PECB

When Recognition Matters

WHITEPAPER

OCTAVE

RISK ASSESSMENT WITH OCTAVE

CONTENT

PRINCIPAL AUTHORS

Eric LACHAPELLE, PECB

Fitim RAMA, PECB

INTRODUCTION

As it can be seen from the Oxford dictionary's definition, risk will most probably bring us unpleasant or unwelcomed things which we don't want to happen to us, and still, organizations, governments and individuals continually expose themselves to the risk. So one may ask, why does this happen? It is simply because the reward for any work cannot come without taking chances, without taking risks. Moreover, managing risks is a key element to success, as Theodore Roosevelt once said: "Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you." Therefore, it is crucial for organizations, governments and individuals to make their best attempts to properly mitigate risks, rather than eliminate them, and as such to use risks only as a good opportunity and not eliminate it all.

In order to have a better risk management and mitigation roadmaps that would enable organizations to seize opportunities and achieve strategic goals, many organizations have established robust information security control frameworks that would serve as an answer. One such framework is the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) approach that is developed by the Software Engineering Institute (SEI) in order to address the information security compliance challenges faced by many organizations.

OCTAVE methodologies were merely created to tackle the information security challenges faced by the U.S. Department of Defense (DoD), but as it has shown its effectiveness, now this methodology is open for public. The main aim of OCTAVE is to help organizations ensure that their goals and objectives are connected with their information security activities.

ABOUT OCTAVE

OCTAVE is a risk assessment methodology to identify, manage and evaluate information security risks. This methodology serves to help an organization to:

- develop qualitative risk evaluation criteria that describe the organization's operational risk tolerances
- identify assets that are important to the mission of the organization
- identify vulnerabilities and threats to those assets
- determine and evaluate the potential consequences to the organization if threats are realized
- initiate continuous improvement actions to mitigate risks

OCTAVE methodology is primarily directed toward individuals who are responsible for managing an organization's operational risks. This can include personnel in an organization's business units, persons involved in information security or conformity within an organization, risk managers, information technology department, and all staff participating in the activities of risk assessment with the OCTAVE method.

This framework has been present in the market since 1999, and since then, many updates have been made to this approach.

HISTORY

Date	Title
September 1999	OCTAVE Framework, v1.0
September 2001	OCTAVE Framework, v2.0
December 2001	OCTAVE Criteria, v2.0
September 2003	OCTAVE-S, v0.9
March 2005	OCTAVE-S, v1.0
June 2007	OCTAVE Allegro, v1.0

In response to continuous issues about risk management, especially risk assessment, SEI developed the first OCTAVE Framework approach in 1999. This framework was intended merely for large corporations with more than 300 employees which have multi-layered hierarchy and are responsible for their own software infrastructure. The evaluation criteria using this framework are based by a three-phased approach that includes Organizational View, Technological View, and Risk Analysis.

In 2003, the update of the original framework was developed and named OCTAVE-S approach. This approach was intended for small organizations with less than 100 employees that have flexible hierarchy and more specialized team members. The three-phased approach is used in this approach as well, and is dedicated to small teams within organizations that would deal with this approach.

Finally in 2007, the Computer Emergency Response Team (CERT), a program of SEI, has developed the latest update of OCTAVE named OCTAVE Allegro approach. It is intended to all organizations which focus primarily on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are exposed to threats, vulnerabilities, and disruptions as a result. Allegro version has reduced a lot of requirements and process to make it easier to use. In other words, Allegro has shifted the OCTAVE approach from a technology asset-centric, to an information asset-centric risk assessment.

OCTAVE ALLEGRO

OCTAVE Allegro is a methodology to restructure and optimize the measurement process of information security risks in order for an organization to achieve the necessary results with a small investment in time, people and other resources. Through this methodology, organizations will tend to consider people, technology, and facilities in regards to their correlation with information, business processes, and the services they support.

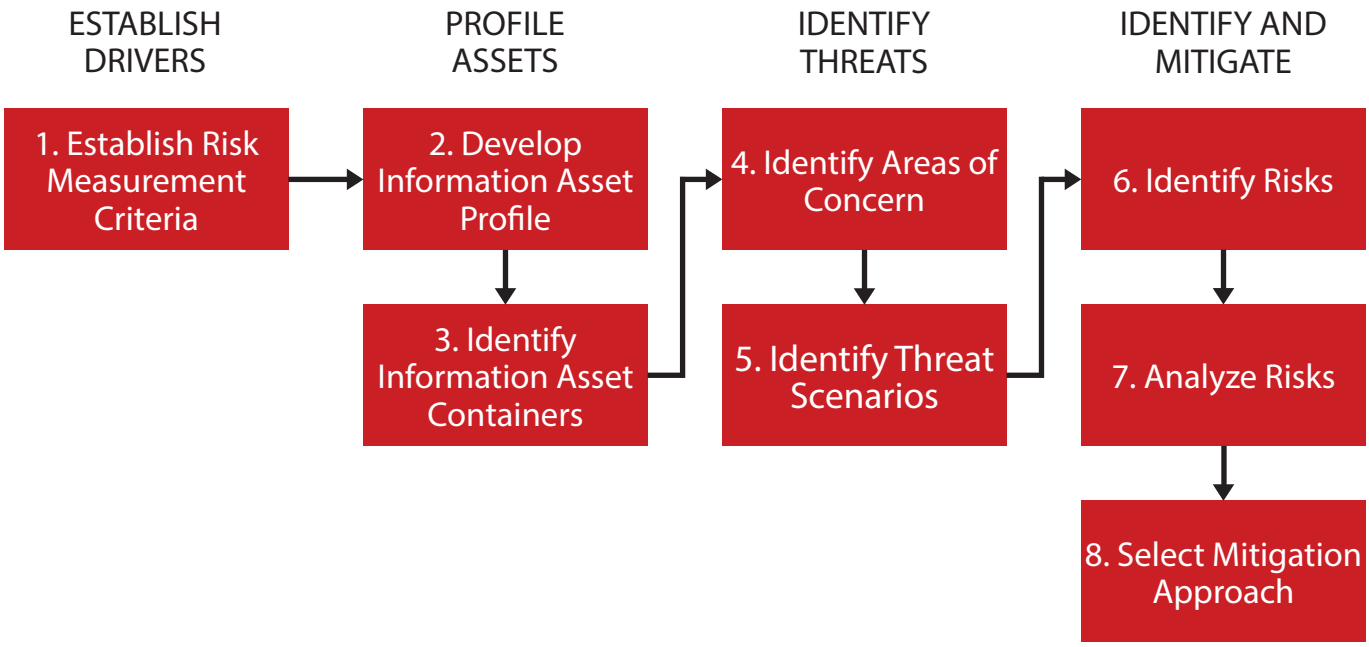
OCTAVE Allegro defines the critical components of a systematic information security risk assessment framework by referring to risk with their confidentiality, integrity and availability of assets. Through this approach, organizations will no longer have the problem of defining critical assets from which the risk may come, that has not been clearly defined with other methodologies. Allegro gives clear instructions how to identify critical assets in the same time connecting organizational goals and objectives to information security goals and objectives. This means that information security teams will work together with the operational teams to address the information security needs in order to properly protect critical data. Thus, critical decisions will no longer be made from IT departments, but rather from a conjunction of involving departments.

"The first step in the risk management process is to acknowledge the reality of risk denial is a common tactic that substitutes deliberate ignorance for thoughtful planning."
– Charles Tremper

Organizations that use OCTAVE Allegro methodology will be required to information asset profiles to have better and unambiguous definitions for asset boundaries. These profiles will enable organizations to define security requirements, assign their ownership and to set their value. Once the profiles are created, they can be updated and modified for future assessments in regards to organization's needs.

ROADMAP STEPS

To make the whole process easier to be used, Allegro has reduced a lot of requirements and complications that were included in the previous versions of OCTAVE. Allegro rather contains an eight-step process divided in four categories that enables organizations to identify, analyze, assess, and mitigate potential risks. The relationship between the activity areas and the actual steps of the methodology are shown in the chart below.



I. ESTABLISH DRIVERS – This area contains only the first step through which the organization develops risk measurement criteria that are consistent with organizational drivers. These drivers will be used to evaluate the risk effects to an organization's mission and its objectives.

II. PROFILE ASSETS – This area contains step 2 and 3, through which the information asset profiles are created. After the profiles are identified and created, the assets' containers are identified and the profile for each asset is captured on a single worksheet. A profile represents an information asset that describes its unique features, qualities, characteristics, and value.

III. IDENTIFY THREATS – This area includes steps 4 and 5 where threats to the information assets are identified and documented through a structured process. In this category, areas of concern present real-world scenarios that can happen to organizations, and threat scenarios that contain additional threats are identified.

IV. IDENTIFY AND MITIGATE RISKS – This is the last stage of risk assessment. In this category risks are identified and analyzed based on threat information, and mitigation strategies developed to address those risks. In this step, the threats identified in the previous category will be analyzed and mitigated.

What makes this process unique is that the outputs from each step in the process are seized on worksheets which are then used as inputs to the next step in the process.

HOW TO USE OCTAVE?

Information security community has accepted OCTAVE methodologies as one "de facto" standard to conduct risk assessments. To effectively manage operational risk, OCTAVE methodologies are always a clever choice for every organization that wants to implement a successful risk assessment strategy. To properly implement the OCTAVE methodologies, organizations need to take two major steps: preparing for OCTAVE, and performing an assessment.

PREPARING FOR OCTAVE

One of the most critical factors in successfully performing OCTAVE methodologies is getting the sponsorship from the organization's top management. Senior management should be convinced that OCTAVE is what an organization needs, and they will also require actions from the implementer to show continuous improvement such as:

- to support OCTAVE activities
- to encourage the staff participation
- to delegate roles and responsibilities to the analysis team
- commitment to allocate resources
- to present ideas how to continually improve

After the approval from the senior management is received, organizational resources should be allocated in order to implement OCTAVE. A team ranging from one to seven professionals (depending on organization's hierarchical structure) should be created as the analysis team that should support the implementation. Furthermore, best industry practice has shown that organizations whose assessment team has received training have managed to successfully implement OCTAVE methodologies.

PERFORMING AN ASSESSMENT

The OCTAVE Allegro methodology developed by CERT includes guidance, worksheets, and questionnaires that are necessary to perform an OCTAVE Allegro assessment. Organizations wanting to perform an assessment with OCTAVE will have to go through all the materials that will prepare and help them to successfully implement the assessment.

It is very important that before the judgment of the assessment team, organizations should identify and select information assets that will be the basis of the implementation, set the risk measurement criteria that reflect the management's risk tolerance, and repeat an assessment every time there is a significant change in the information asset.

BENEFITS OF RISK ASSESSMENT WITH OCTAVE

OCTAVE methodologies bring a unique perspective that involves collaboration between risk identification, assessment and mitigation. By bringing together the importance and sensitivity of data to the IT teams, and the proper communication to the top management, OCTAVE provides the "organizational connection" within companies that before has been absent. As a result of the collaborations, many gaps that reduce the ability to mitigate risks are exposed, such as gaps in organizational communication and gaps in practice. By exposing these gaps, organizations will have a diversity of understanding, opinions and experiences which strengthen the quality of the risk assessment.

Other benefits of using OCTAVE methodologies for risk assessment are listed below:

- OCTAVE methodologies have highly qualitative considerations and descriptions against risk assessment methodologies, rather than quantitative ones.
- OCTAVE brings a formal and systematic process to analyze the risks it faces which is easier for organizations to adapt.
- A formal risk assessment process enables organizations to implement controls only where they are needed, rather than opinion based controls. Moreover, such process is more cost-effective since only risks that are out of the risk measurement criteria (unacceptable risks) will be addressed and fewer expenses in incidents will occur.
- Allows senior management to perform due diligence and understand the actual state of the organization whilst being informed about the whole assessment strategy as well.
- Helps organizations in shifting the organizational culture into a more risk-based and qualitative culture.

CONCLUSION

In general, every organization needs to be in control of the various risks that they face in different circumstances. Identifying, analyzing and mitigating risks have become crucial to a better risk management that all organizations must chase in order to maintain all stakeholders satisfied.

Through OCTAVE methodologies, such goals are achievable by mainly focusing on critical assets and the risks of those assets. OCTAVE methodologies are very practical since they can be led by small teams from within organization's staff, and their formal systematic, context-driven and self-directed approach makes the whole process easy to operate.

Organizations that have taken this approach have successfully managed to maintain a proactive security posture and are able to bring the organizational perspective to information security risk management activities. Moreover, using this approach, organizations have managed to succeed in mitigating risks and lowering costs of risk management as well.

Professional Evaluation and Certification Board (PECB) is a certification body for various standards including OCTAVE methodologies. PECB offers individual examination and certification services for professionals wanting to obtain the expertise to master risk assessment with OCTAVE Allegro approach. Our aim is to provide the best industry practices to our clients by developing, maintaining, and continually improving high quality recognized certification programs.

PECB has earned a reputation for integrity, value and best practice by providing this assurance through the evaluation and certification of professionals against rigorous, internationally recognized competence requirements.

This whitepaper is intended for risk and security professionals by providing an introduction to risk assessment with OCTAVE methodologies. To gain a comprehensive understanding of the OCTAVE approach, criteria and various methods of implementation, some forms of formal training and practical exposure to implementation are recommended. For further information about OCTAVE training, please don't hesitate to contact us at: training@pecb.com.

STEPS FOR OBTAINING A PECB CERTIFICATION

To ensure that organizations or individuals achieve planned and desired results, the following steps will serve as guidance on how to become PECB Certified Lead Privacy Implementer.

For organizations:	For individuals:
1. Implement the privacy framework	1. Participate in the training course
2. Perform internal audit and reviews	2. Register for the certification
3. Select preferred certification body	3. Sit for the certificatio exam
4. Perform a pres-assessment audit (optional)	4. Apply for the certification scheme upon successfull exam completion and fulfillment of certification requirements (stated on our website)
5.Perform the stage 1 audit	5. Obtain certification
6. Perform the stage 2 audit (on-site)	
7. Perform a follow	
8. Register the certification	
9. Assure continual improvement by conducting surveillance audits	

For further details relating the types of trainings and certifications that PECB offers, please visit our website: www.pecb.com

PECB

+1-844-426-7322

customer@pecb.com

Customer Service

www.pecb.com