DATA SECURITY MANAGEMENT

FACILITATED RISK ANALYSIS PROCESS (FRAP)

Thomas R. Peltier

INSIDE

Facilitated Risk Analysis Process (FRAP) Overview; Why the Need for FRAP; Introducing the FRAP to Your Enterprise; The Pre-FRAP Meeting; The FRAP Team; The FRAP Facilitator; The FRAP Session; Post-FRAP Meetings

INTRODUCTION

Most enterprises are attempting to manage the same types of risks that face every other organization. With the changing business culture, the successful security teams have had to modify the process of responding to new risks in the high-profile, E-business environment.

Even with the change of focus, today's organizations must still protect the integrity, confidentiality, and availability of information resources they rely on. While there is an increased interest in security by upper management, the fact remains that the business of the enterprise is business. The security program must assist the business units by providing high-quality reliable service in helping them protect the enterprise's assets.

FACILITATED RISK ANALYSIS PROCESS (FRAP) OVERVIEW

The Facilitated Risk Analysis Process (FRAP) was developed as an efficient and disciplined process for ensuring that information security-related risks to business operations are considered and documented. The process involves analyzing one system, application or segment of business operation at a time and convening a team of individuals that includes business managers who are familiar with business information needs and technical

PAYOFF IDEA

The Facilitated Risk Analysis Process (FRAP) is an efficient and disciplined process for ensuring that information security-related risks to business operations are considered and documented. The process involves analyzing one system, application, or segment of business operation at a time and convening a team of individuals that includes business managers who are familiar with business information needs and technical staff who have a detailed understanding of potential system vulnerabilities and related controls. The sessions, which follow a standard agenda, are facilitated by a member of the project office or information protection staff who is responsible for ensuring that the team members communicate effectively and adhere to the agenda.

staff who have a detailed understanding of potential system vulnerabilities and related controls. The sessions, which follow a standard agenda, are facilitated by a member of the project office or information protection staff and is responsible for ensuring that the team members communicate effectively and adhere to the agenda.

During the session, the team brainstorms to identify potential threats, vulnerabilities, and resultant negative impacts on data integrity, confidentiality, and availability. Then the team will analyze the effects of such impacts on business operations and broadly categorize the risks according to their priority level. 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 vulnerabilities obtained from national incident response centers, professional associations and literature, and their own experience.

When assembling the team, it is the experience that allows 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 use
- specific loss estimates are generally not needed to determine if a control is needed

After identifying and categorizing risks, the team identifies controls that could be implemented to reduce the risk, focusing on the most cost-effective controls. The team will use a starting point of 26 common controls designed to address various types of risk. Ultimately, the decision as to what controls are needed lies with the business managers, who take into account the nature of the information assets and their importance to business operations and the cost of controls.

The team's conclusions as to what risks exist, what their priority is, and what controls are needed are documented and sent along to the project lead and the business manager for completion of the action plan. Here the security professional can assist the business unit manager in determining which controls are cost-effective and meet their business needs. Once each risk has been assigned a control measure or has been accepted as a risk of doing business, then the senior business manager and technical expert participating 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 records-management procedures (usually seven years).

Each risk analysis process is divided into four distinct sessions:

1. The pre-FRAP meeting takes about an hour and has the business manager, project lead, and facilitator.
2. The FRAP session takes approximately four hours and includes 7 to 15 people, through sessions with as many as 50 and as few as four people have occurred.
3. FRAP analysis and report generation usually takes 4 to 6 days and is completed by the facilitator and scribe.
4. Post-FRAP session takes about an hour and has the same attendees as the pre-FRAP meeting.

The rest of this article examines why the FRAP was developed, what each one of the four phases entails, and what are the deliverables from each phase.

WHY THE NEED FOR FRAP

Prior to the development of the FRAP, risk analysis was often perceived as a major task that required the enterprise to hire an outside consultant and could take an extended period of time. Often the risk analysis process took weeks to complete and was a major budget item. 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.

The results of the old process were business managers who did not understand the recommended controls, did not want the recommended controls and often undermined the implementation process.

What was needed was a risk analysis process that is driven by the business managers, takes days instead of weeks or months, is cost effective, and uses the in-house experts. FRAP meets all of these requirements and adds another in that in can be conducted by someone with limited knowledge of particular system or business process, but with good facilitation skills.

FRAP is a formal methodology developed through understanding the previously developed qualitative risk analysis processes and modifying them to meet current requirements. It is driven by the business side of the enterprise and ensures that controls enable the business process to meet its objectives. There is never a discussion about controls as security or audit requirements. FRAP focuses on the business need and the lack of time that can be spent on such tasks.

By involving the business units, FRAP uses them to identify risks and threats. Once the resource owners are involved in identifying threats, then they generally set up and look for assistance in implementing cost-effective controls to help limit the exposure. FRAP 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 FRAP are a comprehensive document that identifies threats, assigns priorities to those threats and identifies controls that will help mitigate those threats. It provides the enterprise with a cost-effective action plan that meets the business needs to protect enterprise resources while conducting business. Most importantly, with the involvement of the business managers, FRAP provides a supportive client or owner who believes in the action plan.

Introducing the FRAP to Your Enterprise

When beginning FRAP, it will be necessary to explain what FRAP is and how it works. This will be necessary for the first few months of the introduction of the process to your enterprise. You might want to conduct FRAP overview sessions to assist you in this process. It will be most beneficial to conduct these sessions initially with the applications and systems development groups. Eventually, the business units should be introduced to the process.

It will be necessary for you to sell this service to your business community. Use some of the arguments discussed above, but let them know that this cost-effective process will allow the business units to control their own destiny. The FRAP has been implemented to assist the enterprise in meeting business objectives and that the completion of a risk analysis process is the cost of doing business in today's environment.

The key will be that the process will help identify business risks. The risk will be classified as undesirable or unauthorized events not in terms of their effect on security or audit requirements, but in terms of their effect on completing the business objectives or mission of the enterprise.

It will be necessary to ensure that all employees understand some basic definitions in FRAP. There will be more definitions later, but for now, it will be necessary to ensure that employees understand five key definitions:

1. *Risk* — is a potential event that will have a negative impact on the business objectives or mission of the enterprise.
2. *Control* — is a measure taken to avoid, detect, reduce or recover from a risk to protect the business process or mission of the enterprise.
3. *Integrity* — information is as intended, without unauthorized or undesirable modification or corruption.
4. *Confidentiality* — information has not undergone unauthorized or undesirable disclosure.
5. *Availability* — applications, systems, or information resources are accessible when necessary.

FRAP objectives are to identify potential undesirable or unauthorized events — risks that could have a negative impact to the business objec-

tives or mission of the enterprise. Once these risks have been identified and prioritized, then appropriate controls will be identified to help mitigate the risk level.

The team will examine all types of risks, whether accidental or deliberate. The facilitator will assist the team though the brainstorming process by asking leading question. Try to get the team to examine other courses of risk. "What do you think of this?" or "What would happen if this occurred?"

The Pre-FRAP Meeting

The pre-FRAP meeting is the key to the success of the project. The meeting normally lasts about an hour and is usually conducted at the client office. The meeting should have the business manager (our representative), the project development lead, and the facilitator. There will be five key components that come out of this one-hour session.

1. *Scope statement* — the project lead and business manager will have to create a statement of opportunity for review. They are to develop in words what exactly is going to be reviewed.
2. *Visual* — there will need to be a visual model. This is a one-page or foil diagram depicting the process to be reviewed. The visual model will be used during the FRAP session to acquaint the team with where the process begins and ends.
3. *Establish the FRAP team* — A typical FRAP has between 7 to 15 members and has representatives from a number of business and support areas. We will discuss FRAP-team make up later in this article.
4. *Meeting mechanics* — this is the business unit manager's meeting and that individual is responsible for getting the room, setting the schedule, getting the materials needed (overhead, flip charts, coffee and doughnuts).
5. *Agreement on definitions* — the pre-FRAP session is where the agreement on FRAP definitions is completed. You will want to agree on the definitions if the review elements (integrity, confidentiality, availability). In addition to the review elements, it will be necessary to agree on:
   - risk
   - control
   - impact
   - vulnerability

During the pre-FRAP session, it will be important to discuss the process for prioritizing the threats. There are two schools of thought for how to go about this process. The first is to have the FRAP team review all identified threats as if there are no controls in place. This will establish the "ideal"

logical control set. This will allow the FRAP to be used a gap analysis between "as-is" and "to-be" demonstrating the gap and vulnerability.

The second method is to assess threats with existing controls in place. The key phrase here is "assess." There are three phases in the information protection process:

1. *Risk analysis* — to review the existing environment, identify threats, prioritizes the threats ad recommend safeguards.
2. *Safeguard implementation* — determine which safeguards make sound business sense and implement those.
3. *Security assessment* — review the safeguards (controls) and determine their effectiveness.

The FRAP Team

During the pre-FRAP meeting, the business manager and project lead will need to identify who should be part of the FRAP session. The ideal number of participants is between 7 and 15. It is recommended that representatives from the following areas be included in the FRAP process:

- Functional owner
- System user
- System administrator
- Systems analysis
- Systems programming
- Applications programming
- Database administration
- Information security
- Physical security
- Telecommunications
- Network administration
- Service provider
- Auditing (if appropriate)
- Legal (if appropriate)
- Human resources (if appropriate)
- Labor relations (if appropriate)

There are no hard and fast rules as to who should attend, but to be successful, it will be necessary for the functional business owner and system users to be part of the FRAP. It is their business process that will be reviewed and it will be important that hey be part of the process.

The systems group is also an important pat of the FRAP team. The system administrator is normally found in the user department and has had some training in the new application or system and is the initial point of contact for users when they have problems.

The systems analysis group are those bilingual individuals that speak fluent business and information systems. That can be vital in ensuring that what is spoken at a FRAP is understood by all parties.

The Systems programming group is those individuals that support the platforms and ensure that the current operating environment is working and properly configured.

Applications programming is the individuals that will either create the new application or will customize existing application or third-part software to meet the functional owner's needs.

The database administrators are the technical individuals that understand how the mechanics of the database works and are often responsible for ensuring that database security mechanisms are working properly.

Information security should have a representative as part of the FRAP team. Many FRAPs are facilitated by someone from information security, but this is often a conflict of interest. The facilitator is to have an aura of neutrality about them.

Physical security or someone from facility engineering should be part of the team. They will bring a perspective of viewing concerns from the physical operations of the environment.

If the resource under review is going to access the network or other telecommunication devices, then representatives from those areas must be part of the process.

Any Web-based applications will require representatives from the Internet support organization, including the Web Master, and the firewall administrator.

The next four groups are all classified as "if appropriate." The audit staff is a group that can offer some good ideas, but they often impact the free flow of information. Unless you have a very good working relationship with the audit staff, it is recommended that they not take part in the FRAP session. The audit team will see the results of the FRAP later and will probably use the output when they conduct an audit of the resource.

The legal staff is normally too busy for every FRAP. However, if there is a resource under review that has a major impact on the enterprise, it will probably be appropriate to extend an invitation to them. I recommend that you meet with the legal staff and discuss what the FRAP is, as we discussed above, and attempt to establish a guideline when they need to either be part of the process or to see specific risk concerns.

Whenever a resource under review is going to impact employees, then human resources and, for represented employees, labor relations need to be involved in the FRAP.

This list is not all-inclusive nor does it represent the correct mix of players if the FRAP moves away from the traditional information security risk analysis. The key here is to understand that to be a successful FRAP, there must be representation from a wide spectrum of employee groups.

The FRAP Facilitator

Facilitation of a FRAP requires the use of a number of special skills. These skills can be improved by attending special training and by facilitating. The skills required include the ability to:

- *Listen* — having the ability to be responsive to verbal and non-verbal behaviors of the attendees. Being able to paraphrase responses to the subject under review and to be able to clarify the responses.
- *Lead* — getting the FRAP session started and encouraging discussion while keeping the team focused on the topic at hand.
- *Reflect* — repeating ideas in fresh words or for emphasis.
- *Summarize* — being able to pull themes and ideas together.
- *Confront* — being able to feed back opinions, reacting honestly to input from the team and being able to take harsh comments and turn them into positive statements
- *Support* — creating a climate of trust and acceptance.
- *Crisis intervention* — helping to expand a person's vision of options or alternatives and to reinforce action points that can help resolve any conflict or crisis.
- *Center* — helping the team to accept others' views and build confidence for all to respond and participate.
- *Solve problems* — gathering relevant information about the issues at hand and help the team establish an effective control objective.
- *Change behavior* — look for those that appear not to be part of the process and bring them into the active participation.

Basic facilitation rules must be observed by all facilitators if the FRAP is to be successful.

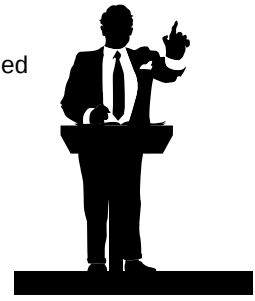
1. FRAP leaders must observe carefully and listen to all that the team says and does.
2. Recognize all input and encourage participation.
3. Be observant for non-verbal responses.
4. Do not lecture, listen and get the team involved.
5. Never loose sight of the objective.
6. Stay neutral (or always appear to remain neutral).
7. Learn to expect hostility, but do not become hostile.
8. Avoid being the "expert authority." The facilitator's role is to listen, question, enforce the process and offer alternatives.
9. Adhere to time frames and be punctual.
10. Use breaks to free a discussion.
11. The facilitator is there to serve the FRAP team.
12. Stop the FRAP if the group is sluggish and difficult to control.

As the FRAP facilitator it will be necessary to develop your own FRAP tool kit. This tool kit should include:

EXHIBIT 1 — FRAP 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
—Apply the 3-minute rule
—Be: Prompt
Fair
Nice
Creative

Have Fun!



- Flip charts
- Masking tape or push pins
- Colored pens (I like the Mr. Sketch Scented Markers (12))
- Tent cards
- Session agreements

The Session Agreements were developed a number of years ago, and some of my team members have had theirs laminated and post them in the FRAP session room.

The agreements require that:

- *Everyone participate* — you will see how we work that out in the FRAP session process.
- *Stay with identified roles* — the facilitator will facilitate and the scribe will scribe, everyone else will participate.
- *Stick to the agenda and current focus* — the scope statement and visual will be posted or given to all attendees.
- *All ideas have equal value* — where George Orwell said that "all were equally, but some where more equal than others," here we try for equality.
- *Listen to other points of view* — get the team to actually listen to the speaker and not just wait for their turn with the token.
- *No "plops" … all issues are recorded* — Jack Durner of the Mendon Group gave us this term, nothing "plops" onto the floor.

- *Deferred issues will be recorded* — if an item is outside the scope of what is under review, then it is recorded on the deferred issues list and will have someone assigned to look into the issue.
- *Post the idea before discussing it* — get it on the flip chart first.
- *Help the scribe ensure all issues are recorded* — I bring a scribe along with me to record what is posted on the flip charts.
- *One conversation at a time* — here is where your facilitation skills will be tested.
- *One angry person at a time* — I usually volunteer for this job.
- *Apply the 3-to-5 minute rule* — all discussions must be concluded within the agreed to timeframe.
  Be:
  - prompt
  - fair
  - nice
  - creative
- Have fun.

The FRAP Session

The FRAP session generally is scheduled for four hours. Some organizations have expanded the process to last as long as three days, but typically, the four-hour limit is based on busy schedules and the flexibility of the FRAP. The FRAP session can be divided into three distinct sections, with nine elements driving out three deliverables.

Phase 1 — Logistics — during this phase the FRAP team will introduce itself, giving name, title, department, and phone number (all of this will be recorded by the Scribe). The roles of the FRAP team will be identified and discussed. Typically there are five roles:

1. The Owner
2. The Project Lead
3. The Facilitator
4. The Scribe
5. The Team Members.

During this initial phase, the FRAP team will be given an overview of the process that they are about to take part in. They will also be exposed to the Scope Statement and then someone from the technical team will give a five-minute overview of the process under review (the Visual model). Finally, the definitions will be reviewed and each member should be given a copy of the definitions.

Once the preliminaries are complete, the FRAP team will begin the Brainstorming process (see Exhibit 2). This is Phase 2 and will take each review element (integrity, confidentiality, and availability) and identify risks, threats, concerns, and issues for each element.

EXHIBIT 2 — Brainstorming Definition and Sample Risks

Note: Examples of risks (NOT a complete list)
Threats to Confidentiality:
- Access without authorization
- Disclose without authorization
- Observe or monitor transactions
- Copy without authorization
- Packet sniffing on network
- Contractor accessing confidential information

Definition:
Confidentiality: information has not undergone unauthorized or undesirable disclosure.

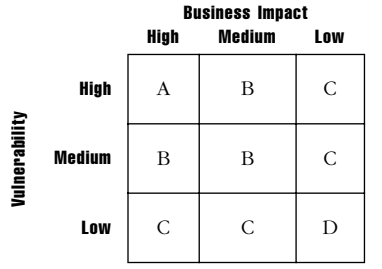
The process for brainstorming is that the facilitator will display the definition and some working examples of risks. The team is then given three minutes to write down risks that are of a concern to them. The facilitator will then go around the room getting one risk from each team member. Many will have more than one risk, but the process is to get one risk 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 risks that the team can think of).

The brainstorming process continues until each of the review elements has been completed. Once this process is complete, it is recommended that the team be given a coffee break. When they come back into the conference room, have them review the risks posted around the room and then take a few minutes to clean up duplicate risks and to make any edits where deemed appropriate.

Once the cleanup is complete (only allow about 10 to 15 minutes for this process), the team will now concentrate in prioritizing the risks. This is done by determining the enterprises vulnerability to the risk and the business impact if the risk where to occur. These definitions are agreed upon at the pre-FRAP meeting and are presented to the team during the introduction. A typical set of definitions might be:

- *High* vulnerability: very substantial weakness exist in the systems or the operational routine, and where the business impact potential is severe or significant, the control *must* be improved.
- *Medium* vulnerability: some weakness exist and where the business impact potential is severe or significant, the controls can and should be improved.
- *Low* vulnerability: the system is already well constructed and operated correctly. No additional controls are needed to reduce vulnerability.

EXHIBIT 3 — Sample Priority Matrix



- *Severe* impact (High): likely to put us out of business or severely damage our business prospects and development.
- *Significant* impact (Medium): will cause us significant damage and cost, but we shall survive.
- *Minor* impact (Low): the type of operational impact we expect to have to manage as part of the ordinary business life.

The team would be aided by using the priority model shown in Exhibit 3.

The box selected will correspond to a letter grade assigned to the risk as its priority. The response from the FRAP team will be as follows:

- A — corrective action must be implemented
- B — corrective action should be implemented
- C — requires monitoring
- D — No action required

There are a number of different ways in which the team can assign the priority to each risk. The three most popular are:

1. The facilitator goes over each risk one by one and the team discusses each risk and then reaches consensus.
2. The facilitator reviews the first three or four risks to ensure that the team has the right idea on how the process works, and then each team member is given a colored marker and asked to assign a priority. If they have no opinion, then they leave that one blank and move on to the next risk. When the team is done, then the facilitator will review the work and where there appears to be a conflict, the facilitator will open the process up for discussion. As an example — where there are 15 FRAP team members, and ten assign a value of "C" to the risk and 5 assign either an "A" or a "B," then the facilitator will want to discuss the issue to ensure that "C" is the most correct answer.

EXHIBIT 4 — FRAP Session Deliverables

Risk #	Risk	Type	Priority	Controls
1	Information accessed by personnel not intended to have access	INT	B	3, 5, 6, 11, 12, 16
2	Unclear or nonexistent versioning of the information	INT	B	9, 13, 26
3	Database could be corrupted by hardware failure, incorrect, bad software	INT	D	
4	Data could be corrupted by an incomplete transaction	INT	C	
5	Ability to change data in transit and then changing it back in order to cover the activity	INT	C	
6	A failure to report integrity issues	INT	A	7, 11, 12, 13, 20, 21
7	Incompletely run process or failure to run a process that could corrupt the data	INT	B	1, 2, 12, 13, 14, 15, 18, 20, 21, 25
8	Lack of internal processes to create and control, manage data across functions	INT	A	7, 13, 17, 20, 23, 25
9	No notification of integrity problems	INT	A	7, 13, 26
10	Information being used in the wrong context	INT	B	11, 12, 19
11	Third-party information may have integrity issues	INT	B	7, 13, 26
12	Third-party access to information	INT	A	3, 4, 5

3. The third method I have seen used is that the facilitator gives each team member 10 dots (the kind you can get at any office store and then have a self-adhesive). The each team member is allowed to vote for 10 "Major" risks. Those with dots will require a control; those without are considered minor risks.

The FRAP session will generate three deliverables:

1. The identification of risks
2. The prioritization of risks
3. Suggested controls for major or high priority risks

In Exhibit 4, the Risk column indicates some of the 120 risks that were identified in this FRAP process. The key to Exhibit 4 is:

- *Risk* = actual risk voiced by FRAP team member
- *Type* = Integrity, Confidentiality, or Availability risk
- *Priority* = Priority level A, B, C, or D
- *Controls* = controls identified to help mitigate the risk

The final process in the FRAP session is to identify controls for those risks identified as requiring them. When the invitation to the FRAP ses-

sion was sent out, the business manager included a list of 26 controls, as shown in Exhibit 5, that will be used during this phase of the FRAP session. The list of controls is contained in the documentation for the FRAP and currently is part of an EXCEL spreadsheet. The 26 controls are an amalgamation of controls developed by various FRAP facilitators over the past few years. The Controls List is used as a starting point for the FRAP team and can be modified or added to as required by the team. If any changes are made during the session, then those changes must be made in the EXCEL Tab titled "Controls."

The controls can be identified generally in two ways:

1. The facilitator can go to each high priority risk and have the team call out the number of the risk that they feel will help alleviate that risk.
2. The facilitator can work the first three or four priority risks and then allow the team to get back up and write down their choices. If a risk that they would choose has already been selected, it is not necessary to put it up there again.

The team needs to understand that what they select is not what will be implemented. For example, in Row 7 of Exhibit 4, the team selected nine possible controls. The business manager, project lead and facilitator will work together in the post-FRAP meeting to determine which one or two controls will work best.

The FRAP team must understand that trade-off must be made between business objectives and risks. Every control or safeguard will impact the business process in some manner as resources are expended to implement the control. Accidents, errors, and omissions generally account for more losses than deliberate acts. No control can or should be 100 percent effective. The ultimate goal is to achieve an acceptable level of security.

The FRAP will not eliminate every risk. Management has the duty to determine which risks it will implement controls on and which ones to accept. The FRAP team is to assist management in making that informed business decision.

The FRAP session is complete when the three deliverables are finished. Those three steps are:

1. Risks identified
2. Risks prioritized
3. Controls identified

Post-FRAP Meetings

Just as the 30-minute risk analysis is a misnomer, so is the concept that the FRAP can be completed in four hours. As we have seen, the pre-FRAP meeting takes and hour and the FRAP session will take around four

EXHIBIT 5 — FRAP Controls List

Control Number	Class	Control Description
1	Backup	Backup requirements will be determined and communicated to the service provider, including a request that an electronic notification that backups were completed be sent to the application system administrator. The service provider will be requested to test the backup procedures.
2	Recovery plan	Develop, document, and test recovery procedures designed to ensure that the application and information can be recovered, using the backups created, in the event of loss.
3	Access control	Implement an access control mechanism to prevent unauthorized access to information. This mechanism will include the capability of detecting, logging, and reporting attempts to breach the security of this information.
4	Access control	Access sourced: implement a mechanism to limit access to confidential information to specific network paths or physical locations.
5	Access control	Implement user authentication mechanisms (such as firewalls, dial-in controls, secure ID) to limit access to authorized personnel.
6	Access control	Implement encryption mechanisms (data, end-to-end) to prevent unauthorized access to protect the integrity and confidentiality of information.
7	Application control	Design and implement application controls (data entry edit checking, fields requiring validation, alarm indicators, password expiration capabilities, checksums) to ensure the integrity, confidentiality, and/or availability of application information.
8	Acceptance testing	Develop testing procedures to be followed during applications development and/or during modifications to the existing application that include user participation and acceptance.
9	Change management	Adhere to a change management process designed to facilitate a structured approach to modifications, to ensure appropriate steps and precautions are followed. "Emergency" modifications should be included in this process.
10	Anti-virus	(1) Ensure LAN administrator installs the corporate standard anti-viral software on all computers. (2) Training and awareness of virus prevention techniques will be incorporated in the organization IP program.
11	Policy	Develop policies and procedures to limit access and operating privileges to those with business need.
12	Training	User training will include instruction and documentation on the proper use of the application. The importance of maintaining the confidentiality of user accounts, passwords, and the confidential and competitive nature of information will be stressed.
13	Audit/monitor	Implement mechanisms to monitor, report, and audit activities identified as requiring independent reviews, including periodic reviews of user-ids to ascertain and verify business need.

EXHIBIT 5 — FRAP Controls List *(Continued)*

Control Number	Class	Control Description
14	Backup	Operations controls: training for a backup to the system administrator will be provided and duties rotated between them to ensure the adequacy of the training program.
15	Training	Operations controls: application developers will provide documentation, guidance, and support to the operations staff (service provider) in implementing mechanisms to ensure that the transfer of information between applications is secure.
16	Access control	Operations controls: mechanisms to protect the database against unauthorized access, and modifications made from outside the application, will be determined and implemented.
17	Interface dependencies	Operations controls: systems that feed information will be identified and communicated to the service provider to stress the impact to the functionality if these feeder applications are unavailable.
18	Maintenance	Operations controls: time requirements for technical maintenance will be tracked and a request for adjustment will be communicated to management if experience warrants.
19	Training	User controls: implement user programs (user performance evaluations) designed to encourage compliance with policies and procedures in place to ensure the appropriate utilization of the application.
20	Service level agreement	Acquire service level agreements to establish level of customer expectations and assurances from supporting operations.
21	Maintenance	Acquire maintenance and/or supplier agreements to facilitate the continued operational status of the application.
22	Physical security	In consultation with facilities management, facilitate the implementation of physical security controls designed to protect the information, software, and hardware required of the system.
23	Management support	Request management support to ensure the cooperation and coordination of various business units, to facilitate a smooth transition to the application.
24	Proprietary	Proprietary controls
25	Corrective strategies	The development team will develop corrective strategies such as: reworked processes, revised application logic, etc.
26	Change management	Production migration controls such as search and remove processes to ensure data stores are clean.

hours. These two together are only the information-gathering portion of the risk analysis process. To get a complete report, the business manager, project lead and facilitator will have to complete the action plan.

The post-FRAP process has five deliverables:

1. The Cross Reference Sheet
2. Identification of existing controls
3. Consulting with Owner on open risks
4. Identification of controls for open risks
5. Final Report

Under its current level of technical advance, the Cross Reference Sheet is the most time-consuming process for the facilitator or scribe. This document takes each control and identifies all the risks that would be impacted by that single control.

Fore example, in Row 2 in Exhibit 4, the FRAP team has identified three controls (9,13,26) that would help control risk number 2. The cross reference sheet for control number 9 would look like the table in Exhibit 6.

In this example, control 9 would help mitigate 11 different risks. The Cross Reference Sheet helps the business manager determine where scarce resources can best be used.

Once the Cross Reference Sheet is complete, and I normally give my facilitator and scribe two working days to complete it, the Action Plan and Cross Reference Sheet are sent to the business manager.

As we saw above, the FRAP session will generate a report like the one shown in Exhibit 7. With the Action Plan and the Cross Reference Sheet, the facilitator and project lead normally sit down to determine which controls are already in place. Once this is completed, then they meet with the business manager to review the document and recommend which controls can help those risks that are still open.

The framed items in Exhibit 7 were already closed, that is controls were already in place. In most risk analysis processes, when the team gets down to this level they find that nearly 80% of the risks already have some form of control in place.

For those open risks, the facilitator, project lead, and business manager determine which controls will be most cost-effective and then determine who will implement them and by what date. Remember, if a third party will be required to implement the control, then some discussion with them must take place to determine the completion date.

Once all open risks have either an assigned control or that the owner has indicated in the comment section that they are accepting the risk, the Final Report, as shown in Exhibit 8, is ready to be initiated.

CONCLUSION

The Facilitated Risk Analysis Process (FRAP) is currently the most widely used form of qualitative risk analysis being used today. The FRAP consists of three major parts:

EXHIBIT 6 — Cross-reference Sheet Example

Control Number	Control Description	Risk #	Risk	Type	Priority
9	Adhere to a change management process designed to facilitate a structured approach to modifications, to ensure appropriate steps and precautions are followed. "Emergency" modifications should be included in this process.	2	Unclear or nonexistent versioning of the information	INT	B
		16	Impact to business by using information that is incorrect	INT	B
		23	Not responding to requests in a timely manner	INT	A
		25	E-business integrity policies conflict with existing corporate policies	INT	A
		29	Wrong document or data is published	INT	A
		35	Incorrect use of the modification process in the application development process (change code without testing)	INT	B
		40	Personal information for staff might be posted on the Internet without authorization	CON	A
		44	New technologies leading to breaches of confidentiality	CON	A
		47	Loss of sales and increased costs due to release of competitive advantage information without company knowledge	CON	B
		50	Electronic eavesdropping of company sites	CON	B
		9	Incorrectly made hardware or software changes	AVA	B

EXHIBIT 7 — Selected Controls for Action Plan

Owner Action	By Who	When	Additional Comments
ACF2 has been implemented and the access control list will be reviewed to identify authorized users	Owner & IP	7/15/00	
Change management procedures already in place	Operations	complete	
Employee training sessions scheduled	HR	8/15/00	
Backup SLA to be reviewed with operations.	Owner & Operations	7/31/00	
SLA with service provider to be implemented.	Owner	8/20/00	
SLA with service provider to be implemented.	Owner	8/20/00	

1. The pre-FRAP Meeting which last about one hour and has five deliverables:
   a. Scope statement
   b. Visual diagram
   c. Team members
   d. Meeting Mechanics
   e. Definitions
      (1) Risk
      (2) Control
      (3) Review elements (integrity, confidentiality, availability)
      (4) Vulnerability Impact
2. The FRAP session which normally lasts about four hours and has three deliverables:
   a. Identified risks
   b. Prioritized risks
   c. Suggested controls
3. The post-FRAP process which can take up to 10 days and has three elements:
   a. Creation on the Cross Reference Sheet
   b. Identification of existing controls
   c. Selection of controls for open risks or acceptance of risk

Most organizations agree that risk considerations and related cost-benefit trade-offs are the primary focus of effective security programs. Security cannot be viewed as an end in itself, but as a set of policies and processes designed to support business operations. Implementing a risk

EXHIBIT 8 — Sample of Final Report Letter

Date: (enter date)

To: Mr. Owner
IS Security Center of Excellence (SCoE) Manager
Owner/Owner's Representative

From: Ms. Facilitator
IS Information Management Center of Excellence (IMCoE) Manager

Subject: *Facilitated Risk Analysis*

The Information Protection group facilitated a Risk Analysis session on the functionality named below. The Risk Analysis attendees identified the risks and controls shown on the attached Action Plan. The attendees included you, or your representative, to ensure that the concerns of your organization were properly addressed.

The Action Plan shows which of the controls identified during the Risk Analysis have been, or will be implemented. You should have made the decisions as to if and when the controls will be implemented.

FRAP Date: 6/8/00
System/Application: IS E-commerce Functionality
Owner: Mr. Owner
Facilitator: Ms. Facilitator

Please read the Statement of Understanding below, sign it, and return it to me.

STATEMENT OF UNDERSTANDING: I, the Owner, understand that the risks identified on the attached Risk Analysis Action Plan could cause the integrity, confidentiality, and/or availability of this system/application's information to be negatively impacted. I have decided to implement the controls according to the schedule on the attached Risk Analysis Action Plan. I understand that any risks that are not controlled could adversely affect corporate information and company business.

I am aware that a copy of the Risk Analysis Action Plan will be forwarded to the Audit organization.

_____ _____
Owner/Owner's Representative Date
IS Security Center of Excellence (SCoE) Manager

_____ _____
IS Information Management Center of Excellence (IMCoE) Manager Date

analysis process that is to use and geared to support the business processes will make acceptance of controls that much easier.

Information and the systems that process these resources are critical assets essential to supporting the business or mission of our enterprises and must be protected. An effective risk analysis process ensures that these business needs are met.

Additional Reading

1. Caroline Hamiltion, New Trends in Risk Assessment, *Data Security Management,* April 1998, No. 85-01-25

Tom Peltier, CISSP, is Director, Methods & Administration, Global Security Practice, Netigy Corp. (www.netigy.com). He is the author of *Information Security Risk Analysis* (Auerbach Publications, 2001).