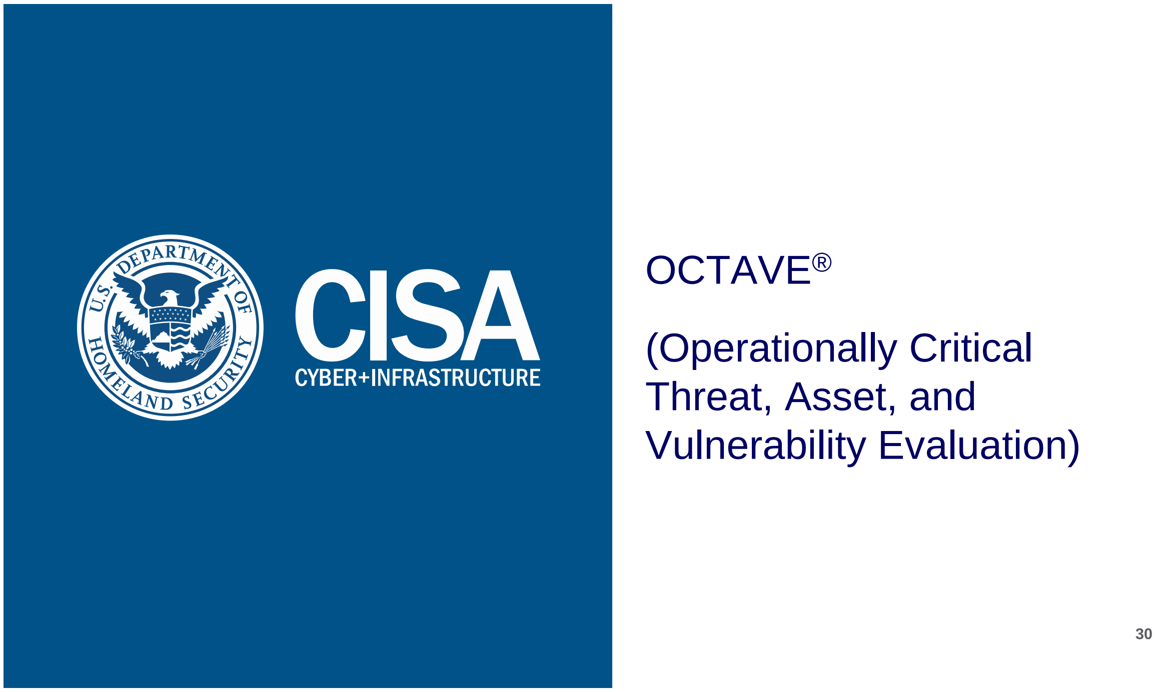
OCTAVE

Table of Contents

OCTAVE ® (Operationally Critical Threat, Asset, and Vulnerability Evaluation)



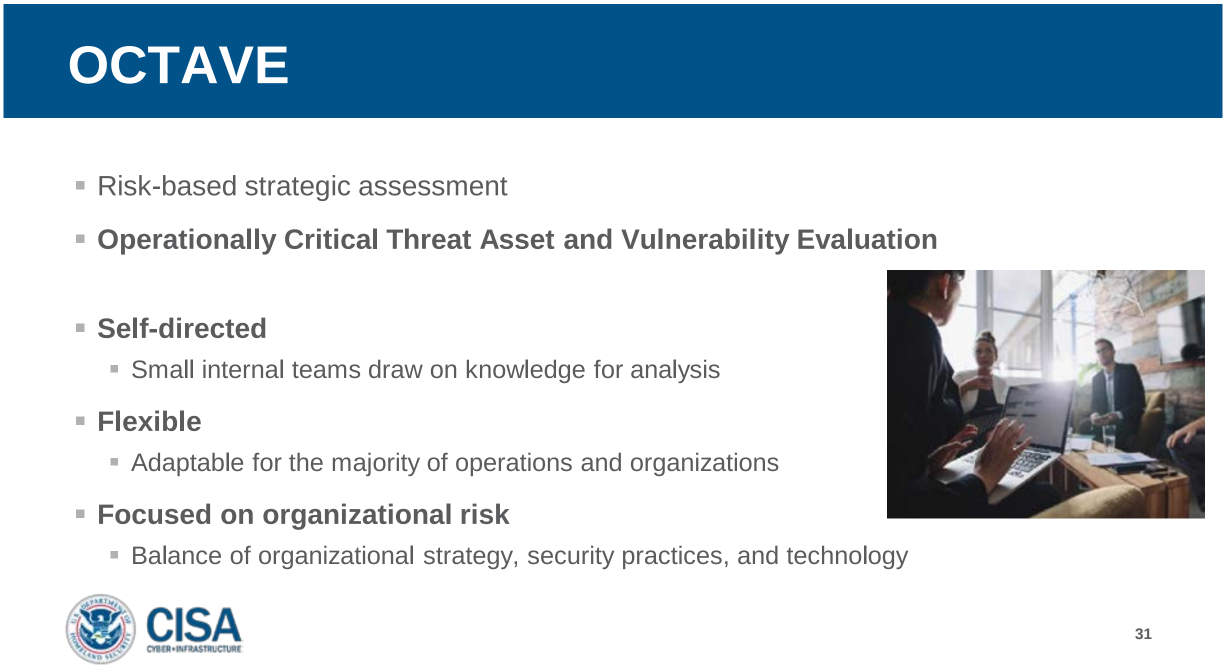
OCTAVE®

(Operationally Critical Threat, Asset, and Vulnerability Evaluation)

30

**030 Instructor: OCTAVE stands for operationally critical threat, asset, and vulnerability evaluation.

OCTAVE



OCTAVE

- Risk-based strategic assessment
- **Operationally Critical Threat Asset and Vulnerability Evaluation**
- **Self-directed**
  - Small internal teams draw on knowledge for analysis
- **Flexible**
  - Adaptable for the majority of operations and organizations
- **Focused on organizational risk**
  - Balance of organizational strategy, security practices, and technology

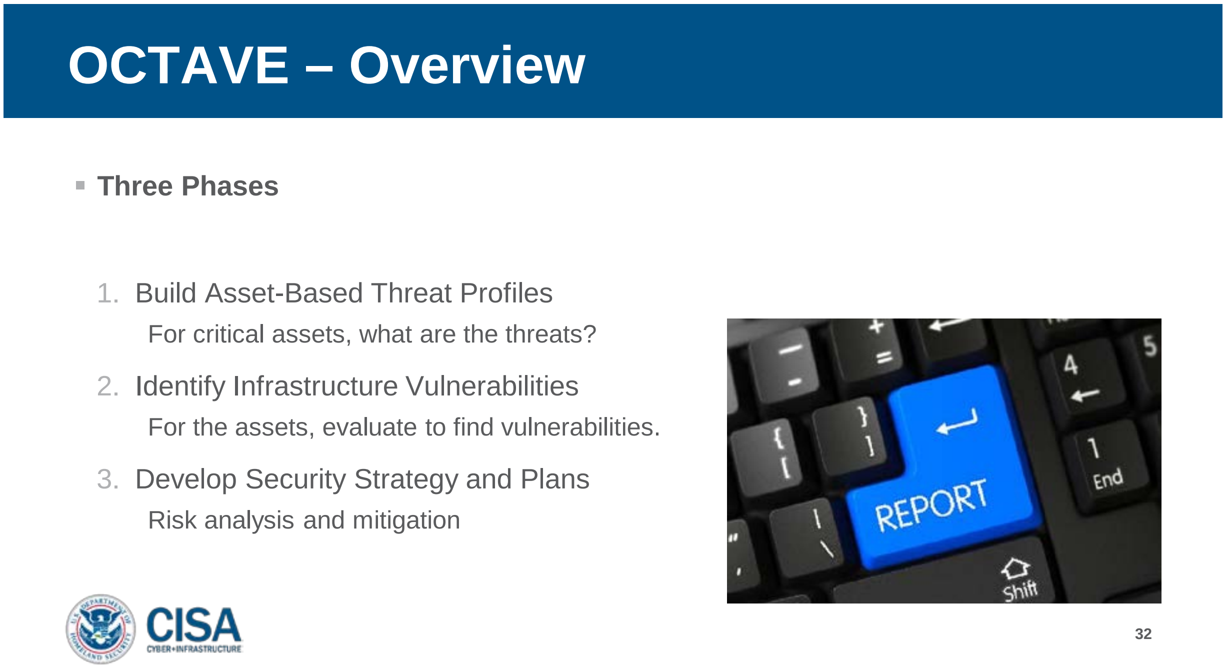
CISA CYBER+INFRASTRUCTURE

31

**031 And what it is is no more than a risk-based strategic assessment. You're actually slicing and dicing the risks to understand what it is that is most critical to your enterprise and how they might be threatened. by the elements that we talked about before. Remember, What we're trying to do is understand what the threats are, what the vulnerabilities are, and how likely they are to incur an impact on your organization.

The good news about this process is it is self-directed. You can actually educate teams to know and learn how to do the process. And once they do that, they can conduct the analysis largely on their own. It's pretty flexible, too. You can adapt it to any types of operations that you may be doing, and it actually is very focused on organizational and operational risk and related security practices.

OCTAVE – Overview



OCTAVE – Overview

- **Three Phases**

1. Build Asset-Based Threat Profiles
   For critical assets, what are the threats?
2. Identify Infrastructure Vulnerabilities
   For the assets, evaluate to find vulnerabilities.
3. Develop Security Strategy and Plans
   Risk analysis and mitigation

CISA
CYBER+INFRASTRUCTURE

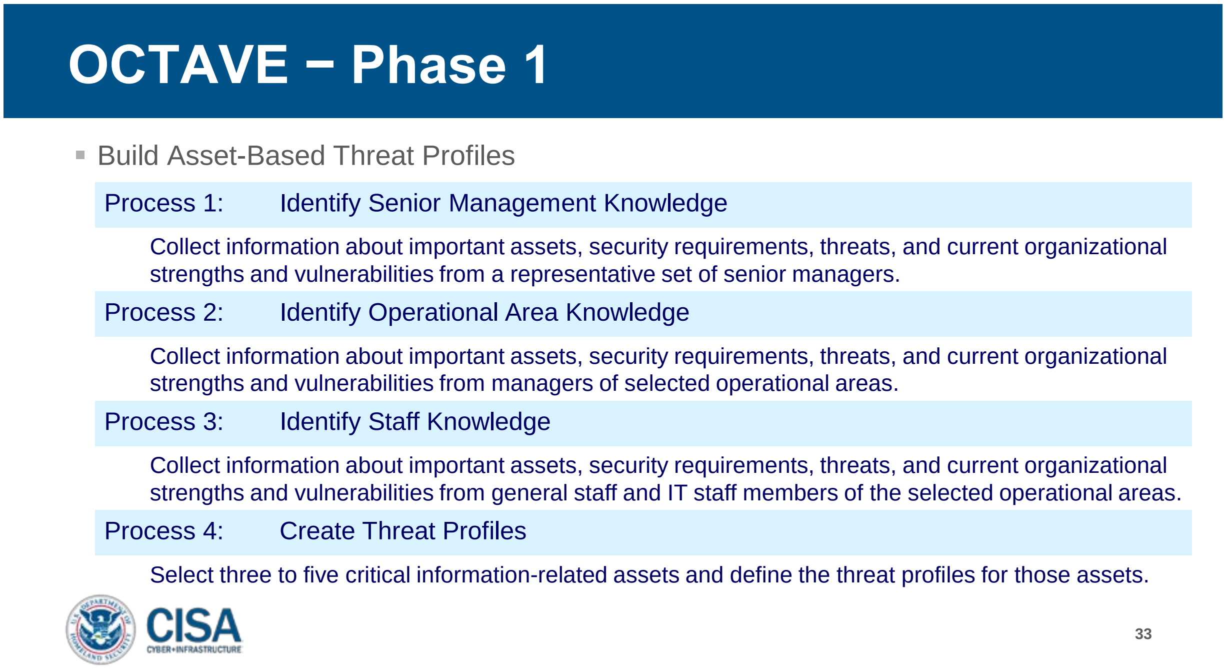
32

REPORT
Shift
End

**032 There are three distinct phases that you'll go through. One is you have to understand what assets you have in the organization. So, you understand-- once you understand what those assets are, you also have to understand what the threats are to those assets. So, what do we have that's critical in the organization? What are the threats looking for?

And then you're going to go back and look at where are the vulnerabilities. Where are the gaps in the walls that those threats can get through and actually create negative impacts on those assets? From that, you're going to develop a security plan or a strategy. So, that way you can control those threats from ever really being able to incur those impacts.

OCTAVE – Phase 1



OCTAVE – Phase 1

- Build Asset-Based Threat Profiles

Process 1: Identify Senior Management Knowledge

Collect information about important assets, security requirements, threats, and current organizational strengths and vulnerabilities from a representative set of senior managers.

Process 2: Identify Operational Area Knowledge

Collect information about important assets, security requirements, threats, and current organizational strengths and vulnerabilities from managers of selected operational areas.

Process 3: Identify Staff Knowledge

Collect information about important assets, security requirements, threats, and current organizational strengths and vulnerabilities from general staff and IT staff members of the selected operational areas.

Process 4: Create Threat Profiles

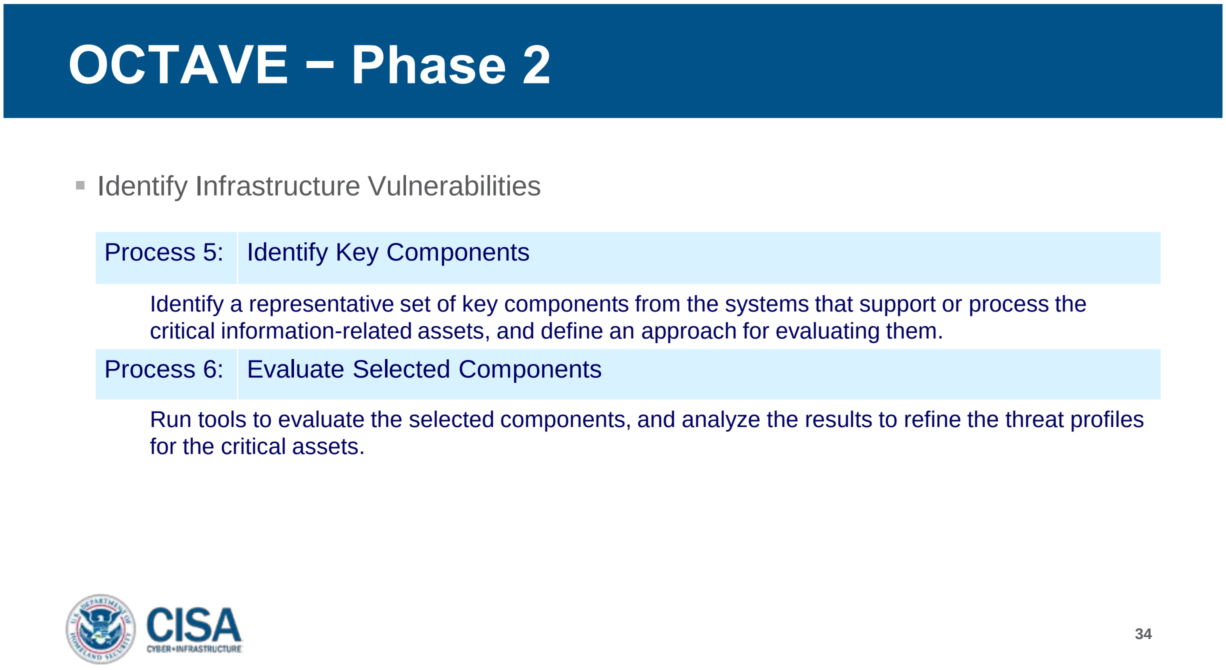
Select three to five critical information-related assets and define the threat profiles for those assets.

33

**033 So, the first thing you're going to do is let's talk about that threat profile idea. And there are several processes here. But at a high level, what we really want to do is we want to identify the people in the organization, and at what level of that organization, need to be knowledgeable about these risks. All right? We're going to actually talk to subject matter experts, and we're going to understand what the server requirements are, security requirements, what the threats may be, and what the strengths of the organization are that may already be existing.

We're also going to want to understand the operational areas and knowledge. So, this is where you're really going in deep and learning what the subject matter experts are in the business in terms of who is operating the assets and what do they know about it. We also want to look at our staff, and we want to know what they're doing on a day-to-day basis. This may include people who are actually in your IT staff, maybe people are working in your security operations center if you have one. You're actually going to want to go about establishing threat profiles. So, you're going to want to look at these assets, and you're going to want to look at what are the primary threats that are going to be looking to impact each of those assets.

OCTAVE – Phase 2



OCTAVE – Phase 2

- Identify Infrastructure Vulnerabilities

Process 5:	Identify Key Components

Identify a representative set of key components from the systems that support or process the critical information-related assets, and define an approach for evaluating them.

Process 6:	Evaluate Selected Components

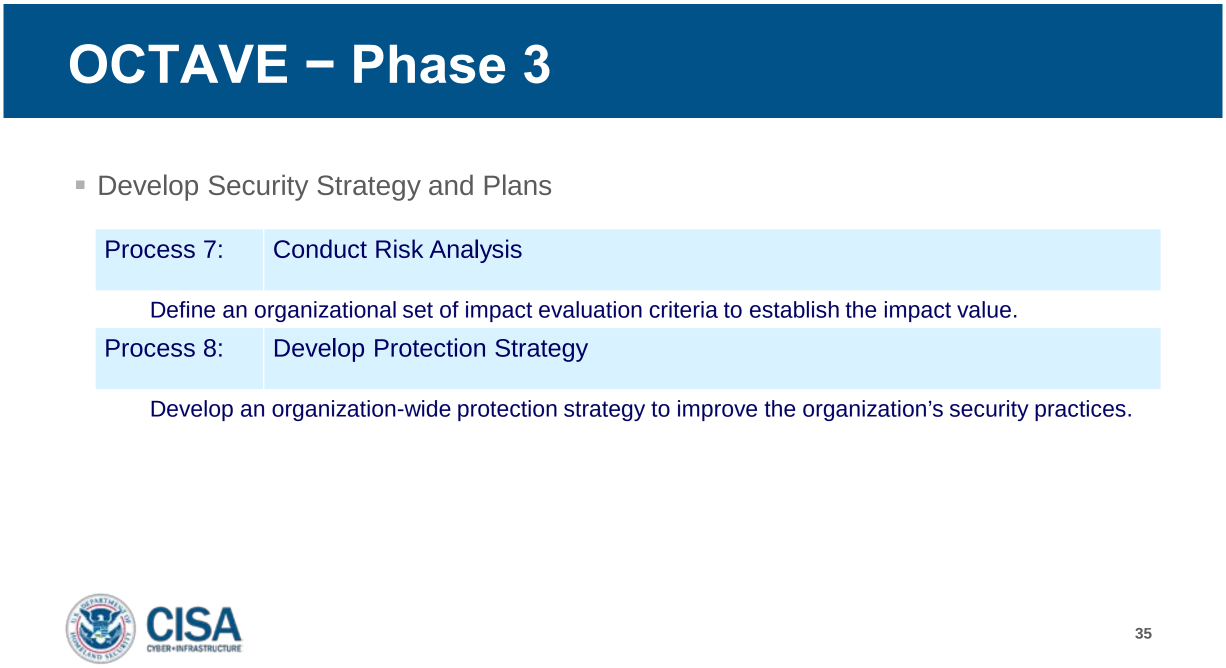
Run tools to evaluate the selected components, and analyze the results to refine the threat profiles for the critical assets.

CISA
CYBER+INFRASTRUCTURE

34

**034 And then you're going to look at key components that are in your systems. So, these are the weak points, if you will, where you might likely find your vulnerabilities. And from that, you're going to evaluate these components, and you're going to try and find out how the threats that exist in those profiles can actually victimize those critical assets.

OCTAVE – Phase 3



OCTAVE – Phase 3

- Develop Security Strategy and Plans

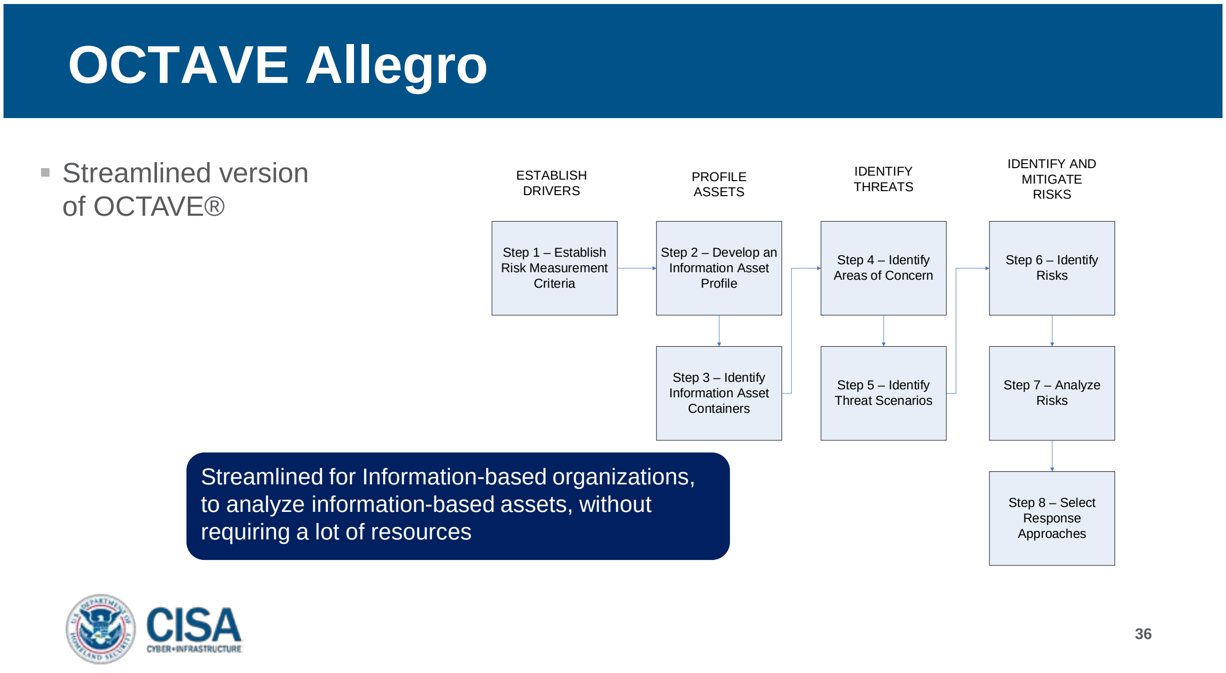
Process 7:	Conduct Risk Analysis
Define an organizational set of impact evaluation criteria to establish the impact value.	
Process 8:	Develop Protection Strategy
Develop an organization-wide protection strategy to improve the organization’s security practices.	

CISA
CYBER+INFRASTRUCTURE

**035 Further from that, you're going to do a deep analysis. You're going to look at what are the unknowns, and you're going to understand what those risks are. And you're going to actually-- and this is the step where you're going to actually establish what the impact to the organization may be if you lost that critical asset.

Now that we have the asset understood, now you want to establish how you're going to actually protect those assets. So, this is where you're going to put together a security strategy or some kind of response plan to those risks in Process 8.

OCTAVE Allegro



OCTAVE Allegro

- Streamlined version of OCTAVE®

ESTABLISH DRIVERS

PROFILE ASSETS

IDENTIFY THREATS

IDENTIFY AND MITIGATE RISKS

Step 1 – Establish Risk Measurement Criteria

Step 2 – Develop an Information Asset Profile

Step 3 – Identify Information Asset Containers

Step 4 – Identify Areas of Concern

Step 5 – Identify Threat Scenarios

Step 6 – Identify Risks

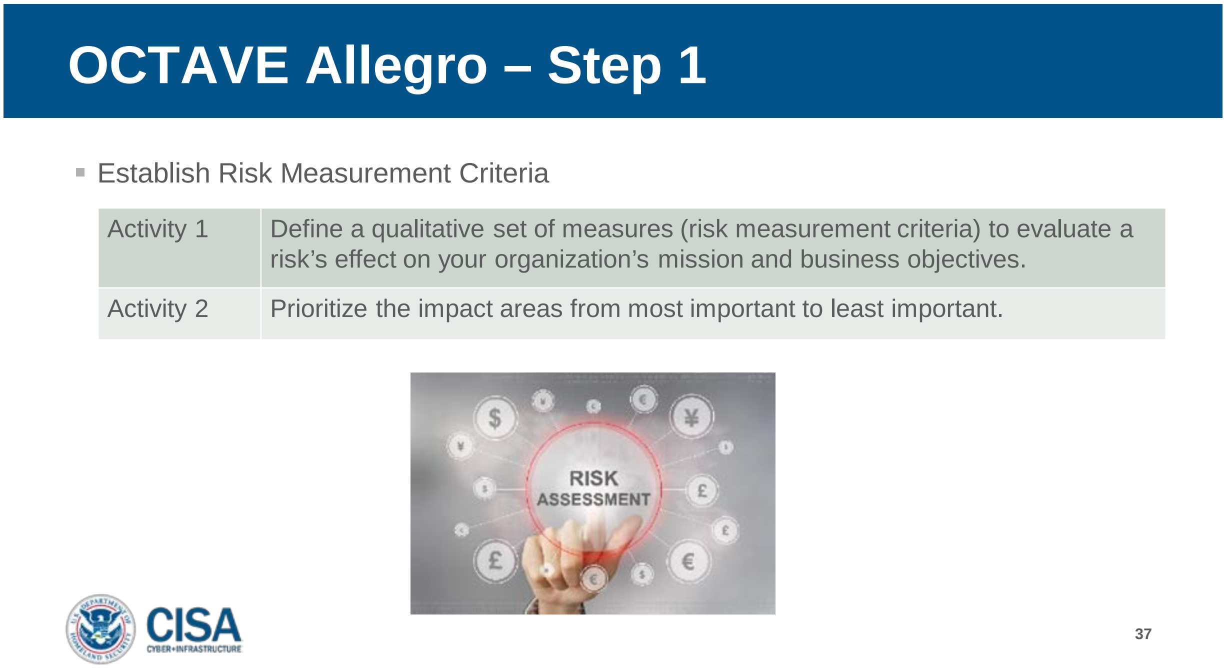
Step 7 – Analyze Risks

Step 8 – Select Response Approaches

Streamlined for Information-based organizations, to analyze information-based assets, without requiring a lot of resources

**036 Here it is mapped out. There's eight steps. There are some items that we picked out from this process. It is a very effective process, and I like it because it is very operational, and I like the fact that it is flexible. And many people across the enterprise, once they're educated in the process, can do it. And I encourage you to look at the SEI website to look up more on the OCTAVE processes. We have a number of documents that are available to learn and actually do this process.

OCTAVE Allegro – Step 1



OCTAVE Allegro – Step 1

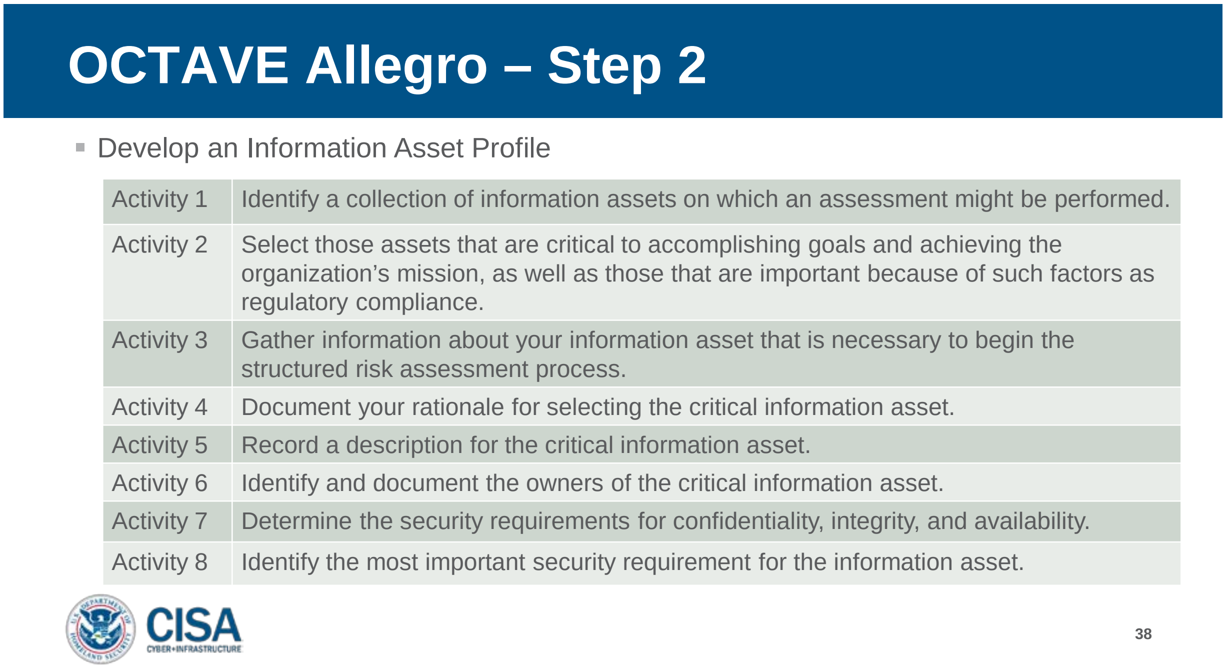
- Establish Risk Measurement Criteria

Activity 1	Define a qualitative set of measures (risk measurement criteria) to evaluate a risk's effect on your organization's mission and business objectives.
Activity 2	Prioritize the impact areas from most important to least important.

**037 That said, we recognize too though that, with each of these steps, there are specific activities that you need to be familiar with. That way you can actually execute the process yourself.

So, let's do a little bit of a deep dive on that. It's not going to be too much. Let's talk about, for example, establishing risk measurement criteria. So, you're going to actually want to define what are the measures that you have in your enterprise. By the way, I encourage you to go back and look at the NIST documentation we talked about because they provided some of what those qualitative assessments or measures may look like. In Activity 2, we're going to actually prioritize the impact areas and what may be most important to least important in your enterprise.

OCTAVE Allegro – Step 2



OCTAVE Allegro – Step 2

- Develop an Information Asset Profile

Activity 1	Identify a collection of information assets on which an assessment might be performed.
Activity 2	Select those assets that are critical to accomplishing goals and achieving the organization’s mission, as well as those that are important because of such factors as regulatory compliance.
Activity 3	Gather information about your information asset that is necessary to begin the structured risk assessment process.
Activity 4	Document your rationale for selecting the critical information asset.
Activity 5	Record a description for the critical information asset.
Activity 6	Identify and document the owners of the critical information asset.
Activity 7	Determine the security requirements for confidentiality, integrity, and availability.
Activity 8	Identify the most important security requirement for the information asset.

**038 Let's talk a little bit more about how we develop that information asset profile. This is an eight-step process. It may seem overwhelming at first. But really once you get to it, it's not that bad. You identify and collect what assets you have in the organization and you're going to look at those that are going to be the most critical. And then you're going to gather information about those assets. Remember, what we're doing here is a risk assessment. So, we're trying to understand what controls we have in place. And we may understand too the additional-- what are previous vulnerabilities that may have existed, what threats may be most important thinking about when you're going to be assessing what risks are related to this asset. At all times, we're going to be documenting what we're finding through this. And we're going to look to record a description of what critical information may actually be resident on that asset.

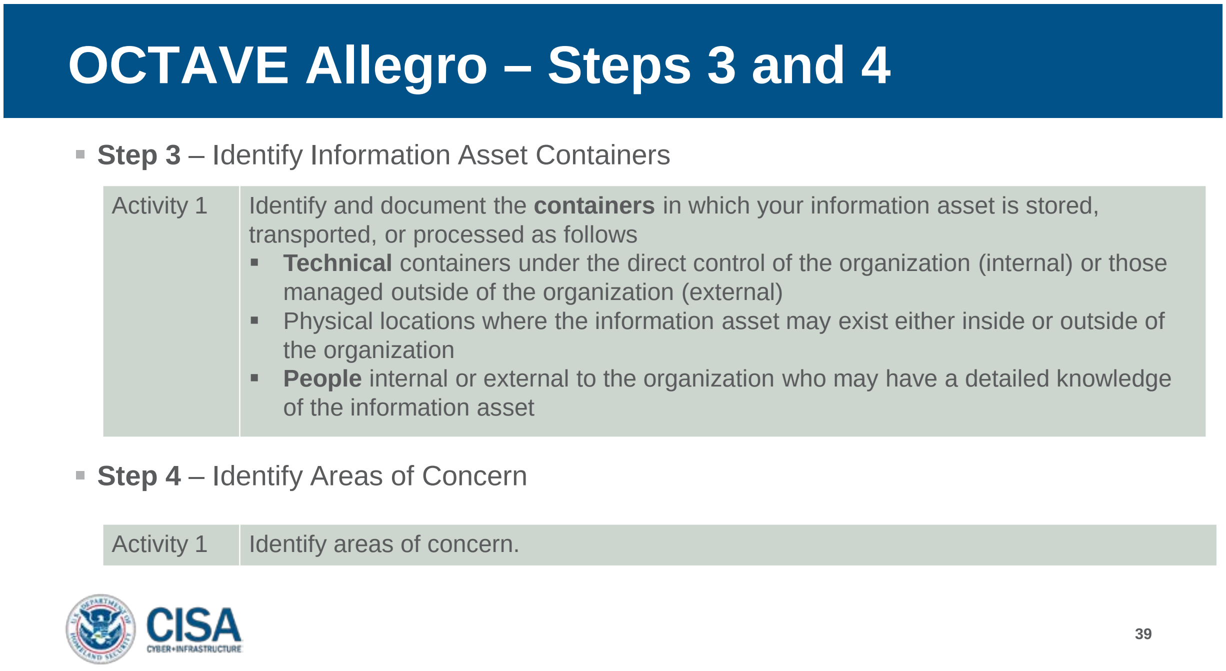
We also want to look at who owns these assets. Now, it's challenging actually at times to understand who actually owns data in a system. Is it the people who are actually putting the data in the system? Maybe it's the people who are processing it, or maybe it's the people who are owning it-- or excuse me, not just owning it, the people who are using it. Excuse me.

And then we could also look at what are the requirements behind that information. Remember this data could be sensitive. It could have information we do not want adversaries to get. So, there's this element of confidentiality around it.

Maybe it's a matter that we don't want the information to be violated. We don't want it to be changed such that at a later date, when we come back and use that data, that it's not useful or it's inaccurate. So, that's an integrity issue.

We also want to look at the idea as to is it available in the organization. Can people access it when it's necessary? And then we're going to want to think about the requirements of security that we want to place around those assets.

OCTAVE Allegro – Steps 3 and 4



OCTAVE Allegro – Steps 3 and 4

- **Step 3** – Identify Information Asset Containers

Activity 1	Identify and document the **containers** in which your information asset is stored, transported, or processed as follows ▪ **Technical** containers under the direct control of the organization (internal) or those managed outside of the organization (external) ▪ Physical locations where the information asset may exist either inside or outside of the organization ▪ **People** internal or external to the organization who may have a detailed knowledge of the information asset

- **Step 4** – Identify Areas of Concern

Activity 1	Identify areas of concern.

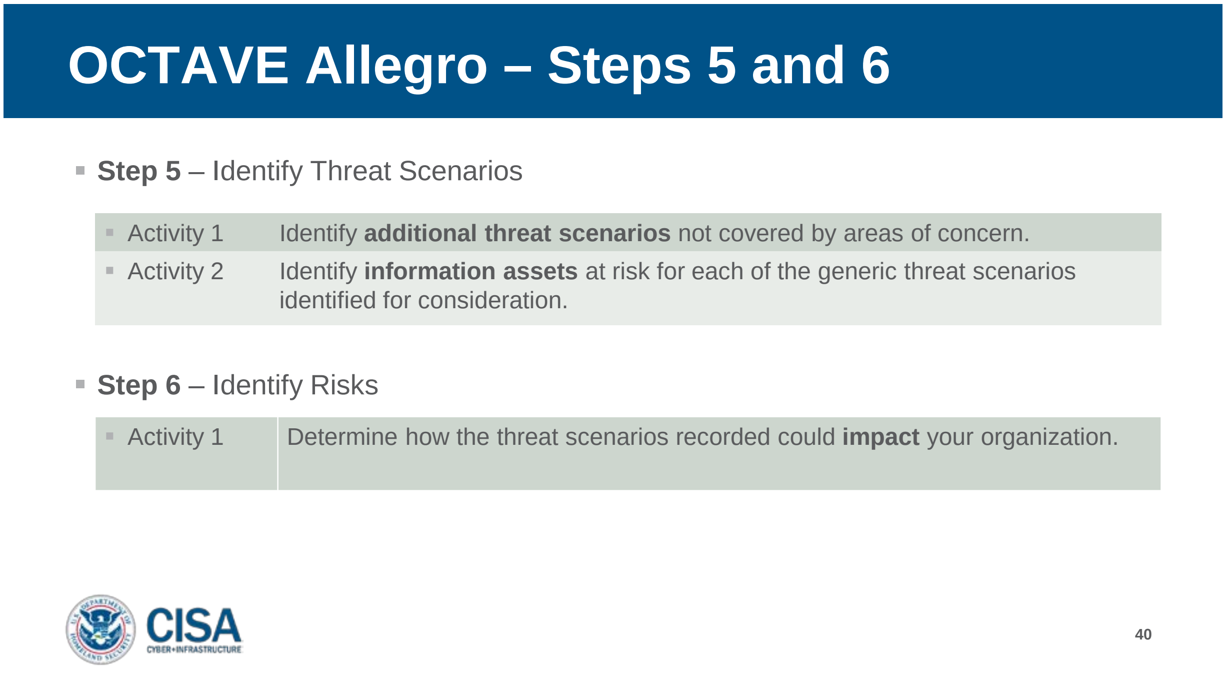
39

**039 Now, this information, it's resident somewhere. It lives somewhere. We call this, in OCTAVE, an asset container. And we want to identify what those containers are. And there are three different basic types of container we can think about. They're technical containers. So, when you think about those of--maybe it's a database. Maybe it's an actual computer that is actually storing the information. We have physical locations. So, this is the idea that that computer could be stored within a facility like a building. We can also think about people because maybe they house information. Maybe they have knowledge of how to operate the system, or they have information in their head that they actually contain, and they're walking around with it. So, you're going to have to think about how you're going to actually insulate that asset as well.

Okay, and now, we want to think about areas of concern.

So, these are areas that you may find that are weaknesses or gaps in the organization.

OCTAVE Allegro – Steps 5 and 6



OCTAVE Allegro – Steps 5 and 6

- **Step 5** – Identify Threat Scenarios

Activity 1	Identify **additional threat scenarios** not covered by areas of concern.
Activity 2	Identify **information assets** at risk for each of the generic threat scenarios identified for consideration.

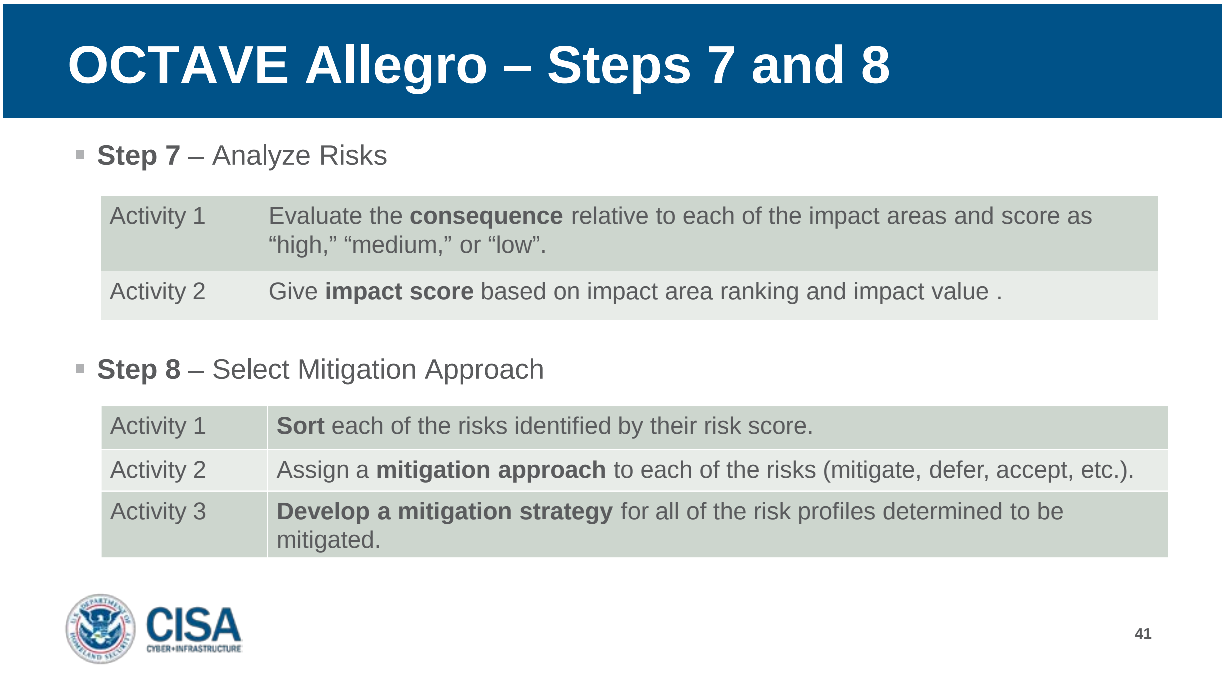
- **Step 6** – Identify Risks

Activity 1	Determine how the threat scenarios recorded could **impact** your organization.

40

**040 You think about the threat scenarios and how they can actually exploit those different concern areas. And finally, from that, we're going to identify the risks and what the impacts to the organization could be if they come to light.

OCTAVE Allegro – Steps 7 and 8



OCTAVE Allegro – Steps 7 and 8

- **Step 7** – Analyze Risks

Activity 1	Evaluate the **consequence** relative to each of the impact areas and score as "high," "medium," or "low".
Activity 2	Give **impact score** based on impact area ranking and impact value .

- **Step 8** – Select Mitigation Approach

Activity 1	**Sort** each of the risks identified by their risk score.
Activity 2	Assign a **mitigation approach** to each of the risks (mitigate, defer, accept, etc.).
Activity 3	**Develop a mitigation strategy** for all of the risk profiles determined to be mitigated.

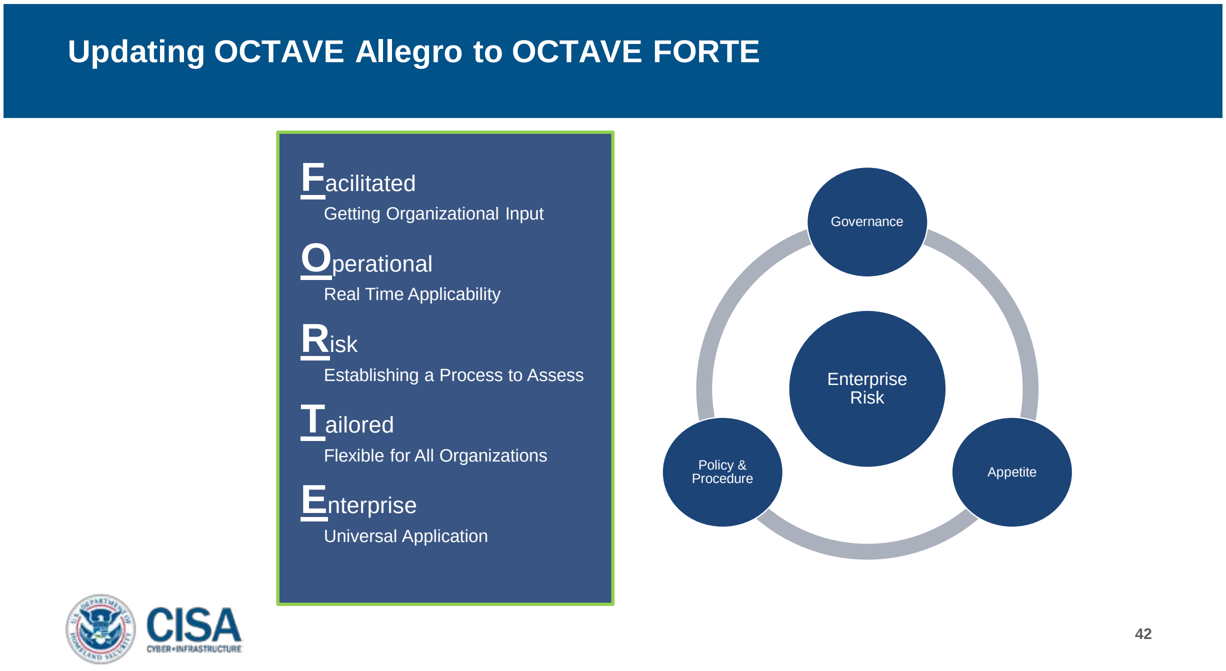
CISA
CYBER+INFRASTRUCTURE

41

**041 Once we have that, we can start analyzing the risks at a deeper level, and we can actually assign them scores, We talked about the qualitative scoring that we give them, the high, medium, low, based on the consequences that you may have if the risk comes to light. But then we also think about it in terms of ranking. So, we can actually start putting these scores together and prioritizing the risks.

Once we've done that, we can think about how we're going to actually mitigate that risk. So, we can sort them by score, and we can figure out what actions we can take that would be most effective. And then we can have an overall mitigation strategy related to that risk profile that we've established.

Updating OCTAVE Allegro to OCTAVE FORTE



Updating OCTAVE Allegro to OCTAVE FORTE

Facilitated
Getting Organizational Input

Operational
Real Time Applicability

Risk
Establishing a Process to Assess

Tailored
Flexible for All Organizations

Enterprise
Universal Application

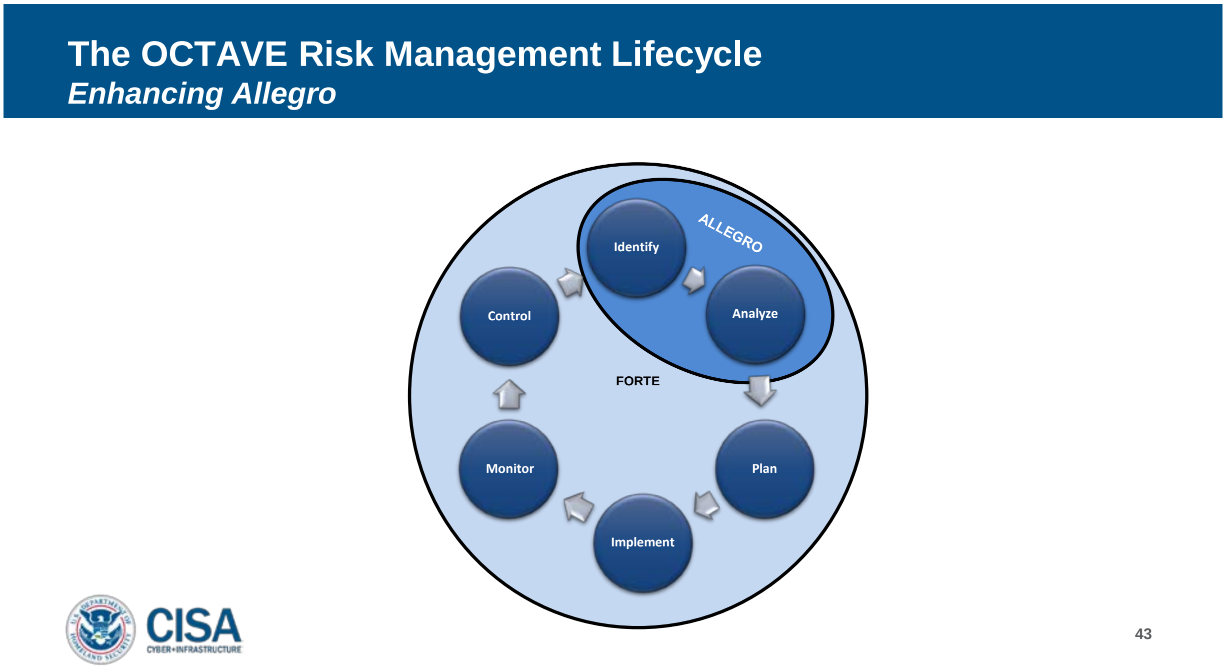
42

**042 Now, like I said, Allegro's a great process. And as I've just gone through, and hopefully with your additional research, you can find that it could be used very broadly across the organization, especially at the tactile levels of the organization.

But that said, the SEI went back and we rethought what OCTAVE was truly delivering. We're really concerned about how the executive levels would digest and understand the analysis that took place within OCTAVE Allegro. And we recognized that we needed some facilitated means to bring those risks to that executive level and have them understand what the operational real-time applicability of that information was, how to use it, how to make risk-based decisions. And we also needed a process that could be tailored to that executive management team so that they could manage the enterprise broadly.

So, we came up with the OCTAVE FORTE process. It actually uses the classic enterprise risk management tool set to use what was delivered in Allegro and actually make it more digestible and effective at the executive level. It focuses on governance, risk appetite, policy, and procedures.

The OCTAVE Risk Management Lifecycle Enhancing Allegro

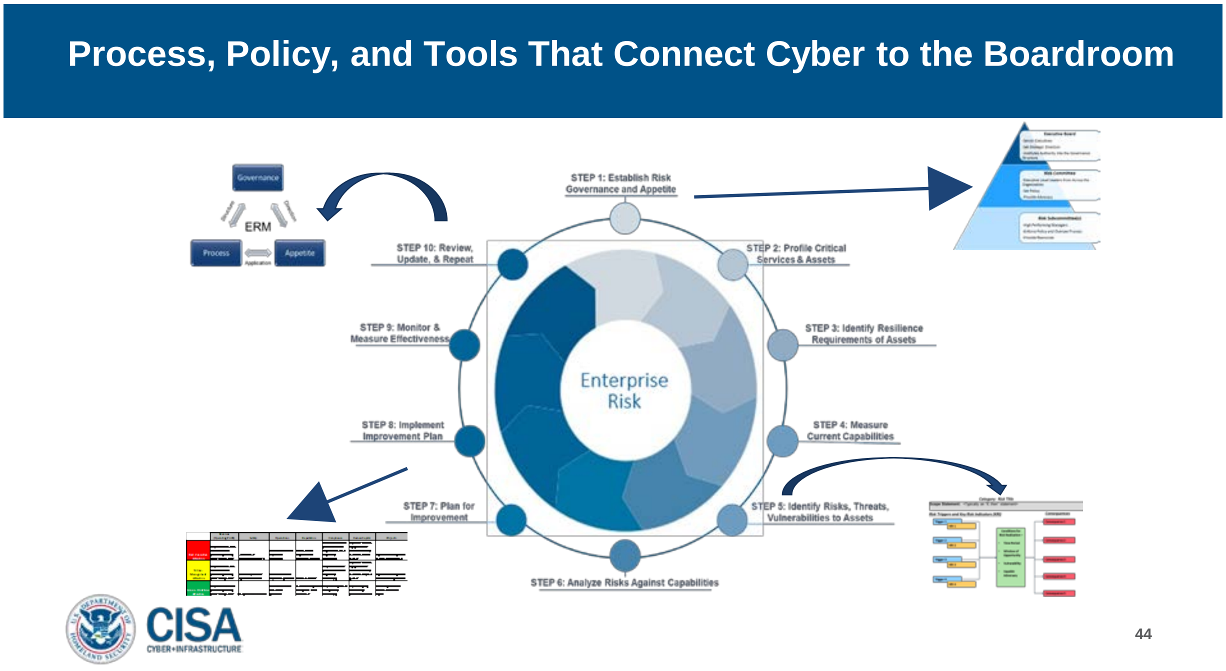


The OCTAVE Risk Management Lifecycle

Enhancing Allegro

**043 Here's a little overlay to understand that a little better. Now, truly this is not a perfect diagram. Allegro does span other elements within this document, but really it had focus on that identify/analyze piece. FORTE tries to go more broadly with the risk process, and it tries to also take a more iterative approach to how risks are managed.

Process, Policy, and Tools That Connect Cyber to the Boardroom



Process, Policy, and Tools That Connect Cyber to the Boardroom

Governance
ERM
Process
Appetite
Application
STEP 1: Establish Risk Governance and Appetite
STEP 2: Profile Critical Services & Assets
STEP 3: Identify Resilience Requirements of Assets
STEP 4: Measure Current Capabilities
STEP 5: Identify Risks, Threats, Vulnerabilities to Assets
STEP 6: Analyze Risks Against Capabilities
STEP 7: Plan for Improvement
STEP 8: Implement Improvement Plan
STEP 9: Monitor & Measure Effectiveness
STEP 10: Review, Update, & Repeat
Enterprise Risk

CISA
CYBER+INFRASTRUCTURE

44

**044 So, let's go through that process a little bit here. It's a ten-step process. And I encourage you also to look more into the OCTAVE FORTE process.

Moving on though, let's go through that ten-step process. In the first step, what we're really looking to do is establish what I would consider the three primary pillars to any good risk management program, the first being a governance structure. And we talked about this a little bit too and how this was covered in NIST, the tiered structure you may recall in the past. It may look different for any given enterprise. You don't necessarily have to follow that. Maybe you think about your risk governance structure in terms of executives making decisions, managers making decisions underneath them, and then frontline professionals making decisions there. At each level, you need advisory bodies maybe that are managing those risks and understanding how those decisions are impacting enterprise.

So, let's go back again. At that executive level, maybe we have a risk committee or maybe a board. Maybe at the next level, we have subcommittees, and maybe they're functionally specific. Maybe they're area of knowledge specific. Either way, those subcommittees could feed up to that risk committee.

Now, the next element that you would need is risk appetite. I just talked about this governance structure, and these subcommittees for example would need to be able to communicate with the risk committee. So, you're going to have actually policy/procedure going down into the enterprise with direction. You're going to have risks bubbling up from the enterprise back up into the governance structure to tell them hey, here's what we found. That has to be done within the context of a risk appetite. How is it that we go about scoring these risks and understanding them such that we know what level the organization cares about any given risk? We can do that with an appetite statement.

The final piece that you need there is policy and procedure. And this is the notion that who would really execute the process if it isn't written down and given proper direction. This is harder than it sounds. If you read any given policy, it can be challenging at times to understand exactly who is doing what. So, it has to be written at the most base level so that everybody in the enterprise can embrace it and execute the direction that's followed in the procedure.

So, next, what we want to do is we want to look at what the critical services and assets are. And we've talked about this before. We're trying to understand what it is that is key to the enterprise to keep it operational, to keep it moving. And then what we want to do is we want to look at the existing requirements that we have for those assets. Now, it may be that this analysis leads us to new resilient requirements because maybe the threat picture has changed. And remember, this is an iterative process. So, I may be going through this a second, third, or maybe even fourth time. And we want to document what those resilience requirements are.

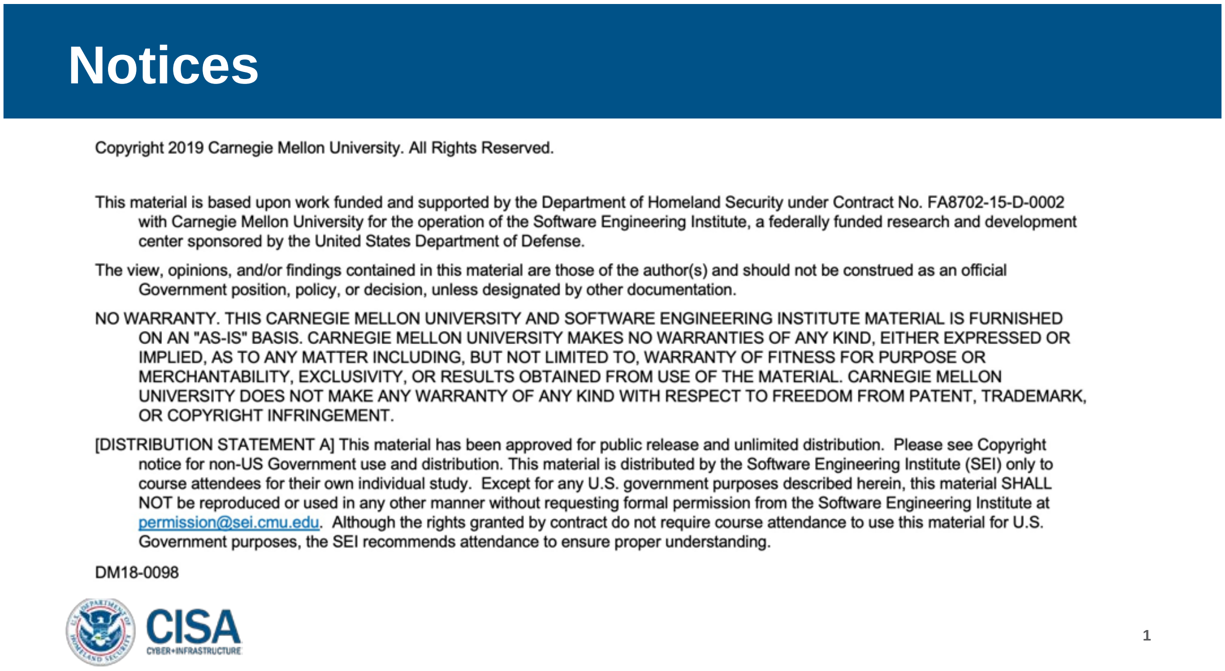
And then what we want to do is we want to look at our current capabilities that we have in place. Once again, this is the example of suppose I have a risk for fire in my organization. I have existing controls that may be in place. Maybe it's a sprinkler system. Maybe it's fire extinguishers. Maybe it's some kind of alarm system. If that's the case, I want to document that too and understand what those controls are in place so that way I don't replicate them and expend resources unnecessarily.

Then I want to really take yet another turn on identifying what those risks are. What are the uncertainties? What are the threats? What are the vulnerabilities? This is where that nice overlap lies with OCTAVE Allegro, and you can get a lot out of it in those first steps up through about step five in getting that analysis. The important part here, and what the OCTAVE FORTE process allows you, are additional tools such as risk trees to understand what, at a high level, executives need to know in terms of what are the drivers. What are the things that need to happen to actually make the risk come to light? What's the context that those risks take place in? And finally, how you feel the pain, what's the impact in the enterprise? And that way you can put it to a level of abstraction that an executive can quickly appreciate what you're trying to relate to them, and that way you don't get mired down in the bits and bytes discussion where so many cyber risks lie.

So, now you want to look against existing capabilities in the organization, and you're going to make sure that you're not, once again like I said, replicating responses. And here's where too where you're actually going to start planning for improvement. You're going to start thinking about what are the new responses that I need that can actually help me control these risks better.

And then what you're going to do is you're going to follow it. You're going to implement that plan. You're going to set up a project plan maybe to actually put those controls into place. And you're going to want to continue iteratively to monitor and measure that effectiveness to make sure you're getting what you paid for. And by the top, by step ten, you're really doing one of two things. You're looking at your program broadly to make sure that this process is delivering what you need in terms of managing your risk portfolio. And you're also looking at the individual risks. You're looking to see that they're actually being controlled too. And these two things can feed off each other in terms of metrics, measurement, and understanding how the organization's performing in terms of risk management.

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

CISA
CYBER+INFRASTRUCTURE