FRAUD-RELATED INTERNAL CONTROLS

ACFE®

Association of Certified Fraud Examiners

GLOBAL HEADQUARTERS • THE GREGOR BUILDING
716 WEST AVE • AUSTIN, TX 78701-2727 • USA

Figure 2.1

COSO defines an *internal control* as "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."

This definition is broad but is meant to emphasize the following:

- Achievement of objectives is related to one or more of the following categories: operations, reporting, and compliance.
- A process should be ongoing; not a onetime occurrence.
- Internal controls are enacted by people at all levels of an organization and the actions they take, not just in the form of policies and procedures.
- Reasonable assurance, not complete assurance is the goal; complete assurance would be difficult, if not impossible to design, and the cost to implement it could significantly outweigh the benefits.
- Controls should be flexible and adaptable to various entity structures and their subunits.

Achievement of Objectives

Three categories of objectives allow management to focus on different aspects of internal control:

- *Operations objectives* relate to how effective or efficient an organization operates. They include operational and financial goals along with safeguarding assets against loss.
- *Reporting objectives* relate to financial and nonfinancial reporting whether internal or external. They also include standards set by regulators or an organization's policies regarding the timeliness, reliability, or transparency related to reporting.
- *Compliance objectives* relate to the adherence to laws and regulations to which an organization may be subject.

Even though these objectives are separated into three categories, they can overlap because an organization's needs sometimes fall under the responsibility of different individuals.

A Process

Internal control is referred to as a *process* because it permeates an organization's operating activities and is an integral part of basic management activities. Internal control provides reasonable—not absolute—assurance because the possibilities of human failure, collusion, and management override of controls make this process imperfect. An internal control can comprise multiple processes. These processes might be in the form of documented policies or procedures or a written communication from management. Processes might also come in the form of actual activities, such as planning or checking. When internal controls are embedded in multiple processes, they are likely to be much more effective.

Affected by People

Even though an internal control system is ultimately the responsibility of management, everyone within the organization can play a part in helping ensure that a control is working effectively. This can be achieved if people are familiar with the organization's objectives and have aligned their specific objectives accordingly. One individual's objectives might vary from another's due to their differing roles and responsibilities. Even though their specific objectives are not the same, they should still align with the organization's objectives. Management sets the tone for the organization and should ensure that all employees are aware of the importance of internal controls and have a clear understanding of management's expectations regarding standards of conduct.

Reasonable Assurance

An effective system of internal controls provides management with reasonable assurance that an organization's objectives will be achieved. Reasonable assurance acknowledges that limitations exist within all systems of control. Unforeseen events occur, and absolute assurance is impossible to attain. Human error, bad judgment, and external events are a few examples of limitations that are out of management's control. Collusion and management overrides are also limitations, but they are intentionally meant to affect the control environment. Management should keep in mind that even though an internal control system is designed to prevent and detect these types of limitations, a well-designed system of control can still fail.

Adaptability to Entity Structure

Not all entities are structured the same. Many differ based on the types of products or services provided. Reporting might be for a group of consolidated organization units or a subsidiary located in a foreign country. Some entities prefer to recruit and train their own employees, while others use outsourced service providers. Management at some large organizations might prefer to remain privately held, while leaders at a smaller company decide to go public. Regardless of an entity's structure, effective internal controls can be implemented to assist with the achievement of objectives.

Objectives

Every organization sets out to accomplish something. To do this, management (1) creates a mission or vision, (2) sets a strategy, (3) establishes objectives, (4) and develops a plan to achieve the objectives. Objectives might vary from entity to entity and can be established for the whole entity or be specific to one or more targeted areas. Even though most organizations establish objectives specific to their operations, many do not realize that their objectives are shared by other organizations. For example, most organizations set objectives to achieve success, comply with laws, maintain a positive reputation, and report to stakeholders.

Objectives are set by management, with board oversight and usually reflect their decisions regarding how the organization should create, maintain, and realize value for its stakeholders. Objectives might also align with the organization's operational needs, regulatory standards, or a combination of both. Before management can implement internal controls, they must set reasonable objectives so that risks related to their achievement can be identified and assessed. Measurable, observable, and relevant objectives are easier for people to achieve. Objectives fall into three categories: operations, reporting, and compliance.

Operations Objectives

Operations objectives relate to the fundamental reason an organization exists and can vary based on management's decision on how to operate the organization, where to operate it, and how it should perform. Operations objectives can also include sub-objectives. For example, management might set objectives for overall operations and then set specific objectives for divisions or subsidiaries within the operations.

Operating objectives might relate to quality, productivity, innovation, or customer satisfaction. For example, a nonprofit organization might be concerned with spending and revenues but focus more on increasing the number of donors. Regardless of the objective, management must ensure that it is clearly understood so it is achievable.

Safeguarding assets, or the protection or preservation of assets, falls under the operation-objectives category. Management that sets objectives related to loss prevention or the reporting of losses would be forming a basis on which to assess risk. Once risks have been identified, management could then develop controls to mitigate risks. Keep in mind that assets related to loss prevention through waste or bad management are not specific to the safeguarding of assets; these assets fall under the operations objectives just in a broader sense. Examples include extending credit to unworthy creditors, not retaining key employees, or pricing products too low. In addition, laws and standards regarding the safeguarding of assets have created the expectation that management's report on internal controls includes preventive and detective controls related to the acquisition or disposing of assets.

Reporting Objectives

Reporting objectives relate to reports prepared for the organization and others that might rely on them such as stakeholders. These objectives might relate to: (1) financial, (2) nonfinancial, (3) internal, or (4) external reporting. Internal reporting is used by management within the organization to assist with decision-making related to performance metrics, operations, and strategies. External reports are usually required by external regulators and standard-setting bodies.

External financial reporting objectives are set to meet the needs and expectations of stakeholders. Many external entities, such as investors, analysts, and creditors rely on these financial reports to assess their own investments or that of their peers. Examples include earnings releases or annual financial statements. External nonfinancial reporting can include internal control reports or custody of assets reports.

Internal financial and nonfinancial reporting objectives are used internally by an organization's management team to assist with strategies and decisions. Examples include financial reports by division or customer satisfaction surveys. When management needs reasonable assurance that a specific reporting objective will be met, all five components of internal control are needed. For example, if an organization is considering a merger, internal reports from each of the parties might be useful in the decision-making process.

Compliance Objectives

Most organizations are required to comply with various laws and regulations specific to their industry or operating model. To set compliance objectives, management must first understand what regulations and laws apply. There are some regulations or standards common to all organizations, such as laws related to the hiring or firing of employees, taxes, and workplace safety. Then there are laws specific to a country or industry. For example, management might decide to expand operations to a foreign country. Laws regarding registrations or permits may be required before any business can be conducted.

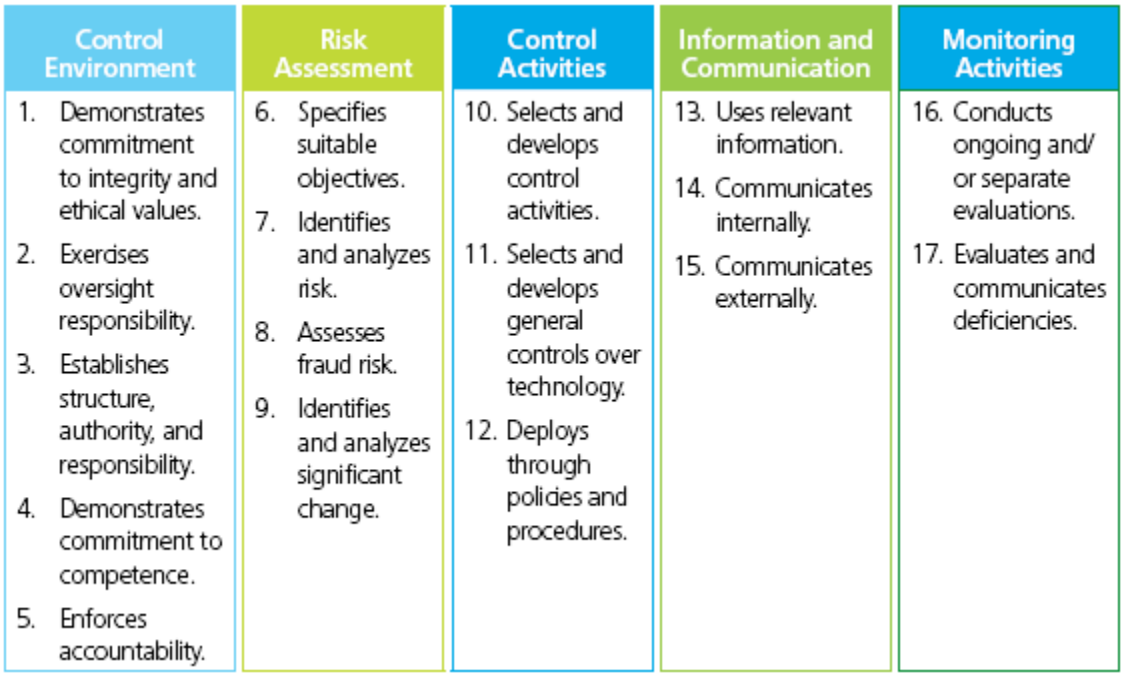
Components and Principles of Internal Control

After the executives set the objectives, they must develop an internal control process that addresses all five components: (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring activities.

Associated with each component are principles or concepts that can be applied to any objective—17 in total that address the five components. Figure 2.2 illustrates these relationships.[3]

[3] Diagram created by Deloitte to illustrate control components and principles. Jennifer Burns and Brent Simer, "COSO Enhances Its Internal Control—Integrated Framework," *Deloitte Heads Up* (June 10, 2013).

Figure 2.2



Control Environment—Component 1

The first component in an internal control system is the *control environment*. This component includes the standards, processes, and structures that form the foundation for carrying out internal controls across an organization. Senior management is responsible for setting the tone at the top when it comes to establishing and communicating internal controls and expectations toward conduct. These expectations can then be reinforced by management at all other levels within the organization. This component encompasses: the organization's ethical values, the board of director's oversight responsibilities, management structure, recruiting and retaining competent employees, and setting performance and accountability standards. The following five principles relate to the control environment:

- The organization's management demonstrates a commitment to integrity and ethical values.
- The board of directors demonstrates independence from management and exercises oversight of the development, and performance of internal control.
- Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- Management demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- Management holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Commitment to Integrity and Ethical Values—Principle 1

It is important for management to create an organizational culture that stresses integrity and ethical values. Management can do this by endorsing integrity as a basic principle of the company, as well as by personally and actively teaching and practicing it. For example, leaders should make it clear that honest reports are more important than favorable reports. Management should not assume that everyone accepts honesty, and it should consistently reward and encourage honesty. If management openly addresses both honest and dishonest behavior, employees are likely to more consistently make ethical decisions.

Management should develop clear policies that explicitly describe honest and dishonest behaviors. These policies should focus on issues that are uncertain or unclear, such as conflicts of interest and the acceptance of gifts. For example, most purchasing agents would agree that accepting a $5,000 bribe from a supplier is dishonest, but a weekend vacation at a hunting cabin is not as clear-cut of a decision. Dishonesty, to a large degree, results from rationalizing such situations. All dishonest acts should be thoroughly investigated, and those found guilty should be dismissed. Enough dishonest employees should be prosecuted so that all employees know that future dishonesty will be punished, not tolerated.

Oversight Responsibility—Principle 2

The board of directors provides oversight of the internal control system but remains independent from management. This allows them to be more objective when evaluating and making decisions related to organizational strategies. To ensure effective oversight, it is important that board members are competent and have the knowledge and experience required to accomplish their duties. They should have general knowledge about the organization, stakeholders, and any relevant risks that might affect the achievement of objectives. An organization's structure might demand additional oversight. For example, many publicly traded organizations must have compensation committees to oversee policies related to salaries and bonuses paid to senior management. In addition, audit committees are commonly formed to oversee the processes related to internal control over financial reporting. Even though the board is responsible for oversight, the CEO and other senior leaders are responsible for developing and implementing the internal control system.

Organizational Structure, Authority, and Responsibility—Principle 3

A company's organizational structure defines the lines of authority and responsibility, and provides the overall framework for planning, directing, and controlling its operations. Important aspects of organizational structure include:

- The centralization or decentralization of authority
- The assignment of responsibility for specific tasks
- The way responsibility allocation affects management's information requirements
- The organization of the accounting and information system functions

The more responsible management's philosophy and operating style is, the more likely it is that employees will behave responsibly in working to achieve the organization's objectives. If management shows little concern for internal controls, employees are less diligent and effective in achieving specific control objectives. Management's philosophy and operating style can be assessed by answering questions such as:

- Does management take unnecessary risks to achieve its objectives, or does it assess potential risks and rewards prior to acting?
- Does management attempt to manipulate performance measures (e.g., net income) so that its performance can be seen in a more favorable light?
- Does management pressure employees to achieve results regardless of the methods, or does it demand ethical behavior? In other words, does it believe the end justifies the means?

An overly complex or unclear organizational structure might indicate more serious problems. ESM, a brokerage company dealing in government securities, used a multi-layered organizational structure to hide a $300 million fraud. Company officers funneled cash to themselves, hiding it in their financial statements by reporting a fictitious receivable from a related company.

In today's business world, drastic changes are occurring within management. Hierarchical organizational structures, with many layers of management who supervise and control the work of those under them, are disappearing. They are being replaced with flat organizations that have self-directed work teams composed of employees formerly assigned to separate and segregated departments. Team members are empowered to make decisions and no longer must seek multiple layers of approvals to complete their work. There is an emphasis on continuous improvement rather than the periodic reviews and appraisals characteristic of earlier evaluators. These changes have an enormous impact on a company's organizational structure and on the nature and type of controls used in organizations.

Commitment to Competence—Principle 4

Organizations must employ competent individuals to be successful; this includes the board, management, and any supporting staff. A *competent individual* is someone qualified to carry out tasks for which they are assigned. These qualifications might come in the form of professional experience, certifications, or training. It is usually the role of the human resources function to assist management in finding competent individuals to fill specific roles or functions. It is vital that management set clear objectives that allow the human resource function to attract, train, mentor, evaluate, and retain competent individuals who support these objectives. In addition, when determining the number of resources or types of jobs to be filled, management should assess risks associated with this process to ensure company objectives can be achieved.

Enforces Accountability—Principle 5

Management should assign objectives to specific departments and individuals and then hold them accountable for achieving those objectives. Authority and responsibility can be assigned through formal job descriptions, employee training and operating plans, schedules, and budgets. Of particular importance is a formal company code of conduct addressing such matters as standards of ethical behavior, acceptable organization practices, regulatory requirements, and conflicts of interest.

A written policy and procedures manual is an important tool for assigning authority and responsibility, and spelling out management policies with respect to handling specific transactions. It often includes the organization's chart of accounts and sample copies of forms and documents. The manual is a helpful on-the-job reference and a useful tool in training new employees. Policies regarding working conditions, compensation, job incentives, and career advancement can be a powerful force in encouraging efficiency and loyal service.

Risk Assessment—Component 2

The second component of COSO's internal control model is *risk assessment.* All organizations face some form of risk, but some are more tolerant than others. According to COSO, *risk* is defined as the possibility that an event will occur and adversely affect the achievement of objectives. A risk assessment helps management determine whether their objectives are attainable. The following principles relate to risk assessments:

- Management specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
- Management identifies risks to the achievement of its objectives across the entity and analyzes risk as a basis for determining how the risks should be managed.
- Management considers the potential for fraud in assessing risks to the achievement of its objectives.
- Management identifies and assesses changes that could significantly impact the system of internal control.

Specify Suitable Objectives—Principle 6

Objectives form the basis on which risk assessments are performed. When setting reasonable objectives, management should ask the following:

- Do the objectives align with the organization's strategic priorities?
- Are the terms used to articulate the objectives specific, measurable, or attainable?
- Have risk tolerances for each objective been identified?
- Do the objectives align with laws or regulations that are applicable to the organization?

Management should be objective and honest when answering these questions. An honest assessment allows for a set of clear objectives on which an effective risk assessment can be performed.

Identify and Analyze Risk—Principle 7

Risk identification is an ongoing, all-inclusive process, meaning risks at all levels within the organization are considered as well as risks related to external parties with which an organization interacts. Examples include outsourced service providers, suppliers, and even customers. Both internal and external factors are considered when analyzing risk. Examples of risk factors include the severity of the risk, the likelihood of its occurrence, the impact on operations, and the potential loss of assets. When considering these factors, management should understand their tolerance for risk or how much risk they can accept and still operate efficiently.

Since the risk identification process is ongoing, management might consider implementing a schedule to periodically review risks, while reserving the ability to accelerate reviews if a company objective changes or risk factors—internal or external—increase. For example, if management is considering an acquisition, it might want to reevaluate risk factors to determine how the decision could impact operations.

Assess Fraud Risk—Principle 8

An important part of assessing risk is identifying the potential for fraud. Fraud that goes undetected can result in significant monetary loss and ruin an organization's reputation. When considering the potential for fraud risk, management should consider:

- What types of fraud could occur (e.g., loss of assets or fraudulent reporting)?
- What incentives or pressures can contribute to potential fraud?
- What opportunities are available for unauthorized use of assets, disposing of assets, or altering financial records?
- How might management or others engage in or justify their actions if caught?

Fraud-related risk can be significantly mitigated if management identifies high-risk areas and takes preventive action. If fraud is detected after a risk assessment was performed, management should revisit or amend the risk assessment accordingly.

Identify and Analyze Significant Change—Principle 9

The risk identification process includes changes in an organization's external environment, business model, and leadership. As the economy and regulatory environments change, management might need to alter operations to adapt to these external changes. For example, a natural disaster could result in lost raw materials used to manufacture a key component in a product. To sustain operation, a company's leaders need to find another supplier or consider substitute material.

When management changes how it does business, such as adding a new product line or expanding operations to a foreign market, it affects the business model. This shift in operations usually results in changes to previously identified risks. Some risks might be eliminated, some might increase, and new

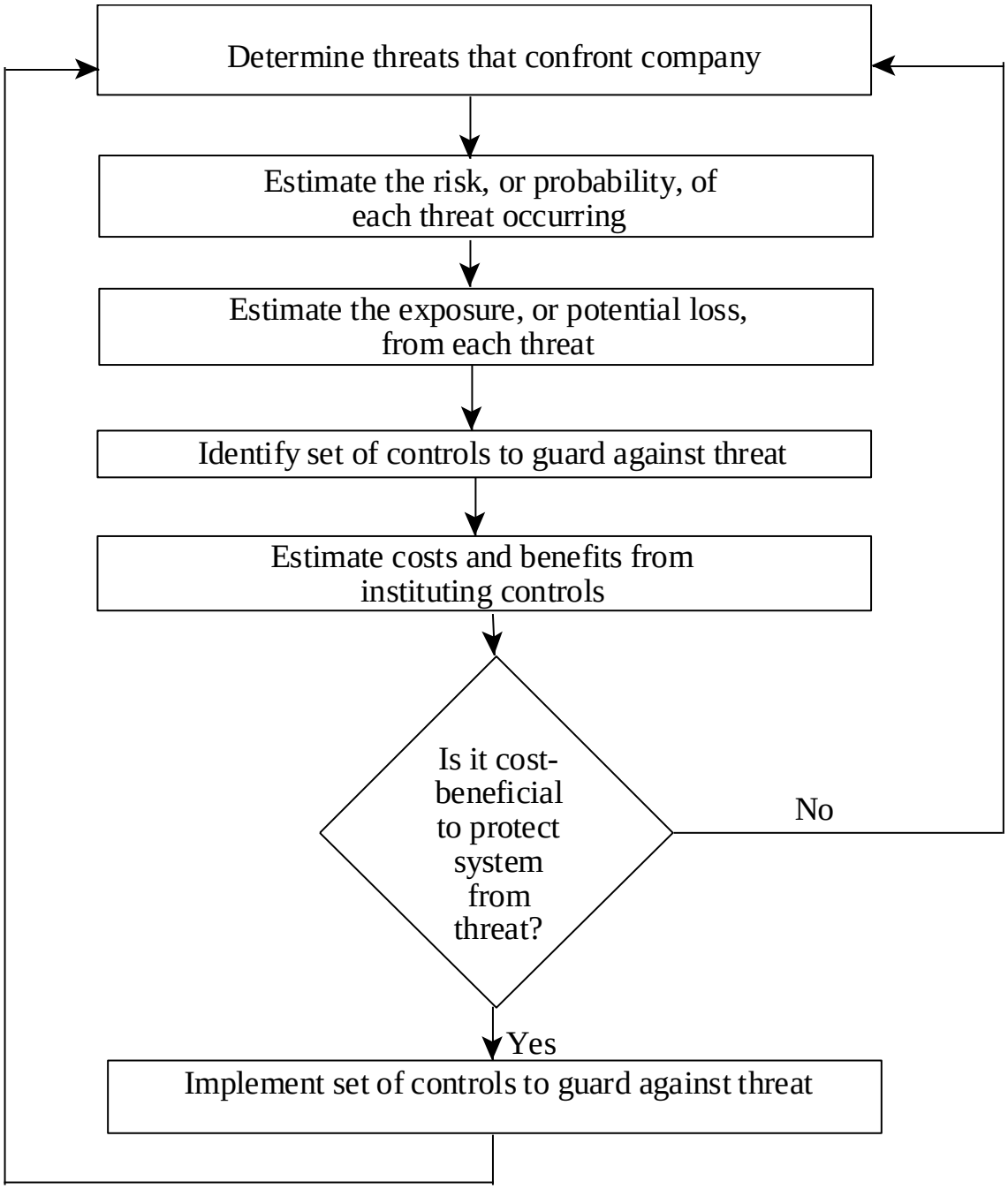
ones might be identified. Regardless of how the business model is impacted, management should be proactive in identifying risks in all processes affected.

A change in leadership can impact an organization's culture, productivity, and personnel retention, posing risks for the company. For example, a new member of senior management might have a different opinion on employee performance and compensation and eliminate all incentives tied to employee productivity. This decision could lead to increased turnover of highly qualified personnel, resulting in decreased productivity and the potential for increased risk.

Top management is ultimately responsible for ensuring that adequate controls are in place, so it usually oversees the risk assessment process; it might, however, select competent individuals within the organization to perform the assessments or reviews. The number and type of individuals involved in this process varies based on the size of the company, the complexity of its functions, and the type of services or products provided. Regardless, management should ensure that the individuals involved in the risk assessment process are competent, objective, and clearly understand the area or function they are reviewing.

Once a risk assessment has been completed and key risks identified, a review of the control environment is performed. For each key risk identified, there should be at least one effective control in place to mitigate that risk. Some organizations have found that their control environment was not as effective or almost nonexistent based on a risk assessment. Some have noted that certain areas or functions within their organization had never been assessed for risk; therefore, no controls were ever put in place, leaving them vulnerable to significant exposure and loss. Management must be careful when deciding which controls to implement or revise. A cost-benefit analysis should be performed to determine what is reasonable; this varies from company to company. Once controls are implemented, they should be reviewed periodically for effectiveness. Figure 2.3 provides an approach for developing effective internal controls based on a risk assessment.

Figure 2.3: Risk Assessment Approach to Designing Internal Controls



IDENTIFY THREATS

Management must identify the threats they face. These threats can be:

- Strategic, such as doing the wrong things
- Operational, such as doing the right things but in the wrong way

- Financial, such as having financial resources lost, wasted, or stolen, or incurring inappropriate liabilities
- Information, such as faulty or nonessential information, unreliable systems, and incorrect or misleading reports

Many organizations, for instance, implement electronic data interchange (EDI) systems that provide instantaneous communications and eliminate paper documents. An EDI system allows staff to create electronic documents, transmit them over private networks or the Internet to customers and suppliers, and receive electronic responses.

Organizations with an EDI system must identify threats to the system, such as:

- Choosing an inappropriate technology—The company might move to EDI before its customers and suppliers are ready or when there is a more effective means of communicating with external partners electronically.
- Unauthorized system access—Hackers can break into the system and sabotage it or steal data.
- Tapping into data transmissions—Hackers can "listen" to data transmissions and copy them, distort them, or prevent them from arriving at the destination.
- Loss of data integrity—Errors might be introduced into the data by employee or software errors, faulty transmissions, and so on.
- Incomplete transactions—The receiving computer does not receive all of the data from the sending computer.
- System failures—Hardware or software problems, power outages, sabotage, employee mistakes, or other factors might make the EDI system fail or be unavailable for a period of time.
- Incompatible systems—Some organizations' EDI systems cannot interact with other systems.

ESTIMATE RISK

Some threats pose a greater risk because the probability of their occurrence is more likely. For example, a company is more likely to be the victim of a computer fraud than a terrorist attack, and employees are more likely to make unintentional errors than to commit intentional acts of fraud.

ESTIMATE EXPOSURE

The risk of an earthquake might be very small, but the exposure can be enormous; it could destroy a company and force it into bankruptcy. Fraud exposure is usually not as great, and most frauds do not threaten a company's existence. The exposure from unintentional errors could range from miniscule to huge, depending on the nature of the error and how long it persists. Risk and exposure must be considered together. As either factor increases, the materiality of the threat and the need to protect against it rise.