The OCTAVE® Approach to Information Security Risk Assessment

Parthajit Panda, CISA, CISM, CISSP, PMP, is head of IT and chief information security officer (CISO) at a central government establishment in Hyderabad, India. Over a 15-year period, Panda has been involved in various IT and information security initiatives. In addition, Panda frequently mentors and coaches CISA and CISSP aspirants. He is an active member of the ISACA Hyderabad Chapter and has conducted study circle sessions and workshops at the chapter on the OCTAVE approach. Panda can be contacted at *parthajit.panda@gmail.com.*

The superior man, when resting in safety, does not forget that danger may come. When in a state of security, he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come.

—Confucius

Today's world requires that digital data be accessible, dependable and protected from misuse. Unfortunately, this need for accessible data also exposes organisations to a variety of new threats that can affect their information. Often organisations invest huge resources trying to protect their IT infrastructure without assessing the risks to their critical information. These organisations fail to realise that the primary objective is to protect mission-critical information rather than the IT infrastructure.

Organisations deploy established information security control frameworks as business needs and regulatory requirements become imminent. Most of these frameworks have evolved from industry best practices and recommend information security risk assessment aligned to the organisation's risk management framework as one of the control objectives. The challenge enterprises face today is in adopting a robust, process-oriented information security risk assessment framework to comply with the control objective.

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE®) approach is one such framework that enables organisations to understand, assess and address their information security risks from the organisation's perspective. OCTAVE is not a product, rather it is a process-driven methodology to identify, prioritise and manage information security risks. It is intended to help organisations:

- Develop qualitative risk evaluation criteria based on operational risk tolerances
- Identify assets that are critical to the mission of the organisation
- Identify vulnerabilities and threats to the critical assets
- Determine and evaluate potential consequences to the organisation if threats are realised
- Initiate corrective actions to mitigate risks and create practice-based protection strategy

The OCTAVE approach was developed by the Software Engineering Institute (SEI) at Carnegie Mellon University to address the information security compliance challenges faced by the US Department of Defense (DoD). SEI is a US federally funded research and development centre sponsored by the DoD.

THE NEED FOR OCTAVE

Determining Optimal Security

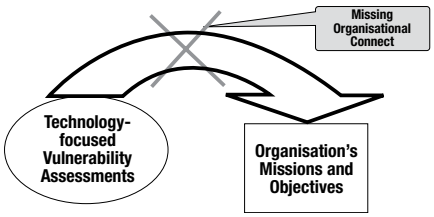
Information systems are essential to most organisations today. The confidentiality, integrity and availability of information are critical to organisations' missions. The need for these organisations is to focus on their most important information assets when making decisions about protecting them to achieve optimal return on security investments (ROSI). Adopting security controls to protect information assets without proper assessment of risks will either overprotect assets, making security a hindrance to business operations, or underprotect and expose the business-critical asset to threats.

For example, a health care company might consider its customers' records to be one of its important information assets. Likewise, a military establishment might consider its data on troop deployment to be an important information asset. Often organisations today form their protection strategies by focusing solely on information infrastructure weaknesses rather than organisational requirements and fail to establish the effect of the infrastructure weaknesses on information assets, such as customers' records or troop deployment data. This leads to a gap between the organisation's operational requirements and IT requirements.

The Generic Approach to Security

Often, the computing infrastructure is set up without IT staff having a clear understanding of the organisation's mission or business objectives and it is not clear to them if critical and/or sensitive information is being adequately protected or not. Such a situation leads to absence of what can be termed as 'organisational connect' (see **figure 1**) between the technology and organisational objectives. Likewise, significant effort might be directed towards protecting relatively unimportant information. In such situations, the operational or business units of the organisation and the IT department need to collaborate and communicate effectively to address the organisation's mission or business-related needs.

Figure 1—Organisational Connect



Often, information protection decisions are made in an *ad hoc* manner, based on the IT department's prior experience with vulnerabilities and the threats about which they currently know. Thus, risks tend not to be systematically managed or are managed by the wrong people.

Some current approaches to information security risk management tend to be incomplete, expert-driven or both. These approaches fail to include all the components of information security risk (i.e., assets, threats and vulnerabilities). In such cases, the organisation has insufficient data to fully match and develop a protection strategy to its security risks.

Many organisations outsource information security risk assessments because they do not have in-house capability to perform this vital service. They hire experts to perform risk assessments, and the resulting assessment is only as good as the experts who perform it. Often the consumers of such services have no way to understand if the risk assessment performed for them is adequate for their organisation.

What OCTAVE Provides

OCTAVE enables organisations to avoid these problems by defining the essential components of a systematic information security risk assessment framework. By following the OCTAVE approach, organisations can make information protection decisions based on risks to the confidentiality, integrity and availability of critical information assets. The operational or business units and the information technology team work together to address the information security needs of the organisation. The ability to connect organisational goals and objectives to information security goals and objectives is the primary benefit of OCTAVE.

OCTAVE WAY TO MANAGING RISKS

The OCTAVE approach to managing risks is governed by the OCTAVE criteria, which are essential requirements comprising principles, attributes and outputs. Principles are the fundamental concepts driving the OCTAVE evaluation process. Attributes are derived from principles and are the tangible elements, and outputs are the required results that must be achieved. There can be many methods to implement OCTAVE, but there is only one set of criteria with which all methods must be consistent. Organisations can develop methods that are consistent with the OCTAVE criteria or adopt any of the existing methodologies.

OCTAVE is led by a small, interdisciplinary team from within the organisation's personnel and focuses on critical assets and the risks to those assets. It is a comprehensive, systematic, context-driven and self-directed evaluation approach. Organisations that successfully apply this approach are consistently able to maintain a proactive security posture and are able to bring the organisational point of view to information security risk management activities.

THE EVOLUTION OF OCTAVE APPROACH

Three OCTAVE-consistent methodologies have been developed by SEI. The OCTAVE® Method was designed for large organisations (300 or more employees) and it was introduced in 1999, while OCTAVE-S was developed subsequently in 2003 for smaller organisations (100 employees or fewer).

In 2007, SEI introduced the next generation of OCTAVE methodology, called OCTAVE® Allegro. It aims to streamline and optimise the process of assessing information security risks so that organisations can obtain sufficient results with a small investment in time, people and other limited resources. The new method attempts to overcome limitations that have been experienced in deploying the first two methods and

the new challenges organisations face today in managing the change in the landscape of information security risks.

The OCTAVE approach has been evolving over the last nine years; a brief summary of its evolution is available in **figure 2**.

Figure 2—OCTAVE Evolution

Date	Publication
June 1999	OCTAVE Framework, Version 1.0
September 2001	OCTAVE Method, Version 2.0
December 2001	OCTAVE Criteria, Version 2.0
September 2003	OCTAVE-S, Version 0.9
March 2005	OCTAVE-S, Version 1.0
June 2007	OCTAVE Allegro, Version 1.0

OVERVIEW OF OCTAVE APPROACH AND METHODOLOGIES

OCTAVE is a risk-based strategic assessment and planning technique for information security. It is self-directed, meaning that people from within the organisation assume responsibility for setting the organisation's security strategy. The approach leverages people's knowledge of their organisation's security-related practices and processes to capture the current state of security practice within the organisation. Risks to the most critical assets are used to prioritise areas of improvement and set the security strategy for the organisation.

Unlike the typical technology-focused assessment that is targeted at technological risks and focused on tactical issues, OCTAVE is targeted at organisational risk and focused on strategic, practice-related issues. It is a flexible evaluation that can be tailored for most organisations.

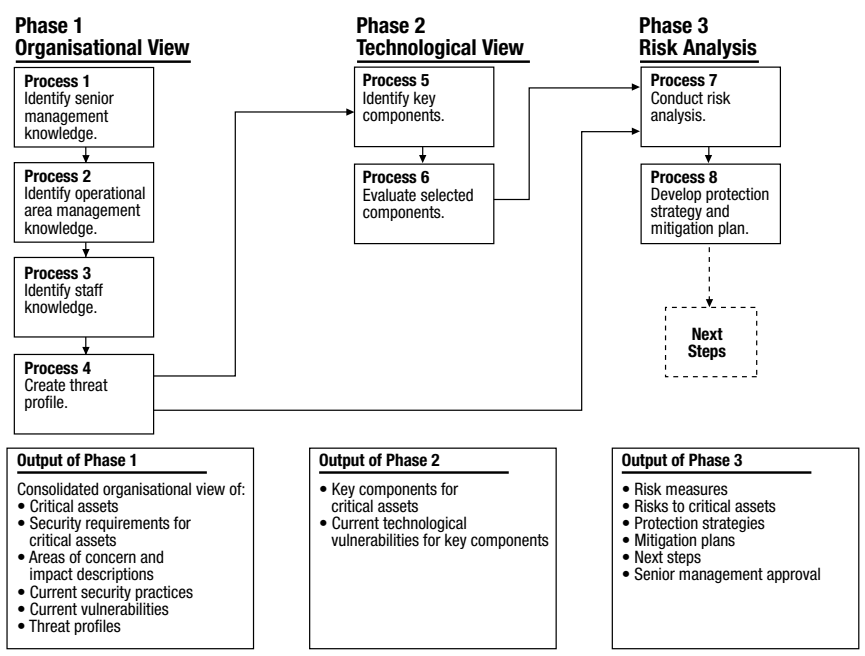
When applying OCTAVE, a small team of people from the operational or business units and the IT department works together to form the analysis team and addresses the security needs of the organisation. The analysis team:

- Identifies critical information assets
- Focuses risk analysis activities on these critical assets
- Considers the relationships amongst critical assets, the threats to these assets and the vulnerabilities (both organisational and technological) that can expose assets to threats
- Evaluates risks in operational context, i.e., how the critical assets are used to conduct the organisation's business and how they are at risk due to security threats and vulnerabilities
- Creates practice-based protection strategy for organisational improvement as well as risk mitigation plans to reduce the risk to the organisation's critical assets

The OCTAVE Method

The OCTAVE Method has been designed for large organisations having multi-layered hierarchy and maintaining their own computing infrastructure. The organisational, technological and analysis aspects of an information security risk evaluation are undertaken by a three-phased approach with eight processes (**figure 3**):

Figure 3—The OCTAVE Method



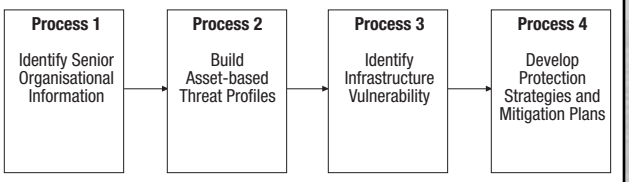
- **Phase 1: Build asset-based threat profiles (organisational evaluation)**—The analysis team determines critical assets and what is currently being done to protect them. The security requirements for each critical asset are then identified. Finally, the organisational vulnerabilities with the existing practices and the threat profile for each critical asset are established.
- **Phase 2: Identify infrastructure vulnerabilities (technological evaluation)**—The analysis team identifies network access paths and the classes of IT components related to each critical asset. The team then determines the extent to which each class of component is resistant to network attacks and establishes the technological vulnerabilities that expose the critical assets.
- **Phase 3: Develop security strategy and mitigation plans (strategy and plan development)**—The analysis team establishes risks to the organisation's critical assets based on analysis of the information gathered and decides what to do about them. The team creates a protection strategy for the organisation and mitigation plans to address identified risks. The team also determines the 'next steps' required for implementation and gains senior management's approval on the outcome of the whole process.

OCTAVE-S

OCTAVE-S is suited for smaller organisations with flat hierarchical structures. The method is similar and based on the three phases described in the OCTAVE Method; however, it is streamlined into just four processes (**figure 4**):

- **Process 1: Identify organisational information**—Processes one to three of the OCTAVE Method are performed here in just one step as small organisations are assumed to have a flat organisational hierarchy.
- **Process 2: Build asset-based threat profiles**—This is mapped to process 4 of the OCTAVE Method to identify current organisational vulnerabilities and the threats to each critical asset.
- **Process 3: Identify infrastructure vulnerabilities**—This is mapped to processes 5 and 6 of the OCTAVE Method. The analysis team examines the computing infrastructure to identify components related to the critical assets and establish technology vulnerabilities.
- **Process 4: Develop protection strategy and mitigation plan**—This is mapped to processes 7 and 8 of the OCTAVE Method.

Figure 4—OCTAVE-S (for small organisations)



OCTAVE ALLEGRO

Like the previous methods, OCTAVE Allegro is focused on risk assessment in an organisational context, but offers an alternative approach and attempts to improve an organisation's ability to perform risk assessment in a more efficient and effective manner. One of the insights acquired from earlier experiences has been the need to move to a more information-centric risk assessment.

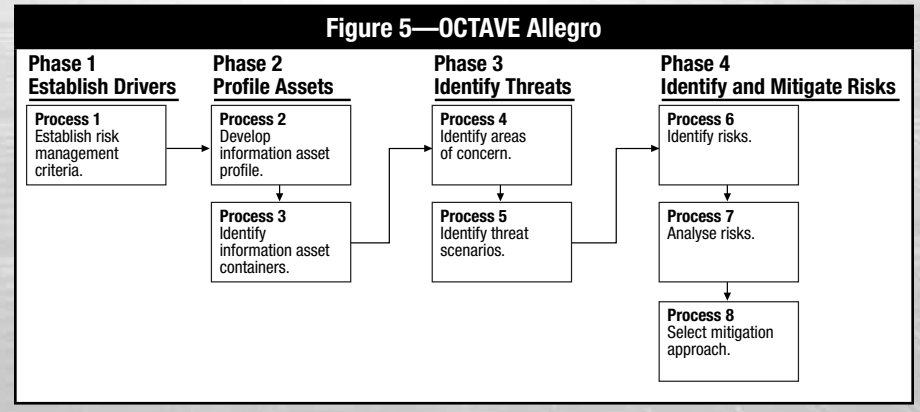
One of the guiding philosophies of Allegro has been that when information assets are the focus of the security risk assessment, all other related assets are considered 'information containers', storing, processing or transporting the information assets. Information containers can be people (since people access information and gain knowledge), objects (piece of paper) or technology (database). Thus, threats to information assets are analysed by considering where they live and effectively limiting the number and types of assets brought into the process.

Some key drivers that led SEI to formulating this new methodology include:

- Improving ease of use
- Refining the definition of assessment scope by introducing the container concept
- Streamlining data collection and threat identification processes
- Reducing training and knowledge requirements
- Improving institutionalisation and repeatability
- Reducing the technology view

The OCTAVE Allegro approach comprises eight processes and is organised into four phases (**figure 5**):

- **Phase 1: Establish drivers**—The organisation develops risk measurement criteria consistent with organisational drivers.
- **Phase 2: Profile assets**—Information assets that are determined to be critical are identified and profiled. This profiling process establishes clear boundaries for the asset; identifies its security requirements; and identifies all of the locations where the asset is stored, transported or processed.



- **Phase 3: Identify threats**—Threats to critical information assets are identified in the context of the locations where the asset is stored, transported or processed.
- **Phase 4: Identify and mitigate risks**—Risks to information assets are identified and analysed and the development of mitigation approaches commences.

HOW TO GET STARTED

Organisations looking forward to implementing a robust security risk assessment framework can adopt the OCTAVE approach. Adopting either the OCTAVE Method or OCTAVE-S to start is an excellent idea. Depending on the employee base and the organisational hierarchy structure, organisations need to choose between the two methodologies. Once the decision is made, senior management must identify an OCTAVE champion—the person who will steer the evaluation process and gain senior management sponsorship. Senior management will work with the champion to select and form a small interdisciplinary analysis team (three to five people) representing both IT and business domains. The analysis team, in turn, selects participants representing the entire organisation to conduct the knowledge elicitation workshops.

It is always advisable to have the analysis team trained on the OCTAVE approach. This training can be done through, for example, a case-study-based workshop, where attendees can become familiar with the process.

Key success factors for OCTAVE include:

- Getting senior management sponsorship
- Selecting a champion and an analysis team to lead the evaluation
- Selecting the scope of evaluation
- Selecting participants for evaluation activities

Senior management sponsorship is the top critical success factor for OCTAVE and requires:

- Visible and continued support of OCTAVE activities
- Active encouragement of staff participation
- Delegation of responsibility and authority to the analysis team
- Commitment to allocate resources
- Agreement to review results and decide on next steps

CONCLUSION

The OCTAVE approach essentially is driven by the OCTAVE criteria, which act as the foundation to the whole concept. The OCTAVE Method and OCTAVE-S have withstood the test of time and have been deployed by many organisations successfully. OCTAVE Allegro is SEI's new methodology, which attempts to simplify the process by streamlining the existing methods to improve effectiveness and efficiency. The streamlining process has eliminated and/or simplified many of the existing processes of the earlier methodologies. For OCTAVE Allegro to prove its robustness *vis-à-vis* the earlier methods and confirm its effectiveness, deployment in real-time scenarios is essential.

This article is an introduction to OCTAVE and meant to bring awareness among security professionals. To gain in-depth understanding of the OCTAVE approach, the OCTAVE criteria and the various methods of implementation, some form of formal training and practical exposure to implementation are recommended.

REFERENCES

Software Engineering Institute (SEI) at Carnegie Mellon University, OCTAVE, *www.cert.org/octave/*

Software Engineering Institute (SEI), OCTAVE training, *www.sei.cmu.edu/products/courses/cert/octave.html*