Information Security Risk Analysis

Third Edition

THOMAS R. PELTIER

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Information Security Risk Analysis

Third Edition

Information Security Risk Analysis

Third Edition

THOMAS R. PELTIER

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20130312

International Standard Book Number-13: 978-1-4398-3957-7 (eBook - PDF)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

To Lisa and Winston, my two best buddies.

Contents

Acknowledgments

No one ever writes a book by himself and this book is no exception. As I worked on a third version of the risk assessment process I found myself going back to the people on whom I relied when I was creating the initial Facilitated Risk Assessment Process (FRAP). Good friends and associates such as John Blackley and David Lynas have been and continue to be sources to information. Additionally, they are excellent at providing feedback when new ideas and concepts are being formulated.

This process has come a long way since Lisa Bryson, Sherry Giardano, Ken Jaworski, Mike Kadar, and I put it together nearly fifteen years ago as a way to implement risk assessment quickly and efficiently within our company. It was founded on solid concepts and ideas, some of which we got from Gareth Davis and Dan Erwin.

When undertaking a book such as this, it helps to have a publisher/editor who understands what the process is and why the deadline seems to keep moving. Rich O'Hanley has been an excellent editor and friend.

A number of years ago the FRAP was introduced to a company called Netigy. This company, under the direction of Mike Corby, put together the best security team ever: Alec Bass, John Blackley, Genny Burns, Terri Curran, Stan Dormer, Beck Herold, Pat Howard, Cheryl Jackson, David Lynas, Justin Peltier, Nan Poulios, John Sherwood, Peter Stephenson, and Fred Trickey.

Establishment of a good foundation of learning and experience began at Chevrolet Engineering with my boss Larry Degg, who encouraged and supported me as I moved the security program further down the road. My best friend, Mike Cannon, was part of this team which included John Riske and Gene Traylor.

The Computer Security Institute, founded by John O'Mara, was where I got my start presenting risk assessment concepts. When I contacted John circa 1988 and told him I needed a class on risk analysis, he told me the best way to get a good class was for me to develop one. I did my research and created a risk analysis class, and for the first two years prayed that no one would ask any questions. Over the past twenty years I think I have finally begun to understand a little bit about risk assessment. Working alongside John O'Leary, Richard Power, Patrice Rapalus, and Pam Salaway, I was able to improve the risk assessment classes.

I have enjoyed the challenges presented by the risk assessment process and I hope you find the concepts easy to use.

About the Author

Thomas R. Peltier is the president of Thomas R. Peltier Associates, LCC, an information security training and consulting firm that conducts training on topics such as risk analysis, policies, standards, procedures, network vulnerability assessments, fundamentals of information security, and Certified Information Systems Security Professional (CISSP®) prep courses in North America as well as on four other continents. He is also the founder of the Southeast Michigan Computer Security Special Interest Group, one of the largest information security professional organizations in the United States, and has taught the information security curriculum for a master's certificate at Eastern Michigan University. Currently he is an adjunct professor at Norwich University in the Information Assurance master's program.

Prior to this, Peltier was director of policies and administration for Netigy Corporation's Global Security Practice, where he helped integrate security services and solutions into the Netigy Corporation suite of offerings. He also refined the techniques for policy and procedure development and the Facilitated Risk Analysis and Assessment Process (FRAAP) based on the ISO 17799, managed the Total Information Protection Strategies (TIPS) team, consisting of seven senior subject matter experts, and helped establish a consultant training program to prepare personnel to sit for the CISSP exam.

For CyberSafe Corporation, Peltier was the national director for consulting services, which included conducting network security assessments using a top-down, bottom-up approach and the development and implementation of the Facilitated Risk Analysis Process (FRAP).

At Detroit Edison, Peltier implemented the development of a corporate information protection program that was recognized for excellence in the field of computer and information security by winning the CSI's Information Security Program of the Year for 1996.

Peltier has also served as president at Blaier & Associates, as an information security specialist for General Motors Corporation, as an information security officer for the Chevrolet-Pontiac-Canada Group, and in various positions at the Chevrolet Engineering Center (CEC).

In 1993, Peltier was awarded the Computer Security Institute (CSI) Lifetime Achievement Award, and in 1999 the Information Systems Security Association (ISSA) Individual Contribution to the Profession Award. In 2001, Mr. Peltier was inducted into the ISSA Hall of Fame. He was also awarded the CSI Lifetime Emeritus Membership Award.

Peltier is the former chairman of the Computer Security Institute's Advisory Council, and chairman of the 18th Annual CSI Conference. He has also served as technical advisor to Commonwealth Films, Boston, in the production of nationally distributed films including *Locking the Door; Virus: Prevention, Detection, Recovery; Back in Business*; and other security awareness and training films. Peltier's published works include *The Complete Manual of Policies and Procedures for Data Security*; *Information Security Policies and Procedures: A Professional Reference*; *Information Security Risk Analysis*; *Information Security Policies, Standards, and Procedures*; *How to Manage a Network Vulnerability Assessment*; and *Information Security Fundamentals.* Peltier also coauthored the *2007 Complete Guide to CISM Certification,* and has been both a contributing author and editor of *The Total CISSP Exam Prep Book (2002),* as well as a contributing author to the *Computer Security Handbook* and *Data Security Management.*

Introduction

The goal of *Information Security Risk Analysis* is to give you the tools and skill set needed to do exactly that. Over the course of this book we will examine many different ways to improve the risk assessment process to work best for you and your organization.

The book is designed in such a manner that the initial discussions will relate to the actual risk assessment process. We will examine each of the steps necessary to complete a successful risk assessment. We will discuss the basic concepts and then we will entertain variations of the theme.

The process that we will use is called the Facilitated Risk Analysis and Assessment Process (FRAAP). This is a qualitative risk assessment process that has been used throughout the world for the past fifteen years. The guiding factor in the development of the FRAAP was that we had neither a budget to purchase a risk assessment product nor the time to implement a product. My team and I began to discuss what the outer limits of time were that we could expect the infrastructure and business people to be able to complete one risk assessment. It was this time factor that drove the development of the FRAAP and over the years added to its refinements. Throughout the book you will be given examples of checklists, forms, questionnaires, and other tools needed to complete a risk assessment.

Once we have covered the basics on how to complete a risk assessment, we will then examine other important concepts and how to implement them. We will examine the concept of risk analysis and how it relates to the risk assessment process. We will discuss where risk analysis fits into the system development life cycle (SDLC) and how it is used in project management processes.

We will discuss the SDLC and how risk analysis, risk assessment, risk mitigation, and vulnerability assessment fit into this structure. We will also review the gap analysis process and see how this can be used to support the quality control objectives of the risk assessment process. We will examine the difference between a gap analysis and a security or controls assessment.

It will be necessary to discuss the cost–benefit analysis process because it is found in a number of other concepts we will discuss.

We will discuss also how to use the concepts developed throughout the book to implement a business impact analysis (BIA) process and an information classification methodology.

The final concept we will explore is the pre-screening methodology. Over the years we have come to the conclusion that not every application, system, or business process needs to have a full-blown risk assessment or BIA run against it. To reach that conclusion, it will be important to create a methodology that will enable the organization to determine what needs analysis and what can benefit best by implementation of a baseline set of controls. Through understanding gap analysis, controls assessment, and information classification requirements, we will be able to generate a baseline set of controls and a methodology to determine whether a risk assessment or BIA is required.

The book is meant to be a reference guide to help you create the components you will need to implement a successful risk assessment process. I have included sample documents that include a management summary and a completed risk assessment action plan. Copies of the following worksheets, checklists and other documents are available at http://www.infosectoday.com/Risk_Assessment.

Chapter 1 The Facilitated Risk Analysis and Assessment Process
Table 1.8 Pre-FRAAP Meeting Checklist
Table 1.32–34 Post-FRAAP Worksheet

Chapter 2 Risk Analysis (Project Impact Analysis)
Table 2.2 Project Impact Analysis Questionnaire

Chapter 4 Business Impact Analysis
Figure 4.2 BIA Sample Worksheet
Table 4.3 BIA Financial Impact Worksheet
Table 4.4 BIA Worksheet Example
Table 4.14 BIA Sample Summary Report

Chapter 5 Gap Analysis
Table 5.3 Gap Analysis Example 1
Table 5.6 Gap Analysis Example 2
Table 5.7 Gap Analysis Example 3

Appendix G Sample Threat Checklist
Sample Threat Checklist

Appendix H Sample BIA Questionnaire
Sample BIA Summary Report
Business Impact Analysis Checklist
Sample Threat Checklist
BIA Consolidated Report

During the discussions additional material is given that can allow you to present a more quantified view of risk assessment. The key element of risk assessment in our business environment is time. If you have more time, you can do more things. During my days in the business world, time was always at a premium.

Chapter 1

The Facilitated Risk Analysis and Assessment Process (FRAAP)

1.1 Introduction

After being in the information security profession for over thirty years and information technology for over forty, I have found that most organizations have the ability to identify threats that can impact the business objectives or mission of the organization. What they cannot do in a systematic manner is to determine the level of risk those threats pose to the organization.

Years ago I worked with a delightful gentleman named Irving Ball. Irv was six feet seven inches, and I am five feet two. One morning Irv came in with a fresh abrasion on his forehead. I inquired about what happened, and Irv said, “Didn’t you see that scaffolding in the parking lot?” I said that I thought that I had. As we headed to my car at lunchtime, we passed the scaffolding and noted that it posed a threat to both of us; however, the probability of my hitting the portion of the scaffolding that Irv had hit was much lower. So the scaffolding was a threat for both of us but the risk to me was lower because the probability and impact were lower.

Just because a threat exists does not mean that the organization is at risk. This is what risk assessment is all about: identifying the threats that are out there and then determining if those threats pose a real risk to the organization.

With the changing business culture, successful security professionals have had to modify the process of responding to new threats in the high-profile, ultra-connected business environment. With outside regulatory agencies and external auditors gaining more oversight strength over recent years, organizations are met with an increased motivation to implement an effective, inexpensive risk assessment process.

Even with the change of focus, today's organizations must still protect the integrity, confidentiality, and availability of information resources they rely on. Although senior management is becoming increasingly interested in security, the fact remains that the business of the enterprise is business. An effective security program must assist the business units by providing high-quality, reliable service in helping them protect the assets of the enterprise.

1.2 FRAAP Overview

The Facilitated Risk Analysis and Assessment Process (FRAAP) was developed as an efficient and disciplined methodology for ensuring that threats to business operations are identified, examined, and documented. The process involves analyzing one system, application, platform, business process, or segment of business operation at a time. By convening a team of internal subject matter experts, the FRAAP will rely on the organization's own people to complete the risk assessment process. These experts must include the business managers and system users who are familiar with the mission needs of the asset under review, and the infrastructure staff who have a detailed understanding of potential system vulnerabilities and related controls. The FRAAP sessions follow a standard agenda and are facilitated by a member of the project office or information security staff. The facilitator is responsible for ensuring that the team members communicate effectively and adhere to the project scope statement.

The team's conclusions about what threats exist, what their risk level is, and what controls are needed are documented for the business owner to use in developing an effective action plan. The FRAAP is divided into three phases:

1. The pre-FRAAP
2. The FRAAP session
3. Post-FRAAP

During the FRAAP session, the team will brainstorm to identify potential threats that could impact the task mission of the asset under review. The team will then establish a risk level of each threat based on the probability that the threat might occur and relative impact in the event that it actually does occur. We will go into more detail on this process later in the book.

The team does not usually attempt to obtain or develop specific numbers for the threat likelihood or annual loss estimates unless the data for determining such factors is readily available. Instead, the team will rely on their general knowledge of threats and probabilities obtained from national incident response centers, professional associations and literature, and their own experience.

When assembling the team, experience causes them to believe that additional efforts to develop precisely quantified risks are not cost effective because:

- Such estimates take an inordinate amount of time and effort to identify and verify or develop.
- The risk documentation becomes too voluminous to be of practical value.
- Specific loss estimates are generally not needed to determine if a control is needed.

After identifying the threats and establishing the relative risk level for each threat, the team identifies controls that could be implemented to reduce the risk, focusing on the most cost-effective controls. The team will use a common set of controls designed to address various types of threats. We will discuss the controls selection process later in this chapter. Ultimately, the decision as to what controls are to be identified in the action plan rests with the business owner.

Once the FRAAP session is complete, the security professional can assist the business owner in determining which controls are cost effective and meet the business needs. Once each threat has been assigned a control measure or has been accepted as a risk of doing business, the senior business manager and participating technical expert sign the completed document. The document and all associated papers are owned by the business unit sponsor and are retained for a period to be determined by the organization's records-management procedures (usually seven years).

Each risk assessment process is divided into three distinct sessions:

1. The pre-FRAAP meeting, which normally takes about an hour, is attended by the business owner, project lead, scribe, and facilitator, and has seven deliverables.
2. The FRAAP session takes approximately four hours, and includes fifteen to thirty people though sessions with as many as fifty and as few as four people have occurred.
3. Post-FRAAP is where the results are analyzed and the management summary report is completed. This process can take up to five work days to complete.

Over the course of this chapter we will examine why the FRAAP was developed, what each one of the three phases entails, and what the deliverables from each phase are.

1.3 FRAAP History

Prior to the development of the FRAAP, risk assessment was often perceived as a major task that required the enterprise to hire an outside consultant, and could take weeks, if not months to complete. Often the risk assessment process was shrouded in mystery and it seemed that elements of voodoo were being used. The final report sometimes looked as if the name of an organization was simply edited into a standard report template.

By hiring outside consultants, the expertise of the in-house staff was often overlooked and the results produced were not acceptable to the business unit manager. Additionally, business managers who were not part of the risk assessment process found that they did not understand the recommended controls, did not want the recommended controls, and often worked to undermine the controls implementation process.

What was needed was a risk assessment process that:

- Was driven by the business owners
- Took days instead of weeks or months to complete
- Was cost effective
- Used the in-house experts

The FRAAP meets all of these requirements and adds another: it can be conducted by someone who has limited knowledge of a particular system or business process but good facilitation skills.

The FRAAP is a formal methodology developed through understanding the previously developed qualitative risk assessment processes and modifying them to meet current requirements. It is driven by the business side of the enterprise and ensures that the controls selected enable the business owners to meet their mission objectives. With the FRAAP, controls are never implemented to meet audit or security requirements. The only controls selected focus on the business need.

The FRAAP was created with an understanding that the internal resources had limited time to spend on such tasks. By limiting the information-gathering session to four hours, the subject matter experts (SMEs) are more likely to participate in the process. Using time as a critical factor, the FRAAP addresses as many risk assessment issues as possible. If there is more time, then there are more tasks that can be performed.

By involving the business units, the FRAAP uses them to identify threats. Once resource owners are involved in identifying threats and determining the risk level, they generally see the business reason why implementing cost-effective controls is necessary to help limit the exposure. The FRAAP allows the business units to take control of their resources. It allows them to determine what safeguards are needed and who will be responsible for implementing those safeguards.

The results of the FRAAP are a comprehensive set of documents that will identify threats, prioritize those threats into risk levels, and identify possible controls that will help mitigate those high-level risks.

The FRAAP provides the enterprise with a cost-effective action plan that meets the business needs to protect enterprise resources while ensuring that business objectives and mission charters are met. Most importantly, with the involvement of the business managers, the FRAAP provides a supportive client or owner who believes in the action plan.

1.4 Introducing the FRAAP

As with any new process, it is always best to conduct user awareness sessions to acquaint employees before the process is rolled out. It will be necessary to explain what the FRAAP is, how it works, and how it will help the business meet its specific objectives.

To be successful, the awareness program should take into account the needs and current levels of training and understanding of the employees and management. There are five keys to establishing an effective awareness program:

1. Assess current level of risk assessment understanding.
2. Determine what the managers and employees want to learn.
3. Examine the level of receptiveness to the security program.
4. Map out how to gain acceptance.
5. Identify possible allies.

To assess the current level of risk assessment understanding, it will be necessary to ask questions of the audience. Although some employees may have been part of a risk assessment in the past, most employees have little firsthand knowledge of risk assessment. Ask questions such as why they believe there is a need for risk assessment. Listen to what the employees are saying and scale the training sessions to meet their specific needs. In the awareness field, one size or plan does not fit for everyone.

Work with the managers and supervisors to understand what their needs are and how the risk assessment process can help them. It will become necessary to understand the language of the business units and to interpret their needs. Once you have an understanding, then you will be able to modify the presentation to meet these special needs. No single awareness program will work for every business unit. There must be alterations and a willingness to accept suggestions from non-security personnel.

Identify the level of receptiveness to the risk assessment process. Find out what is accepted and what is meeting with resistance. Examine the areas of non-compliance and try to find ways to alter the program, if at all possible. Do not change fundamental risk assessment precepts just to gain unanimous acceptance; this is an unattainable goal. Make the process meet the greater good of the enterprise and then work with pockets of resistance to lessen the impact.

The best way to gain acceptance is to make employees and managers partners in this process. Never decree a new control or policy to the employee population without involving them in the decision-making process. This will require you to do your homework and to understand the business process in each department. It will be important to know the peak periods of activity in the department and what the manager's concerns are. When meeting with the managers, be sure to listen to their concerns and be prepared to ask for their suggestions about how to improve the program. Remember: the key here is to partner with your audience.

Finally, look for possible allies. Find out which managers support the objectives of the risk assessment process and those that have the respect of their peers. This means that it will be necessary to expand the area of support beyond risk management and the audit staff. Seek out business managers that have a vested interest in seeing this program succeed. Use their support to springboard the program to acceptance.

A key point in this entire process is never to refer to the risk assessment process or the awareness campaign as "my" program. The enterprise has identified the need for risk assessment and you and your group are acting as the catalysts to moving the process forward. When discussing the process with employees and managers, it will be beneficial to refer to it as "your" risk assessment process or "our" process. Make them feel that they are key stakeholders in this process.

Involve the user community and accept their comments whenever possible. Make the risk assessment process their process. Use what they identify as important in the awareness program. By having them involved, the risk assessment process truly becomes theirs and they are more willing to accept and internalize the results.

1.4.1 Key Concepts

The FRAAP is a formal methodology for risk assessment that is driven by the owner. Each FRAAP session is called by the owner, and the team members are invited by the owner. The concept of what constitutes an owner is normally established in the organization's information security policy. The policy generally addresses the concepts of information asset owner, custodian, and user. A typical company policy may resemble the following:

> Information created while employed by the company is a company asset and is the property of the company. All employees are responsible for protecting company information from unauthorized access, modification, destruction, or disclosure, whether accidental or intentional. To facilitate the protection of company information, employee responsibilities have been established at three levels: owner, custodian, and user.
>
> *Owner:* The highest level of company management of the organizational unit where the information resource is created, or management of the organizational unit that is the primary user of the information resource. Owners have the responsibility to:
>
> - Establish the classification level of all corporate information within their organizational unit.

- Identify reasonable and prudent safeguards to ensure the confidentiality, integrity, and availability of the information resource.
- Monitor safeguards to ensure they are properly implemented.
- Authorize access for those who have a business need for the information.
- Delete access for those who no longer have a business need for the information.

Custodian: Employees designated by the owner to be responsible for maintaining the safeguards established by the owner.

User: Employees authorized by the owner to access information and use the safeguards established by the owner.

Senior management must ensure that the enterprise has the capabilities needed to accomplish its mission or business objectives. As we will see, senior management of a department, business unit, group, or other such entity is considered to be the functional owner of the enterprise's assets, and in their fiduciary duty, act in the best interest of the enterprise to implement reasonable and prudent safeguards and controls. Risk management is the tool that will assist them in the task (Table 1.1).

As you can see in Table 1.1, the risk assessment process assists management in meeting its obligations to protect the assets of the organization. By being an active partner in the risk assessment process and acting in the owner capacity, management gets the opportunity to see what threats are lurking around the business process. The FRAAP allows the owner to identify where control weaknesses are and to develop an action plan to remedy the risks in a cost-effective manner.

The results of the FRAAP are a comprehensive risk assessment document that has identified the threats, risk levels, and controls as well as an owner-created action plan, which includes action items, identifies responsible entities, and establishes a time frame for completion. The FRAAP assists management in meeting its obligation to perform due diligence.

The FRAAP is conducted by a trained facilitator. This individual will lead the team through the identification of threats, the establishment of a risk level by determining probability and impact, and the selection of possible safeguards or controls. Because of the subjective nature of qualitative risk assessment, it will be

Table 1.1 Management Owner Definition

Typical Role	*Risk Management Responsibility*
Management owner	Under the standard of due care, senior management is charged with the ultimate responsibility for meeting business objectives or mission requirements. Senior management must ensure that necessary resources are effectively applied to develop the capabilities to meet the mission requirements. They must incorporate the results of the risk assessment process into the decision-making process.

Table 1.2 FRAAP Facilitator Definition

Typical Role	*Risk Management Responsibility*
FRAAP facilitator	A facilitator is someone who skillfully helps a group of people understand their common objectives and assists them to plan to achieve them without taking a particular position in the discussion. The facilitator will try to assist the group in achieving a consensus on any disagreements that pre-exist or emerge in the FRAAP so that an action plan can be created.

Table 1.3 Fraap Scribe Definition

Typical Role	*Risk Management Responsibility*
FRAAP scribe	The scribe is the individual responsible for recording the oral discussions in a written format. The scribe ensures that the threats are properly recorded and all actions of the risk assessment team are captured accurately.

the responsibility of the facilitator to lead the team into different areas of concern to ensure that as many threats as possible are identified (Table 1.2).

Instead of concentrating on establishing audit or security requirements, the facilitator ensures that the risk assessment process examines threats that might impact the business process or the mission of the enterprise. This ensures that only those controls and countermeasures that are truly needed and cost effective are selected and implemented.

Helping the trained facilitator is an individual acting as a recording secretary that will transcribe the meeting and help create the risk assessment documentation. As a scribe, this individual will accurately record the identifications of threats and all other relevant information. Unlike an editor, the scribe does not alter the written word once the team has agreed that the meaning of the statement has been properly captured (Table 1.3).

1.5 The Pre-FRAAP Meeting

The pre-FRAAP meeting is the key to the success of the project. The meeting is normally scheduled for an hour and a half and is usually conducted at the business owner's office. The meeting should be attended by the business owner (or representative), the project development lead, facilitator, and the scribe. The session will result in seven deliverables.

1. *Pre-screening results*: The pre-screening process is conducted earlier in the system development life cycle. Because the risk assessment is a historical record of the decision-making process, a copy of the pre-screening results should be

entered into the official record and stored in the risk assessment action plan. The pre-screening process is discussed in chapter 3.

2. *Scope statement:* The project lead and business owner will have to create a statement of opportunity for the risk assessment. They are to develop in words what exactly is going to be reviewed. The scope statement process is discussed in detail in Appendix C and an example of a risk assessment scope statement can be found in Appendix C. During the pre-FRAAP meeting, the risk assessment scope statement should be reviewed and edited into final language.

   It is during the development of the scope statement that threat categories need to be determined. In a typical information security risk assessment, we would include the C-I-A triad of confidentiality, integrity, and availability. For a more-detailed discussion on threat category issues, refer to Appendix E.
3. *Visual diagram (visual model):* This is a one-page or foil diagram depicting the process to be reviewed. The visual model will be used during the FRAAP session to acquaint the team with where the process begins and ends.

   There is a good reason to require the inclusion of a visual diagram or an information flow model as part of the FRAAP. Neural-linguistic programming is the study of how people learn. This process has identified three basic learning types:

   i. *Auditory:* These people have to hear something in order to grasp it. During the FRAAP, the owner will present the project scope statement to the team and those that learn in this manner will be fulfilled.

   ii. *Mechanical:* These people must write down the element to be learned. Those taking notes during meetings are typically mechanical learners.

   iii. *Visual:* Most of us fall into this category. Visual learners need to see a picture or diagram to understand what is being discussed. People that learn via this method normally have a whiteboard in their office and use it often. So the visual diagram or model will help these people understand what is being reviewed.
4. *The FRAAP team established:* A typical FRAAP has between fifteen to thirty members. The team is made up of representatives from a number of business infrastructure and business support areas. FRAAP team makeup is discussed in Appendix B.
5. *Meeting mechanics:* This is the business unit manager's meeting. The business unit manager is responsible for scheduling the room, setting the risk assessment time, and having the appropriate materials (overhead, flipcharts, coffee, and doughnuts) on hand.

   This risk assessment meeting is the responsibility of the owner. As the facilitator, you are assisting the owner in completing this task. It is not an information security, project management office, audit, or risk management meeting. It is the owner's meeting and that person is responsible for scheduling the place and inviting the team.

Table 1.4 Risk Assessment Definitions

Term	*Definition*
Asset	A resource of value. An asset may be a person, physical object, process, or technology.
Threat	The potential for an event, malicious or otherwise, that would damage or compromise an asset.
Probability	A measure of how likely it is that a threat may occur.
Impact	The effect of a threat being carried out on an asset, expressed in tangible or intangible terms.
Vulnerability	Any flaw or weakness in the asset's defenses that could be exploited by a threat to create an impact on the asset.
Risk	The combination of threat, probability, and impact expressed as a value in a pre-defined range.

6. *Agreement on definitions:* The pre-FRAAP session is where agreement on FRAAP definitions is completed. These definitions will eventually become a standard used in the risk assessment process. However, it is always a good idea to review the concepts that will be used in the risk assessment (Table 1.4).
7. *Mini-brainstorming session:* Once agreement has been reached on the other 6 items in the pre-FRAAP session, I have found it helpful to conduct a mini-threat identification session. Here the assembled members would identify four of five threats for each business attribute. Table 1.10 is an example of the results of this process. These threat examples will be used in the FRAAP session.

You will want to agree on the definitions of the business attributes be used as the will review elements. For many of risk assessments we have examined the (integrity, confidentiality, availability). Recently a group of my fellow information security professionals and I examined the idea of what attributes should be examined. For years we have concentrated on examining the threats associated with the C-I-A security triad.

Although C-I-A is a traditional form for a risk assessment, it is important to understand that there are other business attributes that can be used in the process. When I was in Psychology 101 class, we discussed functional fixedness, which is a cognitive bias that limits a person to using an object only in the way it is traditionally used. When you give a child a present, the child will oftentimes have more fun playing with the wrapping or the box. That is because the wrapping can be anything. I use this example in my training classes to remind audit, information security, and risk management that there are a vast number of business attributes that can be used to determine risk. Even if your primary use of risk assessment is to determine threats to assets based on examining confidentiality, integrity, and availability, try to remain open to other possibilities.

I posed the following to my colleagues:

> When we are conducting risk assessments, we often examine threats based on C-I-A. We also discussed earlier this week that instead of C-I-A, we could consider reliability -performance -cost (for capital) or portability -scalability -market penetration (for software) as examples. Does the use of these categories confuse our way of thinking — instead of risk categories could these be titled Threat Categories? Also, do we do it this way because it is required or because it helps us think better within set boundaries?
>
> C-I-A, reliability -performance -cost, and portability -scalability -market penetration are just 9 of the hundreds of such things defined in the SABSA method since 1996. We call them "business attributes" and the business attributes profile is used as the basis for all risk management.
>
> The default prompt list/modeling tool kit has the 80 attributes that are most often re-used internationally (see http://www.sabsa.org) although each organization has a different context and thus a different set.
>
> We have a whole section dedicated to users' definitions of these things and demonstrating case studies on the Institute's web site. Sadly that part of the site (it is in the member discussion area) isn't publicly accessible yet but we've about 200 people impatiently waiting on it out of the hundreds that are now certified in the method. We have 60 courses already on the schedule for 2008 so it will be well over a thousand by end of year and that's not counting what happens with it as an MOD standard or as a built-in part of the CISM exams.
>
> *Could this be titled Threat Categories?*
>
> I don't believe so. They are not threats but the areas/things of value we want to protect from the threats, i.e., ultimately the business issues that are at risk. Thus the use of the term "business attributes" seems to fit best.
>
> However, they can easily be used to create a threat modeling taxonomy … and they often are used that way in daily practice. Also, while you have correctly seen potential demarcation lines between different types (you used capital and software) a whole enterprise-wide taxonomy can be constructed that defines the things of value both unique to a division/stakeholder/department/team/project and to the enterprise as a whole. That in turn provides the basis for risk aggregation … see my article in your year-in-review thingy.
>
> *Also, do we do it this way because it is required or because it helps us think better within set boundaries?*
>
> I believe that it is the latter. It isn't actually required but it helps. Boundaries and structure of many kinds help to remove the horrendous subjectivity and variable response we would get from a blank unbounded or unstructured risk management canvas.

Table 1.5 Business Attribute Definitions (C-I-A)

Term	*Definition*
Confidentiality	The assurance that information is not disclosed to inappropriate entities or processes.
Integrity	Assuring information will not be accidentally or maliciously altered or destroyed.
Availability	Assuring information and communications services will be ready for use when expected.

Table 1.6 Business Attribute Definitions (Capital Expenditure)

Term	*Definition*
Reliability	The extent to which the same result is achieved when a measure is repeatedly applied to the same asset.
Performance	A quantitative measure characterizing a physical or functional attribute relating to the execution of a mission/operation or function.
Cost	The total spent for goods or services including money, time, and labor.

Table 1.7 Business Attribute Definitions (Software Procurement)

Term	*Definition*
Portability	A measure of system independence; portable programs can be moved to a new system by recompiling without having to make any other changes.
Scalability	The ability to expand a computing solution to support large numbers of users without impacting performance.
Market penetration	The share of a given market that is provided by a particular good or service at a given time.

The business attributes that are going to be used in the risk assessment process must be discussed and agreed upon during the pre-FRAAP session. A formal set of definitions must also be established. Table 1.5 through Table 1.7 are examples of some of the many business attributes that can be used to examine threats and establish risk levels.

During the pre-FRAAP session, it will be important to discuss the process for prioritizing the threats. When examining the probability and impact of threats, it will be necessary to determine before the meeting if the threats are to be examined as if no controls are in place. This is typically the case when doing a risk assessment on an infrastructure resource. These resources include the information processing network, the operating system platform, and even the information security program.

For other applications, systems, and business processes, the examination of threats takes into account existing controls. When we discuss the FRAAP session, we will examine each of these methods and how they work. This decision should be made during the pre-FRAAP meeting. Once the risk assessment process has been established, this discussion will not be necessary as the organization will standardize the risk-level protocol.

1.5.1 Pre-FRAAP Meeting Checklist

When I attend a pre-FRAAP meeting, I like to take with me a checklist (Table 1.8) that will ensure that I receive all of the items I need to complete the pre-FRAAP process. (Table 1.9 lists the directions to fill out the pre-FRAAP meeting checklist.) By completing this checklist the elements for the project scope statement will be nearly complete. The categories of assumptions and constraints are two of the key elements contained in the checklist and must be part of the project scope statement. It is important that we understand what these are and how they impact the risk assessment process.

I have a client who brings me in from time to time to conduct FRAAP refresher training for employees; those who have taken the training before have an opportunity to be exposed to new ideas and concepts, other employees have the opportunity to be exposed to the process for the first time. Typically this process is done over three or four days. It consists of a day and a half of training, and the pre-FRAAP meeting is conducted during the afternoon of day two. The following day the FRAAP session is conducted, and then that afternoon and the following day I work with the project lead and the facilitator to complete the risk assessment documentation. On the afternoon of day one, the project lead and project lead backup informed me that they had a meeting to attend and would be back the following day. Not only did they miss the afternoon training of day one, they also did not return for any of the day-two training. On the afternoon of day two, the attendees decided to try to put together a project scope statement. The audience was almost exclusively information security and audit professionals. The scope statement lacked the business side, but at least we were able to be ready for the following day. Because of the team makeup, we did not address assumptions or constraints.

On the day of the FRAAP session, the project leads returned with the owner. This was the first time the owner had ever been exposed to a risk assessment process. We presented them with the scope statement that we had created and the owner said that it looked OK to her. So after a brief introduction and an overview of the methodology, we began the process of identifying threats. After about two hours the team had identified nearly one hundred fifty threats. As we were working through the FRAAP session, I noticed that the owner seemed very concerned and I approached her during the break to see if there was a problem. She informed me that the system was going into production on the following Monday and there was no way she could tell her bosses that one hundred fifty threats were uncovered. I sat down with her to review the scope statement and to fill in the assumptions area. A number of the identified threats were directly related to elements within the information security program:

Table 1.8 Pre-FRAAP Meeting Checklist

Issue	*Remarks*
Prior to the meeting	
1. *Date of pre-FRAAP meeting:* Record when and where the meeting is scheduled.	
2. *Project executive sponsor or owner:* Identify the owner or sponsor who has executive responsibility for the project.	
3. *Project leader:* Identify the individual who is the primary point of contact for the project or asset under review.	
4. *Pre-FRAAP meeting objective:* Identify what you hope to gain from the meeting — typically, the seven deliverables will be discussed.	
5. *Project overview:* Prepare a project overview for presentation to the pre-FRAAP members during the meeting.	
Your understanding of the project scope	
The FRAAP methodology	
Milestones	
Pre-screening methodology	
6. *Assumptions:* Identify assumptions used in developing the approach to performing the FRAAP project.	
7. *Pre-screening results:* Record the results of the pre-screening process.	
During the meeting	
8. *Business strategy, goals, and objectives:* Identify what the owner's objectives are and how they relate to larger company objectives.	
9. *Project scope:* Define specifically the scope of the project and document it during the meeting so that all participating will know and agree.	
Applications/systems	
Business processes	
Business functions	
People and organizations	
Locations/facilities	

Table 1.8 (continued) Pre-FRAAP Meeting Checklist

Issue	*Remarks*
10. *Time dependencies:* Identify time limitations and considerations the client may have.	
11. *Risks/constraints:* Identify risks and constraints that could affect the successful conclusion of the project.	
12. *Budget:* Identify any open budget/funding issues.	
13. *FRAAP participants:* Identify by name and position the individuals whose participation in the FRAAP session is required.	
14. *Administrative requirements:* Identify facility and equipment needs to perform the FRAAP session.	
15. *Documentation:* Identify what documentation is required to prepare for the FRAAP session (provide the client the FRAAP document checklist).	

- Passwords being posted on workstations
- Employees leaving workstations logged on and unattended
- Employees leaving work materials out after hours
- Shoulder surfing for passwords or other access codes
- Unauthorized access to restricted areas

Although these were important threats, they were already addressed in the risk assessment conducted on the information security infrastructure and were not unique to the specific application under review. We modified the assumptions section of the scope statement to include a reference to the fact that it was assumed that a risk assessment had been conducted on the information security infrastructure and that compensating controls were in place or were being implemented. We also addressed the processing infrastructure and applications development methodology in the same manner. By making sure the assumptions were properly identified, we reduced the number of threats from approximately one hundred fifty to about thirty.

The FRAAP was not diminished in any way. The one hundred twenty or so threats that were excised from the risk assessment report had already been identified in the infrastructure risk assessments and were being acted upon.

If other risk assessments have been conducted, enter that information into the assumptions area. If the infrastructure risk assessments have not been conducted, enter that information into the constraints area. This allows the risk assessment to

Table 1.9 Pre-FRAAP Meeting Checklist Directions

Issue	*Activity*
Prior to the meeting	
1. Date of pre-FRAAP meeting	Record the date the actual pre-FRAAP meeting is scheduled to occur.
2. Project executive sponsor or owner	Record the full name and proper title of the owner of the asset that is to be reviewed.
3. Project leader	Record the full name and proper title of the project lead for this specific asset or task.
4. Pre-FRAAP meeting objective	There are seven deliverables for the pre-FRAAP meeting: ■ Scope statement ■ Visual model ■ Assessment team ■ Definitions ■ Meeting mechanics ■ Pre-screening results ■ Mini brainstorming results
5. Project overview	If the FRAAP is a new concept to the owner or project lead, provide an overview of the process.
Your understanding of the project scope	
The FRAAP methodology	
Milestones	
Pre-screening methodology	
6. Assumptions	Record any issues that are needed to support the project scope statement.
7. Pre-screening results	Record the pre-screening results.
During the meeting	
8. Business strategy, goals, and objectives	Record the mission of the asset under review and how it supports the overall business objectives or mission of the enterprise.
9. Project scope	Draft the FRAAP scope statement.
■ Applications/systems	
■ Business processes	

Table 1.9 (continued) Pre-FRAAP Meeting Checklist Directions

Issue	*Activity*
■ Business functions	
■ People and organizations	
■ Locations/facilities	
10. Time dependencies	Identify any time issues and enter them into the constraints section of the scope statement.
11. Risks/constraints	Record any issues that may impact the results of the FRAAP.
12. Budget	Where appropriate, establish a work order number or project identification number that FRAAP team members can use in time reporting.
13. FRAAP participants	Record who the stakeholders and other team members are, as requested by the owner.
14. Administrative requirements	Record any special requirements needed for the FRAAP session.
15. Documentation	Record all laws, regulations, standards, directives, policies, and procedures that are part of the infrastructure supporting the asset under review.

concentrate on the specific asset at hand, but puts the organization on notice that other risk assessments must be scheduled.

Other constraints might include the concerns about the use of obsolete operating systems, those that are no longer supported by the manufacturer. The back level of patch applications might also be a constraint to identify.

Assumptions and constraints allow the risk assessment team to focus on the asset at hand. The organization must conduct the other risk assessments to make certain that the infrastructure is as secure as possible.

In recent years an extra process has been added to the pre-FRAAP portion of the risk assessment process. That extra element is a brief mini-brainstorming process (Table 1.10). At the end of the pre-FRAAP session, those in attendance should conduct a quick threat identification process. Using each of the business attributes that are to be examined, the pre-FRAAP team will identify threats to the asset just as the entire team will during the FRAAP session. It will be important to get four or five threats for each business attribute. This information will be used by the FRAAP facilitator during the FRAAP session.

Table 1.10 Mini-Brainstorming Results

Integrity	*Confidentiality*	*Availability*
Data stream could be intercepted.	Insecure e-mail could contain confidential information.	Files stored in personal directories may not be available to other employees when needed.
Faulty programming could (inadvertently) modify data.	Internal theft of information.	Hardware failures could impact the availability of company resources.
Written or electronic copies of reports could be diverted to unauthorized or unintended persons.	Employee is not able to verify the identity of a client, e.g., phone masquerading.	A failure in the data circuit could prohibit system access.
Data could be entered incorrectly.	Confidential information is left in plain view on a desk.	"Acts of God": tornado, tsunami, hurricane.
Intentional incorrect data entry.	Social discussions outside the office could result in disclosure of sensitive information.	Upgrades in the software may prohibit access.

1.5.2 Pre-FRAAP Meeting Summary

The pre-FRAAP meeting sets the stage for the FRAAP session and all of the work that is to follow. It is very important that each of the seven deliverables is as complete as possible. If they are not complete, then this could be a major constraint to the risk assessment process.

1.6 The FRAAP Session

1.6.1 Overview

The FRAAP session is typically scheduled for four hours. This is a very tight time frame that can be expanded if you have the time and resources available. In recent years I have been out in the field conducting FRAAPs for various clients and I have found that the four-hour window is sufficient to capture threats associated with the business attributes of a specific asset. Then identify existing controls and conduct a risk-level analysis of the threats to identify those that require risk remediation.

As we discussed earlier, the key component in the development of the FRAAP was the time commitment that was available from the team members. Think about the typical employee's weekly work schedule. How much free or available time

Table 1.11 FRAAP Session Agenda

Agenda	*Responsibility*
■ Explain the FRAAP process	Facilitator
■ Review scope statement	Owner
■ Review visual diagram	Technical support
■ Discuss definitions	Facilitator
■ Review objectives – Identify threats – Establish risk levels – Identify possible safeguards	Facilitator
■ Identify roles and introduction	Team
■ Review session agreements	Facilitator

does an employee have each week? Many of us spend at least twelve hours of our workweek in meetings. For the people that will be asked to participate in the risk assessment process, there will be an impact to their available time. The FRAAP is designed to meet the needs of an effective risk assessment while impacting the team members as little as possible.

1.6.2 FRAAP Session Introduction

Once the FRAAP session is called together, the executive responsible for the asset under review will address the team with opening remarks. This overview will help the team members understand why they were asked to be part of the FRAAP and how important senior management considers the risk assessment process to be. When the overview is complete, the facilitator will present the agenda to the team. A typical agenda might resemble Table 1.11.

The facilitator will explain the FRAAP to the team. This will include a discussion of the deliverables expected from each stage of the process. With the assistance of the facilitator, the team will identify threats to the asset under review. Using a formula of probability and impact, the team will then affix a risk level to each threat and will finally select possible controls to reduce the risk intensity to an acceptable level.

The business manager owner will then present the project scope statement. It will be important to discuss the assumptions and constraints identified in the statement. The team should have a copy of the scope statement to refer to as needed during the FRAAP session. The assumptions and constraints will be helpful in ensuring that the deliverables are as accurate as possible.

Technical support will then give a five-minute overview of the process using an information flow model or diagram. This will allow the team to visualize the process under review.

Table 1.12 FRAAP Session Agreements

■ Everyone participates.
■ Stay within identified roles.
■ Stick to the agenda/current focus.
■ All ideas have equal value.
■ Listen to other points of view.
■ No "plops"; all issues are recorded.
■ Deferred issues will be recorded.
■ Post the idea before discussing it.
■ Help scribe ensure all issues are recorded.
■ One conversation at a time.
■ One angry person at a time.

The facilitator will then review the term definitions to be used for this FRAAP session. Once the risk assessment process becomes part of the organization's culture, these definitions will become standard and the need for review will diminish. To expedite the process, the FRAAP session definitions should be included in the meeting notice.

The facilitator will then reiterate the objectives and deliverables of this initial stage. At this point, stage two of this process should be briefly discussed. The meeting notice should mention that those individuals needed for stage two will be staying for an additional hour.

At this point, the FRAAP team members should introduce themselves, and the following information should be recorded by the scribe:

- Team member name (first and last)
- Department
- Location
- Phone number

After the introductions, the facilitator will review the session agreements with the team members (Table 1.12).

1.6.3 FRAAP Session Talking Points

- *Everyone participates.* It is important to get input from everyone in attendance. Some will want to sit back for the first few minutes to get comfortable with the lay of the process. Some of this apprehension can be alleviated by having a FRAAP awareness session throughout the organization. Many times, it is the fear of the unknown that causes team members to hold back. Brief awareness sessions that explain the reasons for and the process done by the risk assessment process will afford the team members a greater feeling of participation.

- *Stay within identified roles.* Introduce the facilitator and scribe. Explain that your job is to get the FRAAP completed within the limited time frame. The scribe will record all of the agreed-upon findings of the risk assessment. All others present are team members. As they enter the room, they step out of their regular roles and assume their roles as team members
- *Stick to the agenda/current focus.* The reason that the scope statement and visual model are discussed early in the process is so that everyone is reminded of the focus of the FRAAP meeting. We all have attended meetings where the intended purpose seems to get thrown out and anything else is discussed. It will be your job to keep the team focused.
- *All ideas have equal value.* This one is very difficult. As discussed earlier, some people are a bit intimidated by other team members. Sometimes the users are apprehensive about discussing threats to applications or systems while IT infrastructure personnel are present. It will be necessary for everyone to feel that their ideas are just as important as anyone else's.
- *Listen to other points of view.* Many times in meetings, some attendees break out of the group and carry on private conversations. At the beginning of the session we try to remind the team that the best way we can gain the respect we want is by showing respect to others.
- *No "plops"; all issues are recorded.* At least once in every session someone will comment that "this may seem stupid, but…" and then present a unique twist to the issues being discussed. The question of what was considered is one of many that arise when a risk assessment decision is being questioned. This very question ("what did you consider?") is why it is important to record all issues.
- *Deferred issues will be recorded.* In the FRAAP documentation, there is a spot to record any issue that is outside the scope of the current meeting. This will allow the team to record the concern and assign someone to follow up on it.
- *Post the idea before discussing it.* There will be a period of discussion on a particular threat, followed by some editing, and finally the scribe will post the agreed-upon item.
- *Help the scribe ensure that all issues are recorded.* Although there are time constraints on completing the session, it is vitally important to capture the issues and comments correctly.
- *One conversation at a time.* As we discussed earlier, it is important for the team to keep focused on the task at hand. If a number of separate conversations break out, then the objectives of the FRAAP session may not be completed during the allotted time.
- *Apply the three- to five-minute rule.* When discussing the risk level-setting factors, it is important that, after the first three or four discussions, a time limit be more or less adhered to.

When all of the preliminary activities have been concluded, it is time to begin the risk assessment process.

1.6.4 FRAAP Threats Identification

When I conduct a FRAAP, I like to have the room set up in a "U" shape. This allows me to work closer to the team members and it allows the process to flow around a conference room table. Having the room set up in this manner means everyone is in the front row; if the room is set up classroom style, it is harder to get the people in the back to feel that they are part of the team.

In the room setup it is important to include pads of paper and pens or pencils for the team to use. The team will be writing down ideas, and it is always best to have the implements readily available rather than taking up valuable time trying to find them.

During the FRAAP session, I normally discourage the use of laptops or PDAs. The team has been called by the owner to assist in meeting a due diligence obligation. If the team members are busy answering e-mail or distracted by other activities, the risk assessment will suffer. I also request that all cell phones and pagers be placed on "stun" or vibrate so as not to disturb the other team members.

To begin the brainstorming process, the facilitator will put up the first business attribute to be reviewed (Table 1.13). This will include the definition of the review element and some examples of threats that the team can use as thought-starters. I normally use a PowerPoint slideshow for this process so that the entire team can see what it is that the FRAAP is trying to identify.

The team is given three to five minutes to write down threats that are of concern to them. The facilitator will then go around the room getting one threat from each team member. Many will have more than one threat, but the process is to get one threat and then move to the next person. This way everyone gets a turn at participating. The process continues until everyone passes (that is, there are no more threats that the team can think of).

During the first two rounds, most of the team members will participate. As the rounds progress, the number of team members with new threats will diminish. When it gets down to just a few still responding, you can ask for a new threat from anyone rather than going around the table and calling on each person again.

Table 1.13 FRAAP Brainstorming Attribute 1: Integrity

Definition	*Threats*
Assuring information will not be accidentally or maliciously altered or destroyed.	Data stream could be intercepted.
	Faulty programming could (inadvertently) modify data.
	Written or electronic copies of reports could be diverted to unauthorized or unintended persons.
	Data could be entered incorrectly.
	Intentional incorrect data entry.

If a person passes, it does not mean that person is then locked out of the round. If something new comes into their mind, then they can join back in when it is their turn to do so again. They may hear a threat from someone else that will jog their thought process. This is why I recommend that there be paper and pens available for the team members to write down these quick-hitting ideas. Most of us suffer from terminal CRS (can't remember stuff). By providing paper and pens, the team members can capture these fleeting thoughts.

I am sad to point out that to some people everything is a contest. Too often the brainstorming round will dwindle down to two team members. When this occurs, the battle to be "King of the Threats" begins. They will continue to throw out ever-more-absurd threats until one combatant will finally yield. I share this with you only so that you can be on the alert for such behavior.

Once all of the integrity threats have been recorded, it is time for the facilitator to display the second review element with threat examples and give the team three to five minutes to write down their ideas (Table 1.14).

During this phase, I like to start the threats identification on the opposite side of the room from where I started last time. This allows those who were last to be first and get the best threats. The collecting of threats will continue until everyone has passed and there are no more confidentiality threats. After the scribe has indicated that everything has been captured, it will be time to go to the third element (Table 1.15).

Once the threats have been recorded, the FRAAP documentation will look like Table 1.16.

When I am conducting a FRAAP session, I use different colored pens for each element. Integrity might be recorded in blue, confidentiality in green, and availability in black. This will allow me to keep track of the threats by color coding them. As a flipchart page is filled up, I post it around the conference room. I record each threat sequentially within an element. For example, I will record all integrity threats in blue and number each threat in the order it was received, starting with

Table 1.14 FRAAP Brainstorming Attribute 2: Confidentiality

Definition	*Threats*
The assurance that information is not disclosed to inappropriate entities or processes.	Insecure e-mail could contain confidential information.
	Internal theft of information.
	Employee is not able to verify the identity of a client, e.g., phone masquerading.
	Confidential information is left in plain view.
	Social discussions outside the office could result in disclosure of sensitive information.

Table 1.15 FRAAP Brainstorming Attribute 3: Availability

Definition	*Threats*
Assuring information and communications services will be ready for use when expected.	Files stored in personal directories may not be available to other employees when needed.
	Hardware failures could impact the availability of company resources.
	A failure in the data circuit could prohibit system access.
	"Acts of God": tornado, tsunami, hurricane.
	Upgrades in the software may prohibit access.

Table 1.16 FRAAP Worksheet 1 after Threats Have Been Identified

Business Attribute	*Threat*
Integrity	Data stream could be intercepted.
	Faulty programming could (inadvertently) modify data.
	Written or electronic copies of reports could be diverted to unauthorized or unintended persons.
	Data could be entered incorrectly.
	Intentional incorrect data entry.
Confidentiality	Insecure e-mail could contain confidential information.
	Internal theft of information.
	Employee is not able to verify the identity of a client, e.g., phone masquerading.
	Confidential information is left in plain view.
	Social discussions outside the office could result in disclosure of sensitive information.
Availability	Files stored in personal directories may not be available to other employees when needed.
	Hardware failures could impact the availability of company resources.
	A failure in the data circuit could prohibit system access.
	"Acts of God": tsunami, tornado, hurricane.
	Upgrades in the software may prohibit access.

threat #1. When I move to confidentiality threats, I will switch to a green marker and start the numbering over again with #1. I will do the same when I get to the availability threats.

When all the threats have been posted, I recommend that the team take a fifteen-minute coffee break to do three important activities:

1. Check messages.
2. Get rid of old coffee and get new.
3. Clean up the raw threats.

During the break, have the team review the threats, and delete duplicate threats and combine like threats within a specific element. If a threat is repeated in the integrity and confidentiality elements, it is not considered to be a duplicate. It is only a duplicate if it appears more than once within a specific element. Only allow the break period, fifteen minutes, for the cleanup process.

1.6.5 Identifying Threats Using a Checklist

In recent years, some organizations have faced the task of doing a large number of risk assessments to become compliant with new laws and regulations. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a specific example. A number of healthcare organizations contacted me to help them put together their risk assessment program. When we began to examine their specific needs, we found out that they did not have four hours for the risk assessment process, but they could get people to commit to a two-hour window. So from there we worked to find ways to streamline the process. We were able to meet the two-hour window by creating a checklist of threats to work from. The results of this work are available in Appendix G; also see Table 1.17.

To keep the risk assessment as clear as possible, we will concentrate on the activities that take place using the brainstorming techniques. When we have completed that discussion, we will turn our attention to the checklist style of risk assessment.

Table 1.17 Sample Threats Checklist

Threat	*Applicable (Yes/No)*
Environmental	
Power flux	
Power outage — internal	
Power outage — external	
Water leak/plumbing failure	
HVAC failure	

1.6.6 Identifying Existing Controls

Once the threats list has been completed, the team should quickly review each threat to determine whether there are any existing controls in place that address the threat issue. By identifying those threats that have existing controls in place, the team will be better able to determine the real level of current risk. This is one of the many reasons that the FRAAP needs representation from the various infrastructure groups. Typically, they will know best what controls and safeguards are already implemented (Table 1.18).

1.6.7 Establishing Risk Levels

This is probably the most important portion of the FRAAP and often the most confusing and most fun. You will want to ensure that the team has had an opportunity to examine the definitions used to establish probability and impact threshold levels. I like to include this information in the meeting notice attachments. This process will also be discussed during your FRAAP awareness program and briefly reviewed in the FRAAP session opening remarks.

For our initial review of the risk level-setting process, we will use a very simple example of the probability and impact thresholds. Appendix N has additional examples of more-intricate processes to establish the threat risk level. Recently, I have become aware that management likes “heat maps.” The color coding of issues helps management and the team quickly identify where those issues fall in the severity levels.

At this point in the FRAAP, we have identified threats to the asset under review using the agreed-upon business attributes. We then examined each threat and identified those that had existing controls or safeguards in place. Our next task will be to determine the likelihood of the occurrence of a threat over a specific period of time and the impact to the organization in the event that it did occur (Table 1.19).

The team will discuss how likely the threat is to occur during the specified time frame. You will want to apply a good dose of common sense to the discussion. One of the examples that I like to use is the threat that an unattended workstation could be used by some other person to access the system. A good reality check is what you want to instill in this process. In the thirty years I have been in information security, this threat has always made every discussion list. I am not certain that I can cite one example of this threat actually occurring. So when you discuss probability, you will want them to address whether this threat has actually occurred. If so, when was the last time? This will provide the team with an ongoing reality check. You will want to keep them focused on the fact that the threats are being examined with existing controls in place.

Once the probability has been established, you will want to identify the impact presented by that threat to the asset under review (Table 1.20). Here, again, it will

Table 1.18 FRAAP Worksheet 2 after Existing Controls Have Been Identified

Business Attribute	*Threat*	*Existing Controls*
Integrity	Data stream could be intercepted.	Vacant ports are disconnected.
	Faulty programming could (inadvertently) modify data.	Programs are tested before going into production, and change management procedures are in place. GLBA 's Information Technology Policies & Procedures Manual No. 5-11, ISD Documentation; Test Plan and Test Analysis Report Standard.
	Written or electronic copies of reports could be diverted to unauthorized or unintended persons.	
	Data could be entered incorrectly.	Transaction journals are used. Contracts with third parties include language that addresses data integrity and service level agreements are designed to protect against this risk.
	Intentional incorrect data entry.	Transaction logs are maintained and reviewed to detect incorrect data entry.
Confidentiality	Insecure e-mail could contain confidential information.	
	Internal theft of information.	GLBA 's Code of Conduct Policy.
	Employee is not able to verify the identity of a client, e.g., phone masquerading.	Customer must provide the date of last deposit or other confidential personal information within their file before information is released.
	Confidential information is left in plain view.	
	Social discussions outside the office could result in disclosure of sensitive information.	Code of Conduct/Conflict of Interest Policy; Annual Awareness item.

continued