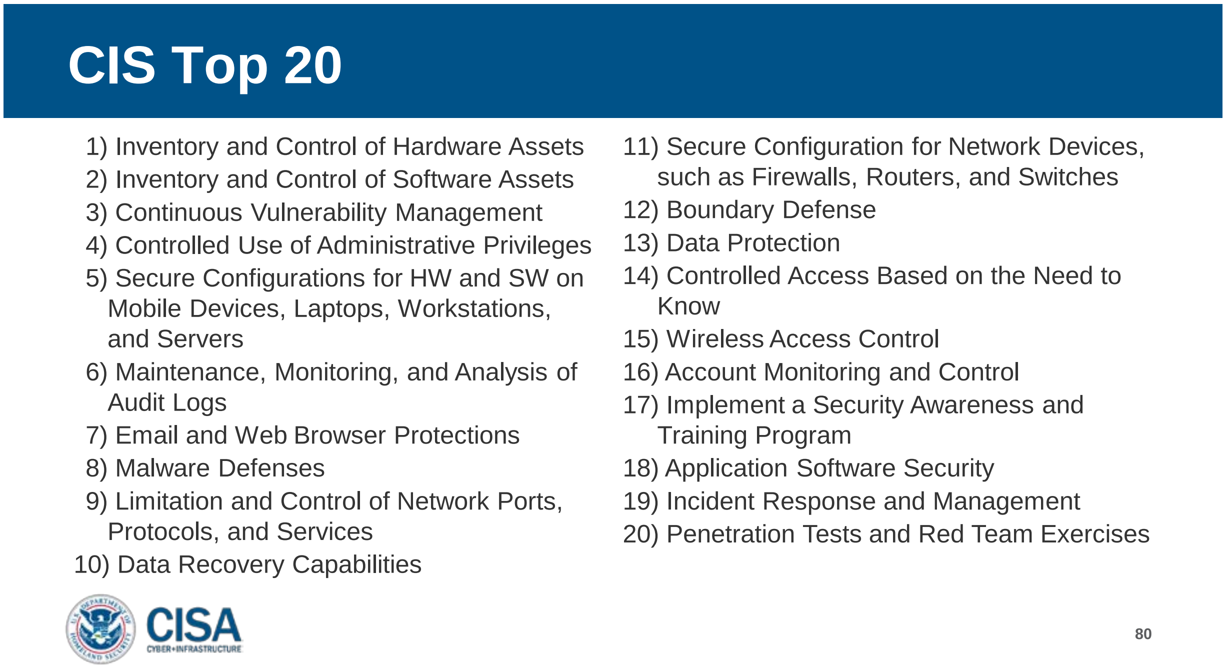


Center for Internet Security Top 20

- The Twenty Critical Security Controls for Effective Cyber Defense
- Also called the Consensus Audit Guidelines or CAG
  - Project initiated between the government and private sector in 2008 as a response to extreme data losses experienced by organizations in the US defense industrial base
  - Publication of best practices for computer security

**079 Let's start with the Center for Internet Security. Now what they've done is they've provided a set of top 20 controls that can help you have better defense in your organization. Note, some people may call this the Consensus Audit Guideline, or the CAG. It started in 2008, but it's certainly evolved since then. It gives you a set of best practices that you can use for computer security in your organization.

CIS Top 20



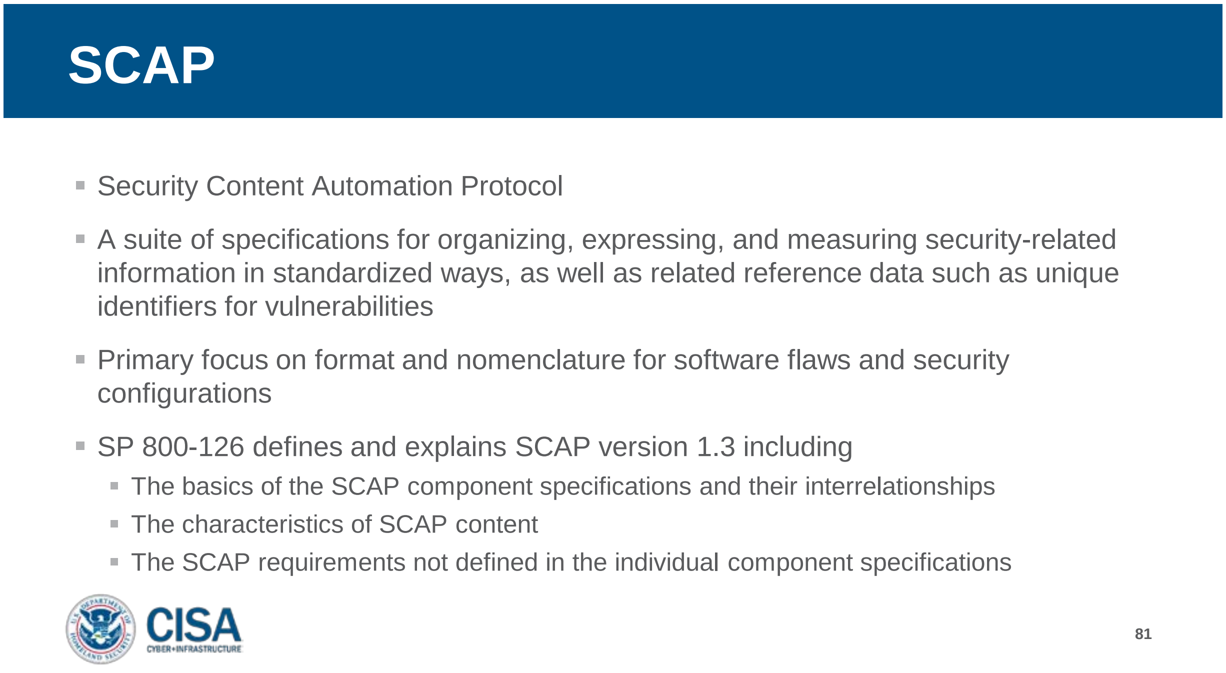
CIS Top 20

1) Inventory and Control of Hardware Assets
2) Inventory and Control of Software Assets
3) Continuous Vulnerability Management
4) Controlled Use of Administrative Privileges
5) Secure Configurations for HW and SW on Mobile Devices, Laptops, Workstations, and Servers
6) Maintenance, Monitoring, and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports, Protocols, and Services
10) Data Recovery Capabilities
11) Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Implement a Security Awareness and Training Program
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises

80

**080 Here's a list of the top 20 that's found on their website. I encourage you to go in and look at each of these recommendations and see which may be best applicable in your organization.

SCAP



SCAP

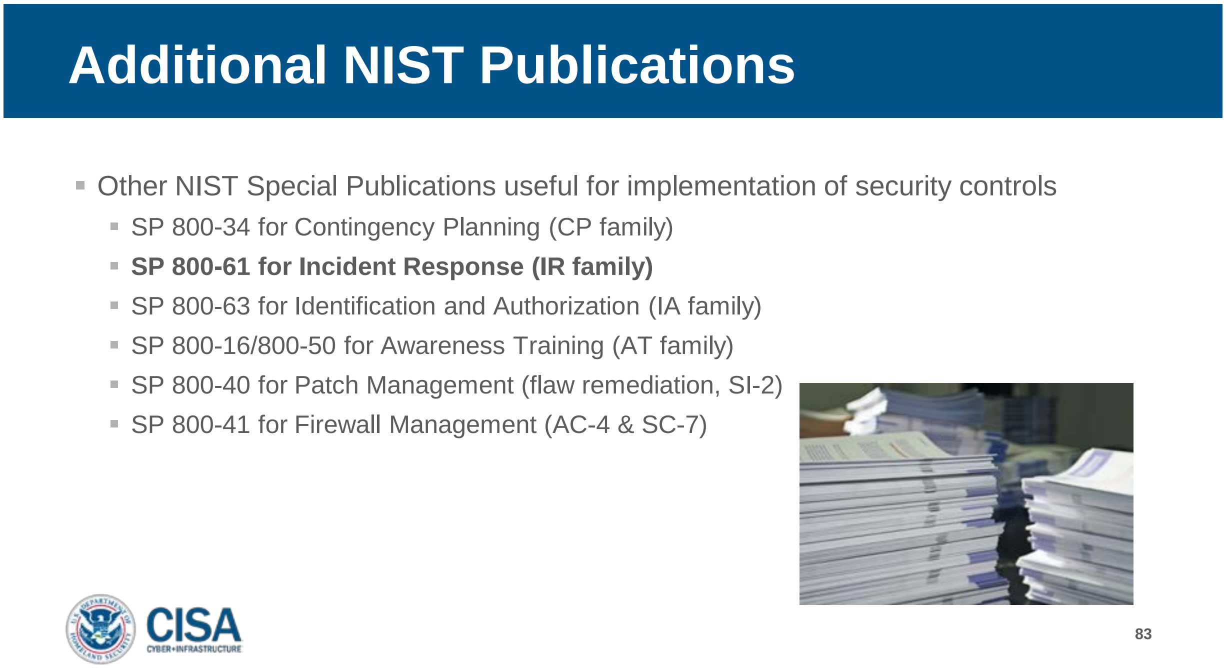
- Security Content Automation Protocol
- A suite of specifications for organizing, expressing, and measuring security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities
- Primary focus on format and nomenclature for software flaws and security configurations
- SP 800-126 defines and explains SCAP version 1.3 including
  - The basics of the SCAP component specifications and their interrelationships
  - The characteristics of SCAP content
  - The SCAP requirements not defined in the individual component specifications

CISA
CYBER+INFRASTRUCTURE

81

**081 You may want to look for amplification on how to implement controls from SP 800-53. There's the Security Content Automation Protocol, also known as SCAP, and what it does is it provides you an amplification of configurations on how you can best meet security flaws per-- by using security configurations. If you turn to SP 800-126, it will give you a good explanation of how SCAP works, and it will give you the basics upon the component specifications and how they're interrelated. It will give you some characteristics behind the content, and it'll also help you with requirements that aren't necessarily defined in other individual component specifications.

Additional NIST Publications



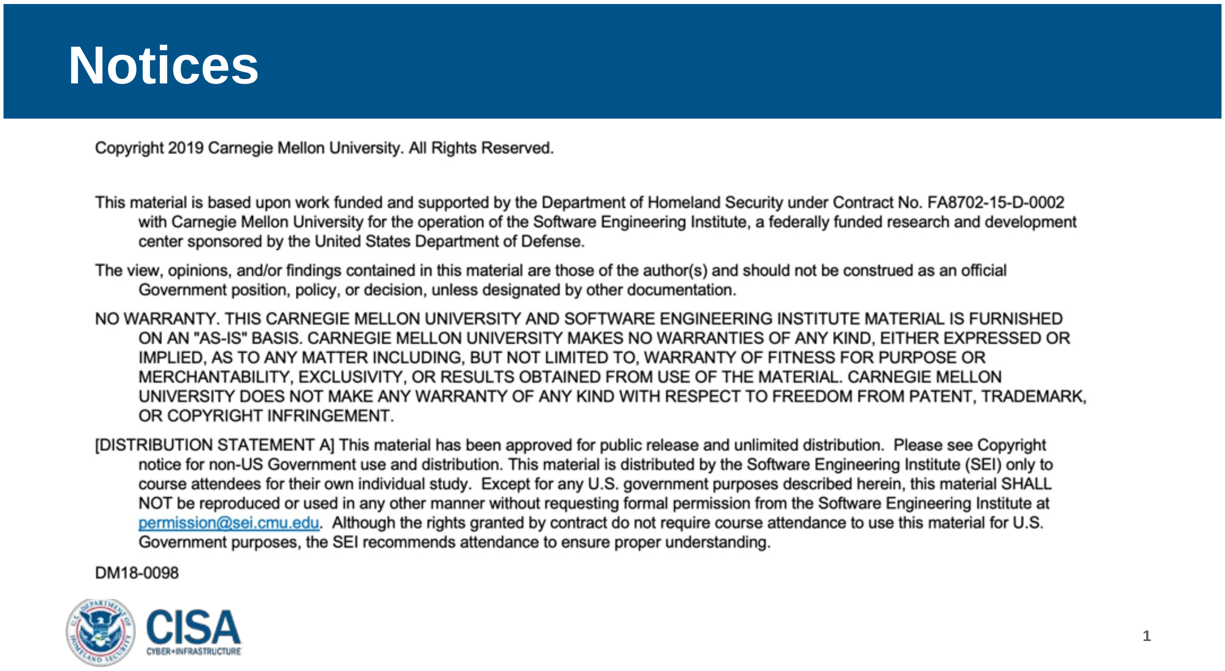
Additional NIST Publications

- Other NIST Special Publications useful for implementation of security controls
  - SP 800-34 for Contingency Planning (CP family)
  - **SP 800-61 for Incident Response (IR family)**
  - SP 800-63 for Identification and Authorization (IA family)
  - SP 800-16/800-50 for Awareness Training (AT family)
  - SP 800-40 for Patch Management (flaw remediation, SI-2)
  - SP 800-41 for Firewall Management (AC-4 & SC-7)

83

**083 Some other publications I list here from NIST include the ones that I have listed here. Now, I'm only going to talk about a few of these. The one I really want to highlight for you here is SP 800-61. It's important that even beyond the idea of selecting security controls that you also start thinking about what is going to take place beyond that cold, dark day of when the risk has come to fruition. This particular document will help you with that incident response.

Notices



Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu. Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM18-0098