Risk Analysis and Risk Management

Thomas R. Peltier

Risk management is the process that allows business managers to balance operational and economic costs of protective measures and achieve gains in mission capability by protecting business processes that support the business objectives or mission of the enterprise. Senior management must ensure that the enterprise has the capabilities needed to accomplish its mission. Most organizations have tight budgets for security. To get the best bang for the security buck, management needs a process to determine spending.

FREQUENTLY ASKED QUESTIONS ON RISK ANALYSIS

Why Should a Risk Analysis Be Conducted?

Management is charged with showing that "due diligence" is performed during decision-making processes for any enterprise. A formal risk analysis provides the documentation that due diligence is performed.

A risk analysis also lets an enterprise take control of its own destiny. With an effective risk analysis process in place, only those controls and safeguards that are actually needed will be implemented. An enterprise will never again face having to implement a mandated control to "be in compliance with audit requirements."

When Should a Risk Analysis Be Conducted?

A risk analysis should be conducted whenever money or resources are to be spent. Before starting a task, project, or development cycle, an enterprise should conduct an analysis of the need for the project. Understanding the concepts of risk analysis and applying them to the business needs of the enterprise will ensure that only necessary spending is done.

Who Should Conduct the Risk Analysis?

Most risk analysis projects fail because the internal experts and subject matter experts are not included in the process. A process such as the Facilitated Risk Analysis Process (FRAP) takes advantage of the internal experts. No one knows your systems and applications better than the people that develop and run them.

How Long Should a Risk Analysis Take?

It should be completed in days, not weeks or months. To meet the needs of an enterprise, the risk analysis process must be able to complete it quickly with a minimum of impact on the employees' already busy schedules.

THOMAS R. PELTIER, CISSP, CISM, is principal of Peltier and Associates (www.peltierassociates.com), an information security consulting and service firm.

What Can a Risk Analysis Analyze?

Risk analysis can be used to review any task, project, or idea. By learning the basic concepts of risk analysis, the organization can then use it to determine if a project should be undertaken, if a specific product should be purchased, if a new control should be implemented, or if the enterprise is at risk from some threat.

What Can the Results of a Risk Analysis Tell an Organization?

The greatest benefit of a risk analysis is whether it is prudent to proceed. It allows management to examine all currently identified concerns, prioritize the level of vulnerability, and then to select an appropriate level of control or to accept the risk.

The goal of risk analysis is not to eliminate all risk. It is a tool to be used by management to reduce risk to an acceptable level.

Who Should Review the Results of a Risk Analysis?

A risk analysis is rarely conducted without a senior management sponsor. The results are geared to provide management with the information they need to make informed business decisions. The results of a risk analysis are normally classified as confidential and are provided only to the sponsor and to those deemed appropriate by the sponsor.

How Is the Success of the Risk Analysis Measured?

The tangible way to measure success is to see a lower bottom line for cost. Risk analysis can assist in this process by identifying only those controls that need to be implemented.

Another way that the success of a risk analysis is measured is if there is a time when management decisions are called into review. By having a formal process in place that demonstrates the due diligence of management in the decision-making process, this kind of inquiring will be dealt with quickly and successfully.

Effective risk management must be totally integrated into the organization's System Development Life Cycle (SDLC). The typical SDLC has five phases and they can be termed almost anything. Regardless of what the phases are labeled, they all have the same key concepts:

1. Analysis
2. Design
3. Construction
4. Test
5. Maintenance

The National Institute of Standards and Technology (NIST) uses the following terms: Initiation, Development or Acquisition, Implementation, Operation or Maintenance, and Disposal.

As Figure 1 points out, risk analysis is mapped throughout the SDLC. The first time risk analysis needs to be done is when there is a discussion on whether a new system, application, or business process is required.

The first time risk analysis needs to be done is when there is a discussion on whether a new system, application, or business process is required.

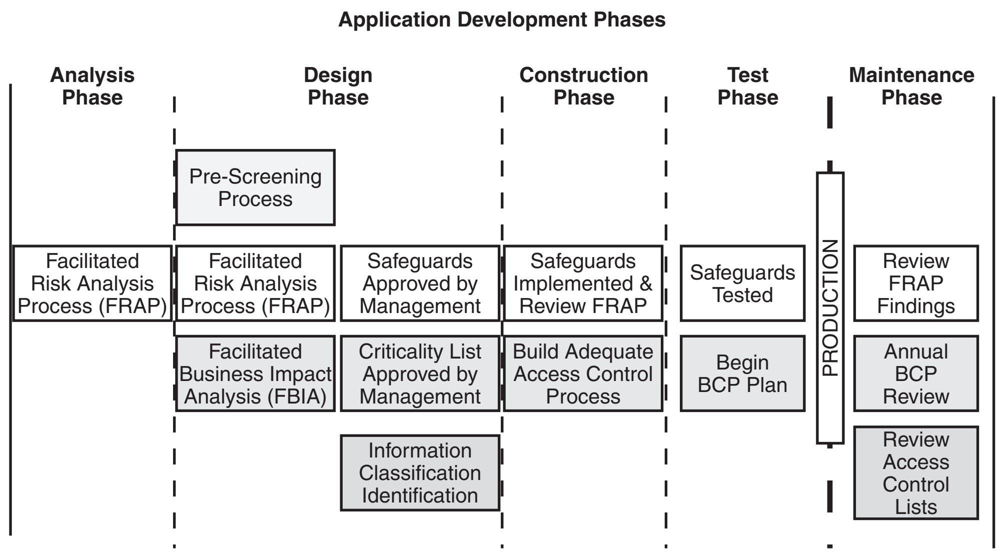
SDLC Phases

- *Analysis.* The need for a new system, application, or process and its scope are documented.
- *Design.* The system or process is designed and requirements are gathered.
- *Development.* The system or process is purchased, developed, or otherwise constructed.
- *Test.* System security features should be configured, enabled, tested, and verified.
- *Maintenance.* When changes and/or updates are made to the system, the changes to hardware and software are noted and the risk analysis process is revisited.

Risk Management Activities

- *Analysis.* Identified risks are used to support the development of system requirements, including security needs.
- *Design.* Security needs lead to architecture and design tradeoffs.

FIGURE 1 System Development Life Cycle

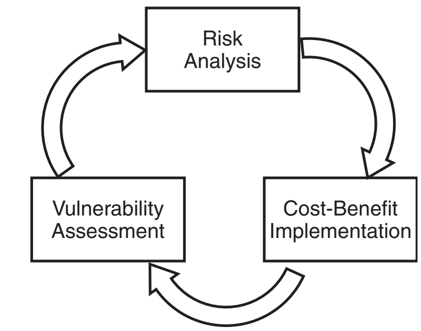

Application Development Phases
Analysis Phase
Design Phase
Construction Phase
Test Phase
Maintenance Phase
Pre-Screening Process
Facilitated Risk Analysis Process (FRAP)
Facilitated Risk Analysis Process (FRAP)
Safeguards Approved by Management
Safeguards Implemented & Review FRAP
Safeguards Tested
PRODUCTION
Review FRAP Findings
Facilitated Business Impact Analysis (FBIA)
Criticality List Approved by Management
Build Adequate Access Control Process
Begin BCP Plan
Annual BCP Review
Information Classification Identification
Review Access Control Lists

- *Development.* The security controls and safeguards are created or implemented as part of the development process.
- *Test.* Safeguards and controls are tested to ensure that decisions regarding identified risks are reduced to acceptable levels prior to movement to production.
- *Maintenance.* Controls and safeguards are re-examined when changes or updates occur or on regularly scheduled intervals.

Risk management is an enterprise management responsibility. Each group has a different role and these roles support the activities of the other roles and responsibilities. Let us examine typical roles found in an organization and what they are responsible for with regard to risk analysis and risk management.

- *Senior management.* 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 analysis process into the decision-making process.
- *Chief Information Security Officer (CISO).* This officer is responsible for the organization's planning, budgeting, and performance including its information security components. Decisions made in this area should be based on an effective risk management program.
- *System and Information Owner.* These are the business unit managers assigned as functional owners of organization assets and are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the information resources that they are assigned ownership. The term "owner" must be established in the asset classification policy.
- *Business Managers.* The managers (aka owners) are the individuals with the authority and responsibility for making cost-benefit decisions essential to ensure accomplishment of organization mission objectives. Their involvement in the risk management process enables the selection of business-oriented controls. The charge of being an owner supports the objective of fulfilling the fiduciary

FIGURE 2 Information Security Life Cycle



responsibility of management to protect the assets of the enterprise.

- *Information Security Administrator (formerly ISSO).* This is the security program manager responsible for the organization's security programs, including risk management. The ISA has changed its designation because designation "officer" is normally restricted to senior executives. The officers can be held personally liable if internal controls are not adequate.

INFORMATION SECURITY LIFE CYCLE

When implementing risk management, it will be necessary to view this process as part of the ongoing information security life cycle (see Figure 2). As with any business process, the information security life cycle starts with a risk analysis. Management is charged with showing that "due diligence" is performed during decision-making processes for any enterprise. A formal risk analysis provides the documentation that due diligence is performed. Typically risk analysis results will be used on two occasions: when a decision needs to be made and when there arises a need to examine the decision-making process.

A risk analysis also lets an enterprise take control of its own destiny. With an effective risk analysis process in place, only those controls and safeguards that are actually needed will be implemented. An enterprise will never again face having to implement a mandated control to "be in compliance with audit requirements."

A risk analysis should be conducted whenever money or resources are to be spent. Before starting a task, project, or development cycle, an enterprise should conduct an analysis of the need for the project. Understanding the concepts of risk analysis and applying them to the business needs of the enterprise will ensure that only necessary spending is done.

Once a risk analysis has been conducted it will be necessary to conduct a cost-benefit analysis to determine which controls will help mitigate the risk to an acceptable level at a cost the enterprise can afford. It is unwise to implement controls or safeguards just because they seem to be the right thing to do or other enterprises are doing so. Each organization is unique and the levels of revenue and exposure are different. By conducting a proper risk analysis, the controls or safeguards will meet the enterprise's specific needs.

Once the controls or safeguards have been implemented, it is appropriate to conduct an assessment to determine if the controls are working. In the information security profession, the term vulnerability has been defined as a condition of a missing or ineffectively administered safeguard or control that allows a threat to occur with a greater impact or frequency or both. When conducting an NVA, the team will be assessing existing controls, safeguards, and processes that are part of the network. This process, the assessment, will ensure that controls are effective and that they will remain so.

RISK ANALYSIS PROCESS

Risk analysis has three deliverables: identify threats, establish a risk level by determining probability that a threat will occur and the impact if the threat does occur, and, finally, identification of controls and safeguards that can reduce the risk to an acceptable level. As we examine the risk analysis portion of the risk management process, we discuss six steps that provide us with the three deliverables we need. Risk is a function of the probability that an identified threat will occur and then the impact that the threat will have on the business process or mission of the asset under review. We examine the six steps necessary to perform the risk analysis portion of the risk management process.

Most failed projects come to grief because the scope of the project was poorly defined to begin with or because the scope was not managed well and was allowed to ‘”creep” until it was out of control.

Asset Definition

The first step in the risk analysis process is to define the process, application, system, or asset that is going to have the risk analysis performed upon it. The key here is to establish the boundaries of what is to be reviewed. Most failed projects come to grief because the scope of the project was poorly defined to begin with or because the scope was not managed well and was allowed to “creep” until it was out of control. If we are going to manage risk analysis as a project, then the asset definition must be looked upon as a scope statement. All of the elements that go into writing a successful scope statement should be used to define the asset and what will be expected from the risk analysis process.

To gather relevant information about the asset or process under review, the risk management team can use a number of techniques. These include questionnaires, on-site interviews, documentation review, and scanning tools. It will be necessary to describe in words exactly what the risk analysis is going to review. Once it has been identified, it will be necessary to determine what resources will be needed to support the asset (platforms, operating systems, personnel, etc.) and what business processes will be influenced by this asset.

Threat Identification

We define a threat as an undesirable event that could have an impact on the business objectives or mission of the business unit or enterprise. Some threats come from existing controls that were either implemented incorrectly or have passed their usefulness and now provide a weakness to the system or platform that can be exploited to circumvent the intended behavior of the control. This process is known as exploiting a *vulnerability.*

We will want to create as complete a list of threats as possible. Typically there are three major categories of threats. These include:

1. *Natural threats.* Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events are considered here.
2. *Human threats.* These are events that are either enabled by or caused by human beings, such as unintentional acts (errors and omissions) or deliberate acts (fraud, malicious software, unauthorized access). Statistically the threat that causes the largest loss to information resources remains human errors and omissions.
3. *Environmental threats.* These include long-term power outages, pollution, chemical spills, and liquid leakage.

To create a complete list of threats there are a number of different methods that can be used. These include developing checklists. Although I think checklists are important and need to be used, I must caution you that if used improperly a checklist will have an impact on the free flow of ideas and information. So use them to ensure that everything gets covered or identified, but don’t make them available at the beginning of the process.

Another method of gathering threats is to examine historical data. Research what types of events have occurred and how often they have done so. Once you have the threat, it may be necessary to determine the Annual Rate of Occurrence (ARO). This data can be obtained from a number of sources. For natural threats, the National Weather Center is a good place to get these rates of occurrence. For accidental human threats an insurance underwriter will have these figures. For deliberate threats, local law enforcement or the organization’s security force will have these numbers. For environmental threats, facilities management and the local power companies will have this information.

The method that I like best is brainstorming. I like to get a number of people (stakeholders) together and give them a structure to focus thought and then let them identify all of the threats they can think of. When we brainstorm there are no wrong answers. We want to ensure that all threats get identified. Once we have completed the information gathering, then we will clean up duplicates and combine like threats.

Determine Probability of Occurrence

Once a list of threats has been finalized, it will be necessary to determine how likely that threat is to occur. The risk management team will want to derive an overall likelihood that indicates the probability that a potential threat may be exercised against the risk analysis asset under review. It will be necessary to establish definitions of probability and a number of other key terms. We discuss sample definitions as soon as we finish addressing the six steps of risk analysis.

Determine the Impact of the Threat

Once we have determined the probability that a threat might occur, it will then be necessary to determine the impact that the threat will have on the organization. Before determining the impact value, it is necessary to ensure that the scope of the risk analysis has been properly defined. It will be necessary to ensure that the risk management team understands the objectives or mission of the asset under review and how it influences the organization's overall mission or objectives.

When determining the risk level (probability and impact) it will be necessary to establish the framework from which the evaluation is to occur. That is, how will existing controls affect the results? Typically, during the initial review, the threats are examined as if there are no controls in place. This will provide the risk management team with a baseline risk level from which controls and safeguards can be identified and their effectiveness measured.

Typically, during the initial review, the threats are examined as if there are no controls in place. This will provide the risk management team with a baseline risk level from which controls and safeguards can be identified and their effectiveness measured.

Although we make the assertion that no controls are in place, in the scope statement we will identify assumptions and constraints. These assumptions might include the concepts that a risk analysis has been performed on the supporting infrastructure elements and that appropriate controls have been implemented. This will mean that such an activity will have to have taken place or is scheduled to be done as soon as possible. By establishing these assumptions, the risk management team can focus on the threats and impacts related directly to the asset under review.

The result of the review of probability and impact is the determination of a risk level that can be assigned to each threat. Once the risk level has been established, the team can identify appropriate actions. Steps two and three determined the likelihood that a given threat may occur, the magnitude of the impact should the threat occur, and the adequacy of controls already in place. The final element will be to identify controls for those high-level threats that have no control or whose control is inadequate.

The risk-level process will require the use of definitions for probability and impact as well as definitions of levels. The following are sample definitions and how they may be used by the risk management team (see Table 1).

- *Probability:* The likelihood that a threat event will occur
  - *High probability:* Very likely that the threat will occur within the next year
  - *Medium probability:* Possible that the threat may occur during the next year
  - *Low probability:* Highly unlikely that the threat will occur during the next year
- *Impact:* The measure of the magnitude of loss or harm to the value of an asset
  - *High impact:* Shutdown of critical business unit that leads to a significant loss of business, corporate image, or profit

TABLE 1 Probablility/Impact Matrix

	Impact		
Probability	**High**	**Medium**	**Low**
High	A	B	C
Medium	B	B	C
Low	B	C	D

A: Corrective action must be implemented.
B: Corrective action should be implemented.
C: Requires monitor.
D: No action required at this time.

– *Medium impact:* Short interruption of critical process or system that results in a limited financial loss to a single business unit
– *Low impact:* Interruption with no financial loss

Controls Recommended

After the risk level has been assigned the team will identify controls or safeguards that could possibly eliminate the risk or at least reduce the risk to an acceptable level. Remember that one of the goals of risk analysis is to document the organization's due diligence when making business decisions. Therefore, it will be important to identify as many controls and safeguards as possible. By doing this the team will be able to document all of the options that were considered.

There are a number of factors that need to be considered when recommending controls and alternative solutions. For instance, how effective is the recommended control? One way to determine the relative effectiveness is to perform the risk-level process (probability and impact) to the threat with the control in place. If the risk level is not reduced to an acceptable point then the team may want to examine another option.

There may also be legal and regulatory requirements to implement specific controls. With so many new and expanding requirements mandated by government agencies, controlling boards, and laws, it will be necessary for the risk management team to be current on these requirements.

When selecting any type of control, it will be necessary to measure the operational impact to the organization. Every control will have an impact in some manner. It could be the expenditure for the control itself. It could be the impact of productivity and turnaround time. Even if the control is a new procedure, the effect on the employees must be reviewed and used in the determination on whether to implement.

A final consideration is the safety and reliability of the control or safeguard. Does the control have a track record that demonstrates that it will allow the organization to operate in a safe and secure mode? The overall safety of the organization's intellectual property is at stake. The last thing that the risk management team wants to do is to implement a control that puts the enterprise at a greater risk.

The expenditure on controls must be balanced against the actual business harm. A good rule of thumb is that if the control costs more than the asset it is designed to protect, then the return on investment is probably going to be low. One way to identify a good "bang for the buck" is to identify each control and cross-reference it to all of the threats that could be mitigated by the implementation of that specific control. This process will provide the team with an initial idea of which control is most cost effective.

In order to be effective the risk analysis process should be applied across the entire organization. That is, all of the elements and methodology that make up the risk analysis process should be standard and all business units trained in its use. The output from the risk analysis will lead the organization to identify controls that should reduce the level of threat occurrence.

Documentation

Once the risk analysis is complete, the results need to be documented in a standard format and a report issued to the asset owner. This report will help senior management, the business owner, make decisions on policy, procedures, budget, and systems and management change. The risk analysis report should be presented in a systematic and analytical manner that assesses risk so that senior management will understand the risks and allocate resources to reduce the risk to an acceptable level.

RISK MITIGATION

Risk mitigation is a systematic methodology used by senior management to reduce organizational risk. The process of risk mitigation can be achieved through a number of different methods. We now discuss the five most common methods of risk mitigation.

1. *Risk assumption*. After examining the threats and determining the risk level, the team's findings lead management to determine that it is the best business decision to accept the potential risk and continue operating. This is an acceptable outcome of the risk analysis process. If, after completing the risk analysis process, management decides to accept the risk, then they have performed their due diligence.
2. *Risk alleviation*. Senior management approves the implementation of the controls recommended by the risk management team that will lower the risk to an acceptable level.
3. *Risk avoidance*. This is where after performing the risk analysis management chooses to avoid the risks by eliminating the process that could cause the risks. For example, forgoing certain functions or enhancements of a system or application that would lead to too much exposure of the organization.
4. *Risk limitation*. This method limits the risk by implementing controls that minimize the adverse impact of a threat that would exercise a vulnerability. Typically the controls would come from the security architecture of controls that include the areas of avoidance, assurance, detection, or recovery controls.
5. *Risk planning*. This is a process where it is decided to manage risk by developing an architecture that prioritizes, implements, and maintains controls.
6. *Risk transference*. Here management transfers the risk by using other options to compensate for a loss such as purchasing an insurance policy.

Whichever risk mitigation technique is used, the business objectives or mission of an organization must be considered when selecting any of these techniques. It may not be practical.

If, after completing the risk analysis process, management decides to accept the risk, then they have performed their due diligence.

CONTROL CATEGORIES

In the information security architecture there are four layers of controls. These layers begin with Avoidance, then Assurance, then Detection, and finally Recovery. Or you can create a set of controls that map to the enterprise such as Operations, Applications, Systems, Security, and so on (see Table 2). Mapping to some standard such as ISO 17799 is another option. When identifying possible controls, it could be beneficial to categorize controls into logical groupings. We examine two such groupings.

Another way to map controls is by using some standard such as ISO 17799 (see Table 3) or requirements from regulations such as HIPAA, GLB, or Sarbanes–Oxley (see Table 4). The numbers in parentheses are the matching section numbers found in ISO 17799. ISO 17799 is actually "a comprehensive set of controls comprising best practices in information security." It is essentially, in part (extended), an internationally recognized generic information security standard.

Its predecessor, titled BS7799-1, has existed in various forms for a number of years, although the standard only really gained widespread recognition following publication by ISO (the International Standards Organization) in December of 2000. Formal certification and accreditation were also introduced around the same time.

The object of the controls list is to identify categories of controls that will lead the team to determine the specific control required. When developing your list, be sure to be thorough, but don't be so pedantic that the list of controls is similar to reading *War and Peace*.

TABLE 2 Control Categories

Operations Controls	Backup	Backup requirements will be determined and communicated to Operations including a request that an electronic notification that backups were completed be sent to the application System Administrator. Operations will be requested to test the backup procedures. Training for a backup to the System Administrator will be provided and duties rotated between them to ensure the adequacy of the training program. A formal employee security awareness program has been implemented and is updated and presented to the employees at least on an annual basis.
	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. Access Sources: Implement a mechanism to limit access to confidential information to specific network paths or physical locations.
	Risk Analysis	Conduct a risk analysis to determine the level of exposure to identified threats and identify possible safeguards or controls. Implement user authentication mechanisms (such as firewalls, dial-in controls, Secure ID) to limit access to authorized personnel.
	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.
	Interface Dependencies	Systems that feed information will be identified and communicated to Operations to stress the impact on the functionality if these feeder applications are unavailable.
	Maintenance	Time requirements for technical maintenance will be tracked and a request for adjustment will be communicated to management if experience warrants. Acquire maintenance and/or supplier agreements to facilitate the continued operational status of the application.
	Service Level Agreement	Acquire service-level agreements to establish level of customer expectations and assurances from supporting operations.
	Change Management	Production Migration controls such as search and remove processes to ensure data stores are clean.
	Business Impact Analysis	A formal business impact analysis will be conducted to determine the asset's relative criticality with other enterprise assets.
Application Controls	Application Control	Design and implement application controls (data entry edit checking, fields requiring validation, alarm indicators, password expiration capabilities, check-sums) to ensure the integrity, confidentiality, and/or availability of application information.
	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.
	Training	Implement user programs (user performance evaluations) designed to encourage compliance with policies and procedures in place to ensure the appropriate utilization of the application. Application developers will provide documentation, guidance, and support to the operations staff (Operations) in implementing mechanisms to ensure that the transfer of information between applications is secure.

TABLE 2 Control Categories (continued)

	Promotion to Production Procedures	Implement a process to control changes to the production environment or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption.
	Corrective Strategies	The Development Team will develop corrective strategies such as reworked processes, revised application logic, etc.
Security Controls	Policy	Develop policies and procedures to limit access and operating privileges to those with business need.
	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.
	Review	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.
	Asset Classification	The asset under review will be classified using enterprise policies, standrads and procedures on asset classification.
	Management Support	Request management support to ensure the cooperation and coordination of various business units.
	Proprietary	Processes are in place to ensure that company proprietary assets are protected and that the company is in compliance with all third-party license agreements.
	Security Awareness	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.
	Access Control	Implement encryption mechanisms (data, end-to-end) to prevent unauthorized access to protect the integrity and confidentiality of information.
		Adhere to a change management process designed to facilitate a structured approach to modifications of the application, to ensure appropriate steps and precautions are followed. "Emergency" modifications should be included in this process,
		Control procedures are in place to ensure that appropriate system logs are reviewed by independent third parties to review system update activities.
		In consultation with Facilities Management, facilitate the implementation of physical security controls designed to protect the information, software, and hardware required of the system.
		Mechanisms to protect the database against unauthorized access, and modifications made from outside the application, will be determined and implemented.
Systems Controls	Change Management	Backup requirements will be determined and communicated to Operations including a request that an electronic notification that backups were completed be sent to the application System Administrator. Operations will be requested to test the backup procedures.
		Implement a process to control changes to the production environment or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption.
	Monitor System Logs	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.
Physical Security	Physical Security	Conduct a risk analysis to determine the level of exposure to identified threats and identify possible safeguards or controls.

TABLE 3 ISO 17799 Control Mapping

ISO 17799 Section	Category	Control Description
	Risk Assessment (2)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of information resources.
Security Policy	Policy (3.1)	Develop and implement an Information Security Policy.
Organizational Security	Management Information Security Forum (4.1)	Establish a corporate committee to oversee information security. Develop and implement an Information Security Organization mission statement.
	Security of Third Party Access (4.2)	Implement a process to analyze third-party connection risks and implement specific security standards to combat third-party connection risks.
	Security Requirements in Outsourcing Contracts (4.3)	Implement standards and user training to ensure that virus detection and prevention measures are adequate.
Asset Classification & Control	Accounting of Assets (5.1)	Establish an inventory of major assets associated with each information system.
	Information Classification (5.2)	Implement standards for security classification of the level of protection required for information assets.
	Information Labeling and Handling (5.2)	Implement standards to ensure the proper handling of information assets.
Personnel Security	Security in Job Descriptions (6.1)	Ensure that security responsibilities are included in employee job descriptions.
	User Training (6.2)	Implement training standards to ensure that users are trained in information security policies and procedures, security requirements, business controls, and correct use of IT facilities.
	Responding to Security Incidents and Malfunctions (6.3)	Implement procedures and standards for formal reporting and incident response action to be taken on receipt of an incident report.
Physical & Environmental Security	Secure Areas (7.1)	Implement standards to ensure that physical security protection exists, based on defined perimeters through strategically located barriers throughout the organization.
	Equipment Security (7.2)	Implement standards to ensure that equipment is located properly to reduce risks of environmental hazards and unauthorized access.
	General Controls (7.3)	Implement a clear desk/clear screen policy for sensitive material to reduce risks of unauthorized access, loss, or damage outside normal working hours.
Communications and Operations Management	Documented Operating Procedures (8.1)	Implement operating procedures to clearly document that all operational computer systems are being operated in a correct secure manner.
	System Planning and Acceptance (8.2)	Implement standards to ensure that capacity requirements are monitored, and future requirements projected, to reduce the risk of system overload.
	Protection from Malicious Software (8.3)	Implement standards and user training to ensure that virus detection and prevention measures are adequate.
	Housekeeping (8.4)	Establish procedures for making regular backup copies of essential business data and software to ensure that it can be recovered following a computer disaster or media failure.

TABLE 3 ISO 17799 Control Mapping (continued)

ISO 17799 Section	Category	Control Description
	Network Management (8.5)	Implement appropriate standards to ensure the security of data in networks and the protection of connected services from unauthorized access.
	Media Handling and Security (8.6)	Implement procedures for the management of removable computer media such as tapes, disks, cassettes, and printed reports.
	Exchanges of Information and Software (8.7)	Implement procedures to establish formal agreements, including software escrow agreements when appropriate, for exchanging data and software (whether electronically or manually) between organizations.
Access Control	Business Requirement for System Access (9.1)	Implement a risk analysis process to gather business requirements to document access control levels.
	User Access Management (9.2)	Implement procedures for user registration and deregistration access to all multiuse IT services.
	User Responsibility (9.3)	Implement user training to ensure users have been taught good security practices in the selection and use of passwords.
	Network Access Control (9.4)	Implement procedures to ensure that network and computer services that can be accessed by an individual user or from a particular terminal are consistent with business access control policy.
	Operating System Access Control (9.5)	Implement standards for automatic terminal identification to authenticate connections to specific locations .
	Application Access Control (9.6)	Implement procedures to restrict access to applications system data and functions in accordance with defined access policy and based on individual requirements.
	Monitoring System Access and Use (9.7)	Implement standards to have audit trails record exceptions and other security-relevant data and that they are maintained to assist in future investigations and in access control monitoring.
	Remote Access and Telecommuting (9.8)	Implement a formal policy and supporting standards that address the risks of working with mobile computing facilities, including requirements for physical protection, access controls, cryptographic techniques, backup, and virus protection.
Systems Development and Maintenance	Security Requirements of Systems (10.1)	Implement standards to ensure that analysis of security requirements is part of the requirement analysis stage of each development project.
	Security in Application Systems (10.2)	Implement standards to ensure that data that is input into applications systems is validated to ensure that it is correct and appropriate.
	Cryptography (10.3)	Implement policies and standards on the use of cryptographic controls, including management of encryption keys, and effective implementation.
	Security of System Files (10.4)	Implement standards. Is strict control exercised over the implementation of software on operational systems?
	Security in Development and Support Environments (10.5)	Implement standards and procedures for formal change control procedures.

TABLE 3 ISO 17799 Control Mapping (continued)

ISO 17799 Section	Category	Control Description
Business Continuity Management	Aspects of Business Continuity Planning (11.1)	Implement procedures for the development and maintenance of business continuity plans across the organization.
Compliance	Compliance with Legal Requirements (12.1)	Implement standards to ensure that all relevant statutory, regulatory, and contractual requirements are specifically defined and documented for each information system.
	Reviews of Security Policy and Technical Compliances (12.2)	Implement standards to ensure that all areas within the organization are considered for regular review to ensure compliance with security policies and standards.

COST-BENEFIT ANALYSIS

To allocate resources and implement cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis. This process should be conducted for each new or enhanced control to determine if the control recommended is appropriate for the organization. A cost-benefit analysis should determine the impact of implementing the new or enhanced control and then determine the impact of not implementing the control.

Remember that one of the long-term costs of any control is the requirement to maintain its effectiveness. It is, therefore, necessary to factor this cost into the benefit requirement of any control. When performing a cost-benefit analysis it will be necessary to consider the cost of implementation based on some of the following:

- Costs of implementation including initial outlay for hardware and software
- Reduction in operational effectiveness
- Implementation of additional policies and procedures to support the new controls
- Cost of possibly hiring additional staff or at a minimum, training existing staff in the new controls
- The cost of education support personnel to maintain the effectiveness of the control

FINAL THOUGHTS

Practically no system or activity is risk free, and not all implemented controls can eliminate the risks that they are intended to address. The purpose of risk management is to analyze the business risks of a process, application, system, or other asset to determine the most prudent method for safe operation. The risk analysis team reviews these assets with the business objectives as their primary consideration. We do not want, nor can we use, a control mechanism that reduces risk to zero. A security program that has as its goal 100 percent security will cause the organization to have zero percent productivity.

The risk analysis process has two key objectives: to implement only those controls necessary and to document management's due diligence. As security professionals we are aware that our goal is to provide support for the organization and to ensure that management objectives are met. By implementing an effective risk management and risk analysis process, this objective will be met and embraced by our user community. ■