OCTAVE

By Matt White

OCTAVE

- OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk-based strategic assessment and planning technique for security. It is a single source comprehensive approach to risk management.
- OCTAVE allows organizations to balance the protection of critical information assets against the costs of providing protection and detective controls.
- The OCTAVE method uses a catalog of good practices, as well as surveys and worksheets to gain information during focused discussions and problem-solving sessions.

- It can assist the organization by enabling an organization to measure itself against known or accepted good security practices, and then to establish an organization-wide protection strategy and information security risk mitigation plan.
- The OCTAVE method uses a catalog of good practices, as well as surveys and worksheets to gain information during focused discussions and problem-solving sessions.

Self-Directed

- The OCTAVE method is a self-directed technique. An analysis team at the organization manages the process and analyzes all the information. This makes sure the organization’s workers are part of the decision making process, which helps personalize the process.

Outsourcing?

- Completely outsourcing risk assessments can often “detach” the organization from the process, which leaves them to completely rely on an expert “stranger” to solve their needs. When the organization and the experts are not on the same track of thinking, the workers may not truly understand the importance of an asset and why it should be protected, or know the possible threats that could occur. When this occurs, it is possible that the process will go unimplemented and just become a waste of money.

Analysis Teams

Analysis teams:

- identify information-related assets (e.g., information and systems) that are important to the organization
- focus risk analysis activities on those assets judged to be most critical to the organization
- consider the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that can expose assets to threats
- evaluate risks in an operational context - how they are used to conduct an organization’s business and how those assets are at risk due to security threats
- create a practice-based protection strategy for organizational improvement as well as risk mitigation plans to reduce the risk to the organization’s critical assets.

Should I use OCTAVE?

- How do you know if you should adopt a plan?
  - It is safe to say that any organization involved with electronic information or has information assets that the organization relies upon for daily business should have a risk evaluation.
  - Some organizations are required by law to do security risk evaluations.
  - If you are interested in improving your overall security practices, OCTAVE is an answer.
  - Some organizations are completely in the dark about where their information security stands, and would just like a reliable assessment of their information security risks.

Benefits

- The OCTAVE method provides extra benefits to the organization other than improved security. It is a highly accredited risk assessment method that can help attract customers by its strength. The US Government has endorsed the OCTAVE method as the preferred risk assessment method. It helps show dedication to proper security and can help sway potential customers the organizations way. The OCTAVE method produces a risk assessment for the organizations unique assets and risks, which will help save wasteful spending.

OCTAVE-S

- OCTAVE-S was developed for organizations that are smaller in size (about 100 people or less). It meets the same OCTAVE criteria as the OCTAVE Method but is adapted to the more limited means and unique constraints of small organizations. The OCTAVE-S is a more streamlined version of the original process, but will still retain the same quality results of its predecessor.

Differences

- Two primary differences in this version of OCTAVE :
  - OCTAVE-S requires a small team of 3-5 people who understand the breadth and depth of the company. This version does **not** include formal knowledge elicitation workshops at the start to gather information on important assets, security requirements, threats, and security practices. The assumption is that the analysis team knows this already.
  - OCTAVE-S includes only a limited exploration of the computing infrastructure. Small companies frequently outsource their IT completely and do not have the ability to run or interpret the results of vulnerability tools.

OCTAVE Phases

- OCTAVE is organized around these three basic aspects enabling organizational personnel to assemble a comprehensive picture of the organization’s information security needs.
- The phases are:
    - *Phase 1: Build Asset-Based Threat Profiles* – This is an organizational evaluation. The analysis team determines what is important to the organization (information-related assets) and what is currently being done to protect those assets. The team then selects those assets that are most important to the organization (critical assets) and describes security requirements for each critical asset. Finally, it identifies threats to each critical asset, creating a threat profile for that asset.

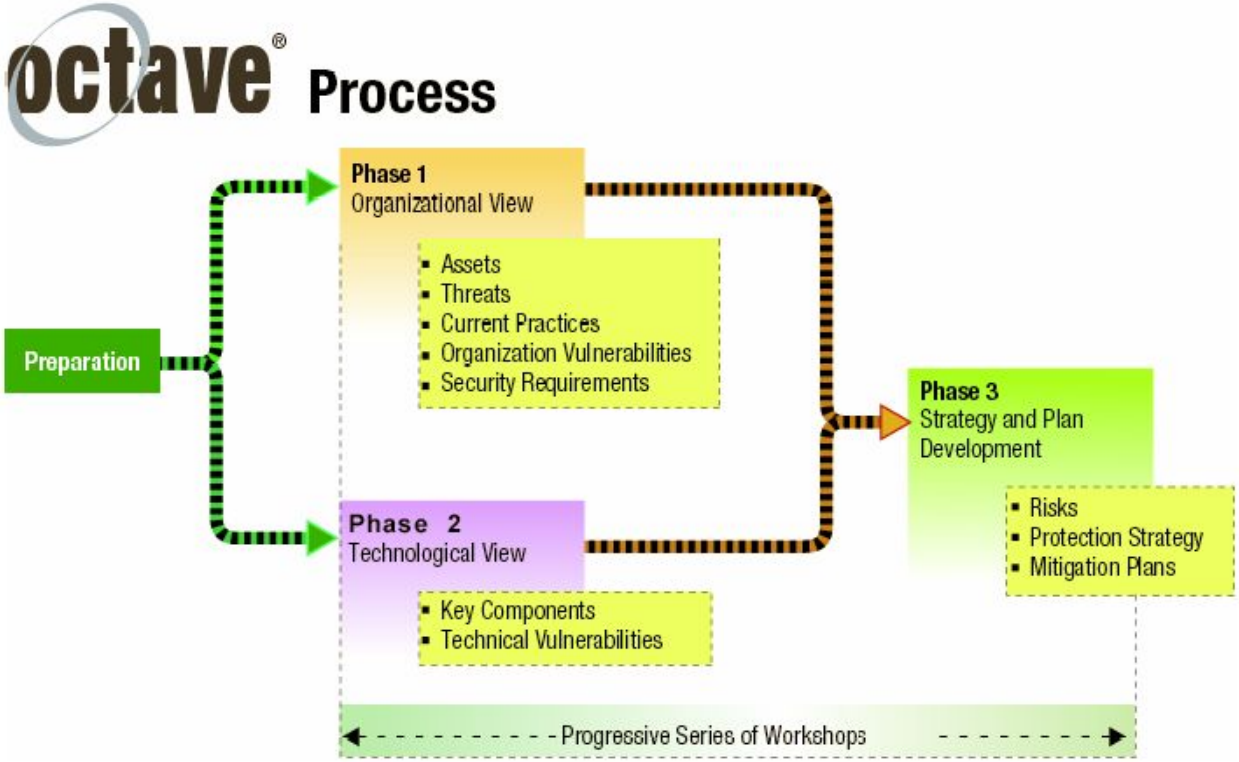
OCTAVE Phases

- *Phase 2: Identify Infrastructure Vulnerabilities* – This is an evaluation of the information infrastructure. The analysis team examines network access paths, identifying classes of information technology components related to each critical asset. The team then determines the extent to which each class of component is resistant to network attacks.

OCTAVE Phases

- *Phase 3: Develop Security Strategy and Plans* – During this part of the evaluation, the analysis team identifies risks to the organization’s critical assets and decides what to do about them. The team creates a protection strategy for the organization and mitigation plans to address the risks to the critical assets, based upon an analysis of the information gathered.

OCTAVE Phases



octave® Process

Preparation

Phase 1
Organizational View

- Assets
- Threats
- Current Practices
- Organization Vulnerabilities
- Security Requirements

Phase 2
Technological View

- Key Components
- Technical Vulnerabilities

Phase 3
Strategy and Plan Development

- Risks
- Protection Strategy
- Mitigation Plans

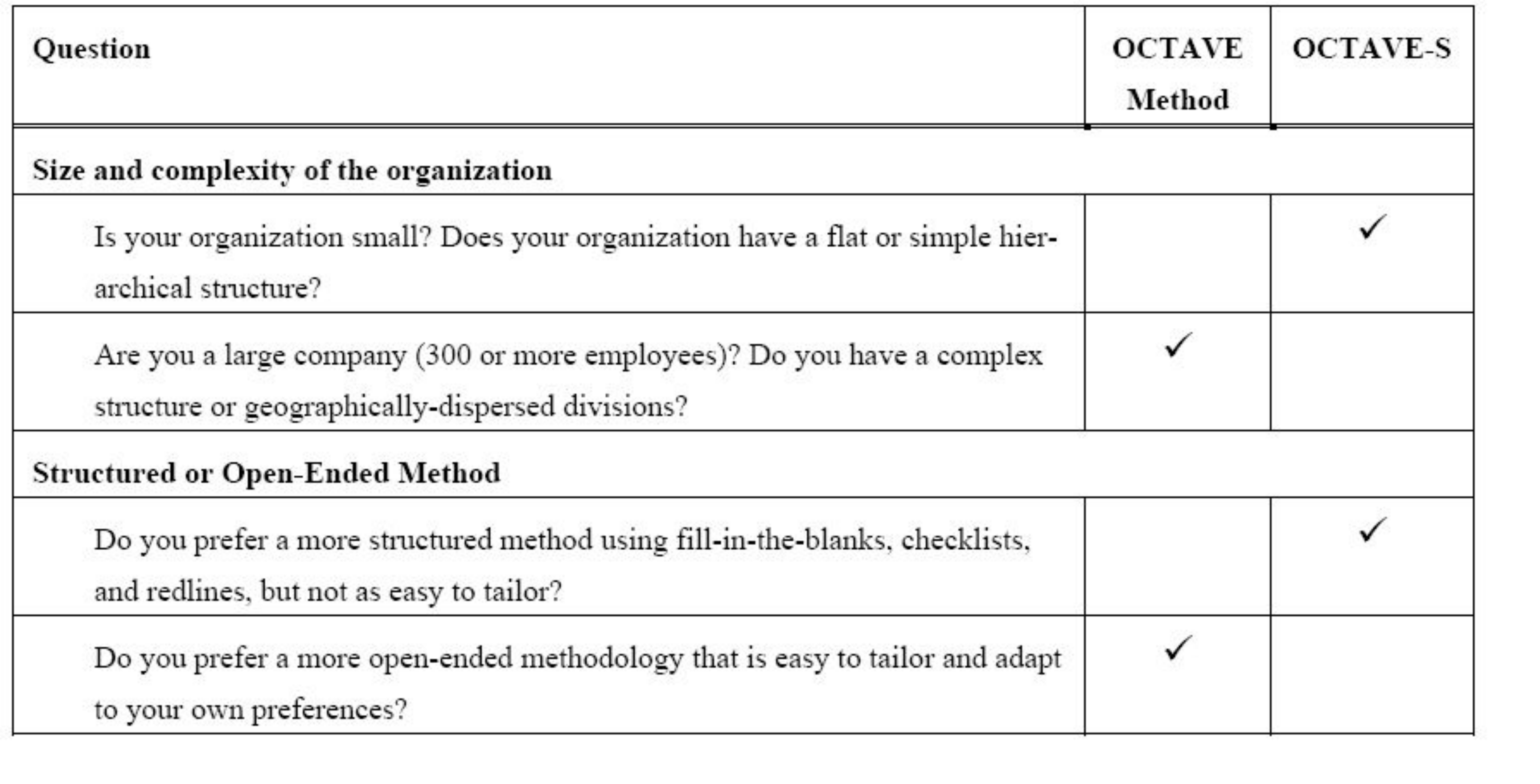
Progressive Series of Workshops

Figure 2: OCTAVE Phases

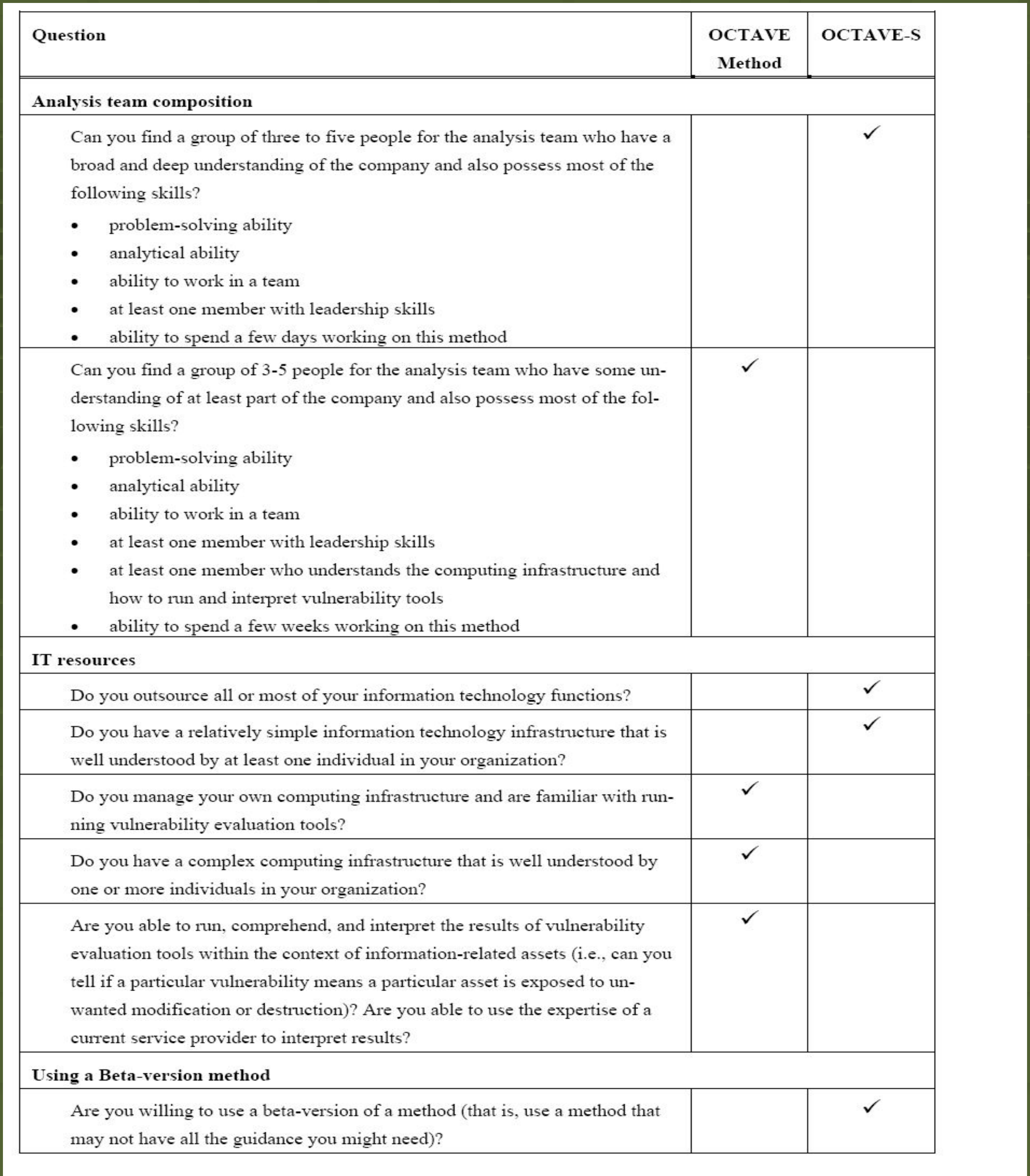
Not a continuous process!

- OCTAVE is an evaluation activity, not a continuous process. Thus, it has a defined beginning and end.
- Periodically, an organization will need to “reset” its baseline by conducting another OCTAVE. The time between evaluations can be predetermined (e.g., yearly) or triggered by major events (e.g., corporate reorganization or redesign of an organization’s computing infrastructure).
- Between evaluations, an organization can periodically identify new risks, analyze these risks in relation to existing risks, and develop mitigation plans for them.

Which to use?



Question	OCTAVE Method	OCTAVE-S
Size and complexity of the organization		
Is your organization small? Does your organization have a flat or simple hierarchical structure?		✓
Are you a large company (300 or more employees)? Do you have a complex structure or geographically-dispersed divisions?	✓	
Structured or Open-Ended Method		
Do you prefer a more structured method using fill-in-the-blanks, checklists, and redlines, but not as easy to tailor?		✓
Do you prefer a more open-ended methodology that is easy to tailor and adapt to your own preferences?	✓	



Question	OCTAVE Method	OCTAVE-S
Analysis team composition		
Can you find a group of three to five people for the analysis team who have a broad and deep understanding of the company and also possess most of the following skills? • problem-solving ability • analytical ability • ability to work in a team • at least one member with leadership skills • ability to spend a few days working on this method		✓
Can you find a group of 3-5 people for the analysis team who have some understanding of at least part of the company and also possess most of the following skills? • problem-solving ability • analytical ability • ability to work in a team • at least one member with leadership skills • at least one member who understands the computing infrastructure and how to run and interpret vulnerability tools • ability to spend a few weeks working on this method	✓	
IT resources		
Do you outsource all or most of your information technology functions?		✓
Do you have a relatively simple information technology infrastructure that is well understood by at least one individual in your organization?		✓
Do you manage your own computing infrastructure and are familiar with running vulnerability evaluation tools?	✓	
Do you have a complex computing infrastructure that is well understood by one or more individuals in your organization?	✓	
Are you able to run, comprehend, and interpret the results of vulnerability evaluation tools within the context of information-related assets (i.e., can you tell if a particular vulnerability means a particular asset is exposed to unwanted modification or destruction)? Are you able to use the expertise of a current service provider to interpret results?	✓	
Using a Beta-version method		
Are you willing to use a beta-version of a method (that is, use a method that may not have all the guidance you might need)?		✓

In Conclusion

- The OCTAVE approach can be very beneficial to certain organizations. If followed correctly, the organization will, in the long run, save money and have a strong security practice in effect.
- Customers are beginning to look for stronger information security when dealing with companies, and laws are being passed to strengthen security all around.
- The OCTAVE method can help ease customer concern and passes some of the stringent security guidelines associated with some organizations.
- The OCTAVE method should be your first thought when it comes to risk management today.