CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Security Risk Assessment Using OCTAVE® Allegro

Key Message: OCTAVE Allegro provides a streamlined assessment method that focuses on risks to information used by critical business services.

Executive Summary

CERT's OCTAVE information security risk assessment method has been in development and use for upwards of ten years. Based on field work and lessons learned, CERT has developed a more streamlined, easier-to-use assessment method. Allegro captures senior leadership risk assumptions and evaluation criteria such as reputation and customer confidence. This method is composed of four phases and eight steps that are documented in a publicly available technical report.

In this podcast, Lisa Young, a senior member of CERT's Survivable Enterprise Management Team, discusses Allegro and how it has evolved from CERT's original OCTAVE work.

PART 1: INTRODUCTION TO ALLEGRO: RATIONALE AND APPLICATION

Background

CERT's OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method was originally developed almost ten years ago to help large, complex organizations evaluate their information security risks.

Allegro was developed to reflect OCTAVE lessons learned and provide a more streamlined method that organizations can implement faster and without extensive training.

Allegro is focused on information risk and how best to protect information (such as personally identifiable information and customer and financial databases).

Protecting Information

In Allegro, one characteristic of information is where it lives, referred to as "containers." Most security controls are applied at the container level.

Asking people where information lives in their networks and their organizations (that is, the containers) makes protecting information easier to understand.

Roles Involved in Conducting an Allegro Assessment

Given Allegro is an information security risk assessment, it is best used by information security (IS) staff.

That said, Allegro can assist in aligning IS with other business roles (such as business continuity) by making business risk assumptions more explicit to operational staff.

Anyone who is an information owner, custodian, or steward, or has concerns about the controls responsible for protecting their information, could initiate an Allegro assessment. This includes business owners.

Risk Evaluation Criteria

Allegro risk evaluation criteria can help harmonize the risk assumptions used by localized risk assessments (information security, audit controls, physical security).

If the risk evaluation criteria are based on what's important to the business and are communicated, then everyone can operate from the same page.

Allegro evaluation criteria categories include:

- reputation
- customer confidence
- life, health, safety
- fines and legal penalties resulting from non-compliance
- financial
- productivity

Benefits of Allegro

Allegro has been applied with equal success as a top-down and as a grass roots effort. Open communication fosters a common understanding of risks which is one of the key benefits.

Governance is strengthened through leaders communicating their risk assumptions.

The results of an assessment such as Allegro can be used to help satisfy compliance requirements

---

PART 2: ALLEGRO'S EIGHT STEPS, AND GETTING STARTED

Components of Allegro

Allegro is composed of four phases and eight steps which are described in the SEI Technical *Report Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*.

The eight steps are:

1. Establish risk measurement criteria which help ensure that risk assumptions are aligned with business objectives.
2. Develop an information asset profile.
3. Identify information asset containers (people, paper, servers, other media).
4. Identify areas of concern (vulnerability).
5. Identify threat scenarios.
6. Identify risks given asset criticality, vulnerability, and threat.
7. Analyze risks.
8. Select mitigation approaches.

Step 1 is the most important as it establishes the business criteria against which risks are evaluated. Criteria can include such factors as reputation, customer confidence, and productivity.

You can assign numbers to criteria based on impact or loss including fines, legal penalties, life, health, and safety.

Allegro evaluation criteria provide a standardized way to uncover what is most important to your business.

Using Allegro

Allegro could be used to evaluate the risks and opportunities when looking at a merger or acquisition, or when offering a new product or service.

Allegro questionnaires are filled out by people in a wide range of roles across the organization. Results provide a useful picture of how issues are viewed by these various roles.

A risk assessment like Allegro only provides a picture at a point in time, so it should not take a great deal of time – 2-3 days to 2-3 weeks depending on the scope.

Assessments that are smaller, more frequent, with a narrower scope, and conducted on a regular basis are more useful for informing business risk decisions.

Observing the changes and trends from one assessment to another can provide useful insight and metrics. Assessment results can help inform which metrics are worth collecting.

Getting Started

Business leaders need to communicate their risk assumptions to business owners, application owners, and operational staff.

Most organizations offer 10-12 key services. Connecting business objectives to business units to services to assets is a means for identifying which services are most critical.

The assets that support critical services are the ones that most likely will benefit from additional risk analysis.

The OCTAVE Allegro technical report [Caralli 2007] provides all of the information, forms, and documents necessary to get started.

Resources

CERT's OCTAVE web site

[Caralli 2007] Caralli, Richard; Stevens, James; Young, Lisa; Wilson, William. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. CMU/SEI-2007-TR-012. Carnegie Mellon University, Software Engineering Institute, May 2007.