# TOPIC 8

# Responding to Risk – Risk Control Strategies

## 8.1 Learning Objectives

By the end of this Chapter you should have understood

a) Introduction to Risk control
b) Risk treatment techniques
c) Common controls for business
d) The role of risk financing and some common risk financing techniques:
e) Controlling major risk events – crisis management and business continuity planning (BCP)
f) Controlling third party risks from suppliers and outsource service Providers

## 8.2 Introduction to Risk Control

**Risk control**, also known as hazard control, is a part of the risk management process in which methods for neutralising or reduction of identified risks are implemented. Controlled risks remain potential threats, but the probability of an associated incident or the consequences thereof have been significantly reduced.

**Risk control** involves implementing measures to reduce the probability or impact of potential risks. This may include strategies such as implementing safety procedures, creating backup systems, or employing preventative measures to reduce the likelihood of bad outcomes.

**Risk control** refers to mitigating or reducing the risks associated with a particular activity or situation. In contrast, **Risk management** is a broader term that encompasses your whole effort to identify, assess, and treat risks across an organization or project.

More specifically, risk control focuses on minimizing the effect of identified risks on a specific activity or project. In other words, risk control is one part of risk management.

### 8.2.1 Different types of Control


a) **Directive controls** give direction. These are the weakest controls. Things like policies are directive controls; they state the practice to be followed but do not stop bad practice from occurring. The Highway Code is an example of a directive control.
b) **Detective controls** aim to identify a breach after the event, an example being a financial review or audit after activity has taken place. They will often lead to corrective action being taken.
c) **Preventative controls** act to nullify the root cause and thus prevent the event. These are often the strongest controls. Common preventative controls include segregation of duties and IT passwords.
d) **Corrective controls** are implemented after an issue or error is detected, aiming to fix the problem and prevent recurrence. They focus on mitigating the impact of an event and restoring normal operations. Corrective controls are designed to correct errors or irregularities that have been detected. These include Suspense Accounts, Control Accounts for instance in Financial Accounting.

## 8.3 Risk Treatment Techniques;

Risk treatment is a collective term for all the tactics, options, and strategies chosen to respond to a specific risk, bound to achieve the desired outcome concerning the threat.

Consequently, risk treatment is not a concept functioning on its own. On the contrary, it should always be examined, understood, and implemented as part of a bigger whole, i.e., risk management.

### 8.3.1 Five Steps of Risk Treatment

In the risk treatment process, it's recommended to follow five main steps to ensure the correct logistics and effectiveness of the strategy:

a) Brainstorming and selecting the right risk treatment option.
b) Planning and use of options chosen.

c) Examining the effectiveness of the chosen tactics.
d) Deciding whether the level of the remaining risk, i.e., residual risk, is acceptable or not.
e) If it's not acceptable, implementing new risk treatment activities to reduce the residual risk.

### 8.3.2 Risk Treatment Options

There are several risk treatment strategies to deal with the risks. Notably, one kind of treatment cannot apply to all possible threats. It's crucial to review each threat individually to predict the effect of each solution.

Notably, the risk treatment options should be chosen based on a detailed analysis of the accompanying factors: the overall risk strategy of the company, its resources, the objectives of the organisation, as well as predicted costs against the benefits.

The risk treatment options include:
a) Risk Avoidance
b) Risk Reduction
c) Risk Transfer
d) Risk Retention
a) **Risk Avoidance;** If the risk assessment concludes that the risk is too high to be mitigated, it's possible to avoid the risk by resigning from performing specific actions or processes. The avoidance strategy is linked to interpreting the risk as unfavourable to the point that it should be excluded entirely. To avoid the risk, the company might choose to perform another action instead, as the alternative generates a lower threat.

   Examples of risk avoidance as part of the risk treatment strategy is to change your processes, equipment, or materials. Treating risks through avoidance is a step that should only be taken if you have determined that the impact and risk level are so high that it could jeopardise the entire organisation. Dealing with a high-risk level is not worth the risk, even if it means sacrificing some opportunities in the process. For example, suppose the launch of a new product line is identified as high-risk, and the impact of the expected cost is deemed as not acceptable. In that case, the product line will be exited and replaced with the one expected not to generate a threat.

b) **Risk reduction;** is an important risk treatment strategy because it requires taking action to reduce the impact of a given risk while maximising the benefits obtained from taking such action(s).

   To reduce the likelihood of risk or to bring its consequences down to an acceptable level, the company might implement safeguards or controls, carefully chosen from the range of the available control processes. By diminishing the risk to the required

level, this option ensures the needed level of security. The controls might occur in different forms, such as fire-suppression systems, joint application design, or best practices in employee training. It's essential to ensure that all tactics are bound to reduce risk to a sufficient level to continue doing business.

When risk controls reduce the risks, it is possible to examine the residual risk, i.e. the threat remaining after implementing the loss reduction treatment.

There are two steps to reduce risk as part of the risk treatment plan. The first one is using preventive methods, such as:

- Human resources and staff training
- Legislation compliance
- Quality control measures
- Auditing
- Regular maintenance
- Security systems installation

The second method to reduce risk involves the implementation of certain procedures upon the occurrence of a risk event:

- Data backups
- Emergency procedures
- Minimise exposure to highest-rated risks

**c) Risk Transfer**

Transferring risk is related to passing a specific portion of the threat to another party to reduce its likelihood or impact on the organisation. However, it's vital that another party - for example, an insurance company - is informed about the consequences of the sharing, the impact of the risk, and the expected transfer cost. This type of risk treatment might be executed by signing a contract with a service provider or purchasing an error insurance.

Notably, this option does not mitigate the risk itself, as it deals only with its consequence. Thus, the transfer treatment should be typically implemented along with other risk treatment plans.

There are various forms of implementing this particular risk treatment option, such as the following:

- Hedging strategies
- Contractual agreements
- Hiring a security company
- Properly vetting suppliers and vendors

**d) Risk Retention**

Suppose the analysis concludes that the risk rating is at acceptable levels, or the mitigation cost of the implemented strategy is higher than the expected damage. Only after the cost-benefit analysis is performed should you decide to choose risk retention as your best risk treatment option.

In that case, the appropriate treatment might be to accept the risk and not take any actions to treat it. However, you must only choose this treatment option assuming the risk should always go hand in hand with implementing a system that would continuously control and monitor the given risk, along with its possible development.

### 8.3.3 Risk Treatment Plan;

It's recommended to create a Risk Treatment Plan to avoid confusion in planning treatment activities. A Risk Treatment Plan is a document in which the company's policy regarding risk treatment is outlined in detail. The outline should contain information about the parties responsible for implementing each control option, the date and the timeframe, the available budget, etc. The detailed form will ensure a clear and unified strategy that will be easier to follow.

## 8.4 Common Controls for Business;

**An Internal Control System;** Processes effected by directors, mgt and other personnel designed to provide reasonable assurance regarding objectives of an organization.

ICS comprises of control environment and control procedures.

Control Environment means the overall attitude, awareness and actions of directors and management regarding ICS and its importance to the entity. It encompasses personnel policies and procedures, organization structure etc. Control Procedures are established to achieve the entity’s objectives.

### 8.4.1 Common Controls for Business;

a) Organisation chart/ Structure; that should define; Duties and responsibilities, Flow of authority and responsibility. How duties should be delegated in particular financial and accounting duties or assignments.
b) Segregation/ Division of Duties; Separation/division of duties and all responsibilities which if combined will enable one single person to process and record the transactions from the beginning to the end hence exposing such persons to committing fraud.
c) Physical Controls/ Safe Guarding of Assets; Limiting accessibility of companies assets to authorized persons at authorized times. Takes the form of physical

measures which are also aimed at limiting direct access to assets e.g. being able to enter the warehouse.

d) Authorisation/ Approval Controls; Aimed at ensuring that all the company's transactions are authorized by responsible officials whose limits of authority are defined such that they match transactions they authorise.
e) Arithmetic and Accounting Controls; Used to check the recording function in the organisation and to ensure that figures in the financial statements are not only genuine but also correct for accounting purposes.
f) Personnel Controls/ competence of staff; Personnel of integrity, competence and qualifications to understand essence of the controls. Such people should have capabilities to carry out responsibilities assigned to them.
g) Supervision; Low level supervision. supervise the company's day-to-day operations, Middle level supervision. done by line managers ensure policies and procedures are adhered to and Managerial supervision and review. by the top management using such tools like budgets, standard costs.
h) Rotation of Duties and Vacations; Duties of routine nature should be rotated to avoid continuity of errors and fraud and also as a means of avoiding routine boredom, which may lead to innocent errors. Employees should also be encouraged to take leave when it falls due.
i) Routine and Automatic Checks; Controls conducted on routine duties and operations are important in that they ensure that these operations are carried on efficiently. Such controls are operated at a surprise basis to minimize errors and frauds.
j) Recording and Record Keeping; The system of recording the business transactions at all stages should be complete and reliable. The records should be kept properly to avoid any losses or alterations.

### 8.5 Risk Financing Techniques;

Risk financing techniques are strategies organizations use to fund potential losses, encompassing methods like insurance, retention, and risk transfer, aiming to manage the financial impact of risks effectively.

#### 8.5.1 Common Risk Financing Techniques;

**a) Risk Retention:**

- Self-Insurance: Organizations establish a reserve fund to cover potential losses, rather than transferring the risk to an insurer.
- Deductibles: Paying a portion of a loss before insurance coverage kicks in, reducing premiums but increasing the financial burden in case of a claim. A deductible is the amount of money you agree to pay out-of-pocket for a covered loss before your insurance policy starts paying.
- Self-Funded Programs: Organizations create their own insurance programs to cover specific risks, such as employee healthcare or workers' compensation.

**b) Risk Transfer:**

- Insurance: Purchasing insurance policies to transfer the financial burden of potential losses to an insurance company.
- Reinsurance: Insurers transfer a portion of their risk to other insurers, spreading the financial impact of large or catastrophic losses.
- Contractual Agreements: Shifting risk to another party through contracts, such as indemnity clauses in agreements.
- Catastrophe Bonds: Risk-linked securities that transfer specified risks from a sponsor to investors, with principal payments contingent on specific trigger conditions. Typically used by insurance companies to share the risk of major disasters with investors wanting the gains should they not happen. The events covered could include earthquakes, hurricanes, floods, and other extreme events.
- Collateralized Reinsurance: Reinsurers fully secure their obligations by setting aside assets equal to the potential liabilities, often in the form of cash or high-quality securities.
- Hedging: Using financial instruments to reduce the risk of potential losses, such as weather derivatives to protect against adverse weather conditions.
- Diversification: Spreading investments or activities across different areas to reduce the impact of any single risk.

### 8.5.2 The Role of Risk Financing

a) Financial Stability: Risk financing helps organizations maintain financial stability by ensuring they have the resources to cover unexpected costs.
b) Business Continuity: By mitigating the financial impact of risks, organizations can better maintain operations and avoid disruptions.
c) Opportunity Creation: In some cases, risk financing can even create opportunities for organizations by allowing them to pursue ventures that might otherwise be too risky.
d) Value for Money: Risk financing aims to provide appropriate and adequate protection while demonstrating value for money.
e) Cost Optimization: Risk financing helps organizations find the optimal balance between risk retention and transfer, leading to more efficient and cost-effective risk management.
f) Improved Planning: Risk financing encourages better planning by forcing organizations to anticipate potential risks and develop contingency plans.
g) Enhanced Decision-Making: By understanding their risk profile, organizations can make more informed decisions about investments, operations, and other strategic initiatives.
h) Risk Mitigation and Monitoring: Risk financing allows for the implementation of risk mitigation measures and monitoring systems, which can help identify and address potential risks early on.
i) Ensuring Regulatory Compliance: A robust risk financing strategy helps organizations ensure compliance with relevant laws and regulations.

j) Encouraging Innovation and Growth

## 8.6 Controlling Major Risk Events- Crisis Management

8.6.1 **Crisis Management** is the process by which an organization deals with a major event that threatens to harm the organization, its stakeholders, or the general public.

Three elements are common to most definitions of crisis: (a) a threat to the organization, (b) the element of surprise, and (c) a short decision time.

Crisis management refers to the identification of a threat to an organization and its stakeholders in order to mount an effective response to it. Due to the unpredictability of global events, many modern organizations attempt to identify potential crises before they occur in order to sketch out plans to deal with them. When and if a crisis occurs, the organization must be able to drastically change course in order to survive.

Even the best-managed businesses may be hit by a crisis caused by external or internal events. Crisis management is the strategy of anticipating crises at the corporate level and planning how to deal with them effectively. Crisis management begins with risk analysis, however, it should not be confused with risk management.

Businesses that put a continuity plan in place in case of unforeseen contingencies can mitigate the effects of a negative event. The process of having a business continuity plan in place in the event of a crisis is known as crisis management.

The COVID-19 crisis that began in early 2020 can be expected to become a textbook example of crisis management. Businesses around the world were forced to shut their doors. Millions of employees were sent home. Essential services struggled to function. History will judge how effective the powers-that-be were in their crisis management skills.

Crisis management is not necessarily the same thing as risk management. Risk management involves planning for events that might occur in the future, crisis management involves reacting to negative events during and after they have occurred.

### 8.6.2 Types of Crises;

A crisis can either be self-inflicted or caused by external forces. Examples of **External forces** that could affect an organization’s operations include natural disasters, security breaches, or false rumors that hurt a business's reputation.

**Self-inflicted** crises are caused within the organization, such as when an employee smokes in an environment that contains hazardous chemicals, downloads questionable computer files, or offers poor customer service that goes viral online.

An internal crisis can be managed, mitigated, or avoided if a company enforces strict compliance guidelines and protocols regarding ethics, policies, rules, and regulations among employees.

### 8.6.3 What Is the Golden Rule of Crisis Management?

The golden rule of crisis management is to be proactive. Rather than taking action when a crisis occurs, it is important to be proactive before a crisis occurs. This involves identifying the possible threats to your business and implementing plans on how the business will react if these problems come to fruition. This will help minimize the damage to your business. Waiting once the problem arrives could be disastrous.

### 8.6.4 What Is the Main Goal of Crisis Management?

The main goal of crisis management is to protect all stakeholders of the firm. This includes employees, customers, and any other parties involved with the business. This can take the form of emergency plan implementation and methods to reduce hazards and increase safety.

### 8.6.5 The main steps of crisis management include:

#### a) Preparation & Prevention (Pre-Crisis Stage):

- Identify Potential Risks:
- Conduct thorough risk assessments to identify potential crises that could impact your organization or community.
- Develop a Crisis Management Plan:
- Create a comprehensive plan outlining roles, responsibilities, communication protocols, and action steps for various crisis scenarios.
- Form a Crisis Management Team:
- Assemble a team of individuals with the necessary skills and expertise to manage a crisis effectively.
- Train and Practice:
- Conduct regular training and simulations to ensure the crisis management team is prepared to respond effectively.
- Establish Communication Channels:
- Identify and establish clear communication channels for internal and external stakeholders.
- Gather Resources:
- Ensure you have the necessary resources, including personnel, equipment, and financial support, readily available.

**b) Response (During Crisis):**

- Activate the Crisis Management Plan: Immediately activate the crisis management plan upon the identification of a crisis.
- Ensure Safety: Prioritize the safety and well-being of people and property.
- Contain the Damage: Implement measures to contain the crisis and prevent it from escalating.
- Communicate Effectively: Provide timely, accurate, and consistent information to internal and external stakeholders.
- Manage the Situation: Implement the action plans outlined in the crisis management plan.
- Maintain Calm and Control: Ensure the crisis management team remains calm and focused on managing the situation.

**c) Recovery (Post-Crisis):**

- Assess the Damage:
- Evaluate the impact of the crisis on the organization or community.
- Implement Recovery Measures:
- Take steps to restore operations, repair damage, and address the needs of affected stakeholders.
- Learn from the Experience:
- Conduct a thorough review of the crisis response to identify lessons learned and areas for improvement.
- Update the Crisis Management Plan:
- Incorporate lessons learned into the crisis management plan to enhance future preparedness.
- Rebuild Trust:
- Focus on rebuilding trust with stakeholders by demonstrating transparency, accountability, and a commitment to learning and improvement.

### 8.6.5 4 P's of Crisis Management (A summary of the Steps)

a) Prevent: Focus on proactively identifying potential risks and implementing measures to minimize their likelihood and impact.
b) Plan: Develop a comprehensive crisis management plan that outlines roles, responsibilities, communication protocols, and procedures for different scenarios.
c) Practice: Regularly conduct drills and simulations to ensure that the crisis plan is effective and that the team is prepared to respond quickly and efficiently.
d) Perform: When a crisis occurs, execute the plan effectively, following established procedures and communicating clearly and transparently with stakeholders.

### 8.6.6 Importance of Crisis Management in Risk Control

The primary goal of crisis management is to ensure the safety and well-being of employees, customers and other stakeholders. This involves implementing emergency

response plans, providing timely and accurate information, and taking necessary actions to mitigate hazards and risks and protect individuals from harm.

a) Proactive Risk Mitigation:
- Crisis management plans help organizations anticipate and prepare for potential crises, allowing them to take proactive steps to mitigate risks before they escalate.
- This includes identifying vulnerabilities, developing contingency plans, and training personnel to respond effectively.
- By anticipating potential problems, organizations can minimize the impact of unexpected events and ensure business continuity.

b) Reputation Protection:
- Effective crisis management can safeguard an organization's reputation by demonstrating transparency, accountability, and a commitment to resolving issues.
- Prompt and clear communication during a crisis can help maintain stakeholder trust and prevent damage to the organization's image.
- Conversely, poor crisis management can lead to significant reputational damage, making it even more important to have a plan in place.

c) Stakeholder Trust:
- During a crisis, stakeholders (employees, customers, investors, and the community) will look to an organization for leadership and guidance.
- By demonstrating competence and empathy in managing a crisis, organizations can build and maintain trust with their stakeholders.
- Effective communication and transparency are key to fostering trust during a crisis.

d) Business Continuity:
- A well-executed crisis management plan can help ensure that an organization can continue to operate, even in the face of a crisis.
- This includes having backup systems, alternative communication channels, and procedures for restoring operations as quickly as possible.
- By minimizing disruption to business operations, crisis management helps organizations to maintain their financial stability and long-term viability.

## 8.7 Controlling Major Risk Events- Business Continuity Planning

Business continuity planning (BCP) is a strategic approach that organizations use to develop a plan to ensure they can maintain or quickly resume critical business functions in the face of disruptions, whether caused by natural disasters, cyberattacks, or other unforeseen events.

BCPs are comprehensive, encompassing all aspects of an organization, including technology, infrastructure, personnel, and processes.

A business continuity plan (BCP) is a document that consists of the critical information an organization needs to continue operating during an unplanned event.

The BCP states the essential functions of the business, identifies which systems and processes must be sustained, and details how to maintain them. It should consider any possible business disruption.

A BCP covers risks including cyberattacks, pandemics, natural disasters and human error. The array of possible risks makes it vital for an organization to have a business continuity plan to preserve its health and reputation. A BCP decreases the chance of a costly power or IT outage.

### 8.7.1 Key Elements of a Business Continuity Plan:

a) Business Impact Analysis (BIA): Identifying critical business functions and their dependencies, and assessing the potential impact of disruptions.
b) Risk Assessment: Evaluating potential threats and vulnerabilities to the organization.
c) Recovery Strategies: Developing plans for restoring critical systems, processes, and data.
d) Communication Plan: Establishing procedures for communicating with stakeholders during and after a disruption.
e) Testing and Review: Regularly testing the BCP and making necessary updates to ensure its effectiveness.
f) Initial data at the beginning of the plan, including important contact information.
g) A revision management process that describes change management procedures.
h) The purpose and scope.
i) How to use the plan, including guidelines as to when the plan will be initiated.
j) Policy information.
k) Emergency response and management procedures.
l) Step-by-step procedures.
m) Checklists and flow diagrams.
n) A glossary of terms used in the plan.
o) A schedule for reviewing, testing and updating the plan.

### 8.7.2 Business continuity planning steps

The business continuity planning lifecycle is a procedure for putting BCP elements into practice. The lifecycle contains the following five steps:

a) Information gathering and analysis. This step consists of both a risk assessment (RA) and business impact analysis (BIA). An RA identifies the possible disruptions that could happen to specific processes. A BIA explains the impact that disrupting a certain process has on a business.
b) Plan development and design. The plan covers all possible disruptions and provides solutions to them.
c) Implementation. In this step, employees learn the details of the BCP and what they must do if it should ever need to be implemented.

d) Testing. The plan undergoes a simulation to test how effective it is. Areas of improvement are identified and addressed.
e) Maintenance and updating. The plan must be regularly reviewed and updated to reflect changing threats, risks and new ways to address and recover from specific disruptions.

### 8.7.3 Benefits:

a) Business continuity planning is a proactive business process that lets a company understand potential threats, vulnerabilities and weaknesses to its organization in times of crisis. The creation of a business continuity program ensures company leaders can react quickly and efficiently to a business interruption.

b) A BCP lets a company continue to serve customers during a crisis and minimize the likelihood of customers going to competitors. These plans decrease business downtime and outline the steps to be taken before, during and after an emergency to maintain a company's financial viability
c) Reduced Downtime: Minimizes the time it takes to restore operations after a disruption.
d) Improved Resilience: Enhances the organization's ability to withstand and recover from unexpected events.
e) Enhanced Reputation: Demonstrates preparedness and builds confidence with stakeholders.
f) Cost Savings: Prevents financial losses resulting from prolonged downtime and disruptions.

### 8.7.4 Examples of Disruption Scenarios:

a) Natural disasters (floods, earthquakes, hurricanes).
b) Cyberattacks (ransomware, data breaches).
c) System failures (hardware, software, network).
d) Pandemics (public health emergencies).
e) Civic unrest.

## 8.8 Controlling Third Party Risk

Controlling third-party risk, or Third-Party Risk Management (TPRM), involves identifying, assessing, and mitigating risks arising from engaging with external entities like vendors, suppliers, and service providers. This includes due diligence, ongoing monitoring, and robust contract management to ensure compliance and protect your organization.

TPRM helps organizations understand and manage the risks associated with outsourcing services and products, ensuring that third-party interactions don't harm the organization's internal and external operations.

### 8.8.1 Benefits/ Objectives of TPRM

Third-party risk management (TPRM) involves identifying, assessing, and controlling risks that occur due to interactions with third parties, including procurement and off-boarding. TPRM employs policies and systems to ensure third parties:

a) Comply with regulations
b) Avoid unethical practices
c) Protect confidential information
d) Strengthen supply chain security,
e) Maintain a healthy and safe working environment
f) Handle disruptions effectively
g) Achieve high performance and quality levels

### 8.8.2 Examples of Third-Party Security Risks;

Here are several third-party security risks:

- Cybersecurity risk—a compromised third party can lead to a cyberattack that may result in data exposure or loss. Organizations can mitigate this risk by performing due diligence before onboarding new vendors and by continuously monitoring the vendor lifecycle.
- Operational risk—a third party can disrupt business operations. Organizations can manage this risk through service level agreements (SLAs), and by setting up a backup vendor to ensure business continuity.
- Compliance risk—a third party can impact the organization's compliance with regulations, agreements, or legislation, such as the EU's General Data Protection Regulation (GDPR). Managing compliance risk is critical for financial services, government organizations, and healthcare facilities.
- Reputational risk—a third party can introduce risks that negatively impact public opinion. Third-party data breaches may occur due to poor security controls. It may lead to inappropriate interactions, poor recommendations, and dissatisfied customers.
- Financial risk—a third party can negatively impact the organization's financial success. For example, poor supply chain management may reduce sales or result in no sales at all.
- Strategic risk—a third party risk may cause organizations to fail to meet business objectives.

### 8.8.3 What Does a Third-Party Risk Management Program Entail?

A TPRM program should feed into an organization's overall risk management strategy. The third party risk management process should include these steps:

a) Vendor evaluation—involves identifying the risks posed by a third-party vendor before onboarding. It is also important to determine the required level of due diligence to manage these risks. For example, organizations can refer to vendor security ratings to see if a given third party has an adequate security posture.
b) Vendor engagement—if the vendor's external security meets the minimum level required, the vendor should also be able to provide additional information regarding internal security measures, which isn't usually accessible to outsiders.
c) Risk remediation—organizations should not onboard a vendor that presents an unacceptable risk, although it may be possible to address these security issues. If the vendor agrees to address the remaining security issues, it may be useful to leverage a remediation tool.
d) Decision—based on the vendor's security posture and ability to remediate issues, the organization decides to approve or reject the vendor. This decision should consider the organization's risk tolerance and compliance requirements and the vendor's criticality.
e) Continuous monitoring—after onboarding, organizations should continue to monitor the third-party vendor's security. Maintaining security is especially important once a third party can access sensitive systems and data.

### 8.8.3 Risk Tiering;

Each vendor presents a different level of risk and importance to the organization. Organizations should thus establish which third parties are of higher or lower priority, based on their criticality.

Organizations typically classify third parties according to three tiers:

a) Tier 1—high criticality and high risk.
b) Tier 2—medium criticality and risk.
c) Tier 3—low criticality and risk.

Most organizations address issues with Tier 1 vendors before dealing with lower-priority risks. These vendors require a higher level of due diligence, with organizations collecting more evidence and expending more resources to ensure security. Tier 1 vendors typically require an in-depth assessment and validation.

The third party's inherent risk often determines its priority tier during the initial evaluation. Organizations can score inherent risk based on business context and industry standards. Prioritization should take into account the following aspects: