Software Engineering Institute

Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

Richard A. Caralli
James F. Stevens
Lisa R. Young
William R. Wilson

May 2007

TECHNICAL REPORT
CMU/SEI-2007-TR-012
ESC-TR-2007-012

CERT Program

Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work is supported, in part, by ictQATAR, through a contract with Carnegie Mellon University.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Figures

List of Tables

Acknowledgements

The authors of this report would like to acknowledge the many internal and external collaborators whose support, input, skills, and guidance have made this work possible.

First, the authors would like to thank Chris Alberts and Audrey Dorofee for their previous efforts in developing the OCTAVE method and OCTAVE-S. Without their hard work, there would be no basis from which to develop and transition the OCTAVE Allegro methodology.

The authors would also like to thank members of the CERT® Survivable Enterprise Management (SEM) team who have contributed to the evolution of OCTAVE since it was introduced. In particular, the authors would like to thank Bradford Willke and Sam Merrell for their review and the constructive feedback they provided on this document and the OCTAVE Allegro method. The authors would also like to acknowledge the support and contributions of William Wilson. As the technical manager for the SEM team, Bill has been the champion for the OCTAVE work since its inception.

The development, piloting, and codification of the OCTAVE Allegro method would not have been possible without the generous input, collaboration, and determination of the employees of Clark County, Nevada. The CERT Program has developed a special relationship with this organization over the past few years, and their willingness to try new methods, provide us with useful feedback, and help to refine techniques that can be used by many organizations is unparalleled. In particular, we would like to thank Michael Smith, IT Security Administrator, who has been a champion for the development and institutionalization of OCTAVE Allegro at Clark County and who has consistently strived to improve the organization's security and resiliency. We have been fortunate to work with him in a challenging and rewarding environment such as Clark County.

The authors would like to thank ictQATAR and Q-CERT for their support in the refinement and transition of the OCTAVE Allegro methodology.

We would also like to thank Jonathan Coleman, Visiting Scientist in the CERT Program, for his expert review and comments. As one of the original users of the OCTAVE method, Jonathan has extensive real-world knowledge that has been very valuable to us in developing OCTAVE Allegro.

Last but certainly not least, the authors would like to thank Pamela Curtis, who consistently provides the SEM team with high-quality editing services and who is willing to teach us rather than to correct us. Through her work, she has had a profound effect on our writing and editing skills.

Abstract

This technical report introduces the next generation of the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology, OCTAVE Allegro. OCTAVE Allegro is a methodology to streamline and optimize the process of assessing information security risks so that an organization can obtain sufficient results with a small investment in time, people, and other limited resources. It leads the organization to consider people, technology, and facilities in the context of their relationship to information and the business processes and services they support. This report highlights the design considerations and requirements for OCTAVE Allegro based on field experience with existing OCTAVE methods and provides guidance, worksheets, and examples that an organization can use to begin performing OCTAVE Allegro-based risk assessments.

1 Introduction

One of the primary goals of the CERT® Survivable Enterprise Management team is to help organizations ensure that their information security activities are aligned with their organizational goals and objectives. The OCTAVE® method—Operationally Critical Threat, Asset, and Vulnerability Evaluation—was created by this team to help organizations perform information security risk assessments in context with the operational and strategic drivers that they rely on to meet their mission.

This technical report introduces the next generation of the OCTAVE method, OCTAVE Allegro. Together with its predecessors OCTAVE and OCTAVE-S, OCTAVE Allegro forms a family of OCTAVE assessments. Like OCTAVE and OCTAVE-S, OCTAVE Allegro is focused on positioning risk assessment in the proper organizational context, but it offers an alternative approach that is specifically aimed at information assets and their resiliency. This alternative approach can improve an organization's ability to position and perform the risk assessment in a way that provides meaningful results in a more efficient and effective manner.

1.1 HISTORY OF OCTAVE

OCTAVE is a methodology for identifying and evaluating information security risks. It is intended 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

The conceptual framework that formed the basis of the original OCTAVE approach was published by the Software Engineering Institute (SEI) at Carnegie Mellon University in 1999 [Alberts 1999]. Working with the Telemedicine and Advanced Technology Research Center (TATRC), the SEI developed the OCTAVE method to address the security compliance challenges faced by the U. S. Department of Defense (DoD) in addressing the provisions of the Health Insurance Portability and Accountability Act (HIPAA)[1] for the privacy and security of personal health.

Since it was first released in September 1999, there have been a number of updates and changes to the OCTAVE methodology. Table 1 provides a brief timeline of significant OCTAVE-related events.

® CERT and OCTAVE are registered in the U. S. Patent and Trademark Office by Carnegie Mellon University.

[1] The Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 101-191) was enacted on August 21, 1996.

Table 1: OCTAVE Timeline

Date	Publication Title
September 1999	OCTAVE Framework, Version 1.0
September 2001	OCTAVE Framework, Version 2.0
December 2001	OCTAVE Criteria, Version 2.0
September 2003	OCTAVE-S v0.9
March 2005	OCTAVE-S v1.0
June 2007	Introduction of OCTAVE Allegro v1.0

1.2 OVERVIEW OF EXISTING OCTAVE METHODOLOGIES

With the publication of this technical report, there are now three distinctive OCTAVE methodologies available for public use: the OCTAVE method, OCTAVE-S, and OCTAVE Allegro. The introduction of OCTAVE Allegro is not intended to supplant previous OCTAVE methodologies. OCTAVE Allegro is a variant that provides a streamlined process focused on information assets. However, each OCTAVE method has broad applicability, and users of these methods can select the approach that best fits their particular information security risk assessment needs.

For reference, the following sections provide a brief overview of each of the OCTAVE methodologies.

1.2.1 The OCTAVE Method

The OCTAVE method[2] was the first OCTAVE-consistent[3] methodology to be introduced [Alberts 2001]. The approach is defined by a method implementation guide (procedures, guidance, worksheets, information catalogs) and training. The method is performed in a series of workshops conducted and facilitated by an interdisciplinary analysis team drawn from business units throughout the organization (e.g. senior management, operational area managers, and staff) and members of the IT department [Alberts 2002].

The intended audience for the OCTAVE method is large organizations with 300 or more employees. More specifically, it was designed for organizations that

- have a multi-layered hierarchy
- maintain their own computing infrastructure
- have the ability to run vulnerability evaluation tools
- have the ability to interpret the results of vulnerability evaluations

[2] The OCTAVE method is fully described by the *OCTAVE Method Implementation Guide v2.0* and is available for downloading at http://www.cert.org/octave/omig.html.

[3] The essential elements, or requirements, of the OCTAVE approach are embodied in a set of criteria. A method that is consistent with this set of criteria is considered to be OCTAVE consistent. Both the OCTAVE method and OCTAVE-S are OCTAVE-consistent methodologies.

The method was also designed to allow for tailoring by organizations adopting it. Most organizations that have utilized the OCTAVE method tailor the approach to suit their unique operating environments.

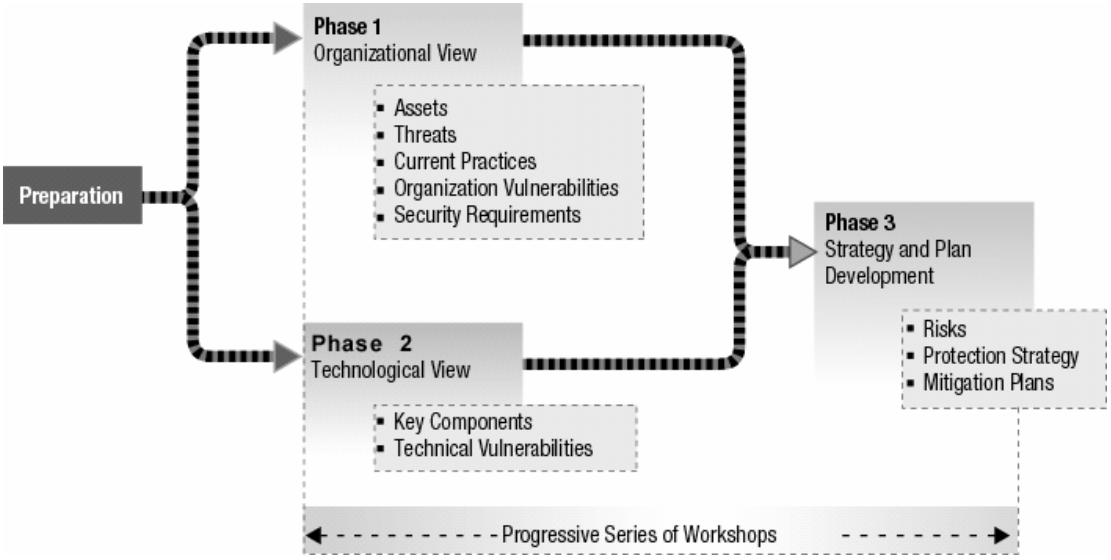


Figure 1: Three OCTAVE Method Phases

The OCTAVE method is performed in three phases. In phase 1, the analysis team identifies important information-related assets and the current protection strategy for those assets. The team then determines which of the identified assets are most critical to the organization's success, documents their security requirements, and identifies threats that can interfere with meeting those requirements. In phase 2, the analysis team performs an evaluation of the information infrastructure to supplement the threat analysis performed in phase 1 and to inform mitigation decisions in phase 3. Finally, in phase 3, the analysis team performs risk identification activities and develops a risk mitigation plan for the critical assets [Alberts 2002].

1.2.2 OCTAVE-S

The development of OCTAVE-S was supported by the Technology Insertion, Demonstration, and Evaluation (TIDE) program at the SEI,[4] with the goal of bringing an OCTAVE-based approach to small manufacturing organizations. The most current version of the OCTAVE-S approach, version 1.0, is specifically designed for organizations of about 100 people or less.

Consistent with the OCTAVE criteria, the OCTAVE-S approach consists of three similar phases. However, OCTAVE-S is performed by an analysis team that has extensive knowledge of the organization. Thus, OCTAVE-S does not rely on formal knowledge elicitation workshops to gather information because it is assumed that the analysis team (typically consisting of three to five people) has working knowledge of the important information-related assets, security requirements, threats, and security practices of the organization.

[4] More information on the TIDE program can be found on the SEI website at http://www.sei.cmu.edu/tide.

Another significant difference in OCTAVE-S is that it is more structured than the OCTAVE method. Security concepts are embedded in the OCTAVE-S worksheets and guidance, allowing less experienced risk and security practitioners to address a broad range of risks with which they may not have familiarity. A final distinguishing feature of OCTAVE-S is that it requires a less extensive examination of an organization's information infrastructure. Because small organizations may not have the resources to obtain and execute vulnerability tools, OCTAVE-S was designed to include a limited examination of infrastructure risks so as to remove a potential barrier to adoption.

1.2.3 OCTAVE Allegro

allegro: (al-leg-ro) *adv.* In a quick and lively tempo.[5]

The OCTAVE Allegro approach being introduced in this technical report is designed to allow broad assessment of an organization's operational risk environment with the goal of producing more robust results without the need for extensive risk assessment knowledge. This approach differs from previous OCTAVE approaches by focusing 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. Like previous methods, OCTAVE Allegro can be performed in a workshop-style, collaborative setting and is supported with guidance, worksheets, and questionnaires, which are included in the appendices of this document. However, OCTAVE Allegro is also well suited for use by individuals who want to perform risk assessment without extensive organizational involvement, expertise, or input.

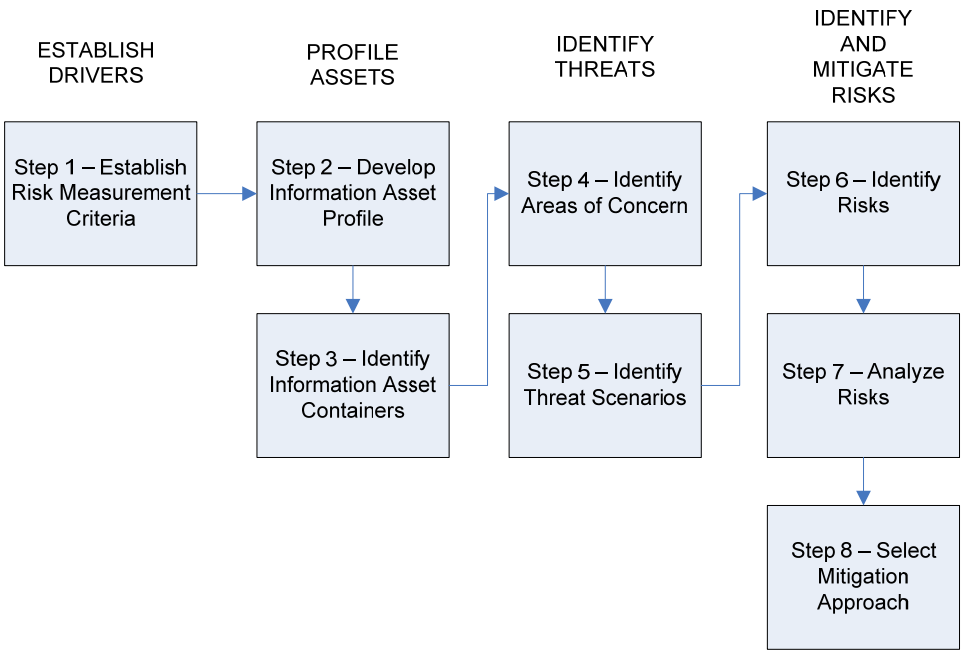


Figure 2: OCTAVE Allegro Roadmap

[5] WordNet 2.1 Princeton University. March 2, 2007. Dictionary.com: http://dictionary.reference.com/browse/allegro

The OCTAVE Allegro approach consists of eight steps that are organized into four phases, as illustrated in Figure 2. In phase 1, the organization develops risk measurement criteria consistent with organizational drivers. During the second phase, information assets that are determined to be critical are 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. In phase 3, threats to the information asset are identified in the context of the locations where the asset is stored, transported, or processed. In the final phase, risks to information assets are identified and analyzed and the development of mitigation approaches is commenced.

1.3 SCOPE OF THIS REPORT

This technical report intends to accomplish several objectives:

- Identify the current limitations of the existing OCTAVE methods for application in a rapidly evolving operational risk management environment.
- Highlight the requirements for evolving the current OCTAVE reference body of knowledge into a more efficient and effective risk assessment methodology.
- Provide a view into future evolution of the OCTAVE method and OCTAVE-related tools, techniques, methodologies, and training.
- Introduce the OCTAVE Allegro methodology guidance and worksheets.

1.4 STRUCTURE OF THIS REPORT

The sections of this document are arranged around the report objectives as follows:

- Introduction and background – Section 1
- The evolution of the OCTAVE method – Section 2
- Introducing the OCTAVE Allegro method – Section 3
- Using OCTAVE Allegro – Section 4
- Future OCTAVE direction and research – Section 5
- Guidance for using the OCTAVE Allegro method – Appendix A
- Worksheets for using the OCTAVE Allegro method – Appendix B
- Questionnaires for identifying threats in OCTAVE Allegro – Appendix C
- OCTAVE Allegro example – Appendix D

1.5 INTENDED AUDIENCE

The content of this technical report 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, information technology department, or in specialty areas such as compliance or audit. Anyone who has familiarity with the OCTAVE method and OCTAVE-S will be easily able to understand the concepts in this technical report and make immediate use of the OCTAVE Allegro methodology.

For those who have limited experience with OCTAVE or risk assessment in general, it is recommended that they obtain a general understanding of OCTAVE by reviewing introductory material on the methodology on the CERT Web site (http://www.cert.org/).

2 Evolving the OCTAVE Method

2.1 EXPERIENCES WITH OCTAVE

There has been a significant diversity in the type, size, and business markets of the organizations that have successfully used existing OCTAVE methods [Woody 2006]. They have found success in applying, tailoring, and institutionalizing the OCTAVE method, either in its original form or in the streamlined OCTAVE-S, to fit their risk assessment philosophy, organizational structure, and culture. The ability to connect organizational goals and objectives to information security goals and objectives is the primary benefit of OCTAVE. Organizations that successfully apply this approach are consistently able to bring an organizational and operational point of view to information security risk management activities, allowing them to evolve from vulnerability management and reactive activities toward information security risk management.

The collaborative aspect of the OCTAVE method provides an interdisciplinary perspective to the risk identification, assessment, and mitigation processes. The workshop-based data collection and subsequent analysis processes of existing OCTAVE methods brings together disparate groups in the organization under a common purpose. As a result of this collaboration, the organization exposes issues that limit its ability to effectively identify and mitigate risks such as

- gaps in organizational communications channels
- varied levels of understanding and communication of policies across organizational levels
- gaps in practices and their intended effects

The collaborative aspect of the method also ensures a diversity of understanding, experience, and opinions, which further strengthens the breadth and quality of the risk assessment and risk mitigation activities.

2.2 MOTIVATION FOR A NEW APPROACH

While organizations continue to successfully deploy and institutionalize OCTAVE and OCTAVE-S, a significant time period has passed since the OCTAVE method and OCTAVE-S were introduced. The landscape of information security risks that must be managed by organizations and the capabilities of organizations to manage those risks have changed considerably since those methods were introduced. In addition, there exists a significant body of knowledge acquired through applying and teaching OCTAVE and observing other organizations using the method over the last eight years that forms the basis for improvement.

One of the insights acquired through these experiences is the need to move to a more information-centric risk assessment. When information assets are the focus of the information security assessment, all other assets can be easily brought into the process as *containers* where information assets are stored, transported, or processed [Stevens 2005]. A container can be a person (since people can store information as knowledge, transport information by communicating, or process information by thinking and acting), an object (e.g., a piece of paper), or a technology (e.g., a da-

tabase). Thus, threats to information assets are identified and examined through the consideration of where they live, which effectively limits the number and types of assets brought into the process. Moreover, focusing on information assets effectively limits the amount of information that must be gathered, processed, organized, analyzed, and understood to perform a risk assessment.

Finally, given the size and complexity of the OCTAVE method, it is easy to imagine that some organizations have significant challenges in embracing and using the OCTAVE approaches. Absorbing hundreds of pages of process documentation, understanding the accompanying worksheets and how to use them, and collecting and organizing the needed data can be challenging tasks. Upon reflection, the sheer volume of data collection is an impediment for some organizations in moving forward with performing the tasks of analyzing and mitigating risks. A streamlined process that reduces ambiguity and is more structured may be more applicable to the needs of organizations that find the existing OCTAVE methods too cumbersome to use.

Reflecting on the knowledge and insights acquired since the first OCTAVE method was introduced indicates that an updated approach to performing information security risk assessment is required. This experience forms the basis for establishing a set of requirements that will evolve the OCTAVE method to meet changing organizational needs and more complex operational risk environments.

In the following sections, specific improvements that have been incorporated into OCTAVE Allegro are identified and discussed in the context of how they improve the overall usability of the risk assessment process.

2.3 GENERAL REQUIREMENTS FOR OCTAVE ALLEGRO

Requirements serve not only to describe what to build and why it is being built but also provide a way to measure whether an activity has been successful. The first step in developing an updated OCTAVE approach is to capture a set of design requirements (derived from field use, observation, and classroom experience). These requirements include

- improving ease of use
- refining the definition of assessment scope
- reducing training and knowledge requirements
- reducing resource commitments
- encouraging institutionalization and repeatability
- producing consistent and comparable results across the enterprise
- facilitating the development of a risk assessment core competency
- supporting enterprise compliance requirements

Each of these general requirements is discussed in the following sections.

2.3.1 Improving Ease of Use

The first requirement for an improved method is that it be easy to use, as defined across several dimensions. These dimensions include

- minimizing the size and complexity of processes that must be learned and applied
- reducing the amount of data that must be collected and managed throughout the process
- controlling the number and variety of worksheets that must be completed
- focusing the process on a definable and manageable information asset scope

Reducing the inherent challenges imposed by the mechanics of existing OCTAVE methods ensures that the process is focused on the risk assessment activity and the identification and analysis of information security risks rather than satisfying an extensive set of guidelines and activities.

2.3.2 Refining Asset Scope

Accurately defining the scope of a risk assessment not only improves the results of the assessment but results in potentially less overall effort. Thus, a primary requirement for OCTAVE Allegro is to allow users to focus on the assets that are most important by ensuring they are selected for review through a systematic and consistent process. By focusing on information assets exclusively and other assets such as people, technology, and facilities through association with information assets, the organization has a better opportunity to define a manageable scope from the outset, thereby potentially reducing the effort required for threat identification, analysis, and mitigation planning.

2.3.3 Reducing Knowledge and Training Requirements

An updated OCTAVE approach should lend itself more readily to institutionalization. One way that this can be achieved is by reducing the required levels of knowledge and training necessary for performing effective risk assessment. Minimizing the amount of risk management and information technology knowledge required effectively increases the pool of personnel who can participate in the assessment process with little investment in training and mentoring. Reduced knowledge and training requirements not only lower overhead costs associated with risk assessment but increase the potential institutionalization of the methodology throughout the organization. In addition, in the case of regulatory compliance, the ability to train more people to perform risk assessment effectively improves the organization's overall capability for managing compliance.

2.3.4 Reducing Resource Commitments

Risk assessment is an essential organizational activity, but a resource-intensive assessment method may not be cost effective enough to justify the investment of people and other resources. To optimize the use of resources, an updated OCTAVE approach should

- be less difficult to use (by reducing required process activities to only those that are meaningful)
- require less data manipulation (by improving process flow, the staging of activities, and the amount and type of data collected)
- streamline processes for identifying and mitigating risk (by focusing on information assets exclusively, improving threat identification methods, and improving the way in which risks are documented and analyzed)

- improve documentation and organization of data (through efficient and effective design of worksheets and reducing the amount of data carry-forward)
- be self-correcting (by building in checks and balances that allow users to realize they are off course before they expend considerable resources)

2.3.5 Encouraging Institutionalization and Repeatability

To be effective, risk assessment activities must be part of a larger continuous risk management process. Properly positioned, risk assessment serves as the diagnostic component of continuous risk management—the organization uses risk assessment to determine the status of controls that it has implemented to manage information security and prepares and implements plans to close any identified gaps. Thus, risk assessment not only helps the organization to establish a baseline from which measurement can occur, but it also helps the organization keep pulse on the current status of its security effectiveness through repeated and consistent use over time.

To encourage the use of risk assessment as a tool in a continuous risk management process, an updated OCTAVE method must be accessible to as many users in the organization as possible, require low levels of effort and investment, and aim to produce consistently meaningful results.

2.3.6 Producing Consistent and Comparable Results Across the Enterprise

An organization must be able to make use of the results of information security risk assessment in a way that supports and enables a larger enterprise risk management effort. This requires that the methodology allow the organization to achieve not only consistent results over time but results that are comparable across operating units and lines of business. In addition, the results produced by the methodology must be a factor of the successful execution of the methodology steps, not dependent solely on the analysis team that is performing the assessment.

2.3.7 Facilitating the Development of a Risk Assessment Core Competency

A risk-aware culture results when employees throughout the organization cultivate their risk management understanding and skill set and use that knowledge as a guiding force for performing their job responsibilities on a daily basis. Learning to perform risk assessment is a foundational way to improve these competencies and to promote a risk-aware culture. However, this requires that the risk assessment methodology be accessible, have low barriers to use (such as the degree to which specialized training is necessary), and produce meaningful results that are purposeful for helping employees to better perform their jobs.

2.3.8 Supporting Enterprise Compliance Activities

The information security activities of many organizations are driven by their need to manage an increasingly regulated environment. While organizations need to be focused on managing risks, they want to be able to act quickly and achieve compliance efficiently. Thus, a risk assessment methodology must be able to easily support information security risk management activities that enable compliance with various laws and regulations.

2.4 SPECIFIC IMPROVEMENTS IN OCTAVE ALLEGRO

The preceding section outlines the basic requirements for updating the existing OCTAVE methods. In this section, specific improvements that have been incorporated into the OCTAVE Allegro methodology to meet these requirements are discussed.

2.4.1 Data Collection and Guidance Streamlined

In the development of OCTAVE Allegro, specific attention was paid to minimizing the footprint of the process. This contributes to the ease of use requirement, supports the achievement of meaningful results with minimal resource commitments, and encourages long-term repeatability of the process.

The workshop-based data collection processes inherent in existing OCTAVE methods have been eliminated and replaced with simplified worksheets and structured guidance. This reduces the necessary resource commitment to the process for individuals outside of the analysis team and eliminates the corresponding overhead involved in the scheduling and coordinating of workshops. In addition, the volume of guidance and required worksheets has been drastically reduced to provide only essential foundational elements and process steps. Thus, the usability of the method has been improved through fewer, more focused activities and has been directed on risk management skill set development rather than cultivating the underlying premises and principles of the method.

2.4.2 Asset Focus Improved

In the existing OCTAVE methods, assets span the realm from people to information, systems, services and applications, and hardware and software. While all of these asset types are important to risk assessment, some users find it confusing to start with assets other than information because it sometimes leads to asset definitions that are too broad or too narrow for risk assessment.

The primary focus of the OCTAVE Allegro method is the information asset. All other assets important to the organization are identified and assessed in the context of the information assets to which they are connected. This eliminates potential confusion about scope and reduces the possibility that extensive data gathering and analysis may be performed for assets that are later found to be poorly defined, outside of the scope of the assessment, or in need of further decomposition.

2.4.2.1 Addition of information asset profiling[6]

OCTAVE Allegro requires that organizations create information asset profiles to facilitate a more accurate definition of the boundaries of an information asset by creating consistent, unambiguous, and agreed upon definitions for the asset. Through the asset profiles, an organization assigns ownership, defines security requirements, and captures the asset's value [Stevens 2005]. Once a profile has been created, it can be reused and updated in subsequent assessments. This supports the establishment of information asset baselines for future assessments and supports the repeatability of the method.

[6] Detailed guidance on creating an information asset profile can be found in a technical note entitled *Information Asset Profiling* [Stevens 2005].

2.4.2.2 Defining and using information asset security requirements

Security requirements—confidentiality, integrity, and availability—are part of an information asset's DNA. They are the asset's requirements for protection and sustainability [Caralli 2007]. Regardless of where the asset is stored, transported, or processed, or who has custodianship of it (either inside or outside of the organization), the asset's security requirements live with it throughout its useful life.

By confining the assignment of security requirements to information assets, OCTAVE Allegro reduces the potential confusion around the definition and application of security requirements in the risk assessment process. In the existing OCTAVE methods, security requirements are not specifically related to information assets (as they are intended to be), and thus users often develop and attempt to apply these concepts to "people" and "technology." This causes some users to have problems in risk identification and analysis. Furthermore, security requirements are a foundational element for devising and implementing risk mitigation plans. OCTAVE Allegro explicitly requires users to consider the implication of risk consequences on security requirements and in the mitigation of risk.

2.4.3 Threat Identification Streamlined

The existing OCTAVE methods use threat trees as a guide for identifying threats. While threat trees provide a structured means for identifying and considering various threat scenarios, they can sometimes be confusing to use, especially for users with limited risk management experience. For example, each path in an OCTAVE threat tree is a generic articulation of a threat; to make effective use of these trees, participants in an OCTAVE assessment must become adept at translating these generic paths to real-world scenarios. When users fail to make this translation, it significantly affects the robustness of the identification of threats and risks.

In addition, users often fail to realize that each path in the threat trees may equate to one or more than one real-world scenario. This is important because even though many threats share the same underlying actor, motive, and outcome, they may require significantly different considerations for mitigation. Over-reliance on threat trees for threat identification (in lieu of active discussion and scenario development) can significantly diminish the overall effectiveness of the risk assessment process.

OCTAVE Allegro uses threat scenario questionnaires rather than threat trees to help users identify the threats associated with an information asset. These questionnaires are based on the threat trees included in the OCTAVE method and thus ensure a broad consideration of potential threats. However, the questionnaires are designed around the container concept to focus users on the threats that are relevant to an information asset when it is stored, transported, or processed in a specific container. This simplifies the structure of the questionnaire and reduces the overall time required to capture a robust collection of potential threats.

2.4.4 "Practice" View Eliminated

The surveys of an organization's current information security practices have been eliminated in OCTAVE Allegro. While these practice surveys provide useful information to the OCTAVE process (because they are considered in developing an organizational protection strategy), they

often serve to distract the analysis team from the information asset-specific risks and threats under consideration. Thus, an organization can consider the effect of insufficient practices as a potential source of threat, but there is no requirement in OCTAVE Allegro to distribute practice surveys, collect and analyze results, and develop an organizational protection strategy separate and distinct from information asset-related risk assessment.

2.4.5 Technology View Scaled Down

OCTAVE Allegro takes a fundamentally different approach to the information technology environment of an organization, and its relationship to information assets, than the existing OCTAVE methods. Instead of running vulnerability tools and using the results to seed threat identification, in OCTAVE Allegro users map an information asset to all of the containers in which it is stored, transported, or processed and consider threats to each of those containers. There is still a technology view, but it is not impeded by the execution of cumbersome tools that require specialized knowledge and resources.

2.4.5.1 Elimination of vulnerability testing

The identification of vulnerabilities is an important means for seeding risk identification. However, it can be a time consuming activity that ultimately draws the risk assessment activity off course. The use and execution of vulnerability tools, as well as the analysis of the output of these tools, are challenging and cumbersome tasks even for organizations that perform these tasks on a regular basis. In practice, many users of existing OCTAVE methods find that performing tool-based vulnerability identification actually results in lost momentum and does not provide significant additional information that cannot be obtained through scenario identification. This is particularly true for organizations that are performing their first risk assessment or that do not have expertise with using such tools.

In addition, because many organizations confuse vulnerability assessment with risk assessment, organizations sometimes truncate the OCTAVE processes in the mistaken belief that vulnerabilities that have been identified are risks. But only through analysis of potential outcome and impact can vulnerabilities be considered risks that must be addressed.

The requirement for running vulnerability tools to complete the technology view of risk is eliminated in OCTAVE Allegro. However, if an organization has a core competency in tool-based vulnerability identification, it can easily be incorporated into several OCTAVE Allegro processes to provide a more robust articulation of risk.

2.4.5.2 Introduction of the container concept

As was mentioned previously, OCTAVE Allegro introduces the container concept to the assessment process. The OCTAVE Allegro method ensures the consideration of all of the containers in which an asset is stored, transported, and processed, whether internal or external to the organization. This effectively bounds the assessment and ensures a proper consideration of scope.

2.4.5.3 Addition of the “environment map” concept

OCTAVE Allegro introduces the concept of the information risk environment map. In essence, this map helps the user to define all of the places where an information asset is stored, transported,

or processed. Through the creation of this map, the analysis team establishes the boundaries (both internal and external) of the threat environment and the scope of the risk assessment. This allows for a more systematic and consistent process for considering all of the places where the asset can be threatened and a more robust consideration of risk. In addition, the map serves as baseline documentation of the risk environment for an information asset for future consideration of threats and controls.

2.4.6 Analysis Capabilities Improved

OCTAVE Allegro significantly improves the analysis capabilities of the existing OCTAVE methods through the introduction of risk sheets and a quantitative analysis component.

2.4.6.1 Development of the information asset risk worksheet

In OCTAVE Allegro all of the relevant information about a specific risk for an information asset is captured on an information asset risk worksheet. On this worksheet, threat and impact information associated with a risk are captured, the relative risk score is computed, and mitigation plans and activities are documented. This significantly reduces the documentation, organization, and data manipulation required to perform the risk assessment and produces a much more concise view of risk that can be communicated and shared. It also helps the organization to organize risk information in a way that enables analysis of root causes and the development of mitigation strategies, particularly where these strategies may address more than one risk. In addition, the development of the worksheets facilitates an organization's ability to perform trend analysis across organizational units because of the standardized and consistent format for documenting and mitigating risk.

2.4.6.2 Performing quantitative analysis

The OCTAVE methods are largely qualitative risk assessment methodologies. That is, they lend themselves to qualitative considerations and descriptions of risk rather than quantitative ones. Although operational risk is by nature difficult to quantify, organizations with significant experience in "numbers-based" risk methodologies find methods such as OCTAVE somewhat difficult to institutionalize because they lack an inherent process for risk prioritization and rank-ordering.

OCTAVE Allegro provides for *simple* quantitative analysis of risk by introducing the concept of a *relative risk score*. A relative risk score is a value derived from a consideration of a qualitative description of risk probability combined with a prioritization of the organizational impact of risk in terms of the organization's risk measurement criteria. The score can be used to compare the relative significance of individual risks. For example, when comparing two risks, the risk with the higher score is considered to be more significant relative to other risks. Since scores are consistently derived from the organization-wide risk measurement criteria, they can be compared between OCTAVE Allegro instances and across time as the organization's operating environment changes.

2.4.7 Risk Mitigation Guidance Improved

Effective risk mitigation strategies must be developed in consideration of an information asset's security requirements and the controls that are (or will be) implemented at the container level where the asset is stored, transported, or processed. The OCTAVE Allegro method (through the

use of the risk worksheet) explicitly requires that these considerations be made by developing specific mitigation strategies for each container where the asset lives. In essence, this forces the user to consider what controls currently exist at the container, whether they are sufficient for preventing or mitigating the risk under consideration, and what additional controls should be implemented.

2.4.8 Training and Knowledge Requirements Streamlined

By combining some of the structured path concepts of OCTAVE-S with an improved and streamlined assessment and mitigation planning process, OCTAVE Allegro significantly reduces the training and knowledge requirements for performing a robust and effective risk assessment. Training in the OCTAVE Allegro method typically takes less time (1.5 days versus 3 days for existing methods), and the level of necessary process, risk management, and technical knowledge required for analysis team participants is related to developing a risk assessment skill set rather than in becoming a risk management practitioner.

All of the improvements described above are reflected in the OCTAVE Allegro method, which is presented at a summary level in Section 3 of this report.

3 Introducing OCTAVE Allegro

In this section, the eight steps of the OCTAVE Allegro methodology are outlined and the worksheets and other artifacts that support the methodology are introduced. This section does not provide detailed instructions for actually performing an assessment. That guidance can be found in "Appendix A – OCTAVE Allegro Method Guidance v1.0" on page 31.

3.1 OCTAVE ALLEGRO METHODOLOGY

There are four distinct areas of activity that are carried out through eight steps in the OCTAVE Allegro methodology. The activity areas are

- Establish drivers, where the organization develops risk measurement criteria that are consistent with organizational drivers.
- Profile assets, where the assets that are the focus of the risk assessment are identified and profiled and the assets' containers are identified.
- Identify threats, where threats to the assets—in the context of their containers—are identified and documented through a structured process.
- Identify and mitigate risks, where risks are identified and analyzed based on threat information, and mitigation strategies are developed to address those risks.

The relationship between the activity areas and the actual steps of the methodology are illustrated in the OCTAVE Allegro roadmap presented in Figure 2 on page 4.

The outputs from each step in the process are captured on a series of worksheets which are then used as inputs to the next step in the process. The individual steps of the methodology are described in more detail below.

3.1.1 Step 1 - Establish Risk Measurement Criteria

The first step in the OCTAVE Allegro process establishes the organizational drivers that will be used to evaluate the effects of a risk to an organization's mission and business objectives. These drivers are reflected in a set of risk measurement criteria that is created and captured as part of this initial step. Risk measurement criteria are a set of qualitative measures against which the effects of a realized risk can be evaluated and form the foundation of an information asset risk assessment. Using consistent risk measurement criteria that accurately reflect an organizational view ensures that decisions about how to mitigate risk will be consistent across multiple information assets and operating or departmental units.

In addition to evaluating the extent of an impact in a specific area, an organization must recognize which impact areas are the most significant to its mission and business objectives. For example, in some organizations an impact to the relationship with its customer base may be more significant than an impact on its compliance with regulations. This prioritization of impact areas is also performed in this initial step.

The OCTAVE Allegro method provides a standard set of worksheet templates to create these criteria in several impact areas and then to prioritize them.

3.1.2 Step 2 - Develop an Information Asset Profile

The OCTAVE Allegro methodology focuses on the information assets of the organization and Step 2 begins the process of creating a profile for those assets. A profile is a representation of an information asset describing its unique features, qualities, characteristics, and value. The methodology's profiling process ensures that an asset is clearly and consistently described, that there is an unambiguous definition of the asset's boundaries, and that the security requirements for the asset are adequately defined. The profile for each asset is captured on a single worksheet that forms the basis for the identification of threats and risks in subsequent steps.

3.1.3 Step 3 - Identify Information Asset Containers

Containers describe the places where information assets are stored, transported, and processed. Information assets reside not only in containers within an organization's boundaries but they also often reside in containers that are not in the direct control of the organization. Any risks to the containers in which the information asset lives are inherited by the information asset.

For example, many organizations outsource some if not all of their IT infrastructure to service providers. These service providers manage the containers that contain the organization's information assets. If a service provider is not aware of the security requirements of an information asset that is stored, transported, or processed in the containers that they manage, the controls that are necessary to protect the information assets may not be adequate, thus exposing the assets to risk.

This problem can become even more pronounced if the service provider in turn contracts for other services (such as data storage) with additional service providers that may be unknown to the information asset owner. Thus, to gain an adequate risk profile of an information asset, an organization must identify all of the locations where its information assets are stored, transported, or processed, whether or not they are within the organization's direct control.

In Step 3 of the OCTAVE Allegro method, all of the containers in which an asset is stored, transported, and processed, whether internal or external, are identified. In this step the analysis team maps an information asset to all of the containers in which it lives, thus defining the boundaries and unique circumstances that must be examined for risk.

3.1.4 Step 4 - Identify Areas of Concern

Step 4 begins the risk identification process by brainstorming about possible conditions or situations that can threaten an organization's information asset. These real-world scenarios are referred to as *areas of concern* and may represent threats and their corresponding undesirable outcomes. Areas of concern may characterize a threat that is unique to an organization and its operating conditions. The purpose of this step is not to capture a complete list of all possible threat scenarios for an information asset; instead, the idea is to quickly capture those situations or conditions that come immediately to the minds of the analysis team.

3.1.5 Step 5 - Identify Threat Scenarios

In the first half of Step 5, the areas of concern captured in the previous step are expanded into threat scenarios that further detail the properties of a threat. But the collection of threats developed from these areas of concern does not necessarily provide a robust consideration of possible threats to an organization's information asset. Thus, in the second half of Step 5, a broad range of additional threats is considered by examining threat scenarios.

A range of threat scenarios can be represented visually in a tree structure commonly referred to as a *threat tree*. Threat trees are brought from the OCTAVE method and are described in Table 2.

Table 2: Description of Threat Trees

Threat Tree	Definition
Human actors using technical means	The threats in this category represent threats to the information asset via the organization's technical infrastructure or by direct access to a container (technical asset) that hosts an information asset. They require direct action by a person and can be deliberate or accidental in nature.
Human actors using physical access	The threats in this category represent threats to the information asset that result from physical access to the asset or a container that hosts an information asset. They require direct action by a person and can be deliberate or accidental in nature.
Technical problems	The threats in this category are problems with an organization's information technology and systems. Examples include hardware defects, software defects, malicious code (e.g., viruses), and other system-related problems.
Other problems	The threats in this category are problems or situations that are outside the control of an organization. This category of threats includes natural disasters (e.g., floods, earthquakes) and interdependency risks. Interdependency risks include the unavailability of critical infrastructures (e.g., power supply).

The threat scenarios derived from the areas of concern correspond to a branch on one or more of these threat trees. To ensure a more robust consideration of threats, each branch of the threat tree is also considered for each information asset. Working through each branch of the threat trees to identify threat scenarios can be a tedious exercise. Thus, a series of threat scenario questionnaires have been developed and are provided to help with this task. These questionnaires can be found in "Appendix C – OCTAVE Allegro Questionnaires v1.0" on page 91.

This step also provides an opportunity for consideration of probability in the description of threat scenarios. Probability helps an organization determine which of the scenarios are more likely given its unique operating environment. This is useful in later steps when an organization begins the process of prioritizing its risk mitigation activities. However, because it is often difficult to accu-

rately quantify probability, especially with respect to security vulnerabilities and events, probability is expressed in the OCTAVE Allegro methodology qualitatively as high, medium, or low.

3.1.6 Step 6 - Identify Risks

In Step 5 threats are identified, and in Step 6 the consequences to an organization if a threat is realized are captured, completing the risk picture. A threat can have multiple potential impacts on an organization. For example, the disruption of an organization's e-commerce system can affect the organization's reputation with its customers as well as its financial position. The activities involved in this step ensure that the various consequences of risk are captured.

3.1.7 Step 7 - Analyze Risks

In Step 7 of this assessment, a simple quantitative measure of the extent to which the organization is impacted by a threat is computed. This relative risk score is derived by considering the extent to which the consequence of a risk impacts the organization against the relative importance of the various impact areas, and possibly the probability.[7] In other words, if reputation is most important to an organization, risks that have an impact on the organization's reputation will generate higher scores than risks with equivalent impacts and probabilities in another area. By prioritizing these impact criteria, an organization ensures that risks are prioritized in the context of its organizational drivers.

3.1.8 Step 8 - Select Mitigation Approach

In Step 8, the final step of the OCTAVE Allegro process, organizations determine which of the risks they have identified require mitigation and develop a mitigation strategy for those risks. This is accomplished by first prioritizing risks based on their relative risk score. Once risks have been prioritized, mitigation strategies are developed that consider the value of the asset and its security requirements, the containers in which it lives, and the organization's unique operating environment.

3.2 OCTAVE ALLEGRO WORKSHEETS

One of the keys to successfully using the OCTAVE Allegro methodology is in understanding and working with the worksheets that support the process ("Appendix B – OCTAVE Allegro Worksheets v1.0" on page 65). The following section briefly reviews each of the worksheets and relates them to process steps. It is worth noting here that working with paper copies of these worksheets while trying to perform the methodology can be cumbersome. The worksheets have been designed so that they would be easily translatable to other electronic formats, and individuals and organizations using the Allegro methodology are encouraged to do so.

3.2.1 Risk Measurement Criteria and Impact Area Prioritization Worksheets

As referenced above, in Step 1 of the OCTAVE Allegro methodology, risk measurement criteria against which an organization can evaluate a risk's effect on its mission and business objectives is

[7] It is up to the organization using the OCTAVE Allegro approach whether to include the consideration of probability into the risk assessment.

created. To facilitate this activity, five standardized worksheets are provided that allow an organization to identify high, medium, and low impacts in the following categories:

- Reputation/customer confidence (Worksheet 1, Appendix B)
- Financial (Worksheet 2, Appendix B)
- Productivity (Worksheet 3, Appendix B)
- Safety and health (Worksheet 4, Appendix B)
- Fines/legal penalties (Worksheet 5, Appendix B)

Many organizations have found that having a standardized set of criteria that only requires filling in the blanks is helpful when first attempting to use the Allegro methodology. Not all of the standardized categories or impacts work for every organization, however, and as an organization matures its risk measurement criteria the impact areas can become very specific to it.

Each of the worksheets has an option entitled "other." This option is used to supplement the standard impact areas with additional categories that may be more meaningful to an organization. In addition to these five worksheets, an additional worksheet is provided solely for user-defined impact areas (Worksheet 6, Appendix B).

The impact area prioritization worksheet (Worksheet 7, Appendix B) is used in computing the relative risk score. With this worksheet the organizational unit performing the Allegro assessment prioritizes the impact areas defined on the previous worksheets or from categories the organization has developed for itself from most important to least important.

3.2.2 Information Asset Profile Worksheet

An information asset profile is a representation of an information asset describing its unique features, qualities, characteristics, and value. The Information Asset Profile worksheet (Worksheet 8, Appendix B) captures all of this information on a single page.

3.2.3 Information Asset Risk Environment Maps

The Information Asset Risk Environment Maps capture all of the places where an information asset is stored, transported, or processed. There are three map worksheets, one for each of the different container types defined by the OCTAVE Allegro method:

- Technical (Worksheet 9a, Appendix B)
- Physical (Worksheet 9b, Appendix B)
- People (Worksheet 9c, Appendix B)

Each of these maps addresses not only containers that are internal to the organization, but also those that are in custodial control of external entities such as suppliers.

3.2.4 Information Asset Risk Worksheets

The creation of the Information Asset Risk Worksheet (Worksheet 10, Appendix B) is a key feature of the Allegro process. On this worksheet both the threat and impacts associated with a risk are captured, the relative risk score is computed, and mitigation plans and activities are captured. Since the identified risk is described on its own worksheet, risks can easily be grouped and regrouped as an

organization moves forward in risk analysis and mitigation activities. The worksheets also facilitate an organization's ability to look across organizational units for similar or systemic risks and use that information to develop more effective and efficient mitigation strategies.

4 Using OCTAVE Allegro

This section of the report provides some practical instruction on using the OCTAVE Allegro method. It describes a collection of lessons learned from organizations that have successfully used the method.

4.1 PREPARING FOR OCTAVE ALLEGRO

Some preparation is necessary before an organization can perform an OCTAVE Allegro assessment. Preparation activities include obtaining management support, allocating appropriate organizational resources to the process, and scoping the assessment activities.

4.1.1 Obtaining Senior Management Sponsorship

Obtaining sponsorship from senior management is a critical factor in successfully performing an OCTAVE Allegro assessment. As with the OCTAVE methods, management must be committed to providing active support to the process and they must be willing to participate in the process when necessary, primarily in developing and sponsoring organization-wide risk measurement criteria. (The level of participation is minimized with the OCTAVE Allegro methodology and can be leveraged throughout the organization, as everyone using the methodology should use the same risk measurement criteria.)

Senior management must also ensure that sufficient resources are allocated to the process, enabling members of the assessment team to devote the necessary time to performing the process. Without this, members of the assessment team are unlikely to develop useful results from the process, and the necessary resources from outside the assessment team are unlikely to be available.

4.1.2 Allocating Organizational Resources

Two important aspects of the OCTAVE Allegro method are the composition and size of the assessment team. In practice, we have observed a range of possibilities for establishing an assessment team, from as few as one to as many as seven. In some cases, senior staff have performed the method by themselves, relying on their knowledge of the operational area; in others, a group of staff from the same operational unit have collaborated on the assessment. In most cases, there is also typically a representative from the information technology department that participates on the team or is directly accessible as necessary. The access to the IT department is most necessary during the mapping of information assets and the development of threat scenarios and risk mitigation plans, as they can provide technical depth that other members of the team may lack.

The time commitment for the process can vary widely depending on the availability, experience, and make-up of the team, the complexity of the information asset, the complexity of the environment in which that asset is stored, transported or processed, and of course, the number of information assets being reviewed. The first time a team performs an assessment on a single information asset often can often take up to several days. As teams become more experienced and learn to efficiently divide tasks between team members, they will be better able to predict the amount of

time required for a given assessment. They will also become more proficient at performing assessments, which will reduce the necessary time commitments.

4.1.3 Training Requirements

Organizations that have previous working knowledge of existing OCTAVE methods are generally able to pick up the guidance, worksheets, and questionnaires associated with the OCTAVE Allegro method and deploy it without significant delay or challenge. However, organizations and organizational units in which risk assessment is essentially a new activity or an area of improvement generally find that they must provide some training and support to assessment team members. In our experience with OCTAVE Allegro to date, users can become functional in the method in approximately a day and a half. However, it should be noted that OCTAVE Allegro was designed to be self-applied, and in many cases, assessment team personnel should be able to use the guidance and worksheets included in this technical report without further instruction.

4.2 PERFORMING AN ASSESSMENT

All of the guidance, worksheets, and questionnaires necessary to perform an OCTAVE Allegro assessment are included in the appendices of this report. *However, please note that these artifacts are intended to be used on a single information asset.* Organizations that desire to assess more than one information asset will need to repeat the process (beginning with Step 2, Activity 3) for each information asset included in their risk assessment scope.

4.2.1 Selecting Information Assets

To date, users of the OCTAVE Allegro methodology have exhibited little difficulty in identifying information assets to be included in the assessment scope, but they sometimes are challenged in selecting a subset of assets that are critical to the organization. This requires an understanding of which assets support critical organizational processes.

If the selection of information assets is left to the judgment of the assessment team, the importance of the asset may be based on its perceived value rather than a more consistent and repeatable method of asset valuation. The use of critical success factors[8] can provide a consistent and repeatable method for selecting and validating critical assets. Performing an affinity analysis in which the pool of information assets are mapped against an organization's (or operational unit's) critical success factors can help to identify the information assets that are essential to meeting the mission of the organization [Caralli 2004].

Critical success factor analysis can also provide insights as to which organizational unit should perform risk assessments. The SEI technical report *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management* [Caralli 2004] provides a methodology for how an organization can identify its critical success factors and notionally describes a process that uses these factors to identify critical organizational assets and critical organizational units.

[8] Critical success factors describe the performance areas that are critical for an organization to accomplish its mission.

4.2.2 Developing Risk Measurement Criteria

The first step in OCTAVE Allegro involves creating risk measurement criteria for the *organization*. Users should consider the development of these criteria as an iterative process that will improve over time. *In all cases, risk measurement criteria should reflect management's risk tolerances and appetite and should be able to be universally applied across the organization to the extent possible.* Otherwise, the results of risk assessments performed in different operational units that use different risk measurement criteria may not be comparable.

4.2.3 Repeating an Assessment

For simplicity, an OCTAVE Allegro assessment should be repeated every time there is a significant change in an information asset's risk environment. In reality, the operational environment of the organization is constantly changing, and because the OCTAVE Allegro assessment is essentially a snapshot, it can quickly become outdated.

Some organizations set up a regular schedule of assessments to ensure that changes in the risk environment are identified at discrete intervals and receive proper attention. The caution in this approach is that if there are significant changes between the intervals, new risks may be introduced without mitigation over a significant period of time. Other organizations require a new assessment any time there is a significant change to an information asset or its environment. For regularly changing environments, this approach can be appropriate, but for more stable environments it is possible that the cumulative effect of small changes in an asset's risk environment over time will be overlooked. Some organizations may find a hybrid of these approaches to be more fitting for their operational environment. In any case, the organization should determine criteria for repeating the OCTAVE Allegro assessment and implement that criteria along with the institutionalization of the process.

5 Next Steps

The OCTAVE Allegro approach described in this report facilitates an organization's ability to understand and manage its information-related security risks by providing a rapid and easily adoptable, organizationally driven assessment and planning tool. But, like the organizations that have used one or more of the existing OCTAVE methods, OCTAVE Allegro will continue to evolve.

In the future, the OCTAVE "brand" will represent a broad range of tools, techniques, and methodologies that define competencies across all phases of continuous information security risk management—from risk identification to assessment and analysis to mitigation. OCTAVE Allegro is specifically positioned to help the organization quickly improve its risk assessment capabilities and will evolve into the skill-based component of a larger philosophy on information security risk management and process improvement.

In the meantime, the ways in which OCTAVE Allegro will become useful to organizations will continue to grow. For example, to help an organization to evolve from a "security" view to an "operational resiliency" view, OCTAVE Allegro will be expanded to include a consideration of information assets in the context of their associated business processes and services. And to move OCTAVE from the operational realm to earlier phases of the asset and systems development life cycle, OCTAVE Allegro will be positioned as a tool for use in information security requirements elicitation and development.

The following section discusses preliminary considerations of using the OCTAVE methodologies in these ways.

5.1 EVOLVING THE OCTAVE ALLEGRO APPROACH

5.1.1 Focusing on Organizational Processes and Services

Assets are charged into production in support of the services that, in effect, define the mission of the organization. Most organizations can be represented by the 10-12 fundamental services that it performs. Evaluating risks to the organization in the context of service delivery will help organizations to ensure that the protection and sustainability strategies developed for risk mitigation are optimized. In other words, the way that risk is mitigated will be directly related to the value of the information and information-related assets to the business processes and services that they support.

In order to gain lasting value from the risk assessment process, an organization must make the important connections between its strategic objectives and information security, systems development, business continuity, and IT operations. Expanding the focus of an OCTAVE assessment to include the services and business processes of an organization will provide the context in which operational practices can be aligned with the overall risk management strategy of the organization.

5.1.2 Expanding View Beyond the Operational Unit

Future work on OCTAVE will take into consideration that information security activities are not performed in an organizational or operational unit vacuum. Information security, systems development, business continuity, and IT operations all contribute to meeting operational objectives. Ensuring that all functional areas of the organization are operating from the same set of risk drivers is one of the fundamental principles of risk management.

OCTAVE Allegro should be easier to adopt and apply because the process is concentrated on essential activities and is focused at the operational unit level within an organization. The resulting assessment plans are by design locally optimized for the organizational unit performing the assessment. However, it should be possible for an organization to use the outputs of the assessment process to understand and manage risks on a broader scale.

In theory, an organization should be able to take the risks identified at the operational unit level and translate them into mitigation strategies that are optimized for the enterprise, perhaps establishing an organizational baseline set of controls. When an operational unit conducts an OCTAVE Allegro-based assessment, it can determine whether the identified risks are addressed by the baseline controls and will only need to implement additional controls when it feels the risks to the asset and therefore the organizational mission outweigh the cost of additional controls.

5.1.3 Applying OCTAVE Allegro in the Systems Development Life Cycle (SDLC)

OCTAVE has traditionally been applied in the operation and maintenance phases of the SDLC. Organizations have used the approach to assess and develop mitigation plans for assets and systems that are already deployed and in operation. Developing and implementing mitigation plans for resources already in operation can be extremely expensive. Ensuring that a system provides all of the necessary controls to protect the assets it stores, transports, and processes instead of bolting them on can reduce operational cost for deployment of software and systems.

Ensuring that a system provides an appropriate set of security controls for the information assets it contains requires that security requirements are captured and included in the development stages of the SDLC. Security requirements that do exist today are typically generated from compliance and best practice driven activities instead of from business objectives.

We believe that OCTAVE Allegro could be used earlier in the SDLC to ensure that security requirements are aligned with organizational goals and objectives and that appropriate controls are developed and implemented for critical assets. An Allegro assessment could be conducted for the information assets that support a process that an organization wishes to automate. This would capture the security requirements of all of the information assets that support the business requirements and would identify the gaps in the current control structure that would need to be provided by the system under development. Once identified, these missing controls can be incorporated into the set of requirements for the system.

5.2 LOOKING FORWARD

The introduction of the OCTAVE Allegro method in this technical report is another step in incorporating the lessons learned from our field experiences to enhance the usability and adoption of the methods.

5.2.1 Expanding the Community of Interest

OCTAVE is accepted in the information security community as one de facto standard for conducting risk assessments. As security and business continuity evolve into resiliency and organizations look for a way to manage operational risk, the community of interest continues to grow. The user communities will be tapped to provide unique views of the applicability of the method in practice and the various ways in which it can be tailored for extensibility to the larger enterprise. The importance of effectively managing operational risk as part of the overall risk portfolio while at the same time continuously improving the underlying processes is the focus of our emerging work in resiliency engineering.

Activities planned for the future include workshops or forums from which we will draw on the experience and expertise of the user community. The collective expertise of the user community in the areas of information security, business continuity, and IT operations will provide a rich source for validating that this work is reflective of the practitioners in the field.

5.2.2 Exploring Connections to the CERT Resiliency Engineering Framework

The CERT® Resiliency Engineering Framework is an emerging body of work at the SEI. The framework is the foundation for a process improvement approach to security and business continuity management. It is a framework of practice that integrates security and business continuity activities by defining the essential organizational processes, related goals, and specific practices that are necessary to manage operational resiliency [Caralli 2007]. We expect the focus on managing operational risk and resiliency to influence future versions of OCTAVE. The assessment process will be strengthened as the relationships between information security processes and operational resiliency processes are identified, and OCTAVE may evolve further to support a resiliency perspective.

5.2.3 Updating and Improving Training

The SEI's course offering on information security risk management and OCTAVE will be modified initially to expose students to OCTAVE Allegro concepts. In the future, we envision a movement toward OCTAVE Allegro-based training and train-the-trainer education. In addition, we also hope to position OCTAVE training as part of a larger focus on all aspects of information security risk management education including risk identification, risk analysis, and risk mitigation.

The movement toward a focus on operational resiliency and away from security will also be reflected in future training efforts as OCTAVE Allegro and related tools, technologies, and methods are created and transitioned.

5.2.4 Obtaining Feedback and Direction

The OCTAVE Allegro guidance, worksheets, questionnaire, and example included in the appendix of this technical report together form Version 1.0 of the OCTAVE Allegro methodology. Readers of this report and users of the OCTAVE methodologies are invited to share their comments and suggestions and descriptions of their experiences with the methodology. Understanding the community's experience with the method is critical to its continued improvement and will be reflected in updates to the methodology artifacts. All feedback can be directed to the project mailbox octave-info@cert.org.

Appendix A OCTAVE Allegro Method Guidance v1.0

INTRODUCTION AND PURPOSE

This guidance provides detailed instructions for performing the eight steps in the OCTAVE Allegro risk assessment methodology. The guidance for each step of the process has the same structure. First background information and definitions are introduced, then more general information necessary for performing the step is provided, and finally specific guidance for performing the step is included. All steps are numbered sequentially for convenience and each step is broken down further into a series of activities. As you complete an activity, it is a good idea to mark the check box next to the activity so that you can track your progress.

"Appendix B – OCTAVE Allegro Worksheets v1.0" on page 65 contains all of the necessary worksheets, and "Appendix C – OCTAVE Allegro Questionnaires v1.0" on page 91 contains all of the necessary threat scenario questionnaires to complete an Allegro assessment for one information asset. You will use the questionnaires to help seed the identification of possible threats to your information asset. Finally, "Appendix D – OCTAVE Allegro Example Worksheets v1.0" on page 99 provides an example of an Allegro-based assessment performed in a medical facility.

Step 1 – Establish Risk Measurement Criteria

BACKGROUND AND DEFINITIONS

- **Impact** – The effect of a threat on an organization's mission and business objectives.
- **Impact value** – a qualitative measure of a specific risk's impact to the organization (high, medium, or low).
- **Risk measurement criteria** – a set of qualitative measures against which the effect of each risk on an organization's mission and business objectives is evaluated. Risk measurement criteria define ranges of high, medium, and low impacts for an organization.

GENERAL NOTES

In Step 1, you establish the organizational drivers that will be used to evaluate the effect of a risk to your organization's mission and business objectives. These drivers are reflected in a set of risk measurement criteria that you will develop.

Risk measurement criteria form the foundation for your information asset risk assessment. Without these criteria, you cannot measure the extent to which your organization is impacted if a risk to your information asset is realized. In addition to recognizing the extent of a specific impact, an organization must recognize which impact areas are the most significant. For example, in some organizations an impact to the relationship with its customer base may be more significant than an impact on its compliance with regulations.

In the Allegro assessment, you will create a set of risk measurement criteria that reflect a range of impact areas that are important (and probably unique) to your organization. For example, impact areas can include health and safety of customers and employees, financial, reputation, and laws and regulations. A standard set of worksheet templates will be used to create these criteria in several impact areas and then prioritize them.

It is important to create a consistent set of risk measurement criteria that can be used for all information asset risk assessments conducted by an organization. The criteria should be focused at an organizational level and should reflect senior management's awareness of the risk environment in which the organization operates. Using risk criteria that accurately reflect an organizational view ensures that decisions about how to mitigate risk will be consistent across multiple information assets and operating or departmental units.

GUIDANCE AND ACTIVITIES

There are two activities in Step 1.

❑ **Step 1 Activity 1**

Define a qualitative set of measures (risk measurement criteria) against which you will be able to evaluate a risk's effect on your organization's mission and business objectives. Document your criteria on the *Risk Measurement Criteria Worksheets*. At a minimum, consider the following impact areas:

- Reputation/customer confidence (Worksheet 1, Appendix B)
- Financial (Worksheet 2, Appendix B)
- Productivity (Worksheet 3, Appendix B)
- Safety and health (Worksheet 4, Appendix B)
- Fines/legal penalties (Worksheet 5, Appendix B)
- User-defined impact area (Worksheet 6, Appendix B)

Fill in any blanks in the criteria worksheets to make them meaningful to your organization. You may also change the descriptions provided or add descriptions as necessary.

Notes: Within each impact area, there is an option entitled "other" to insert a unique set of criteria. There is also an impact area entitled "user-defined" available for new or unique impact areas. If any impact areas do not apply to your organization, cross them out.

If your organization has already developed risk measurement criteria, it can be used in the structured risk assessment, and this activity can be eliminated. However, it is still a good idea to review the organization's criteria to ensure that it represents the current risk environment and tolerances.

❑ **Step 1 Activity 2**

Prioritize the impact areas from most important to least important using the *Impact Area Ranking Worksheet* (Worksheet 7, Appendix B). The most important category should receive the highest score and the least important the lowest.

Notes: If you have five impact areas, rank the most important area as number five, the next most important area as number four, and so on. All impact areas that you will be using for risk measurement must be ranked. This prioritization is used later in the risk assessment to develop a relative risk score that can help your organization determine how to address risks that have been identified in the assessment.

Step 2 – Develop an Information Asset Profile

BACKGROUND AND DEFINITIONS

- **Asset** – An asset is something of value to the enterprise. Assets are used by organizations to achieve goals, provide a return on investment, and generate revenue. The overall value of the organization can be represented collectively by the value of its assets.
- **Critical information asset** – Critical information assets are the most important assets to an organization. The organization will suffer an adverse impact if
  - a critical asset is disclosed to unauthorized people
  - a critical asset is modified without authorization
  - a critical asset is lost or destroyed
  - access to a critical asset is interrupted
- **Information asset** – An information asset can be described as information or data that is of value to the organization, including such information as patient records, intellectual property, or customer information. These assets can exist in physical form (on paper, CDs, or other media) or electronically (stored on databases, in files, on personal computers).
- **Information asset profile** – A representation of an information asset describing its unique features, qualities, characteristics, and value.
- **Information asset owners** – Owners of information assets are those individuals who have primary responsibility for the viability, survivability, and resiliency of an information asset. They set security requirements for the asset and ensure that proper protection strategies have been implemented in the organization to meet these requirements.
- **Information asset custodians** – Custodians of information assets refers to the individuals in the organization who have the responsibility to protect information assets that are stored, transported, or processed in containers. In other words, custodians accept responsibility for the information assets that live in containers that they manage and ensure the protection of the assets per the owner's requirements.
- **People** – In the structured risk assessment, people are a type of container for information assets. They may possess specialized or important information and use it in their jobs, such as intellectual property. In some cases, the information that people know may not exist in any other form in the organization (i.e., it may not be written down).
- **Security requirements** – The requirements that characterize how an information asset is to be protected. These are also often referred to as "security objectives."
  - Confidentiality – Ensuring that only authorized people (or systems) have access to an information asset.
  - Integrity – Ensuring that an information asset remains in the condition that was intended by the owner and for the purposes intended by the owner.
  - Availability – Ensuring that the information asset remains accessible to authorized users.

- **Technology assets** – Technology assets typically describe electronic containers in which information assets are stored, transported, or processed. These assets generally include hardware, software, application systems, servers, and networks.

GENERAL NOTES

The risk assessment that you are performing is focused on the information assets of the organization. In this step, you begin the process of defining those information assets. Later, you will identify the containers in which the information assets "live" and the custodians of those containers. This will help you to fully identify all of the points at which the information assets might be vulnerable to disclosure, modification, loss/destruction, or interruption.

A profile is created for each information asset, forming the basis for the identification of threats and risks in subsequent steps. Information asset profiling is important for ensuring that an asset is clearly and consistently described, that there is an unambiguous definition of the asset's boundaries, and that the security requirements for the asset are adequately defined. The information asset profile can even be extended to include a quantitative value for the asset, if desired.

Guidance and Activities

There are eight activities in Step 2.

❑ **Step 2 Activity 1**

The first activity in this step of the risk assessment involves identifying a collection of information assets on which an assessment might be performed. The assessment provides the most utility when it is focused on the information assets that are most important to the organization. Depending on the level at which you perform this risk assessment, "organization" might be substituted by department, division, or any other sublevel of the organization.

To do this, consider the following questions:

- What information assets are of most value to your organization?
- What information assets are used in day-to-day work processes and operations?
- What information assets, if lost, would significantly disrupt your organization's ability to accomplish its goals and contribute to achieving the organization's mission?
- What other assets are closely related to these assets?

Brainstorm a list of the information assets that are important to your organization and on which you might perform a structured risk assessment.

❑ **Step 2 Activity 2**

"Focusing on the critical few" is an essential risk management principle. Thus, you should perform the structured risk assessment only on 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.

From the list you created in Activity 1, consider the following question:

- Which assets on your list, if compromised, would have an adverse impact on the organization (as defined by your risk evaluation criteria) if one or more of the following occurred?
  - The asset or assets were **disclosed** to unauthorized people.
  - The asset or assets were **modified** without authorization.
  - The asset or assets were **lost** or **destroyed**.
  - Access to the asset or assets was **interrupted**.

Assets that meet one or more of these criteria should be considered critical to your organization and should have a structured risk assessment performed on them.

Beginning with the next activity, you will commence the process of performing a risk assessment on **one** of your critical information assets. Simply repeat all of the steps for each information asset on which you wish to perform a risk assessment.

❑ **Step 2 Activity 3**

In the following activities (3-8) you gather information about your information asset that is necessary to begin the structured risk assessment process. You will use the *Critical Information Asset Profile* (Worksheet 8, Appendix B) to record this information.

To begin, record the name of the critical information asset in column (1) of the *Critical Information Asset Profile*.

❑ **Step 2 Activity 4**

Document your rationale for selecting the critical information asset in column (2) of the *Critical Information Asset Profile*. As you do so, consider the following questions:

- Why is this asset critical to the organization?
- Is this information asset subject to regulatory requirements?

❑ **Step 2 Activity 5**

Record a description for the critical information asset in column (3) of the *Critical Information Asset Profile*. Be sure that you define the scope of the information asset and that you use an agreed-upon, common definition. Examples include "all of the paper medical records for our practice" or "the vendor database."

Consider the following questions when you are describing the information asset:

- What is the common name for this information asset (how do people within the organization refer to it)?
- Is this information asset electronic or physical (i.e., found on paper), or both?

Notes:

Be sure to document any distinguishing factors that are relevant to the value of the information asset and/or the protection needs of the asset. For example, if the information asset is covered under regulations such as HIPAA, you should note that in the description.

You might also want to capture which organizational processes or services that this information asset supports. For example, the customer database might support billing processes, product quality processes, and sales processes.

❑ **Step 2 Activity 6**

Identify and document the owners of the critical information asset. (Refer to the definitions provided above to determine who is an owner.) Record this information in column (4) of the *Critical Information Asset Profile*.

Consider the following questions when you are documenting the information asset owner:

- Who in the organization has the primary responsibility for this information asset?
- Who owns the business processes where this information asset is used? Whose business processes are most reliant on this information asset?
- Who would be responsible for setting the value (monetary or otherwise) of this information asset?
- Who would be most impacted if the information asset was compromised?
- Are there different owners for the different elements of data that compose the information asset?

Notes:

In many cases, an information asset is owned by more than one organizational unit. If this is the case for your information asset, be sure to involve the additional owners in defining the asset and performing the risk assessment. The risk profile of the asset might be incomplete if you do not consider the threat environments of all operating units that own the asset.

Additionally, while recording the actual name of the owner is useful, it is more important to capture the organizational position of the owner or owners. This is especially important in organizations with significant turnover.

❑ **Step 2 Activity 7**

Record the security requirements for confidentiality, integrity, and availability in column (5) of the *Critical Information Asset Worksheet*. Begin by checking the requirements that are applicable to the information asset, and continue by filling in the information that completes each security requirement statement. To the right of these statements you may add requirements or you may make your requirements more specific. It is important to remember during this step that if there is more than one owner of an information asset, the security requirements developed for that asset must reflect the requirements of all the owners.

Security requirements for information assets are often derived from legislation and regulation. You should make sure that the security requirements that you define support any pertinent regulations.

Notes:

A category entitled "other" is provided for additional security requirements that do not fit the categories listed.

❑ **Step 2 Activity 8**

Identify the **most important security requirement** for the information asset by marking an 'X' in the box next to the category of security requirements in column (6) of the *Critical Information Asset Worksheet*. You will use this information when you are determining the potential impact of a risk, so it is important that you choose this security requirement carefully.

Step 3 – Identify Information Asset Containers

BACKGROUND AND DEFINITIONS

- **Information asset container** – An information asset container is where information assets are stored, transported, or processed. It is a place where an information asset "lives." Containers generally include hardware, software, application systems, servers, and networks (technology assets), but they can also include items such as file folders (where information is stored in written form) or people (who may carry around important information such as intellectual property). They can also be both internal and external to an organization.

GENERAL NOTES

The places where an information asset is stored, transported, or processed can become points of vulnerability and threats that put the information asset at risk. Conversely, they can also become places where controls can be implemented to ensure that information assets are protected from harm so that they can be used as intended.

Containers are most typically identified as some type of technical asset—hardware, software, or system—but a container can also be a physical object such as piece of paper or a person that is important to the organization. People containers are particularly important with respect to intellectual property or information that is generally sensitive or confidential. A person who obtains this information essentially becomes a "container" and must be considered when profiling risks to the information asset. In some cases where a person possesses key organizational information (such as production designs), the lack of availability of that person is disruptive to related processes. Risks related to this must be identified and mitigated.

There are three very important points with respect to security and the concept of an information asset container:

- The way in which an information asset is protected or secured is through controls implemented at the container level. For example, to protect the customer database on a server, layers of controls are applied such as permitting only authorized personnel to enter the server room and limiting network access to the database to authorized individuals.
- The degree to which an information asset is protected or secured is based on how well the controls implemented at the container level take into consideration the security requirements of the information asset.
- Any vulnerabilities or threats to the containers in which the information asset lives are inherited by the information asset. This could be the case with people—if an employee is the only one who has a key piece of intellectual property and has never documented it, the loss of this key individual due to illness or termination of employment renders the information asset inaccessible.

In an information security risk assessment, the identification of containers is essential to identifying risks to the information asset itself. By mapping an information asset to all of the containers in

which it lives, this activity defines the boundaries of the technical environment and infrastructure that must be examined for risk.

It is important to recognize that information assets reside not only in containers within an organization's boundaries, but they also often reside in containers that are not in the direct control of the organization. For example, many organizations outsource some if not all of their IT infrastructure to service providers. These service providers manage the containers that contain the organization's information assets. If a service provider is not aware of the security requirements of an information asset that is stored, transported, or processed in the containers that they manage, the controls that are necessary to protect the information assets may not be adequate, thus exposing the assets to risk. This problem can become even more pronounced if the service provider in turn contracts for other services (such as data storage) with additional service providers that may be unknown to the information asset owner. Thus, to gain an adequate risk profile of an information asset, an organization must identify all of the locations where its information assets are stored, transported, or processed, whether or not they are within the organization's direct control.

GUIDANCE AND ACTIVITIES

There is only one activity in Step 3.

❑ **Step 3 Activity 1**

Using the *Information Asset Risk Environment Map* (Worksheets 9a, 9b, and 9c, Appendix B) identify and document the containers in which your information asset is stored, transported, or processed as follows:

- Use Worksheet 9a to identify **technical** containers that are under the direct control of the organization (internal) or those that are managed outside of the organization (external)
- Use Worksheet 9b to identify **physical** locations where the information asset may exist either inside or outside of the organization
- User Worksheet 9c to identify **people** internal or external to the organization who may have a detailed knowledge of the information asset

Begin with Worksheet 9a and complete all of the worksheets in as much detail as possible. Use the *Information Asset Container Guides* located in Tables 1-3 below if you need help in identifying appropriate containers in each of the three classes. Remember that you may need the help of others in the organization in order to develop an accurate "map" of all of the places where your information asset is stored, transported, or processed.

Notes:

You should document the owner of the container for the information asset whenever possible. The owner of the container often takes custodianship of your information asset and therefore may be required to help you to develop and implement risk mitigation strategies for any risks that originate on the container. You may need to talk with the owners of these containers during the risk assessment process to gather additional information.

As with recording the owner of an information asset, it is more important to capture the organizational position of the owner or owners. This is especially important for owners from outside of your organization.

Table 3: Information Asset Container Guide - Technical Containers

Container Type	Questions to Consider
Technical (*see* Worksheet 9a)	***Internal*** ❑ What information systems use or process this information asset? ***Example:*** • ***The vendor database (information asset) is used by the accounts payable system (system).*** ❑ What automated processes are reliant on this information asset? ***Example:*** • ***Paying an invoice (process) requires information in the vendor database (information asset) and is automated in the accounts payable system (system).*** ❑ On what hardware might this information asset be found? Consider: • If the information asset is used by a system, application, or process, what underlying hardware is related to the information asset? ***Examples:*** • ***The vendor database is stored on the "DIAMOND" server.*** ***External*** ❑ Are there customer or partner information systems that are externally managed that use or process this information asset? ***Example:*** • ***The payroll database (information asset) is used by the payroll management system (system) run by the payroll contractor.*** ❑ Are there any automated processes used by customers or business partners that rely on this information asset? ***Example:*** • ***A supplier of medical instruments uses information from the organization's inventory database (information asset) to manage just-in-time restocking in their customer order system (system).*** ❑ On what customer or partner hardware might this information asset be found? Consider: • If the information asset is used by any external customer or partner system, application, or process, what underlying hardware is related to the information asset? ***Examples:*** • ***the contractor's "OMEGA" server or mainframe*** • ***the supplier's dedicated network link segment "xyz"***

Table 4: Information Asset Container Guide - Physical Containers

Container Type	Questions to Consider
Physical (*see* Worksheet 9b)	***Internal*** ❑ Are there places, other than on technical assets, where this information asset exists? Consider: • Do people frequently write this information on paper and keep it on their desks? • Are there paper copies of this information asset that are filed or stored? • Do people process paper-based transactions that include this information asset? • Are there physical storage spaces where this information asset might be stored in physical form? ***Examples:*** • ***Patient records are stored in file folders in the file room on the second floor.*** • ***Doctors have paper copies of patient records stored in their desks.*** ***External*** ❑ Are there places external to the organization, other than on technical assets, where this information asset exists? Consider: • Do partners frequently write this information on paper and take it with them? • Are there paper copies of this information asset that are shared with or stored at other organizations? • Do any customers, partners, or contractors process paper-based transactions that include this information asset? • Are there physical storage spaces located in other organizations where this information asset might be stored in physical form? ***Examples:*** • ***Product designs are shared with significant customers during development stages.*** • ***Paper records are managed and stored at a contractor-owned facility.*** • ***Computer backup tapes are managed and stored by a third party who contracts with your organization's IT service provider.***

Table 5: Information Asset Container Guide – People Containers

Container Type	Questions to Consider
People (*see* Worksheet 9c)	***Internal*** ❑ What people might have detailed knowledge of this information asset? Consider: • Is this information asset considered intellectual property that a person might know? • Is this information asset sensitive or confidential, and could it be known by a few select individuals in the organization? • What people might have access to this information and might retain it or disclose it if they have seen it? ***Examples:*** • ***John Smith developed the paint formulas for our new line of cars. Only he knows the formulas and has never written them down.*** • ***Barbara Jones is a secretary in the medical records department. Although she has not been provided direct access to these records, she frequently sees patient's medical information as files are passed around the office.*** ***External*** ❑ What people, external to your organization, might know about this information asset? Consider: • Is this information asset considered intellectual property and shared with partners, service providers, consultants, or customers? • Are there external parties that might have access to this information and might retain it or disclose it if they have seen it? ***Examples:*** • ***The marketing vice president often discusses specs of new product offerings with the organization's largest customer.***

Step 4 – Identify Areas of Concern

Background and Definitions

- **Area of Concern** – A descriptive statement that details a real-world condition or situation that could affect an information asset in your organization.

General Notes

In Step 4, you begin the process of developing information asset risk profiles. Risk is the combination of a threat (a condition) and the resulting impact of the threat if acted upon (a consequence). In Step 4, you begin to address the threat component of the risk equation by brainstorming about possible conditions or situations that can threaten your information asset. These real-world scenarios are referred to as areas of concern and may represent threats and their corresponding undesirable outcomes. The areas of concern are captured and used to seed the development of risk profiles in Step 5.

Areas of concern may characterize a threat that is unique to your organization and its unique operating conditions. The purpose of this step is not to capture a complete list of all possible threat scenarios for an information asset; instead, the idea is to quickly capture those situations or conditions that come immediately to mind that could affect your asset and record them.

As you perform this step, remember to consider the various actors, motives, and outcomes inherent in the area of concern. Be as specific as you can and keep in mind the security requirements that you have set for your information asset and how they might be compromised due to a threat as you build real-world scenarios.

Guidance and Activities

There is only one activity in Step 4.

❑ **Step 4 Activity 1**

To perform this activity, you will use the *Information Asset Risk Environment Maps* for reference and the *Information Asset Risk Worksheet* (Worksheet 10, Appendix A) to record your areas of concern.

To identify areas of concern, perform the following steps:

1. Using the *Information Asset Risk Environment Maps*, review each of the containers that you have listed to seed a discussion about potential areas of concern.
2. Document each area of concern that you identify on an *Information Asset Risk Worksheet.* On the worksheet, record the name of the information asset and document the area of concern in as much detail as possible. Complete the columns labeled “Information Asset” and “Area of Concern” on the worksheet and remember to use a separate worksheet for each area of concern that you identify.

3. Expand your areas of concern to create threat scenarios. A threat scenario is a more detailed expression of the properties of a threat. For each area of concern that you have recorded on an *Information Asset Risk Worksheet*, complete columns (1) through (4) by recording the actor, means, motive, and outcome. If you cannot complete some of these elements, leave them blank.
4. In column (5) document how this threat would affect the security requirements that have been set for the information asset. Continue to perform this activity for each *Information Asset Risk Worksheet* until all of your areas of concern have been expanded. The remaining risk information will be gathered in a later step.
5. Proceed through each of the containers listed on the *Information Asset Risk Environment Maps* and document as many areas of concern as possible. Remember, a single container may result in the identification of one or more areas of concern.

Notes:

The *Information Asset Risk Worksheet* will be used to collect risk information for your information asset as you proceed through the risk assessment. Each worksheet will uniquely capture a single risk, so you may have several of these worksheets completed throughout the risk assessment.

The following are examples of areas of concern:

Areas of concern
On the primary file server, incorrect file permissions might enable a staff member to accidentally access another employee's medical records.
On the payroll database server, a failure of the authentication controls could allow a user to accidentally view another employee's salary on the payroll system.
John Smith is the only employee who knows the production specs for producing widgets. The specs have never been written down. John Smith has been talking about leaving the company; if he does so, and the widget specs aren't obtained, we can't make widgets.
A patient's medical records, which are contained in folders often left on the nursing station desks, are altered by an unauthorized employee because there is no access control.

Step 5 – Identify Threat Scenarios

Background and Definitions

- **Threat** – A threat is an indication of a potential undesirable event. A threat refers to a situation (or scenario) in which a person could do something undesirable (an attacker initiating a denial-of-service attack against an organization's email server) or a natural occurrence could cause an undesirable outcome (a fire damaging an organization's information technology hardware). A threat is created when a threat actor exploits a vulnerability.
- **Threat scenario** – A threat scenario is a situation in which an information asset can be compromised. It generally consists of an actor, a motive, a means (access), and an undesired outcome. Threat scenarios are simplified ways to determine if a risk exists that could affect your information asset.
- **Threat trees** – A tree structure used to visually represent a range of threat scenarios. Threat trees help you to ensure that you consider a broad range of potential threats to your information asset as the basis for determining risk.

GENERAL NOTES

In Step 4, you documented areas of concern that could affect your information asset. In this step, areas of concern are expanded into threat scenarios that further detail the properties of a threat. To expand areas of concern into threat scenarios, you must first understand the basic components of a threat. A threat has the following properties:

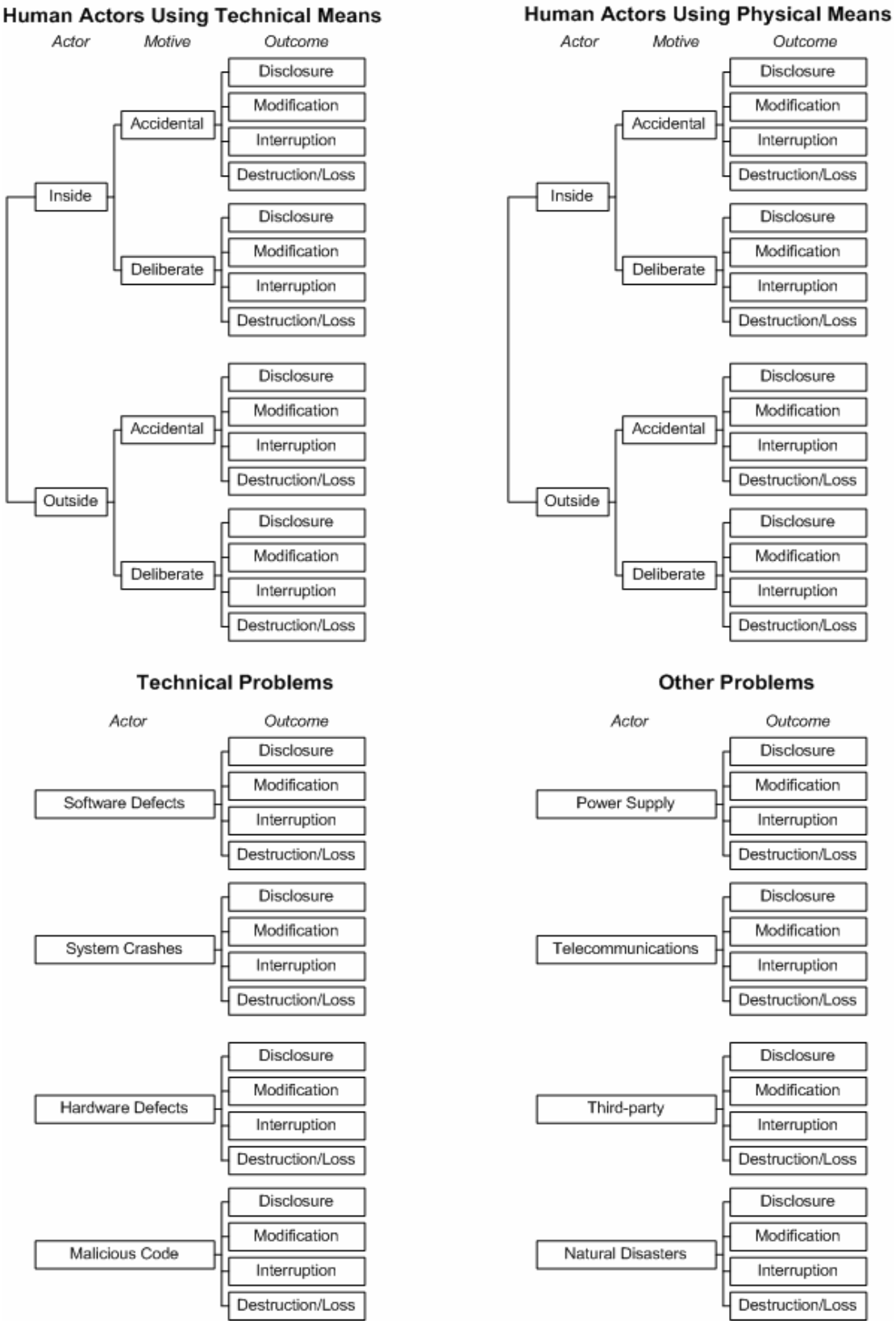
- Asset – something of value to the enterprise
- Access/means – how the asset is accessed by an actor (technical means, physical access). Access applies only to human actors.
- Actor – who or what may violate the security requirements (confidentiality, integrity, availability) of an asset
- Motive – the intent of an actor (e.g., deliberate or accidental). Motive applies only to human actors.
- Outcome – the immediate result (disclosure, modification, destruction, loss, interruption) of violating the security requirements of an asset

A range of threat scenarios can be represented visually in a tree structure to describe these threat properties. This tree structure is often referred to as a threat tree. In the Allegro risk assessment, four threat trees are considered. These trees are described in Table 6 and graphically represented in Table 7.

Table 6: Description of Threat Trees

Threat Tree	Definition
Human actors using technical means	The threats in this category represent threats to the information asset via the organization's technical infrastructure or by direct access to a container (technical asset) that hosts an information asset. They require direct action by a person and can be deliberate or accidental in nature.
Human actors using physical access	The threats in this category represent threats to the information asset that result from physical access to the asset or a container that hosts an information asset. They require direct action by a person and can be deliberate or accidental in nature.
Technical problems	The threats in this category are problems with an organization's information technology and systems. Examples include hardware defects, software defects, malicious code (e.g., viruses), and other system-related problems.
Other problems	The threats in this category are problems or situations that are outside the control of an organization. This category of threats includes natural disasters (e.g., floods, earthquakes) and interdependency risks. Interdependency risks include the unavailability of critical infrastructures (e.g., power supply).

Table 7: Graphical Representation of Threat Trees



The threat scenario derived from your areas of concern corresponds to a branch on these threat trees. To ensure a robust consideration of threats, each branch of the threat tree should be considered for your information asset. Working through each branch of the threat trees to identify threat scenarios can be a tedious exercise. Thus, in the structured risk assessment, a series of threat scenario questionnaires have been developed and are provided to help you with this task. In Step 5 you will use these questionnaires to help you identify additional threat scenarios you will want to consider for your information asset.

GUIDANCE AND ACTIVITIES

There are three activities in Step 5.

❑ **Step 5 Activity 1**	In this activity, you will identify additional threat scenarios that have not been seeded by areas of concern. To do this, you will use "Appendix C – Threat Scenarios Questionnaires." There is one questionnaire for each type of container (technical, physical, and people). Each questionnaire contains a collection of scenarios followed by questions designed to help seed the identification of additional threats. To complete this activity, use the *Information Asset Environment Maps* that you created in Step 4 (Worksheets 9a, 9b, and 9c) as a guide. 1. Proceed to *Threat Scenarios Questionnaire 1 – Technical Containers*. Considering the technical containers you have listed on Worksheet 9a, answer the questions. Circle an appropriate response. 2. Continue through *Threat Scenarios Questionnaire 2 – Physical Containers* and *Threat Scenarios Questionnaire 3 – People.* Use Worksheets 9b and 9c respectively to help guide your completion of the questionnaires. **Notes:** Remember that you may have more than one "yes" answer if there are different conditions, so circle more than one if necessary.

❑ **Step 5 Activity 2**	In this activity, you will complete *Information Asset Risk Worksheets* for each of the generic threat scenarios you identified for consideration on the questionnaires. 1. Review your responses on the Threat Scenarios Questionnaires. You do not have to do anything further for any scenario in which you circled "no." 2. For all "yes" answers, record a new *Information Asset Risk Worksheet.* Complete sections (1) through (5) on this worksheet. If you find that you have answered "yes" to a question, but cannot come up with a corresponding real-life situation, move on. 3. Continue until there is at least one *Information Asset Risk Worksheet* completed for each "yes" answer on any Threat Scenarios Questionnaire. **Notes:** It is possible that you could have more than one real-life situation that is represented by any "yes" answer you circle. If this is the case, you should record as many *Information Asset Risk Worksheets* as necessary for each "yes" answer.

❑ **Step 5 Activity 3**	This activity is optional for all Information Asset Risk Profiles. If you choose to do it, you must do it on all profiles. You may also decide to add probability to the description of the threat scenarios you have captured on your *Information Asset Risk Worksheets*. Probability helps you to determine which of the scenarios are more likely given your unique operating contexts. This will be useful later in determining how to prioritize your risk mitigation activities. Because it is often very difficult to accurately quantify probability (especially with respect to security vulnerabilities and events), probability is expressed in this risk assessment qualitatively as high, medium, or low. In other words, you must determine whether there is a strong (high) chance that the scenario you have documented could occur, a medium chance (neutral), or if the scenario is unlikely (low). If you choose to make this determination, you should check the appropriate probability box in column (6) for each of the risk worksheets that were created. **Notes:** If you decide to use probability, you must assign a probability to each of the threats that you have developed.

Step 6 – Identify Risks

BACKGROUND AND NOTES

- **Impact statement** – A descriptive statement that details how the organization is impacted when a threat scenario is realized. The impact statement is the consequence of the realization of a threat scenario.
- **Risk** – A risk is the possibility of suffering harm or loss. Risk refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence. A risk is composed of
  - an event,
  - a consequence, and
  - uncertainty

GENERAL NOTES

By identifying how the organization is impacted, you are completing the risk equation. This can be illustrated as follows:

Threat (condition) + Impact (consequence) = Risk

[Steps 4 and 5] + [Step 6] = Risk

GUIDANCE AND ACTIVITIES

There is one activity in Step 6.

❑ **Step 6 Activity 1**

In this activity, you determine how the threat scenarios that you have recorded on each *Information Asset Risk Worksheet* could impact your organization.

1. For each threat scenario that you documented on an *Information Asset Risk Worksheet*, determine how your organization would be impacted if this threat scenario was realized. This is the consequence of the threat and completes the risk equation.

2. Document a minimum of one consequence in Section (7) of the *Information Asset Risk Worksheet*. Additional consequences can be documented as necessary. Be as specific as you can. Try to consider the impact areas of the risk evaluation criteria as you consider consequences. Also, pay attention to the "outcome" you considered in Step 5, Activity 5.

The following table provides a few examples.

Threat Scenario	**Consequence**
Incorrect file permissions enable a staff member to accidentally access another employee's medical records.	The medical records of an employee are disclosed, resulting in a lawsuit filed against the organization and a resulting fine of $50,000.
John Smith is the only employee who knows the production specs for producing widgets. The specs have never been written down. John Smith has been talking about leaving the company; if he does so, and the widget specs aren't obtained, we can't make widgets.	Widgets are not produced, resulting in loss of production revenue of $250,000 per day and potential that the company would shut down.
A patient's medical records are altered by an unauthorized employee due to poor authentication controls.	An incorrect dose of medication (or an incorrect medication) is given to a patient resulting in their death and resulting lawsuits, reputation damage, and possible fines.

Step 7 – Analyze Risks

BACKGROUND AND NOTES

- **Impact value** – A *qualitative* value assigned to describe the extent of impact to an organization when a threat scenario and resulting impact is realized. The impact value is derived from the risk measurement criteria.

GENERAL NOTES

In Step 7, you qualitatively measure the extent to which the organization is impacted by a threat by computing a risk score for each risk to each information asset. This scoring information is used for determining which risks you need to mitigate immediately and for prioritizing mitigation actions for the remainder of risks in Step 8.

Risk analysis is a complex undertaking. In the structured risk assessment, you will perform activities that will give you a systematic way to analyze how the organization is impacted by a risk, but these activities are not all-encompassing. You will need to apply your knowledge of the organization and some common sense.

In this activity, you will generate a relative risk score. The relative risk score is derived by considering the extent to which the consequence of a risk affects the organization as compared to the relative importance of the various impact areas. In other words, if the area of "reputation" is most important to your organization and the consequence of a risk causes an extensive impact to reputation, you may need to take action to ensure that this risk is mitigated. By using these criteria, you are ensuring that risks are scored in the context of your organizational drivers.

GUIDANCE AND ACTIVITIES

There are two activities in Step 7. These activities must be performed for each *Information Asset Risk Worksheet*. You may do all of the activities to each risk worksheet at one time or proceed with Activity 1 for all worksheets, then go to Activity 2, etc.

❑ **Step 7 Activity 1**

Begin by reviewing the *Risk Measurement Criteria* that you created in Step 1, Activity 1. Focus on how you defined high, medium, and low impacts for your organization.

Starting with your first risk worksheet, review the consequence statement (or statements) that you recorded.

Using the *Risk Measurement Criteria* as a guide, evaluate the consequence relative to each of the impact areas and record a value of "high," "medium," or "low" in the **"Value"** area of column (8). If you have written more than one consequence statement, be sure to consider all of them as you are assigning values to the impact areas. *You must record a value in each of the impact areas.*

Consider the following example.

Threat Scenario	**Consequence**
Incorrect file permissions enable a staff member to accidentally access another employee's medical records.	The medical records of an employee are disclosed, resulting in a lawsuit filed against the organization and a resulting fine of $50,000.

This consequence indicates direct effects on the organization's reputation, potential monetary losses and lawsuits, and possible fines and penalties. Using the organization's *Risk Measurement Criteria*, the following values were assigned.

Impact Area	**Impact Value**
Reputation/Customer Confidence	Moderate
Financial	Low
Productivity	Low
Safety and Health	Low
Fines/Legal	High

The value of "high" in fines/legal is assigned because the organization has set a threshold of $25,000 as its upper limit. The consequence has little or no effect on productivity, so a value of "low" has been assigned.

❑ **Step 7 Activity 2**

In this step a relative risk score will be computed that can be used to analyze risks and help the organization to determine an appropriate risk strategy. You will perform this step in the "**Score**" area of column (8) on each of the *Information Asset Risk Worksheets.*

1. Compute the score for each impact area by multiplying the impact area rank by the impact value. (Refer to the *Impact Area Ranking Worksheet* that you created in Step 1, Activity 2.) Record the result in the "score" column. Impact values are assigned quantitative values as follows: High – 3, Medium – 2, and Low – 1. Be sure to keep these values consistent throughout the risk worksheets.
2. Total the score column. This total is the relative risk score.
3. Consider the following example. The organization ranked its impact areas as shown below. The financial area is considered to be the most important impact area and safety and health the least important. The impact values were assigned in Activity 1 as the consequences were considered.

Impact Area	Ranking	Impact Value	Score
Reputation	4	Moderate (2)	**8**
Financial	5	Low (1)	**5**
Productivity	3	Low (1)	**3**
Safety and Health	1	Low (1)	**1**
Fines/Legal	2	High (3)	**6**
		Total Score	**23**

Notes:

The scores generated in this activity are only meant to be used as a prioritization tool. Differences between risk scores are not considered to be relevant. In other words, a score of 48 means that the risk is relatively more important to the organization than a score of 25, but there is no importance to the difference of 13 points.

Step 8 – Select Mitigation Approach

BACKGROUND AND NOTES

- **Mitigation approach** – The way that an organization intends to address a risk. An organization has the following options: accept, mitigate, or defer.
  - Accept – A decision made during risk analysis to take no action to address a risk and to accept the stated consequences. Risks that are accepted should have little to low impact on the organization.
  - Mitigate – A decision made during risk analysis to address a risk by developing and implementing controls to counter the underlying threat or to minimize the resulting impact, or both. Risks that are mitigated are those that typically have a medium to high impact on an organization.
  - Defer – A situation where a risk is neither accepted nor mitigated based on the organization's desire to gather additional information and perform additional analysis. Deferred risks are monitored and re-evaluated at some point in the future. Risks that are deferred are generally not an imminent threat to the organization nor would they significantly impact the organization if realized.
- **Residual risk** – Residual risk is the risk that remains when a mitigation approach has been developed and implemented for the range of risks that affect an information asset. Residual risk that remains must be acceptable to the organization.

GENERAL NOTES

In Step 8, you consider which risks you need to mitigate and how. This is done by prioritizing risks, deciding on an approach to mitigate important risk based on a number of organizational factors, and developing a mitigation strategy that considers the value of the asset and the places where it lives.

The decision to accept a risk, mitigate it, or defer it is based on a number of important factors. Impact value is a primary driver, but so is probability. If a risk could seriously or significantly impact the organization but is highly unlikely to occur, you may not want to mitigate it. Unfortunately, there is no decisive path to follow for deciding which risks to mitigate. Often, this is a decision that is driven by the individuals involved in the risk assessment and their knowledge of the organization.

Once the decision is made to mitigate a risk, you must develop an effective and efficient mitigation strategy. Deciding how to mitigate a risk is a complex endeavor and may require discussion with other skilled personnel in your organization. The fact that the owner of an information asset and the custodian of the asset are two different people means that both must collaborate on the best strategy for providing overall protection.

The need for collaboration between business experts and information technology personnel highlights the scenario in which the owner of an information asset is different from the custodian. Frequently, the true owners of information assets are the business subject matter experts who entrust the IT department to manage their technical infrastructure. Unfortunately, these owners are often unaware of their role and abdicate their responsibilities to the custodians of their data. Thus, they relinquish all control of the asset to the IT department and expect them to manage all aspects of the asset, including security.

As the administrators over information system and technical infrastructure, the IT department takes on the job of supporting the business functions of the organization. Since the business functions of the organization are dependent on information assets, the IT department plays an important role in implementing protection strategies that support and protect the organization's information assets. The criticality of their role and their ability to implement technical controls has led many organizations to mistakenly attribute ownership of information assets to them. Excluding them from the development of risk mitigation strategies can be a significant mistake.

A further complication to the owner and custodian problem is that there is often a multitude of information assets being stored, transported, or processed in a single container. Each of the information assets may have different owners and, consequently, potentially different security requirements. This is a challenge because the minimum level of controls on the container must be those that meet the highest level of security requirements needed to secure one or more of the information assets. In other words, the information asset with the most extensive security requirements influences the overall controls applied to the container.

A common consequence of this situation is that some assets in a container will be over-protected because the controls are more extensive than is called for by their security requirements. Most often, however, the controls applied to a container end up failing to accurately meet the security needs of all of the information assets that it stores, processes, or transports (sometimes because de facto controls have been applied across all similar containers). One way to address this issue is to move information assets to other containers (e.g., servers) where they can be protected in a way that better meets their security requirements.

Each of these issues adds a layer of complexity in protecting an organization's information security assets. The asset profiles and maps developed in Steps 2 and 3 can be useful for determining all of the critical information assets that live in a specific container. The security requirements of all assets in that container can then be considered in aggregate when developing a mitigation strategy for their protection. In some cases an organization may determine that allowing certain combinations of assets to coexist prevents the implementation of an effective level of controls, and an owner may choose to move an asset as a result.

To mitigate risk appropriately, you must consider a balanced approach.

- You can *avoid* risk by implementing appropriate controls to prevent threats and vulnerabilities from being exploited.
- You can *limit* risk by implementing strategies that limit the adverse impact on the organization if a risk is realized.

In most cases, it is appropriate to ensure that your mitigation strategies address both avoiding and limiting risk. However, it is also important to consider cost in developing your mitigation strategies. *The cost of avoiding and limiting risk must be commensurate with the value of the asset being protected and the potential impact on the organization if the asset is compromised.* In addition, you must consider that not all risk can be eliminated. Your mitigation strategies may result in residual risk, which you must consider and either accept or mitigate further.

The value of performing a risk assessment is so that mitigation strategies can be based on solid analysis, so these activities may require significant discussion and planning. It is important to have the support of senior management and to collaborate with the IT department and other stakeholders to develop balanced and cost-effective mitigation strategies.

GUIDANCE AND ACTIVITIES

There are three activities in Step 8.

❑ **Step 8 Activity 1**

The first activity in Step 8 is simply to sort each of the risks that you have identified by their risk score. Categorizing your risks in an orderly fashion will help you begin to make decisions on their mitigation status.

There are many ways for an organization to categorize its risks. One straightforward method is to begin by sorting the risks in order from highest to lowest. Then separate the risks into four pools with equal number of risks. The risks with the highest score should be in the first (Pool 1), the risks with the next highest range of scores in the second (Pool 2), the next highest in the third (Pool 3), and the lowest scores in the fourth (Pool 4).

Other categorization schemes may make sense for your organization. If your organization is using probability, you might want to consider developing a risk matrix to categorize the risks identified. The Relative Risk Matrix table below shows an example of how to do this.

RELATIVE RISK MATRIX			
PROBABILITY	RISK SCORE		
	30 TO 45	16 TO 29	0 TO 15
HIGH	POOL 1	POOL 2	POOL 2
MEDIUM	POOL 2	POOL 2	POOL 3
LOW	POOL 3	POOL 3	POOL 4

❑ **Step 8 Activity 2**

Assign a mitigation approach to each of your risks. Consider using the following as a guide, but remember that a decision about a mitigation approach is highly dependent on your organization's unique operating circumstances, so do not use this chart solely to decide how to address the risks that you have identified.

Pool	Mitigation Approach
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Defer or Accept
Pool 4	Accept

Notes:

In some cases it is possible to transfer risk to another party. This can be considered as a mitigation approach for all of the risks under consideration.

Decide how you are going to address each of the risks on each *Information Asset Risk Worksheet* that you have created and document this by checking the appropriate action in the **"Risk Mitigation"** box in column (9). *Every risk on every risk profile must have an approach documented.* For risks that you decide to accept, be sure to go back and review the impact statements and impact values—do not accept any risks that could have serious consequences on the organization.

❑ **Step 8 Activity 3**

For all of the risk profiles that you decide to mitigate, you must develop a mitigation strategy. Keeping in mind the actions that you can take to mitigate risk, begin to consider mitigation strategies for each risk that you have decided to mitigate, as follows:

1. Note the container in which the control will be implemented. (These containers can be found on the *Information Asset Risk Environment Maps*.)

2. Describe the control to be implemented and any residual risk to the asset once the control is implemented.

Consider the following questions when developing a risk mitigation strategy:

- How could the actor be prevented from exploiting a weakness?
- How could the means that the actor would use be prevented?
- How could the motive be prevented?
- How could the resulting outcome be prevented?
- Could the probability of the threat be reduced?
- If no proactive activity can be performed, can the impact of the threat be reduced?
- Can the organization minimize the effect or impact of a realized risk?
- How will the security requirements for this information asset be satisfied by the mitigation strategy?

Appendix B OCTAVE Allegro Worksheets v1.0

In this appendix, you will find all of the worksheets necessary for completing the OCTAVE Allegro assessment for **one information asset**.

Allegro Worksheet 1	Risk Measurement Criteria – Reputation and Customer Confidence		
Impact Area	**Low**	**Moderate**	**High**
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than _____% reduction in customers due to loss of confidence	_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence
Other:			

Allegro Worksheet 2	RISK MEASUREMENT CRITERIA – FINANCIAL		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than _____% in yearly operating costs	Yearly operating costs increase by _____to _____%.	Yearly operating costs increase by more than _____%.
Revenue Loss	Less than _____% yearly revenue loss	_____to _____% yearly revenue loss	Greater than _____% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $_____	One-time financial cost of $_____ to $_____	One-time financial cost greater than $_____
Other:			

Allegro Worksheet 3	RISK MEASUREMENT CRITERIA – PRODUCTIVITY		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	Staff work hours are increased by less than _____% for _____to _____ day(s).	Staff work hours are increased between _____% and _____% for _____to _____ day(s).	Staff work hours are increased by greater than _____% for _____to _____ day(s).
Other:			
Other:			
Other:			

Allegro Worksheet 4	RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated
Other:			

Allegro Worksheet 5	RISK MEASUREMENT CRITERIA – FINES AND LEGAL PENALTIES		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than $_____are levied.	Fines between $_____and $_____are levied.	Fines greater than $_____are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than $_____ are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between $_____ and $_____are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $_____ are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.
Other:			

Allegro Worksheet 6	RISK MEASUREMENT CRITERIA – USER DEFINED		
Impact Area	**Low**	**Moderate**	**High**

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	IMPACT AREAS
	Reputation and Customer Confidence
	Financial
	Productivity
	Safety and Health
	Fines and Legal Penalties
	User Defined

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
(4) Owner(s) *Who owns this information asset?*		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
❑ Confidentiality	❑ Integrity	❑ Availability ❑ Other

Allegro Worksheet 9a	INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1.	
2.	
3.	
4.	
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1.	
2.	
3.	
4.	

Allegro Worksheet 9b	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1.	
2.	
3.	
4.	
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1.	
2.	
3.	
4.	

Allegro Worksheet 9c	INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)
INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	DEPARTMENT OR UNIT
1.	
2.	
3.	
4.	
EXTERNAL PERSONNEL	
CONTRACTOR, VENDOR, ETC.	ORGANIZATION
1.	
2.	
3.	
4.	

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset			
	Area of Concern			
	Threat	(1) Actor *Who would exploit the area of concern or threat?*		
		(2) Means *How would the actor do it? What would they do?*		
		(3) Motive *What is the actor's reason for doing it?*		
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium** ❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
	Reputation & Customer Confidence		
	Financial		
	Productivity		
	Safety & Health		
	Fines & Legal Penalties		
	User Defined Impact Area		

Relative Risk Score

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	❑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		

Appendix C OCTAVE Allegro Questionnaires v1.0

In this appendix, you will find three threat scenario questionnaires, one for each of the container types in which an information asset can be stored, transported, or processed (technical, physical, and people). These questionnaires are used in Step 5 of the OCTAVE® Allegro process to help ensure a robust consideration of threats in the assessment process.

Threat Scenario Questionnaire 1	Technical Containers		
This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Threat Scenario Questionnaire – 1 (cont)	Technical Containers

Scenario 3:

In this scenario, consider situations that could affect your information asset on any technical containers you identified. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

- Unintended disclosure of your information asset
- Unintended modification of your information asset
- Unintended interruption of the availability of your information asset
- Unintended permanent destruction or temporary loss of your information asset

A software defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
A system crash of known or unknown origin occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Ye (interruption)**	**Yes (loss)**
A hardware defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Malicious code (such as a virus, worm, Trojan horse, or back door) is executed	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Power supply to technical containers is interrupted	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Problems with telecommunications occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Other third-party problems or systems	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Threat Scenario Questionnaire – 2	Physical Containers		
This worksheet will help you to think about scenarios that could affect your information asset on the physical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Threat Scenario Questionnaire -2 (cont)	Physical Containers

Scenario 3:

In this scenario, consider situations that could affect your physical containers and, by default, affect your information asset. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

- Unintended disclosure of your information asset
- Unintended modification of your information asset
- Unintended interruption of the availability of your information asset
- Unintended permanent destruction or temporary loss of your information asset

Other third-party problems occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Threat Scenario Questionnaire – 3	People		
This worksheet will help you to think about scenarios that could affect your information asset because it is known by key personnel in the organization. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee has detailed knowledge of your information asset and could, *accidentally* or *intentionally*, cause the information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?[9]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?[10]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?[11]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could, *accidentally* or *intentionally*, cause your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

[9] This case is unlikely, but if a key person in your organization has detailed knowledge of an information asset and communicates this information in an altered way that affects the organization, a risk could result.

[10] This case is about the availability of the information. If a key person in the organization has detailed knowledge that is vital for a business process and is not accessible or available, the information may not be usable for the purpose intended, ultimately impacting the organization.

[11] If a key person in the organization knows the information asset and leaves the organization, and the information is not documented elsewhere, it could pose a risk to the organization.

Appendix D OCTAVE Allegro Example Worksheets v1.0

This section contains example worksheets from an assessment of a hospital patient information database. The purpose of this example is to demonstrate what the OCTAVE® Allegro worksheets generally look like when they are completed and to provide some additional insights into the assessment process. The example includes each of the first nine worksheets and a sampling of actual risks and associated mitigation plans (Worksheet 10). The example, however, does not include a set of completed threat questionnaires. The identified risks were generated from consideration of the questionnaires. For clarity, a consideration of the probability associated with a threat when considering risks and developing mitigation strategies is not included in this example.

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	**Low**	**Moderate**	**High**
Reputation (Staff)	Reputation among non-physician hospital staff is minimally affected; little or no effort or expense is required to recover.	Reputation among non-physician hospital staff is damaged. No more than $100K in time and effort required to recover.	Reputation among non-physician hospital staff is severely damaged. More than $100K in time and effort required to recover. Relationship with staff is affecting reputation with physicians and community. Poor relationship affecting hospital efficiency and having noticeable effect on bed turnover rate.
~~*Customer Loss*~~ *Reputation (Physicians)*	Reputation among physicians is minimally affected; little or no effort or expense is required to recover. Little or no change in hospital occupancy rate.	Reputation among physicians is damaged, causing physician population to reconsider sending patients to hospital. Occupancy rate changes of between one and five percent directly attributable to reputation problem. More than $100K in time and effort required to recover.	Reputation among physicians is severely damaged. Critical staff physicians and hospital affiliated physicians are considering leaving. Occupancy changes of more than five percent are directly attributable to reputation problems. More than $500K in time and effort required to recover.
Other: *Reputation (Community)*	Reputation in community from which hospital draws patients is minimally affected; little or no effort or expense is required to recover. Little or no change in hospital occupancy rate.	Reputation in community is damaged, causing potential patients to balk at doctor recommendations to the hospital. Occupancy rate changes of between one and five percent directly attributable to reputation. More than $100K in time and effort required to recover.	Reputation in community is severely damaged, causing potential patients to refuse doctor recommendations to the hospital. Occupancy rate changes of more than five percent are directly attributable to reputation problem. More than $500K in time and effort required to recover.
Other: Occupancy Rates	A reduction of the hospital occupancy rate of less than 2%	A reduction of the hospital occupancy rate of between 2% and 5%	A reduction of the hospital occupancy rate of more than 5%

Allegro Worksheet 2	RISK MEASUREMENT CRITERIA – FINANCIAL		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	Increase of less than 2.5% in annual operating costs	Increase of between 2.5% and 5% in annual operating costs	Increase of more than 5% in annual operating costs
Revenue Loss	Less than $100K reduction in yearly revenue loss	Between $100K and $1M in yearly revenue loss	More than $1M in yearly revenue loss
One-Time Financial Loss	Less than $100K reduction in yearly revenue loss	Between $100K and $1M in yearly revenue loss	More than $1M in yearly revenue loss
Other:			

Allegro Worksheet 3	RISK MEASUREMENT CRITERIA – PRODUCTIVITY		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	Staff work hours increase labor costs by less than $100K.	Staff work hours increase labor costs between $100K and $1M.	Staff work hours increase labor costs by more than $1M.
Other: Bed Turnover Rate	Turnover rate for hospital beds decreases less than 2%.	Turnover rate for hospital beds decreases between 2% and 5%.	Turnover rate for hospital beds decreases by more than 5%.
Other:			
Other:			

Allegro Worksheet 4	RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH		
Impact Area	**Low**	**Moderate**	**High**
Life	No loss or significant threat to customers' or staff members' lives and no regulatory response.	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment. Only minimal regulatory response and less than $250K in related costs.	Loss of customers' or staff members' lives. Significant regulatory response, lawsuits, and more than $250K in related costs.
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within days. Minimal regulatory response and less than $100K in related costs.	Temporary or recoverable impairment of customers' or staff members' health. Only minimal regulatory response and between $250 and $500K in related recovery costs.	Permanent impairment of significant aspects of customers' or staff members' health. Significant regulatory response involving investigations and more than $500K in recovery costs.
Safety	Safety questioned, but no regulatory response and little to no economic cost.	Safety affected, minimal regulatory response, and less $250K in recovery costs.	Safety violated, significant regulatory response involving investigations, and more than $250K in recovery and response costs.
Other:			

Allegro Worksheet 5	RISK MEASUREMENT CRITERIA – FINES AND LEGAL PENALTIES		
Impact Area	**Low**	**Moderate**	**High**
Fines	Fines less than $100K are levied.	Fines between $100K and $250K are levied.	Fines greater than $500K are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than $100K are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between $100K and $1M are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $1M are filed against the organization.
Investigations	No queries from government or other investigative organizations.	Government or other investigative organization requests information or records (low profile).	Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.
Other:			

Allegro Worksheet 6	RISK MEASUREMENT CRITERIA – USER DEFINED		
Impact Area	**Low**	**Moderate**	**High**

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	IMPACT AREAS
2	Reputation and Customer Confidence
4	Financial
3	Productivity
5	Safety and Health
1	Fines and Legal Penalties
n/a	User Defined

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Patient Billing and Collection Data (PBCD)	**Keeping accurate billing records is essential for negotiating and collecting compensation from insurance organizations. Challenges to bills from insurance organizations can force the hospital to absorb billing differences. Challenges can also significantly delay the time between services being rendered and compensation being received by the hospital.**	**This information asset contains all of the information necessary to bill a patient and his/her insurance company for treatment/services received from the hospital. This includes patient demographic information (names, addresses, social security numbers, and insurance carriers), treatment/service history and associated billing codes, and payment histories.**
(4) Owner(s) *Who owns this information asset?*		
The owner of this information asset is the Director of Patient Billing and Collection (Todd Marnivich).		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	**Members of the hospital financial staff responsible for billing and collection should have "read" access to individual records. Other financial staff can have access to summary information. Data entry personnel should have "read" access to individual records.**

❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	**Only authorized data entry personnel and members of the hospital financial staff may update/change billing record information. Billing records should only be updated with the actual billable services provided to the patient.**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	**The PBCD must be available to data entry personnel for updates to billing and procedures codes and for admitting purposes. The PBCD must be available to financial staff for billing and collection activities.**
	This asset must be available for **24** hours, **7** days/week, **52** weeks/year.	**The PBCD information asset should be available 24x7 as procedures are ordered around the clock at the hospital. It must be available to the financial staff (specifically the patient billing and collection staff) during regular business hours. Short outages would not cause significant problems but extended outages (more than 8 hours) would cause a significant backlog.**
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	**Because these billing records contain patient treatment information, they are subject to HIPAA regulations.**

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

❑ Confidentiality	√ **Integrity**	❑ Availability	❑ Other

Allegro Worksheet 9a	INFORMATION ASSET RISK ENVIRONMENT MAP (TECHNICAL)
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. The PBCD primarily resides on the patient billing management system (PBMS) which consists of two database servers and three application/web servers. This is a vendor proprietary system that provides a web interface for authorized personnel to access/manipulate entries. The underlying operating system is Windows Server 2003.	Managed by hospital IT department.
2. Hospital internal network. All transactions to and from the PBCD system travel on this network.	Managed by hospital IT department.
3. Hospital workstations (e.g., order entry workstations, finance department workstations, and hospital admitting workstations).	Managed by hospital IT department.
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. The Internet. Most bills are electronically shipped in bulk to insurance providers each week. Once billing information arrives at the insurance company, the insurance company is considered to be the owner of the information asset.	Unknown
2.	
3.	
4.	

Allegro Worksheet 9b	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)
INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Paper copies of billing summaries, statements, and histories are regularly printed and kept by members of finance department.	Financial staff
2. Backup tapes of PBCD are created each night and kept onsite until regular pickup by storage vendor.	Managed by hospital IT department.
3.	
4.	
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Paper copies of billing statements are regularly printed and mailed to patients.	Financial staff
2. Paper copies of billing statements, summaries, histories, and reports are regularly printed and mailed to insurance providers.	Financial Staff
3.	
4.	

Allegro Worksheet 9c	INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)

INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	DEPARTMENT OR UNIT
1. Admitting staff	Admissions
2. Order entry staff	Business Services
3. Financial staff	Business Services
4. Hospital messenger service staff	Business Services
EXTERNAL PERSONNEL	
CONTRACTOR, VENDOR, ETC.	ORGANIZATION
1. Insurance organization's claims staff	Hospital Insurance, Inc.
2. Third-party vendor manages the transportation and storage of backup tapes for the PBCD system. Relationship is managed via the hospital IT department.	Safe-N-Secure Data Storage, Inc.
3.	
4.	

Allegro Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	PBCD		
	Area of Concern	Patient billing data is altered when unauthorized individual gains access to PBMS system. (A vulnerability in the Windows 2003 Server operating system is leveraged to gain administrative access to the PBMS system.)		
	Threat	**(1) Actor** *Who would exploit the weakness?*	Disgruntled current employees	
		(2) Means *How would the actor do it? What would they do?*	Using workstation on the internal hospital network, employee launches attack on PBMS system.	
		(3) Motive *What is the actor's reason for doing it?*	Wants to harm hospital because of ongoing labor contract disputes	
		(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ✓ **Modification**	❑ **Destruction** ❑ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Only authorized members of the hospital data entry staff and finance staff should be able to modify PBCD asset.	
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium** ❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	**(8) Severity** *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
If the intruder goes unnoticed, significant financial harm could come to the hospital. If insurance companies are not charged for services, the hospital would lose money. If the insurance companies are over-charged or charged for services not rendered, there will be additional financial repercussions.	**Reputation & Customer Confidence**	Low	2
	Financial	High	12
Significant labor charges will be required to audit and re-enter billing data.	**Productivity**	High	9
	Safety & Health	Low	5
Exposure of patient data may lead to fines and possible lawsuits.	**Fines & Legal Penalties**	Med	2
	User Defined Impact Area		
		Relative Risk Score	**30**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ Accept	❑ Defer	✓ Mitigate	❑ Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Hospital network	▫ Restrict network traffic to ensure that only the workstations of authorized users can access PBMS. ▫ Restrict network traffic to ensure that only valid PBMS transaction traffic can reach the PBMS system. This reduces the number of places from which attacks can be launched against the system and the types of attacks. Asset would still be vulnerable to services that remain exposed.
PBMS	▫ Ensure that transaction auditing is enabled so that improper transactions can be identified and backed out of the system. This control relies on the integrity of the audit log—if it were to be destroyed, it would be impossible to back out transactions.
PBMS	▫ Ensure that PBMS system and the underlying OS/applications are up-to-date with security patches. This control reduces the exposure against known attacks but does nothing to limit unknown vulnerabilities.

Allegro Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	PBCD		
	Area of Concern	Patient information is disclosed to unauthorized individuals, opening hospital to possible HIPAA violations and lawsuits. (PBCD travels on hospital intranet in the clear between workstations and PBMS System.)		
	Threat	**(1) Actor** *Who would exploit the weakness?*	An employee with access to hospital network	
		(2) Means *How would the actor do it? What would they do?*	A network administrator captures traffic on network switching device.	
		(3) Motive *What is the actor's reason for doing it?*	Curiosity about a patient	
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Only authorized personnel can view this information asset.	
		(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium** ❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	**(8) Severity** *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Exposure of patient sensitive information opens the hospital to lawsuits and fines for breaches of HIPAA regulations.	**Reputation & Customer Confidence**	Med	4
	Financial	Low	4
The public's overall perception of the hospital's quality could be negatively affected if patient sensitive information is publicized.	**Productivity**	Low	3
	Safety & Health	Low	5
	Fines & Legal Penalties	Med	2
	User Defined Impact Area		
		Relative Risk Score	**18**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
PBMS	▫ Enable SSL encryption on connections on PBMS server. This will reduce exposure to network captures by introducing end to end encryption on PBMS transactions.
Hospital Network	▫ Enable logging of consoles of networking devices and enact policy to ensure that logs are regularly reviewed. This will reduce likelihood of insider activity and increase the likelihood that outsider activity will be detected.

Allegro Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk — Threat	**Information Asset**	PBCD		
	Area of Concern	Denial-of-service attack against hospital network impedes the hospital's ability to electronically deliver bills to the insurance organizations. (PBCD must traverse Internet to reach insurance organizations.)		
	(1) Actor *Who would exploit the weakness?*	A hacker who wants to see if he can damage the hospital financially		
	(2) Means *How would the actor do it? What would they do?*	Uses DoS toolkit found on hacking website		
	(3) Motive *What is the actor's reason for doing it?*	Entertainment		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ✓ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	The PBCD must be available for billing and collection activities.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium**	❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	**(8) Severity** *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Continual attacks against hospital network add significant delays in the reimbursement process. Hospital must burn CDROMs with the data and messenger them to insurance services. Significant financial and productivity impacts.	**Reputation & Customer Confidence**	Med	4
	Financial	High	12
	Productivity	High	9
	Safety & Health	Low	5
	Fines & Legal Penalties	Low	1
	User Defined Impact Area		
		Relative Risk Score	**31**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ Accept	❑ Defer	✓ Mitigate	❑ Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Internet	▫ Find a new service provider who has more robust connectivity solutions and can be more supportive in preventing DoS attacks.
Internet	▫ Work with insurance companies to develop alternative delivery methods such as a direct connection.

Allegro Worksheet 10	INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk	Information Asset	PBCD	
	Area of Concern	An unauthorized individual is able to view PBCD asset and exposes it to others. (Data entry staff member walks away from workstation connected to PBMS server that is located in a public area of the hospital and thus is freely accessible by patients, other hospital staff, or visitors.)	
	Threat — (1) Actor *Who would exploit the weakness?*	Hospital staff and/or inquisitive patients or hospital visitors	
	Threat — (2) Means *How would the actor do it? What would they do?*	When no one is at the workstation, a hospital worker, patient, or visitor could sit down in front of it and begin to access data.	
	Threat — (3) Motive *What is the actor's reason for doing it?*	Curiosity about famous patient on another floor or general curiosity	
	Threat — (4) Outcome *What would be the resulting effect on the information asset?*	✓ Disclosure ❑ Modification	❑ Destruction ❑ Interruption
	Threat — (5) Security Requirements *How would the information asset's security requirements be breached?*	Only authorized personnel can view this information asset.	
	Threat — (6) Probability *What is the likelihood that this threat scenario could occur?*	❑ High	❑ Medium ❑ Low

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Exposure of patient sensitive information opens the hospital to lawsuits and fines for breaches of HIPAA regulations.	Reputation & Customer Confidence	High	6
	Financial	Med	4
The public's overall perception of the hospital's quality could be negatively affected if patient sensitive information is publicized.	Productivity	Low	3
	Safety & Health	Low	5
	Fines & Legal Penalties	Med	2
	User Defined Impact Area		
	Relative Risk Score		**20**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ Accept	❑ Defer	✓ Mitigate	❑ Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Hospital workstations	▫ Force automatic screen locking for workstations that have been idle for more than five minutes. This would reduce the exposure of the data when workstation is unattended to a much smaller time period.
PBMS	▫ Enable transaction logging on the PBMS system. This would allow the hospital to determine accountability after the fact and could possibly lessen the impact of possible lawsuits and fines.
PBMS	▫ Enable controls in PBMS system to restrict access of data entry staff to only those patients in their specialty group. This will limit the exposure of patient data to only the patient information that the data entry staff is likely to encounter in performing their job functions.
Admit staff	▫ Provide regular refresher training for the admit staff on the responsibilities for protecting patient data and on HIPAA rules and regulations. ▫ Enact policy that all admit staff must sign non-disclosure agreement with the hospital.
Data entry staff	▫ Provide regular refresher training for the data entry staff on the responsibilities for protecting patient data and on HIPAA rules and regulations. ▫ Enact policy that all data-entry staff must sign non-disclosure agreement with the hospital.
Financial staff	▫ Provide regular refresher training for the financial staff on the responsibilities for protecting patient data and on HIPAA rules and regulations. ▫ Enact policy that all financial staff must sign non-disclosure agreement with the hospital.

Allegro Worksheet 10	INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk — Threat	**Information Asset**	PBCD	
	Area of Concern	Paper copies of billing statements are found by an unauthorized individual and patient sensitive data is exposed. (Financial staff members regularly produce paper copies of billing summaries and leave them on their desks.)	
	(1) Actor *Who would exploit the weakness?*	Janitorial staff	
	(2) Means *How would the actor do it? What would they do?*	Sees billing summary while cleaning an office	
	(3) Motive *What is the actor's reason for doing it?*	Curiosity	
	(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Only authorized personnel can view this information asset.	
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium** ❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	**(8) Severity** *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Exposure of patient sensitive information opens the hospital to lawsuits and fines for breaches of HIPAA regulations.	**Reputation & Customer Confidence**	Med	4
	Financial	Low	4
The public's overall perception of the hospital's quality could be negatively affected if patient sensitive information is publicized.	**Productivity**	Low	3
	Safety & Health	Low	5
	Fines & Legal Penalties	Med	2
	User Defined Impact Area		
		Relative Risk Score	**18**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ Accept	❑ Defer	✓ Mitigate	❑ Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Financial staff	▫ Provide regular refresher training for the financial staff on the responsibilities for protecting patient data and on HIPAA rules and regulations. ▫ Enact policy requiring that PBCD information must be in locked cabinets when not in use. ▫ Enact policy requiring that paper copies of PBCD information is shredded when no longer required. ▫ Enact policy that all financial staff must sign non-disclosure agreement with the hospital. ▫ Perform regular audits to ensure that paper information is in fact being properly handled.
Janitorial staff	▫ Enact policy that all janitorial staff must sign non-disclosure agreement with the hospital.

Allegro Worksheet 10	INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk	Information Asset	PBCD	
	Area of Concern	Backup tapes lost and unable to recover transactions. (Only one set of backup tapes is currently being created and stored off site.)	
Threat	(1) Actor *Who would exploit the weakness?*	Third-party backup storage provider	
	(2) Means *How would the actor do it? What would they do?*	Shipment of backup tapes is lost in storage.	
	(3) Motive *What is the actor's reason for doing it?*	Accidental	
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ Disclosure ❑ Modification	✓ Destruction ❑ Interruption
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Only authorized personnel can view this information asset.	
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ High	❑ Medium ❑ Low

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
If there is a system crash and the hospital is unable to recall backup tapes to restore transactions, then all transaction will need to be restored from paper patient records.	Reputation & Customer Confidence	Low	2
	Financial	High	12
There would be significant financial and productivity impacts to restore transaction.	Productivity	High	9
	Safety & Health	Low	5
Likely that during the restoration process many charges would be overlooked or incorrectly added. There would be losses for the missing changes and possibly increased reimbursement time as insurance companies disputed incorrect charges.	Fines & Legal Penalties	Low	1
	User Defined Impact Area		
		Relative Risk Score	31

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	✓ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Backup tapes	▫ Simply add a backup run and keep second copy of the backup tapes stored on site. Keeping a second copy of recent tapes on site will provide some redundancy but will not completely remove risk of being able to restore old transactions.

Allegro Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	PBCD		
	Area of Concern	Billing statement sent to wrong patient address. (Envelopes get out of order and wrong address label is applied and information in bill is not encrypted.)		
Threat	(1) Actor *Who would exploit the weakness?*	Hospital financial staff		
	(2) Means *How would the actor do it? What would they do?*	Envelopes get shuffled between machines.		
	(3) Motive *What is the actor's reason for doing it?*	Accidental		
	(4) Outcome *What would be the resulting effect on the information asset?*	✓ Disclosure ❑ Modification	❑ Destruction ❑ Interruption	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Only authorized personnel can view this information asset.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ High	❑ Medium	❑ Low

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Exposure of patient sensitive information opens the hospital to lawsuits and fines for breaches of HIPAA regulations.	Reputation & Customer Confidence	Low	2
	Financial	Low	4
The public's overall perception of the hospital's quality could be negatively affected if patient sensitive information is publicized.	Productivity	Low	3
	Safety & Health	Low	5
	Fines & Legal Penalties	Low	1
	User Defined Impact Area		
		Relative Risk Score	15

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ Accept	✓ Defer	❑ Mitigate	❑ Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*

Allegro Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk — Threat	**Information Asset**	PBCD		
	Area of Concern	Procedures not performed on a patient are added to billing summary. (No one checks that the data entry staff enters the correct procedures from the chart unless the insurance company complains about a charge.)		
	(1) Actor *Who would exploit the weakness?*	Disgruntled data entry staff		
	(2) Means *How would the actor do it? What would they do?*	Enters codes for test and procedures that were never performed		
	(3) Motive *What is the actor's reason for doing it?*	Wants to harm the hospital		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ✓ **Modification**	❑ **Destruction** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Billing records should only be updated with the actual billable services provided to the patient.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium**	❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	**(8) Severity** *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
If the activity goes unnoticed, significant financial harm could come to the hospital. If patients are charged for services the hospital did not deliver, the hospital would have to return money and might be sued for additional damages or negligence.	**Reputation & Customer Confidence**	**Med**	**8**
	Financial	**High**	**12**
Significant labor charges will be required to audit and re-enter billing data.	**Productivity**	**High**	**9**
	Safety & Health	**Low**	**5**
Insurance companies will likely take longer in reviewing and providing compensation to the hospital. This could cause a significant interruption in hospital's cash flow.	**Fines & Legal Penalties**	**High**	**3**
	User Defined Impact Area		
		Relative Risk Score	**37**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ Accept	❑ Defer	✓ Mitigate	❑ Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Data entry staff	▫ Provide for a separation of duties where one section of the data entry staff is responsible for entering the data and another checks to see if the data is correct against the hospital charts. This would not help in the case of collusion but would decrease the likelihood of the problem.
PBMS	▫ Enable transaction logging on the PBMS system. This would allow the hospital to determine accountability after the fact and could possibly lessen the impact of possible lawsuits and fines.
Financial staff	▫ Perform regular audits of billing entries. This would not prevent fraud but would help limit the extent of the activity.

References

URLs are valid as of the publication date of this document.

[Alberts 1999]
Alberts, C.; Behrens, S.; Pethia, R.; & Wilson, W. *Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE℠) Framework, Version 1* (CMU/SEI-99-TR-017, ADA367718). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. http://www.sei.cmu.edu/publications/documents/99.reports/99tr017/99tr017abstract.html

[Alberts 2001]
Alberts, C. & Dorofee, A. *OCTAVE Criteria, Version 2.0* (CMU/SEI-01-TR-020, ADA396654). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. http://www.sei.cmu.edu/publications/documents/01.reports/01tr020.html

[Alberts 2002]
Alberts, C. & Dorofee, A. *Managing Information Security Risks: The OCTAVE Approach.* Boston, MA: Addison-Wesley, 2002 (ISBN 0-321-11886-3).

[Alberts 2004]
Alberts, C.; Dorofee, A.; Stevens, J.; & Woody, C. *OCTAVE-S Implementation Guide, Version 1* (CMU/SEI-2004-HB-003, ADA453304). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.
http://www.sei.cmu.edu/publications/documents/04.reports/04hb003.html

[Caralli 2004]
Caralli, R. *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management* (CMU/SEI-SEI-2004-TN-010). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.
http://www.sei.cmu.edu/publications/documents/04.reports/04tn010.html

[Caralli 2006]
Caralli, R. *Sustaining Operational Resiliency: A Process Improvement Approach to Security Management* (CMU/SEI-SEI-2006-TN-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.
http://www.sei.cmu.edu/publications/documents/06.reports/06tn009.html

[Caralli 2007]
Caralli, R. *Introducing the CERT® Resiliency Engineering Framework: Improving the Security and Sustainability Processes* (CMU/SEI-2007-TR-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2007.
http://www.sei.cmu.edu/publications/documents/07.reports/07tr009.html

[Stevens 2005]
Stevens, J. *Information Asset Profiling* (CMU/SEI-2005-TN-021, ADA441305). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005.
http://www.sei.cmu.edu/publications/documents/05.reports/05tn021.html

[Woody 2006]
Woody, C. *Applying OCTAVE: Practitioners Report* (CMU/SEI-2006-TN-010, ADA448425). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006. http://www.sei.cmu.edu/publications/documents/06.reports/06tn010.html

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	May 2007	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process	FA8721-05-C-0003

6. AUTHOR(S)

Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2007-TR-012

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	ESC-TR-2007-012

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This technical report introduces the next generation of the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology, OCTAVE Allegro. OCTAVE Allegro is a methodology to streamline and optimize the process of assessing information security risks so that an organization can obtain sufficient results with a small investment in time, people, and other limited resources. It leads the organization to consider people, technology, and facilities in the context of their relationship to information and the business processes and services they support. This report highlights the design considerations and requirements for OCTAVE Allegro based on field experience with existing OCTAVE methods and provides guidance, worksheets, and examples that an organization can use to begin performing OCTAVE Allegro-based risk assessments.

14. SUBJECT TERMS	15. NUMBER OF PAGES
information security, risk evaluation, risk assessment, threat analysis, vulnerability evaluation, information resiliency, computer security risk management, OCTAVE	154

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL