# OCTAVE and OCTAVE Allegro

## Table of Contents

| OCTAVE ® (Operationally Critical Threat, Asset, and Vulnerability Evaluation SM ) | 2 |
| OCTAVE | 3 |
| OCTAVE – Overview | 5 |
| OCTAVE – Phase 1 | 7 |
| OCTAVE – Phase 2 | 10 |
| OCTAVE – Phase 3 | 11 |
| OCTAVE Allegro | 12 |
| OCTAVE Allegro – Step 1 | 14 |
| OCTAVE Allegro – Step 2 | 15 |
| OCTAVE Allegro – Steps 3 and 4 | 18 |
| OCTAVE Allegro – Steps 5, 6 and 7 | 20 |
| OCTAVE Allegro – Step 8 | 22 |
| Notices | 23 |
**030 Chris Evans: Another risk assessment or risk management framework that you can think about using is OCTAVE, the Operationally Critical Threat, Asset and Vulnerability Evaluation, that was pioneered here at the SEI.
**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

**031 So, what is OCTAVE? Well, it's a risk-based assessment process. And when we say risk-based, what are we talking about? We're saying that you're looking at underlying risk to your organization and focusing on those risks, as opposed to a particular threat, or a particular vulnerability. It is self-directed, meaning this is your process; you are running through the process within your organization--small internal teams, or maybe large internal teams--depends on your organization and how big you are--are drawing on knowledge for doing this assessment process. So you might go out and interview people**
within your organization, you might be reviewing documents within the organization. But this is your process, and you are pulling on the knowledge of people, other people, within your organization to do this.

It's not customary that one person is going to be able to do all of this. One person doesn't have complete knowledge of their entire business or their organization. So what they're going to have to do is reach out to other people to say, "Help me with this process. Help me understand the business area. Help me understand the controls and the risks and the vulnerabilities that you've got."

A note that this is flexible. So, this isn't a risk management process tied to a particular type of organization, like banks or restaurants or something like that. So it's a more flexible approach, and it's applicable to other organizations, or a wide range of organizations. And so you can adapt the process here to your particular area.

What does this really mean though? Keep in mind that OCTAVE is a large process, and because it's flexible, you might find that there are other processes, or that you want to fine-tune OCTAVE for your particular organization or your particular business. In fact, we'll talk a little bit about some variations on OCTAVE that have done just that. But it's focused on organizational risk. You're looking at your strategy, the
security practices that you have, the
technology that you have in place,
and you're coming up with a notion
of risk to your organization with this
process.

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

**032 So how does this process actually work?** Well, there are three different phases to this. And you'll see it's very similar to the general process that we've been talking about with the NIST Special Publications, the general risk assessment or risk management process. But within these three phases, you're going to start with your assets. So, what are my critical
assets and what are my threats to those assets? That happens in phase one.

Phase two, you're looking at vulnerabilities. So, given my critical assets, what are my particular vulnerabilities for these assets? Is the server missing a patch? Is there no lock on the front door? What are the vulnerabilities for the things that I've come up with in step one?

And then the last phase here, you're coming up with a security strategy. You're coming up, "What am I going to do about the risk that I found?"

So this follows the general process of: What do I have in my organization, what could go wrong with it-- threats and vulnerabilities-- and what do I do about it? And that's in the last phase here.
**Build Asset-Based Threat Profiles**

<table>
<thead>
<tr>
<th>Process 1: Identify Senior Management Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect information about important assets, security requirements, threats, and current organizational strengths and vulnerabilities from a representative set of senior managers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process 2: Identify Operational Area Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect information about important assets, security requirements, threats, and current organizational strengths and vulnerabilities from managers of selected operational areas</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process 3: Identify Staff Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process 4: Create Threat Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select three to five critical information-related assets and define the threat profiles for those assets</td>
</tr>
</tbody>
</table>

**033 Within phase one, again, you're building threat profiles and you're building a notion of what your assets are within the organization. You'll see that the first three processes here-- one, two and three-- are very similar. What distinguishes process one from two, and two from three? You're doing the same thing, just at different levels. Right? So process one, you're looking at senior management. Process two, you're looking at an operational area or perhaps a business function. Process three, you're looking at individual staff or perhaps systems.**
What does this look like? Remember the tiers to risk management, where we had tier one focusing on strategy, tier two focusing on business or functional areas, tier three focusing on specific systems or applications? This is very similar in structure, and it's set up that way to make sure that during an OCTAVE assessment you are going through and pulling information from the top, middle, and the bottom. Is it sufficient for you to do a risk assessment with just input from the CEO? Probably not. Does the CEO know about the firewall implementation that separates Network A from Network B? Probably not. Chances are good that that's not the case. So how can you accurately get a complete picture of your risk if you don’t interview the guy who runs that firewall, or interview the people who do the applications?

Other side of that. Let's say you just interview the firewall guy. Is that a complete risk assessment, or a complete characterization of an enterprise, an organization? You'll get the technical vulnerabilities and you'll get the, "Here's how we could get hacked," but you're missing the strategic piece. "What's important to my business?" or "What's important to my organization?" All of that comes from the various levels, and so that's why it's important to focus on talking to senior management, talking to the business process leads, talking to the firewall admin or the security staff or the network operations people, because that gives you a
complete characterization of assets, threats, potential vulnerabilities, and that sort of thing.

The last process up here is you're going to create threat profiles. So you're going to pick based on the things that I've learned in my interviews with senior managers and process leads. I'm going to pick some type of critical assets that I know are really important to my business, and I'm going to come up with threat profiles for them: What could go wrong with this asset?
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.

**034 The next phase here, phase two, there are two processes associated with this. You’re coming up with infrastructure vulnerabilities. You’re looking at what are the weaknesses, what are the flaws in the infrastructure or the key components here. So process five says, "Start with the key components." What are they? What are the critical assets here, or the critical parts of the systems that we chose to look at in the previous phase?

Based on that-- so for each of these components, now evaluate them. Find out what are the vulnerabilities.
What could go wrong with these-- or, sorry-- what are the weaknesses or the flaws in these particular systems or components that we’ve selected?

**OCTAVE – Phase 3**

---

**OCTAVE – Phase 3**

Develop Security Strategy and Plans

<table>
<thead>
<tr>
<th>Process 7:</th>
<th>Conduct Risk Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define an organizational set of impact evaluation criteria to establish the impact value</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process 8:</th>
<th>Develop Protection Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop an organization-wide protection strategy to improve the organization’s security practices</td>
<td></td>
</tr>
</tbody>
</table>

**035** And you use the results of that to refine your threat profile from phase one.

And you do that because, on this step, you’re looking at, "What do I do now?" So I have this notion of, “I have my assets, I understand what the threats and vulnerabilities are from that, the threat scenarios or the threat profiles. What do I do?” Well, the first process here, or process
seven now, is to do a risk analysis so I’m looking at impact based on the threats and the vulnerabilities and the assets. What could go wrong with the business? And then I’m going to say, “Okay, what am I going to do about it?” So the last process here is addressing the risks that I found through the previous processes.

**036 That’s OCTAVE. As I said, it’s a large process. It’s very flexible, but because it’s flexible, it’s broad. And so you’ll find that certain organizations are-- it’s appropriate to streamline that process. And so what
SEI did was it came up with OCTAVE Allegro that took OCTAVE and said, "Okay, if you are an information-based organization, if you deal in information"—e.g., you're not a restaurant, or something like that—but "if you're an information-based organization, you can do this process." It's a subset of OCTAVE. It's been streamlined for you, because you are a particular type of organization that focuses on information.

And so you can do an OCTAVE Allegro assessment faster, with fewer resources, than you could if you just did a full-blown OCTAVE assessment. So, the reason they came up with this is organizations said, "You know, I really like OCTAVE. I like the process. It's just too big. There's a lot of stuff that goes into that. I don't have the time, the resources to be able to do a full-blown OCTAVE assessment. But I can do this, because it's been streamlined for me."
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 So, step one in this process, you’re looking at the risk measurement criteria. Again, you want to figure out, "What am actually going to evaluate? What am actually going to look at through this Allegro process?" And then you’re going to prioritize these from least impact, or most impact to least impact. So, again, you’re doing this prioritization step to say, "Okay, some things are more important than others, and those are the things I’m going to concentrate on in this process."
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 The information asset profile.
So now, for your-- at least through step two here-- what you’re going to do here is look at your assets. "What do I have? Do I have servers? Do I have people? What assets do I have that we might want to do an assessment on?"

Then what we're going to do is select from that list that we brainstormed, we're going to come up with a subset of those that we're going to carry on through the risk assessment process. Which ones do we pick? The ones that are most important to our business, or the ones that we define as absolutely critical.
Then what we're going to do is pull as much information as we can--through interviews, through technical reviews, documentation reviews--based on--or from those particular assets that we selected. And then we're going to document why we picked this particular asset for a risk assessment. Why is that important?

Why would we want to document the fact that I picked the firewall to do a risk assessment on? Any guesses?

Think about a risk assessment process. Is it something that you can do in a week, or does it take a month, or two months? It probably takes on order of months. It's not something that you're going to sit down and go, "Okay, by Friday, I'm doing a risk assessment. Yay, I'm done." Probably not going to happen unless you're a really small organization.

The reason you document why you picked something is because a month from now, you're not going to remember why you picked the firewall. Or, worse, you leave and somebody else comes in and sits down and starts doing this risk assessment process, and they go, "Why'd they pick the firewall? The firewall has absolutely no impact on the business. Nobody cares about it." But what you're doing here is you're distilling all of the information that you learned in previous steps, from your interviews or your evaluation of your assets, to go, "This is important." You document
why you picked it, and that’ll help you later in the risk assessment process. One, because it’s a long process and you’ll probably forget. Two, in case there’s any changeover.

So you document why you picked it, a description of the asset itself-- what is the firewall, what does it do, why do we have it. You want to document the owners of the critical asset. Why would you care who owned the firewall? You want to know who to go back to for more information if you have to do further interviews. Or, if you decide that that particular asset needs controls on it, you’re going to have to negotiate with them on, “Okay, well, the firewall doesn’t quite do what we need it to do. We need this patch installed on it. We need this extra piece of hardware put on it.” All of that you’re going to have to negotiate with whoever owns that firewall. So here in activity six, you document who owns it.

The security requirements for confidentiality, integrity and availability. You’re trying to write down here what does this asset give me for-- or what does it need to provide me for maintaining confidentiality of my information, maintaining the integrity of my information? So this is, “What does this particular asset need to do?”

And then you identify the most important ones. So, my asset may need to do these ten things. What are the top two things that it needs
to really do? What’s the most critical function? And I’m going to dig into those later.

**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 that are under the direct control of the organization (internal) or those that are 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

**039 So step three and four here.**
Step three, you’re going to identify containers. So, OCTAVE Allegro puts out there that everything should be in a container based on where-- or information is part of a container, based on where it is or where it's located, transported or processed. So you have this notion of technical containers. This might be a hard drive, a server, a USB drive. The information is actually stored within this technical container. You can
have internal containers. These are ones that you own that are within your boundary; you control it. Or they have external containers. What’s a good example of an external information container, so that's your information but not stored on a system you own, operate, have direct access to?

Think about the cloud. Right? You have a cloud service provider. That’s an excellent example of an external technical container, because it’s your data; it just happens to be on a server in South Africa because that’s where your cloud provider is located.

Physical locations where information exists. So, it’s in the data center. It's on the laptop that I left on the train and now it’s in the possession of somebody else. Oops. Where is your actual data-- could end up, or is stored.

And then people who have knowledge of the-- or who have knowledge. So, people are a container, right? Who has-- let’s say Princess Pizza Companies. Who maintains the secret sauce recipe? It's in the CEO's head. It's his secret family restaurant from Italy 150 years ago, and it's all right here. So if something happens to the CEO, we’ve now lost our secret recipe, right? I hope he wrote it down. But that would be a good control.

So then step four, you’re identifying areas of concern: What could go wrong? What would really concern
me about this asset? Could it be compromised? Could it be disclosed? Could it be modified or changed?

**OCTAVE Allegro – Steps 5, 6 and 7**

---

**Step 5 – Identify Threat Scenarios**

- Activity 1 – Identify **additional threat scenarios** that have not been covered by areas of concern
- Activity 2 – Identify **information assets** at risk for each of the generic threat scenarios you identified for consideration

**Step 6 – Identify Risks**

- Activity 1 - Determine how the threat scenarios that you have recorded could **impact** your organization

**Step 7 – Analyze Risks**

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

---

**040 Step five, you're going to start coming up with threat scenarios, and this is a continuation of the previous step where you're looking at what's the realm of the possible for this particular asset, or this particular-- yeah, asset.**

So, activity two here within step five, you’re going to go back through your scenarios, your threat scenarios, and say, ”Are there other information
assets that need to be included in this?" You're kind of fleshing out the profile that you've got.

Step six, you're going to look at risks. What are the possible risks associated with this particular threat scenario? What are the potential impacts from that? You're kind of brainstorming the realm of the possible for risk here.

And then here in step seven, you're going to carry that another step further and you're going to say: Is this bad, really bad, or end-of-the-world, Armageddon bad? And you're going to assign perhaps a consequence rating. Again, that could be quantitative, one to five. It could be qualitative-- high, medium, or low. And you're also going to give it an impact score that says, "This is the impact to our business." And you want to rank all of these.

So, again, you've got this prioritized list of, "This is really bad. This could mean the end of our business. We're going to focus on this," all the way down to, "You know what? There's a risk here, but I don't really care. It's not important to me." So you do this prioritization step as many times as you can during the process because it's going to help you figure out, "Where do I spend my resources?"

Again, I'm in a resource-constrained environment. I've only got a thousand dollars to spend. Where do I allocate those resources?
Prioritizing based on consequence or impact or effect on the business will help you allocate those resources.

**OCTAVE Allegro – Step 8**

Select Mitigation Approach

- Activity 1 – **Sort** each of the risks that you have identified by their risk score
- Activity 2 – Assign a **mitigation approach** to each of your risks (mitigate, defer, accept, etc.)
- Activity 3 – For all of the risk profiles that you decide to mitigate, you must **develop a mitigation strategy**

**041 So here you're coming up with mitigation approaches. So, based on the fact that I have risk-- "I know I've got a problem. What do I do about it?" You start sorting each of the risks based on that score-- so you've got your prioritized list now, really bad all the way down to not so bad-- and you start coming up with mitigation approaches. "What could I do to prevent this, to minimize the impact from it, prevent it from happening?" And there, in the last
activity here, you’re going to decide on a mitigation strategy. Am I going to accept the risk? Am I going to mitigate it through controls? Am I going to transfer it to somebody else? Or am I just not going to do the activity at all, avoid the risk completely?

Notices

© 2014 Carnegie Mellon University
This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, 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.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

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.

THE MATERIAL IS PROVIDED ON AN “AS IS” BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.