Security Control Assessment

Table of Contents

Security Control Assessment

**001 Instructor: Specifically now we want to talk about security control assessments. To this point, we understand what risk is. We know that it is uncertainty that has distinct elements of a threat, vulnerability, and some kind of impact that the organization is going to feel, and we've assessed those risks and we now understand the security controls that we want to actually use in our system. and now we're at the point we were want to understand how well are those controls operating.

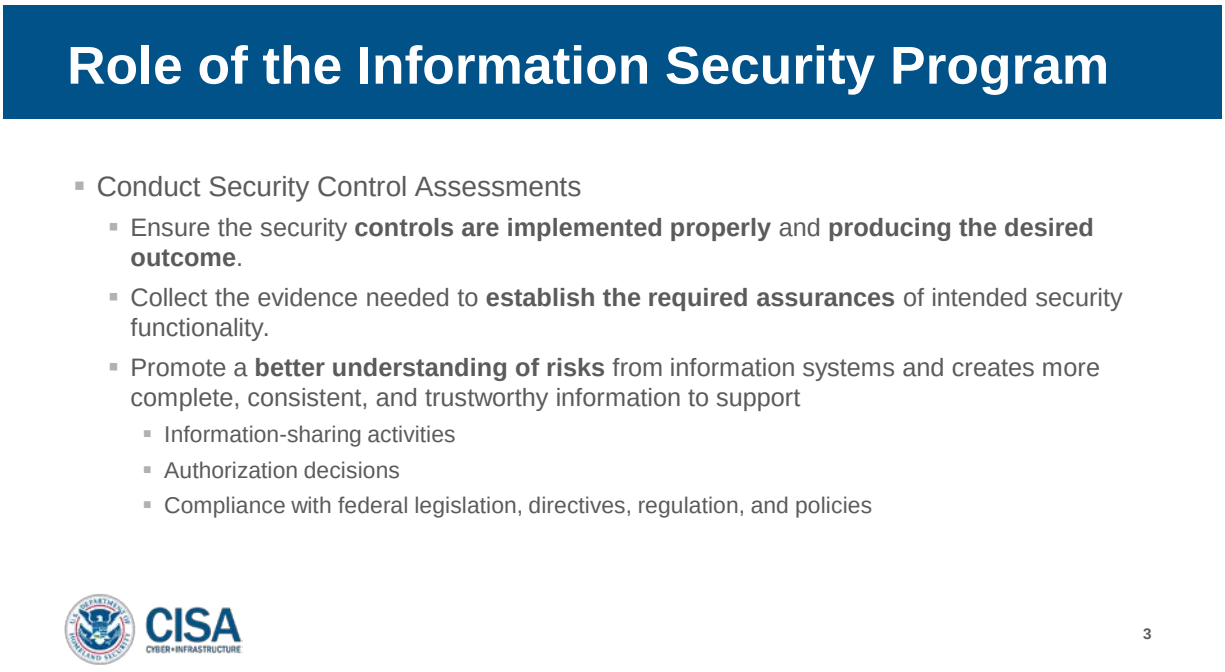
Assessing Security Controls

- A process within an organization's Risk Management Framework (RMF) reviewing
  - Management Controls
  - Operational Controls
  - Technical Controls
- The **assessment determines** the extent that controls found in the System Security Plan are
  - **Implemented correctly**
  - **Operating as intended**
  - **Producing the desired results**

CISA CYBER+INFRASTRUCTURE

2

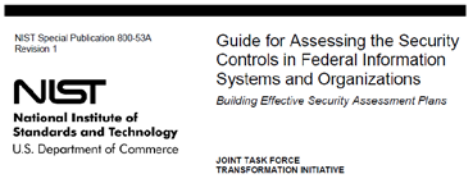
**002 We have to figure out if they've been implemented correctly. We have to know if they're operating as we intended them to do, and we also need to know that we're getting the results out of them that we necessarily have required.



**003 So how are we going to go about doing this? Well, one is we have to establish what the requirements are for those controls. We need to understand that they're meeting their intended security functionality. We need to also use this as an opportunity to enhance and enrich our understanding of the risks related to our systems. So we may think about this in terms of how we have information-sharing activities taking place, how we're actually going about making decisions regarding the authorization of either assets coming into the organization or the controls that we're using, and we also want to double-check to make sure that we're meeting specific compliance requirements. This, by the way, may be federal, it may be organizational--whatever our policies dictate.

NIST Publications

- Appropriate for assessing security controls
  - Guidance – NIST SP 800-53A
    - Provides organizations a repeatable security assessment methodology for each security control identified in NIST SP-800-53
  - Guidance – NIST SP 800-115
    - Provides guidance on basic technical aspects of conducting information security assessments and penetration testing



CISA CYBER+INFRASTRUCTURE

INFORMATION SECURITY

4

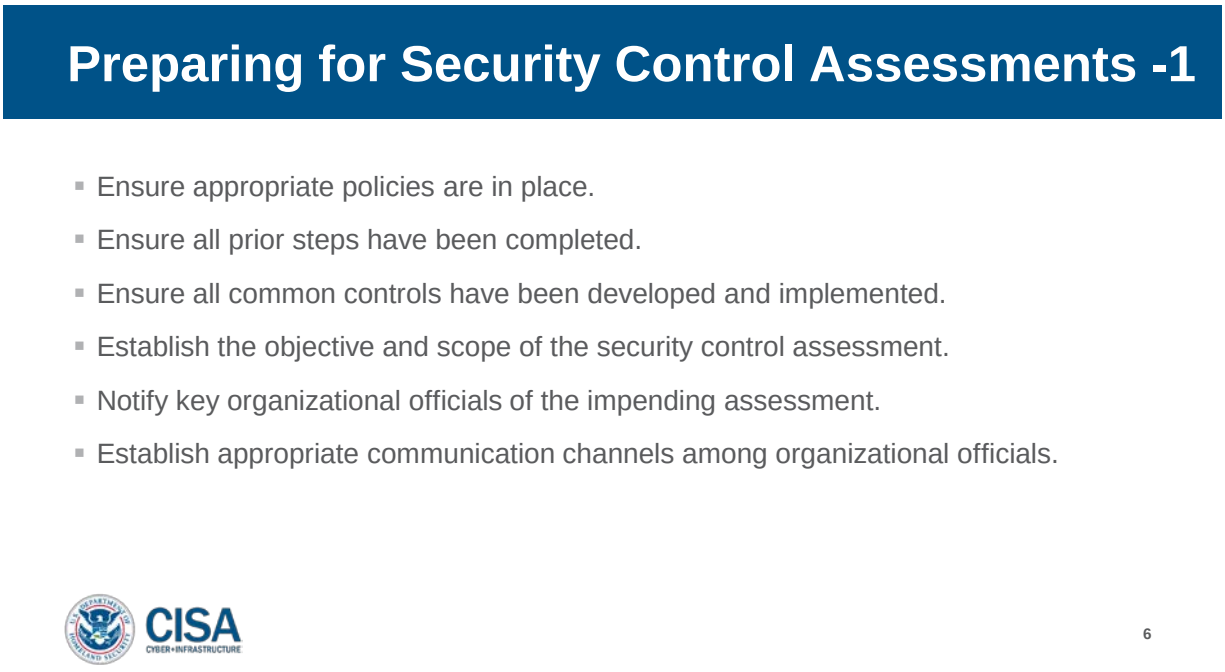
**004 There are a couple publications that I'd like to cite here that may be helpful. One is I would recommend NIST SP 800-53, and this is specifically 53A, so it's going to be an appendix that provides some additional direction on these controls. Also NIST SP 800-115 will provide guidance on the technical aspects that you need to know for conducting these assessments.

NIST SP 800-53A

- Describes developing effective security and privacy control assessment plans (487 pages)
- Provides a NIST process for assessing security and privacy controls
- **Appendix F** – Provides an assessment strategy for each control listed in NIST SP 800-53
- The **Assessment Process** covers
  - Preparing for Security Control Assessments
  - Developing Security Assessment Plans
  - Conducting Security Control Assessments
  - Analyzing Post-Assessment Reports

5

**005 Let's talk about 53A a little bit more. What it really does for you is it gives you a good overview-- and actually, an in-depth overview-- of the type of controls that you want to actually have in place. Appendix Foxtrot will give you an assessment strategy for the controls that you found in SP 800-53. And the process is actually fairly simple. You're going to prepare for that assessment; you're going to develop what your plans are for actually executing the assessment; you're going to actually conduct the assessment itself; and then you're going to look at your post-assessment report; you're going to develop those reports.

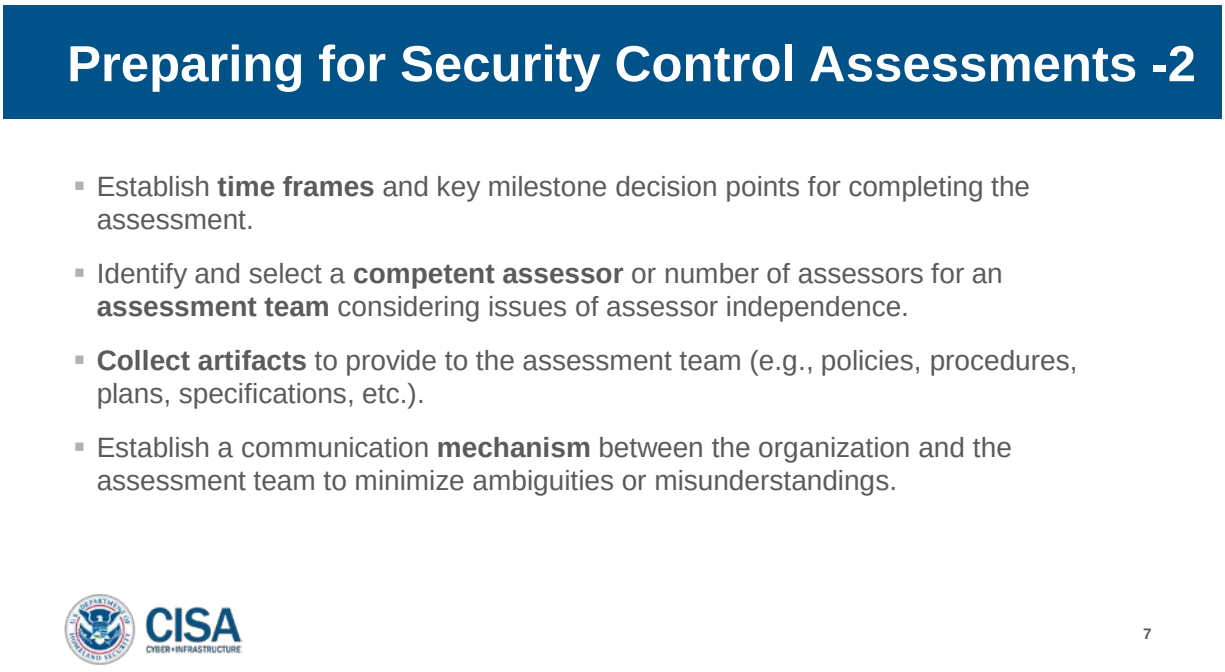


**006 So let's go into these steps a little bit further so that way you understand what's involved in this process.

First of all, you want to make sure that you have the right policies in place so that way you're going to review a whole bunch of documentation to make sure that people are actually adhering to that policy. You also want to make sure that you have an understanding of the control sets being used. Specifically, look at what the common controls are in this system. Remember, a common control is a control that covers multiple portions of a system, so it's one security control for another, rather than having a partitioned control, which may be looking at just one piece of the system.

You also want to look at what your objectives are for the assessment, and you want to make sure you vet those with your management chain. You also want to make sure that the people who are going to be affected by this assessment, to include the management team, anyone who is actually operating the system will know that it's coming. You're not going to want to go doing this assessment without getting approval to do it.

You also want to make sure that the communication channels remain open between yourself and that management team, so that way if things were to go wrong, or maybe they're going super right, either way you want to make sure that you're communicating your results regularly with the team.

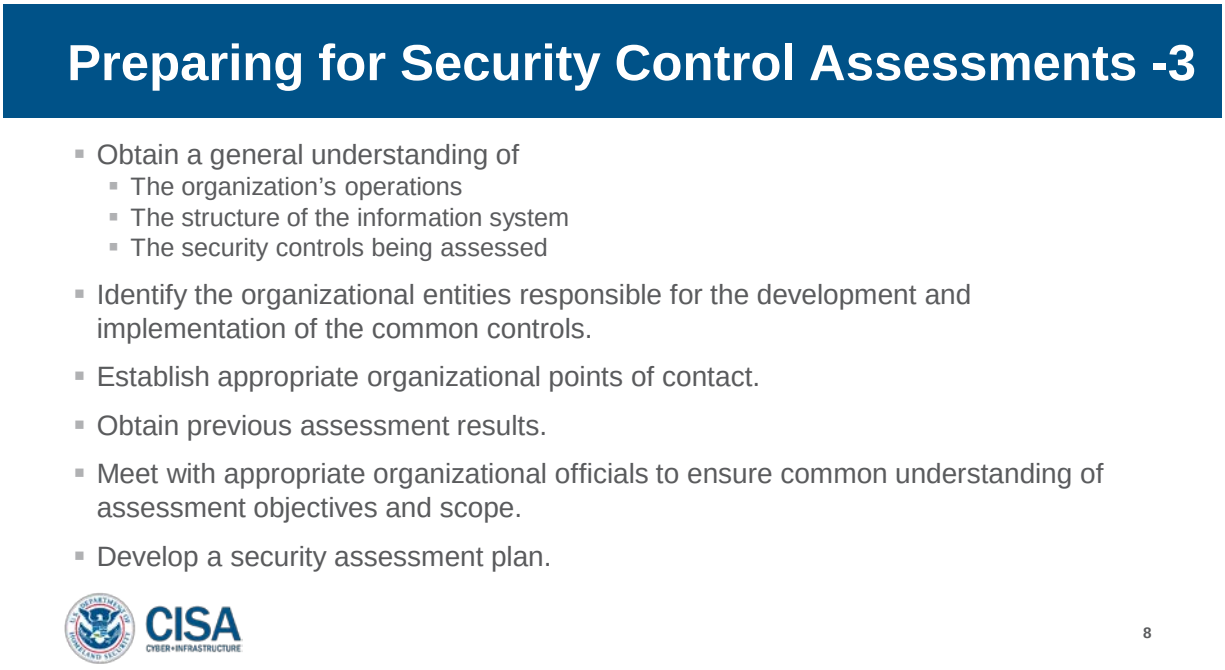


**007 You also want to talk about how long the assessment's going to take, and you really want to communicate that clearly so that way people know how long the interruption may last, if there is a related interruption with this assessment. A more critical element of this is establishing a great team. It's hard finding great team members. You need to make sure that they're competent and they're skilled, and you also need to make sure that they have skills that are related to the specific system that you're actually assessing. It may have to be a diverse team, especially if you come to find out that you're working on a specific operating system, for example.

You also want to help them out by collecting all the artifacts up front.

You're going to get together all the policies, procedures, all the plans and specifications, so that way they don't have to travel too far to find them. They can just ingest them and assess them at will.

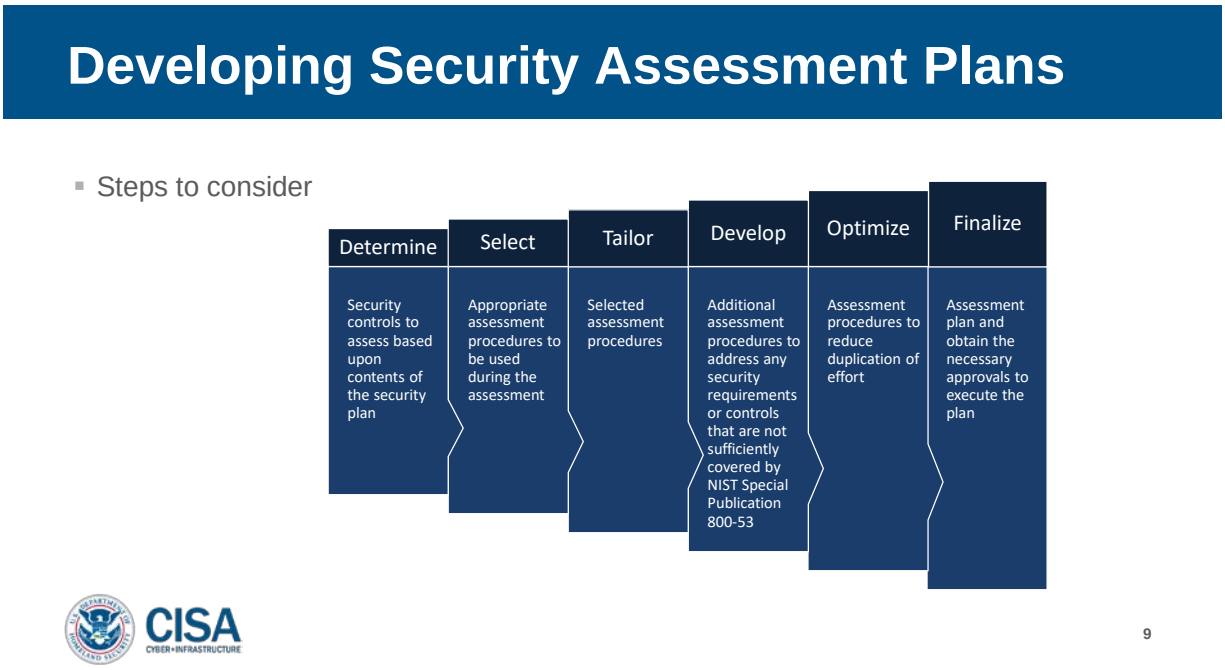
Preparing for Security Control Assessments -3



**008 So as you're going to go about this assessment, you want to get a base understanding of how the organization operates, and you want to look at the structure of their information system, and you want to look at the controls that you're actually going to assess. And make known if you're an independent assessor and you're coming in from outside the organization, this may take a little bit longer than it would if you're internal to the organization and you already have a fair understanding of what's taking place here.

You want to look at the different organizational entities or teams or people or functions that are actually responsible for implementing these controls. You want to have good connections with them communication-wise, and a good rapport, so that way you can ask them tough questions. You actually want to make sure too that you have previous assessment results if there have been assessments done before, so that way you can have a good comparison as to what you're getting today and what you had previously. You can identify gaps a lot easier and see if the organization is actually getting to a new level of maturity.

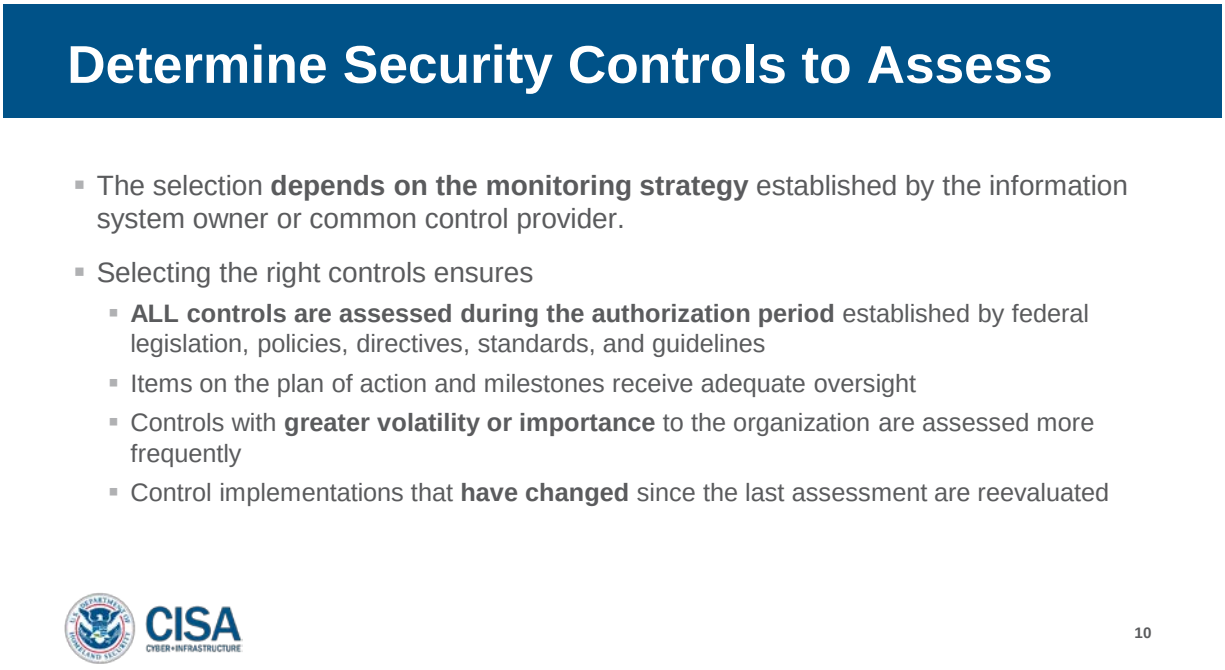
Now, you're going to report these results back, and to do that, you're going to actually develop a security assessment plan to have a vehicle that would eventually deliver that assessment and become a security assessment report that you can deliver to that security-- excuse me-- that management team.



**009 So, the distinct steps you're going to take here. First, you're going to determine what security controls you're going to assess, and then you're going to select the procedures that you're going to use during that assessment. Now, there may be a bit of scoping and tailoring here, especially if you're only looking at certain control sets, or certain risks, for that matter, and also, you may have to go beyond the 800-53 recommended set of controls, so you may have to actually develop your own procedures as well. Ultimately, you're going to want to optimize this whole process too, so in your plan you're going to look at it and you're going to make sure that it's being executed in the most efficient manner to save time, to save resources, to make sure that there's minimum interruption for the

enterprise. Then you're going to actually finalize your results in an assessment plan and then you're going to actually carry out the plan.

Determine Security Controls to Assess



**010 So now you want to determine the secure controls that you're actually going to assess, and it really kind of depends on the monitoring strategy that's taking place here, and also maybe you want to think about who the system owner is and who's actually providing the control for that system.

Now, some of these controls are assessed during certain periods of time, and it may be dictated by, say, federal policy regulation. It may be a local policy or directive that is actually pointing to when these need to be assessed. You want to think about controls that have the most

importance to the organization, and you also want to think about how often they're being assessed. You also want to think about any control sets or any implementations that have changed since they were last assessed as well.

Select Appropriate Procedures

Select Appropriate Procedures

- NIST Special Publication 800-53A, **Appendix F** provides an assessment procedure for each security control and control enhancement in Special Publication 800-53.
- The selected assessment procedures vary from assessment to assessment based on the security plan and the purpose of the security assessment.
  - **Complete** security control assessment
    - Initial system assessment prior to authorization
  - **Partial** security control assessment
    - Re-assessment of Plan of Action & Milestone (POA&M) items

CISA CYBER+INFRASTRUCTURE

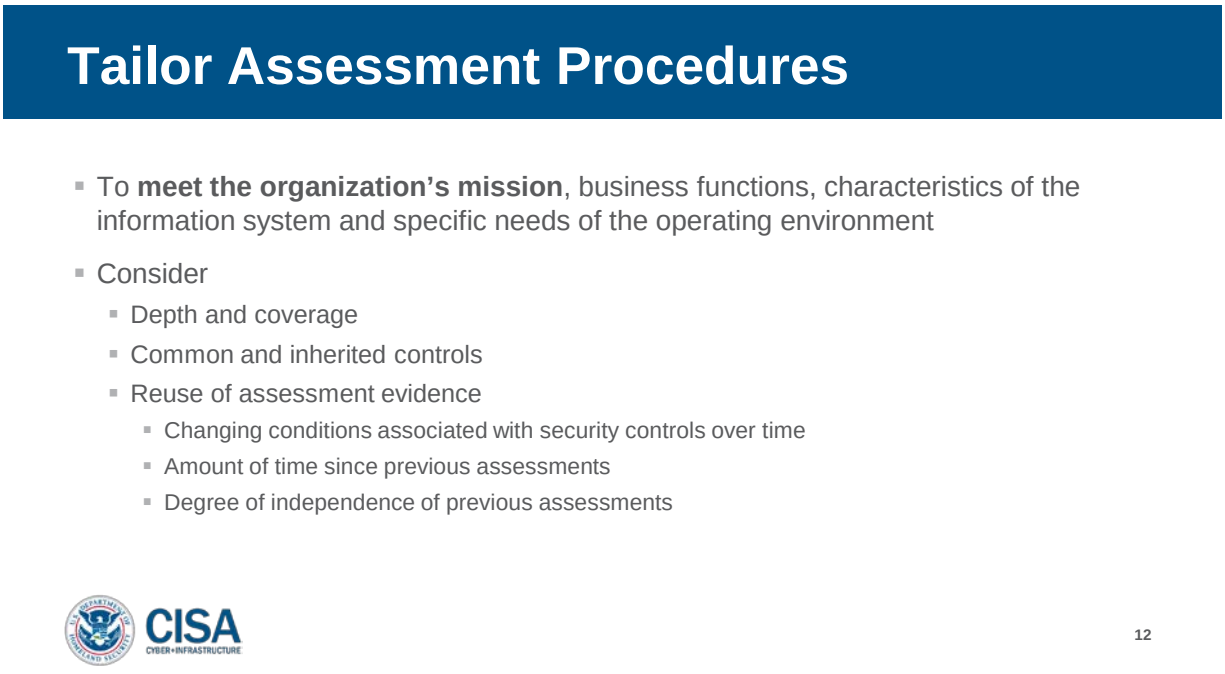
11

**011 So now I want to select the appropriate procedures and the type of assessment that I'm going to execute. Once again, let's go back to that SP 800-53 Appendix Foxtrot. You're going to find a lot of useful information in there, and it really depends upon the security plan of what you're trying to assess as well.

For example, you may conduct a complete security control assessment when the system is new and it's your initial assessment and you've never done it before, prior to the actual

system being authorized to be put into use in the organization. You may want to do a partial security control assessment, which may in fact be a reassessment of security controls that you've reviewed before. For example, there may have been a plan of action or milestones for systems that were being implemented, and now you're going to come back and reassess them now that they are.

Tailor Assessment Procedures

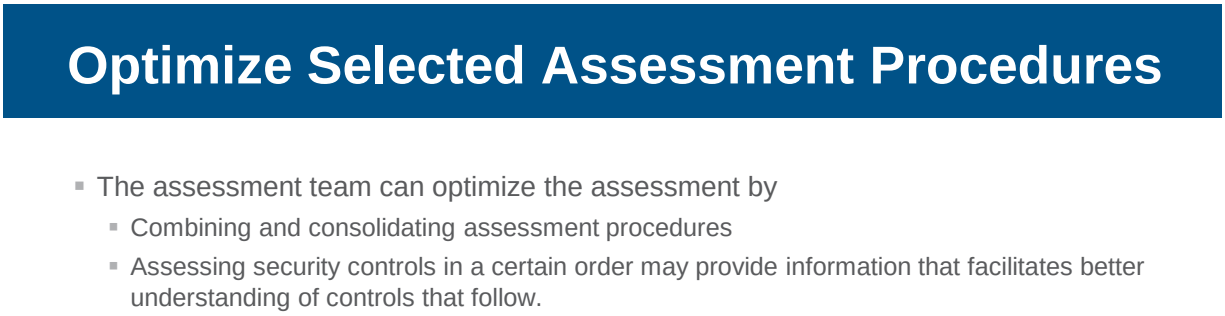


**012 You're going to also want to tailor your procedures so that way you meet the specific business functions and the specifics to the information system that you're reviewing. You want to think about the defense-in-depth, the coverage of the security controls. You want to think about what's the difference between the measure controls; maybe there's some that were

already in the system; and you may want to also consider the reuse of evidence that was found in other previous assessments.

Now, some things that you want to think about though if you're reusing those previous elements from a previous assessment: One is conditions can change over time, so you want to think about that. You want to be very clear to understand how much time has passed since that last assessment, and you also want to know what was the degree of independence that you had from the people who were doing that assessment prior too. You want to avoid bias in your results if at all possible in this regard.

Optimize Selected Assessment Procedures



**013 Also, you're going to want to optimize your assessment. So the

idea here is to try to limit the amount of time you're actually conducting an assessment, and you want to avoid creating any interruptions in the enterprise as you're doing this assessment. So you may combine with other assessments that are taking place at the same time, or you may actually split them out, so that way you limit the burden on the organization. There may be certain security control sets that you go assess first before you do others so that way it's more efficient and it flows better.

Finalize Security Assessment Plan

Finalize Security Assessment Plan

- Once the security assessment plan is completed, the plan is reviewed and approved by appropriate organizational officials.
- Be sure to document the process followed to assemble the plan for reference during future revision.

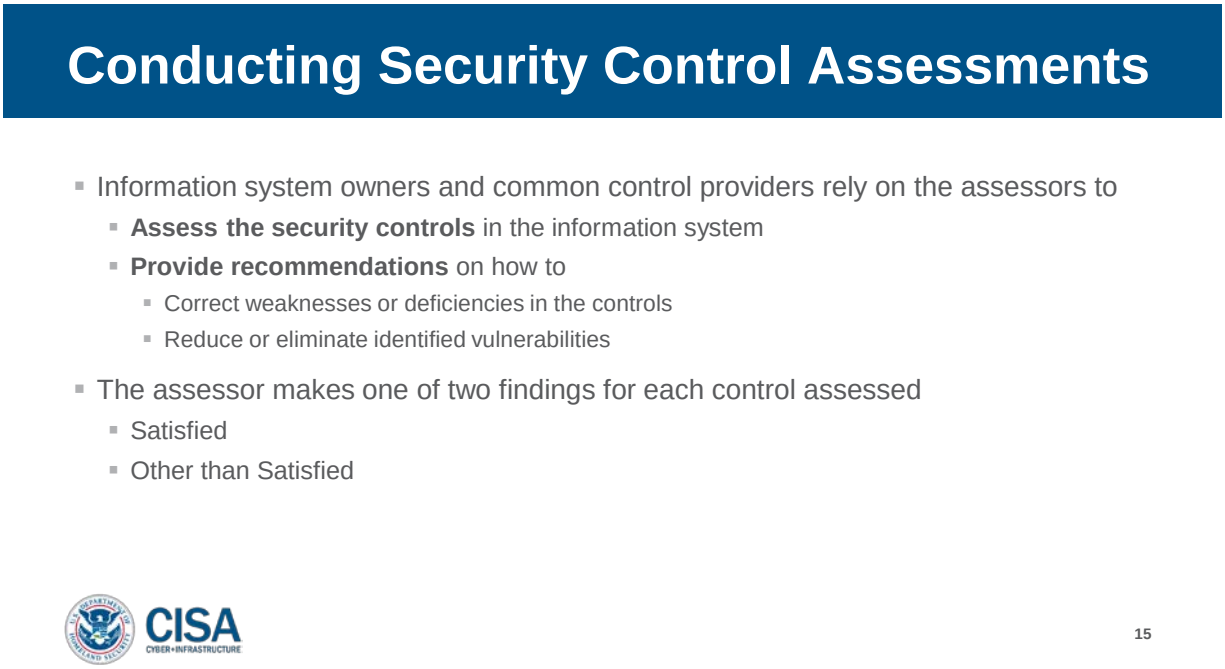
CISA CYBER+INFRASTRUCTURE

14

**014 Once you've done all that, you're going to finalize that plan. Remember, go back and talk to the management team. Review it with them. Make sure that they have approved it before you go execute that plan. If there are any changes,

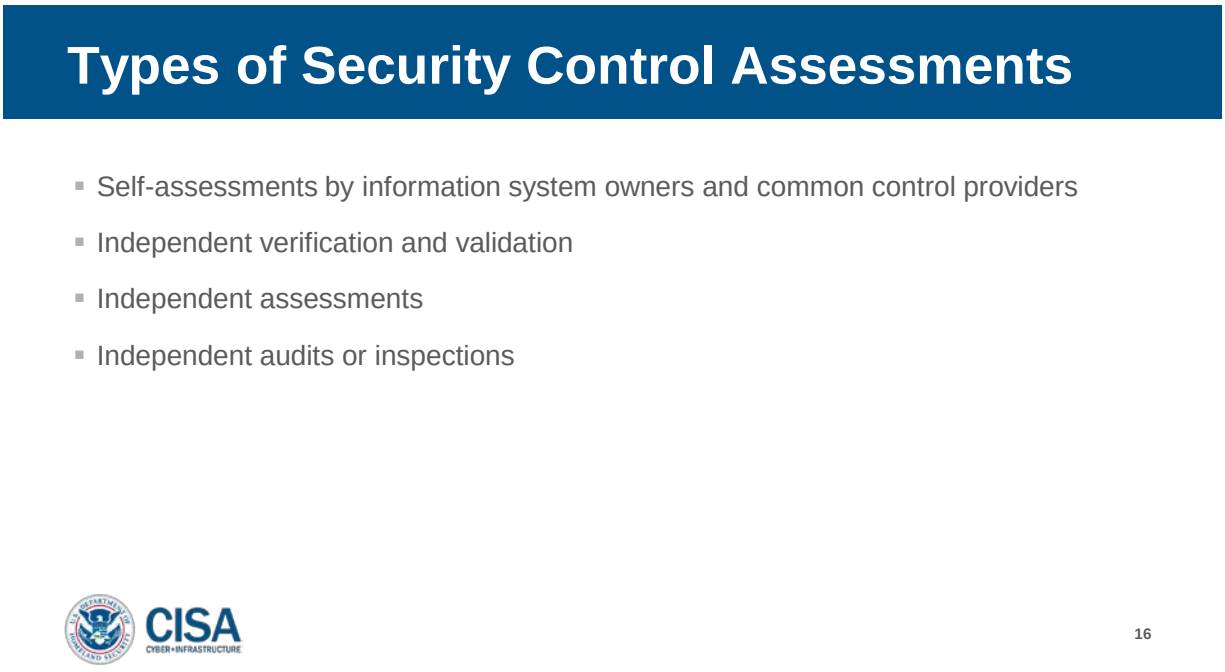
make sure you go back and put them into the plan.

Conducting Security Control Assessments



**015 Now it's time to actually conduct the security control assessment. You're going to be assessing these security controls within the information system, and you're going to be looking to give recommendations back on gaps that you find. These may be vulnerabilities, maybe weaknesses in the control sets. Maybe, it's a possibility, that they weren't implemented correctly. You really want to work hard to reduce these vulnerabilities so that way you have a more robust security stack.

The assessor can make one of two findings. They can either be satisfied with what's been implemented, or something that's other than satisfied.



**016 Now, there are different types of security control assessments as well. Regardless of what you're doing, what I want to call your attention to here is that you can have self-assessments-- so this is an organization that is actually reviewing its own information system. This may be done by system owners, or maybe even the providers, or it can be independent. In other words, I find somebody from outside the organization-- maybe an external auditor-- that can come in and actually do maybe a verification or validation or some sort of audit.

Assessment Methods

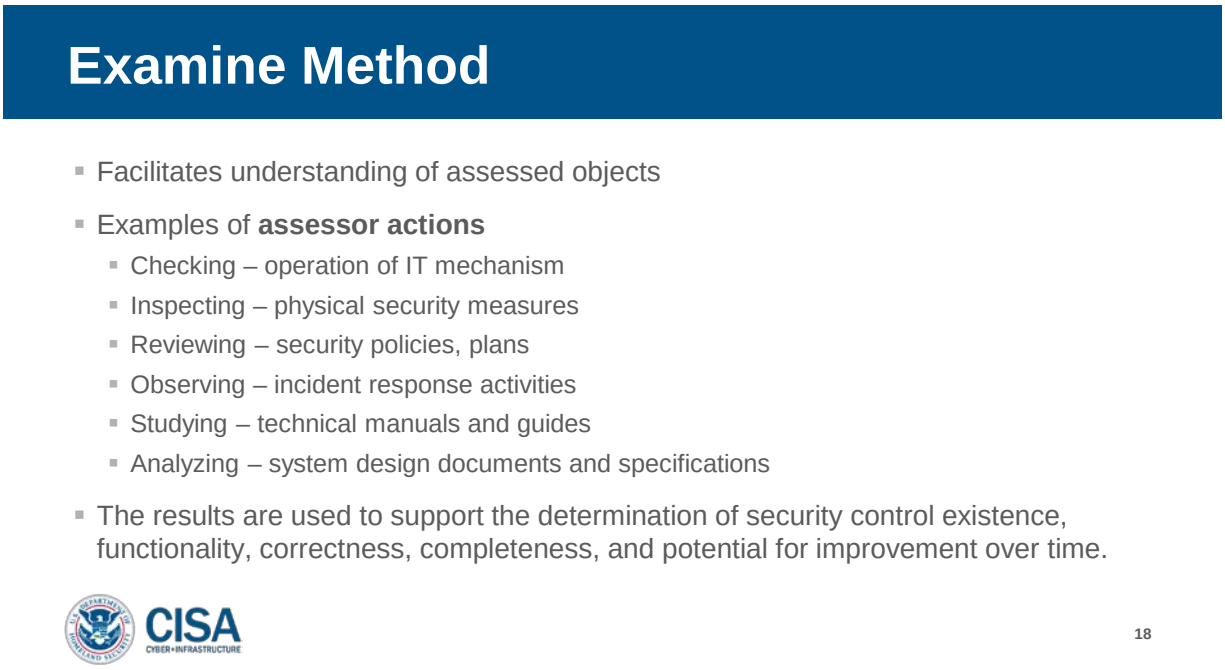
- Examine Method
- Interview Method
- Test Method

Pick one as a strategy for each control you assess.

CISA CYBER+INFRASTRUCTURE

17

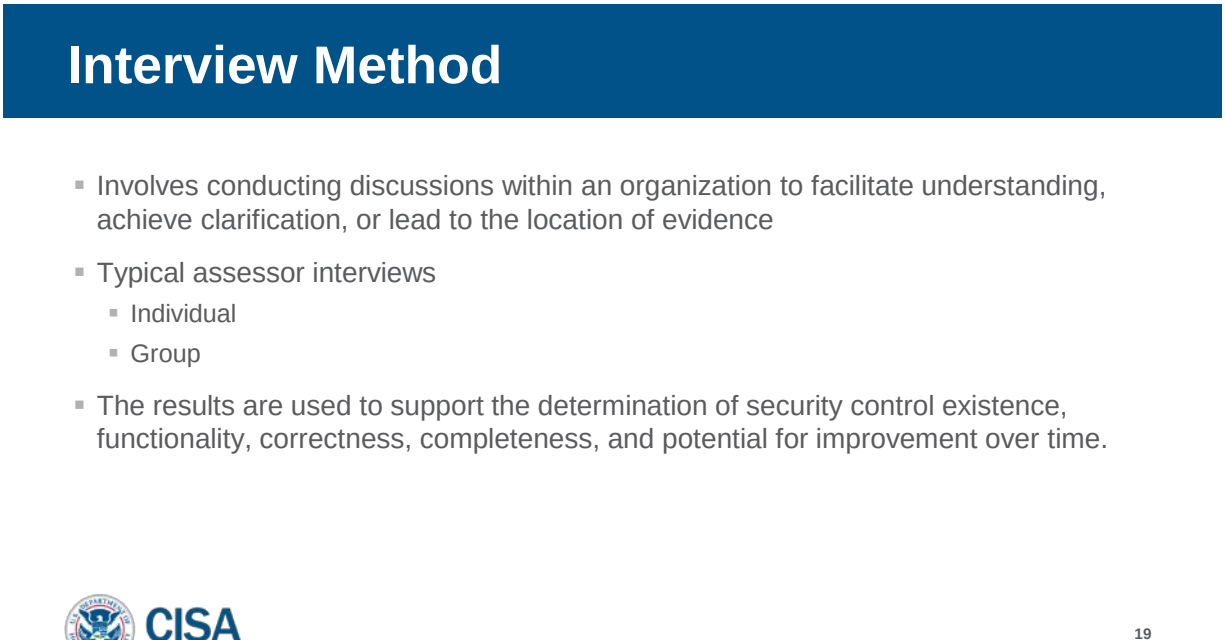
**017 There are different methods here too. I can examine, I can interview, I can test. Let's go through these in a little bit more detail here.



**018 For examining, what I'm doing is I'm taking specific actions that will actually help me facilitate understanding if the objects that I'm actually looking at. So, I may be checking the operation of a certain system. I may be actually physically inspecting it. Maybe I'm reviewing security policies to make sure that they're being followed. I could also go out and observe people actually doing what they're being told to do. This may include if I go out and I look at an incident response. Maybe they're running a drill, or maybe I actually get the opportunity to see a real one happen. You may look over technical manuals and guides that have been published in the enterprise to make sure that they're accurate, technically and in terms of how people actually physically understand them as they read them. You may

also have to look at certain system design documents to make sure that they're accurate as well.

Interview Method

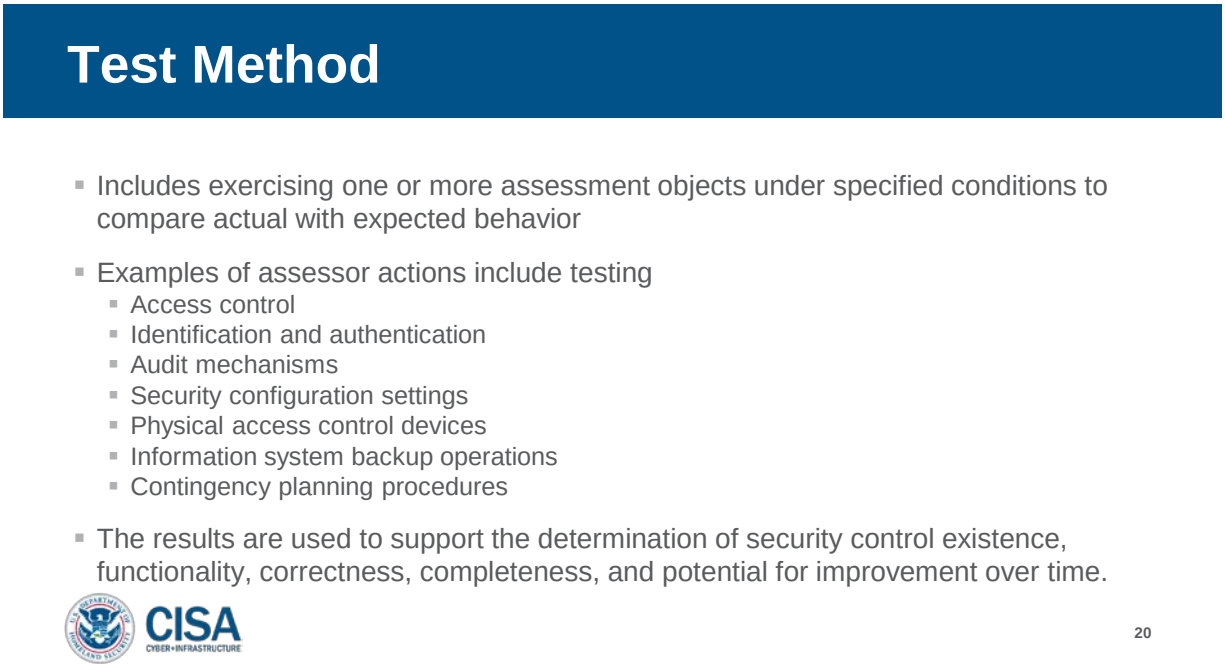


**019 Another method may be interviewing. Now, this is harder than it sounds. You really want to be respectful of the time of the people that you're interviewing. This comes down to whether you're interviewing an individual or a group. You need to prepare. You need to know what questions you're going to ask. You need to make sure that you're going to get the information that you're looking for with the questions that you're asking.

For example, you may not want to ask so many yes/no type questions. You may want to ask questions where people have to actually provide you information. And then

again, you also want to know that you're actually complete in the questions that you're asking and the answers that you're getting back so that way you can conduct a thorough assessment.

Test Method



**020 You can also test folks as well. Now, this may not necessarily be testing the people themselves. You may actually go in and actually test the controls too. It goes both ways. Suppose, for example, I'm actually going to give in and try to test access into a system. Maybe I want to test how people understand how they authenticate into the system, just as much as how the system is going to actually be doing the technical authentication as well.

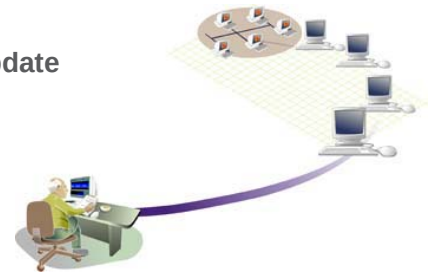
Maybe I want to audit some mechanisms that I've put in place, or

look at some security control configuration settings. You also want to look at maybe some physical access. Who actually is walking around with their badges, and are they using them properly. You also may want to look at contingency planning. If it comes down to incident response, you're going to want to ask people if they understand what they need to do if a risk were to come to light or actually be realized.

Analyzing Post-Assessment Reports

Analyzing Post-Assessment Reports

- Security control assessment **results influence and update**
  - System security plan
  - Plan of action and milestones
  - Security assessment report
  - Risk assessment
- Results should help
  - Determine the **appropriate mitigation steps** required to correct weaknesses and deficiencies identified during the assessment
  - Assist Senior Leadership in ensuring the **organization's resources are effectively allocated** in accordance with organizational priorities before executing the mitigation steps



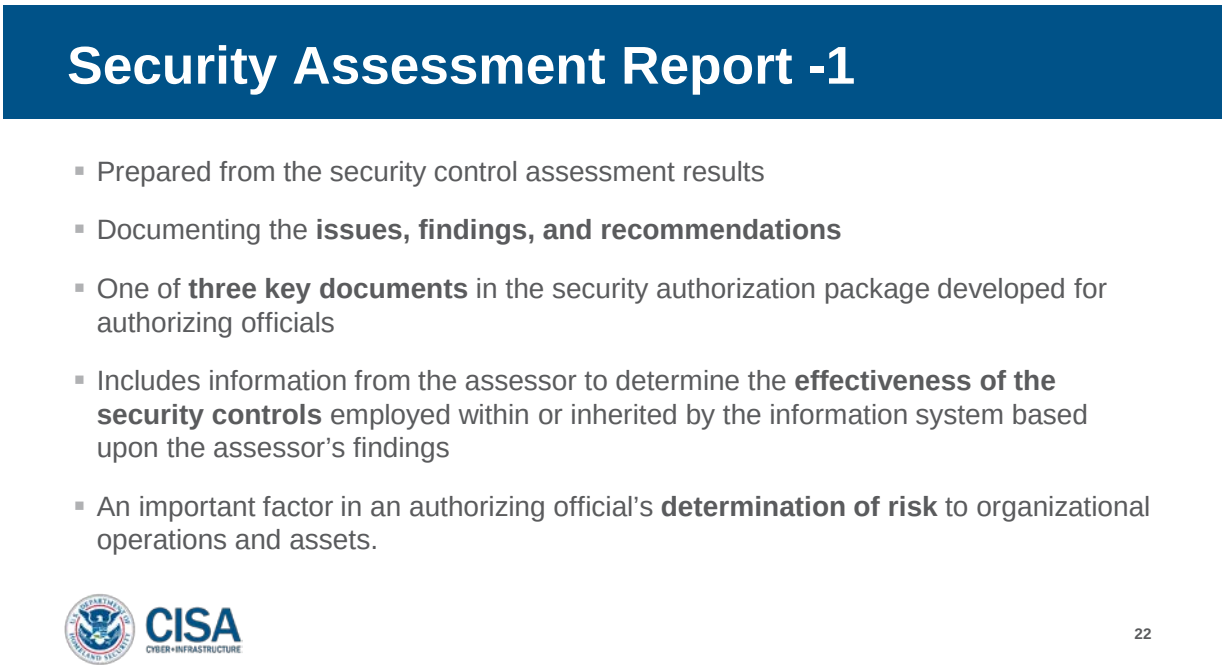
CISA CYBER+INFRASTRUCTURE

21

**021 Now comes the even harder part. Now you've collected all this information, and you got to figure out what exactly you have to report in this assessment. Now, from this, you're going to actually have the system security plan, you're going to have a plan of action and milestones that may come from it because, let's

face it, you're going to find gaps, and if you do, you're going to have to have plans for addressing those gaps, and you're going to have maybe some milestones negotiated with the people who are implementing them so that way they know the timeline of implementation. You're going to actually develop a report and you're going to provide it to the management team, and this may also include a risk assessment, especially if you had previous risk understanding and now that profile or that portfolio of risks have changed.

You should really think about what are the appropriate mitigation steps that you can recommend to correct weaknesses that you've found, and you're going to help the leadership team understand what those are as well. Now, note this, that not all senior leaders are as savvy on cybersecurity as you may be, so you may have to think about this through a different lens and boil down the information to a level that everybody in the organization can appreciate and understand.



**022 So, let's talk a little bit about this security assessment report. So you need a way, or you a need a vehicle, to compile all of these results that you've found. You're going to have issues, you're going to have findings, you're going to have some recommendations, and this is all going to become part of a package that you're going to submit to the management team, and what you're really looking for is the effectiveness of the security controls, and you may also find out that you have additional risk that has come about from these operations and these assets. And by the way, this is going to become an important factor into helping that organization authorize what new assets are going to come into the organization, security or otherwise.

Security Assessment Report -2

- Documented at the level of detail appropriate for the assessment in accordance with the reporting formats prescribed by
  - Organizational policy
  - NIST guidelines
  - OMB policy
- Formatted appropriate for the type of security control assessment conducted

  Example: FISMA reporting is done through CyberScope.
- Findings used to determine the steps required to correct weaknesses and deficiencies identified during the assessment.

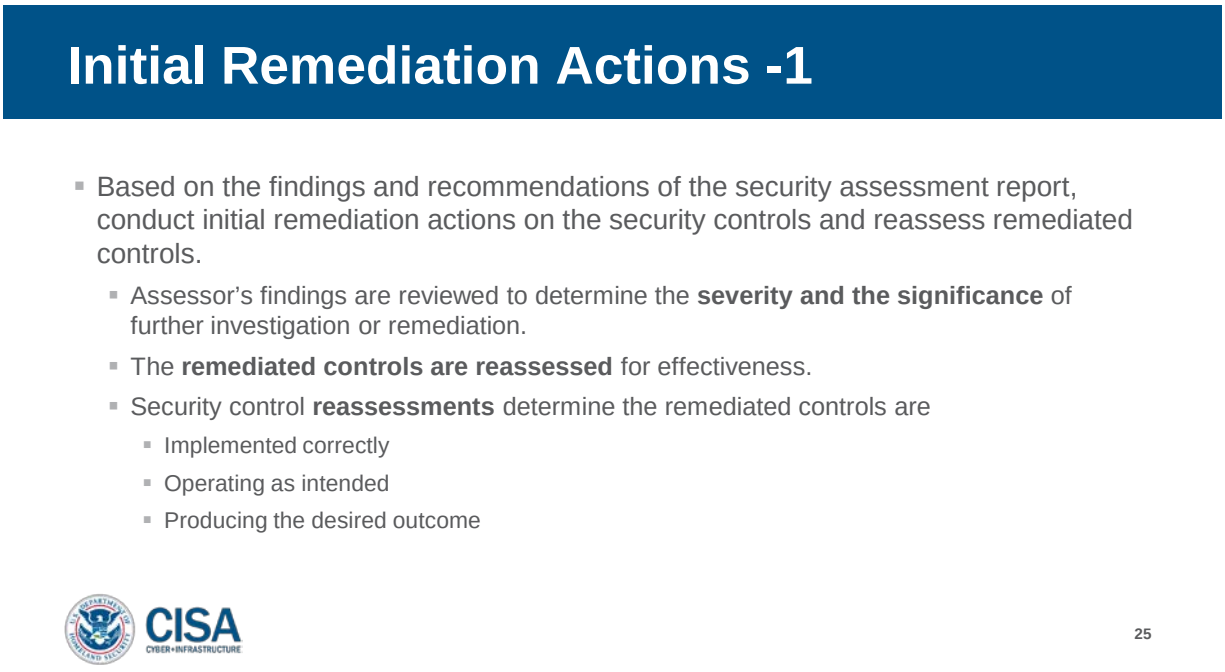
23

**023 Now, you want to make sure that you have the appropriate level of documentation here, and this is really going to be determined by the organizational policies. Maybe you're going to follow certain guidelines, or maybe there's even other policies outside the organization that you may have to abide by. Either way, you can use some other standards out there, maybe like what is recommended by FISMA.

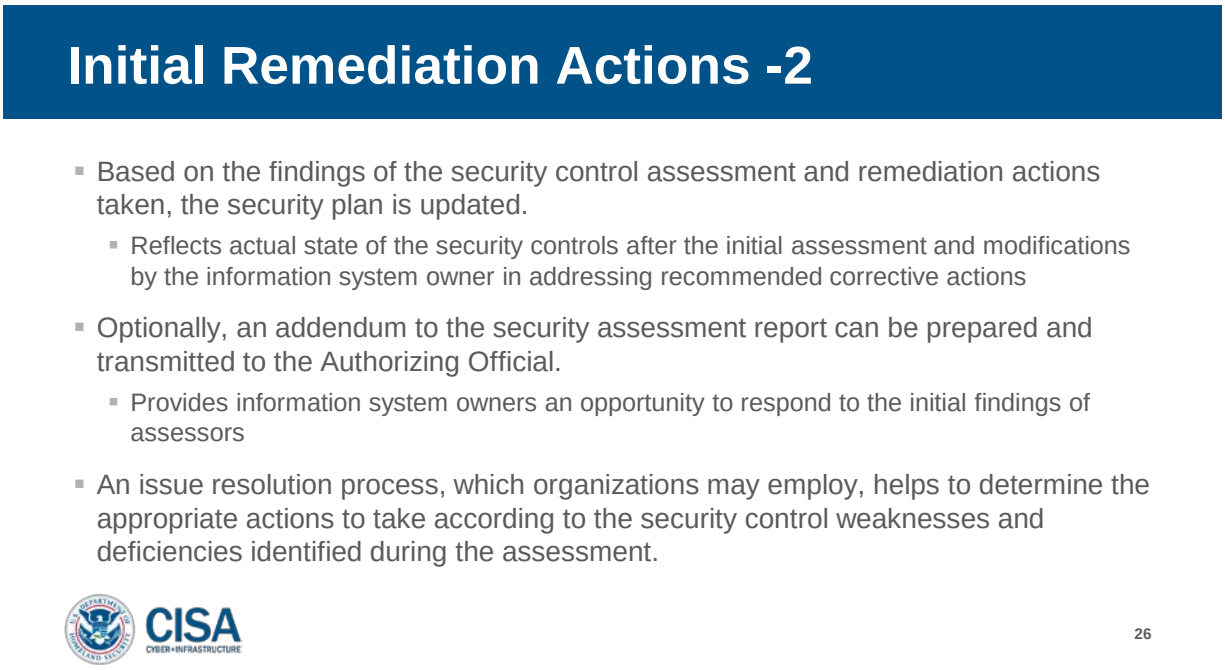
Security Assessment Report -3

- Results are brought forward in an interim report and are included in the final security assessment report.
  - Optionally, an **executive summary** is created from the detailed findings.
    - An abbreviated version of the assessment report
    - Focuses on the **highlights** of the assessment, synopsis of key findings, **recommendations** for addressing weaknesses, and deficiencies in the security controls

**024 So you're going to bring these results forward in a report and you're going to have to brief executives and the management team on what you actually found. Once again, I want to emphasize that not all executives are as technically savvy as you may be, so in the executive summary, you want to make sure that it's very clear, simple, to the point. You may even want to think about providing a highlight, abbreviated summary, almost like an elevator pitch of, "Hey, here's what we found, and go into this report and find details from these highlights and recommendations we're providing you."



**025 Now, you may also be providing some remediation actions that need to take place in the organization. So what you're going to do here is you're going to think about the severity and the significance of what you want to get out of this remediation. There may be some further investigation that's involved. You want to make sure that you're reassessing for effectiveness periodically. You also want to make sure that you're covering the same questions that you started in the beginning. You want to make sure to remember that these controls are implemented correctly. You want to make sure that they're operating as you intended them, or as the organization intended them, and you want to make sure that they're giving you the outcome that you're looking for.

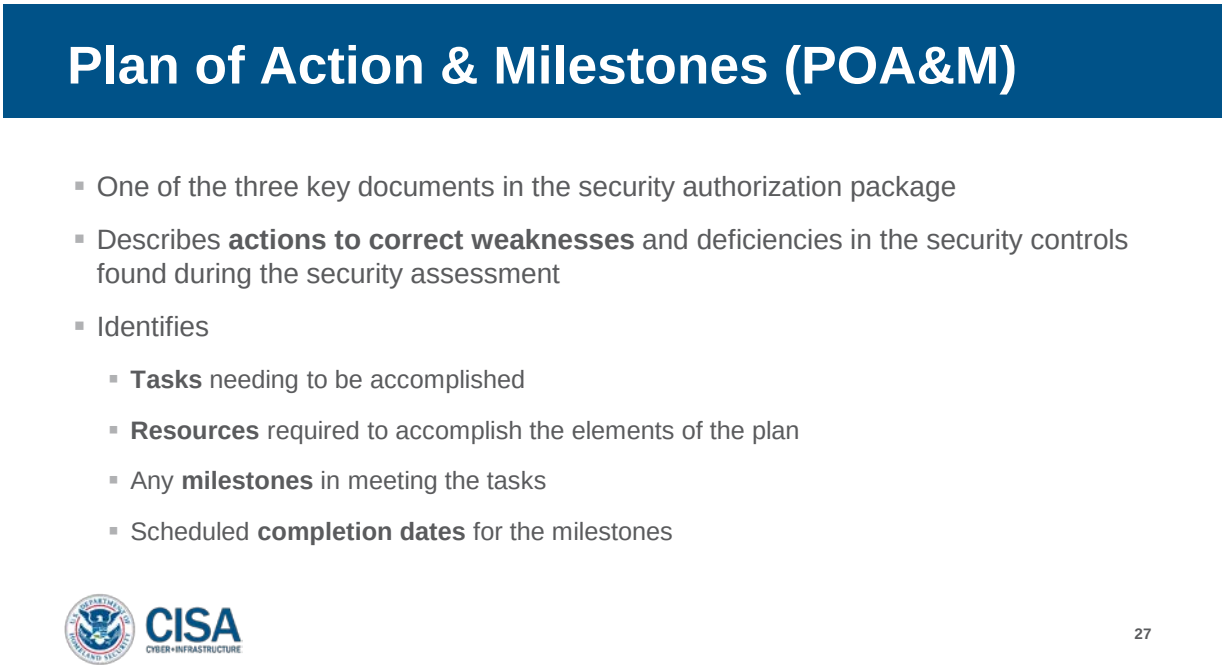


**026 Now, these actions as they're taken, you want to make sure that you are updating that security plan, by the way, so you actually want to know what the actual of your security control stack is after that initial assessment. You want to know changes that are taking place down the line and you want to know the status of corrective actions that are being taken. You could document this in an addendum of your security assessment if you so choose.

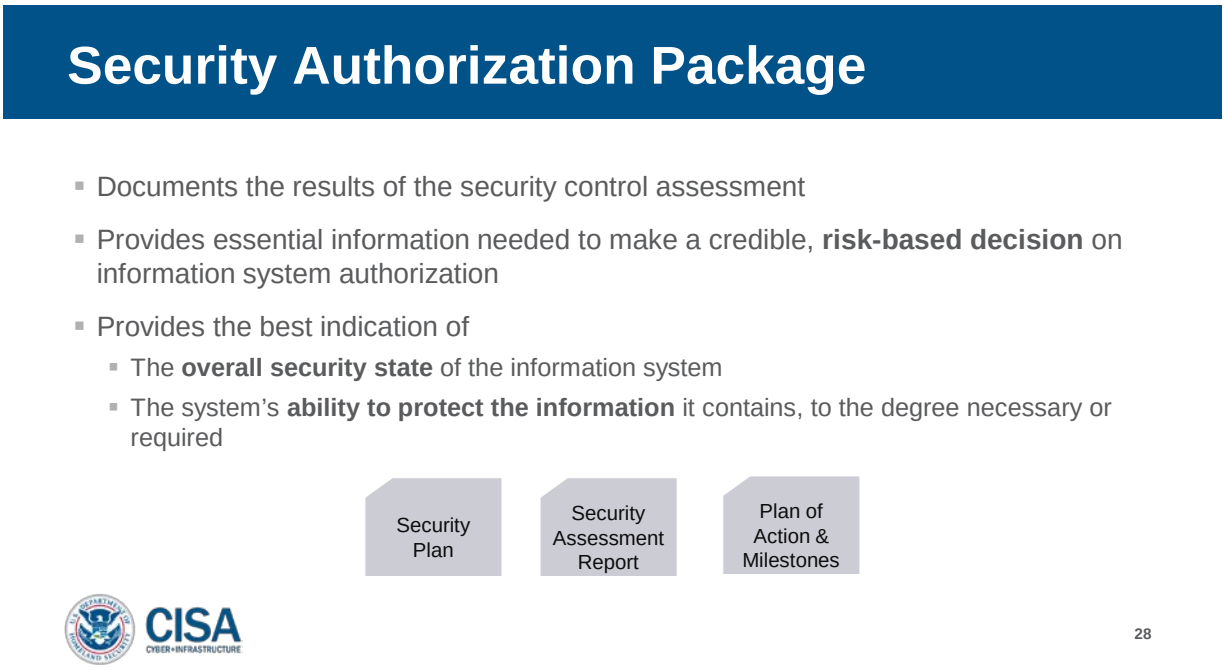
You also may want to think about how to set up an issue resolution process. So if I have this long list of issues that I'm working through with this management team, they're going to know how are they going to get resolved, how is it going to get reported to me, how am I going to know that the issue was resolved in a

manner that answers the weakness or deficiency in the report.

Plan of Action & Milestones (POA&M)



**027 This may come about through a plan of action and milestones. So, what you have are weaknesses that need to be corrected. You're going to boil it down to what actual tasks, what physical tasks, need to be accomplished. You're going to also want to think about what resources am I going to apply to this so that way I know how much money it will take, what people will be necessary. I also want to know what milestones I need to meet along the line. So you want to think carefully about how long it will take to implement, and you want to set reasonable completion dates for these people to actually correct their weaknesses in their system.



**028 This will all amount to the security authorization package. I mentioned those three documents-- remember, the security plan, the security assessment report, and this plan of action or milestones. Once you have those together, you'll really have a clear understanding of the overall security state of your information system. Ultimately, you want to help improve this system and the organization such that they have a better ability to protect their information.

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.

DM18-0098