INNOVEST SME
Accelerating Small Business

Assess, Manage and Mitigate Risk in your Organisation

Rick Chisholm and Tala Chisholm

COPYRIGHT NOTICE

30/192A Kingsgrove Rd
Kingsgrove, NSW 2208
Australia

Phone: +61 2 8007 2907
E-mail: admin@innovestsme.com.au
Website: www.innovestsme.com.au

CONTENTS

A good rule of thumb is to assume that 'everything matters'.

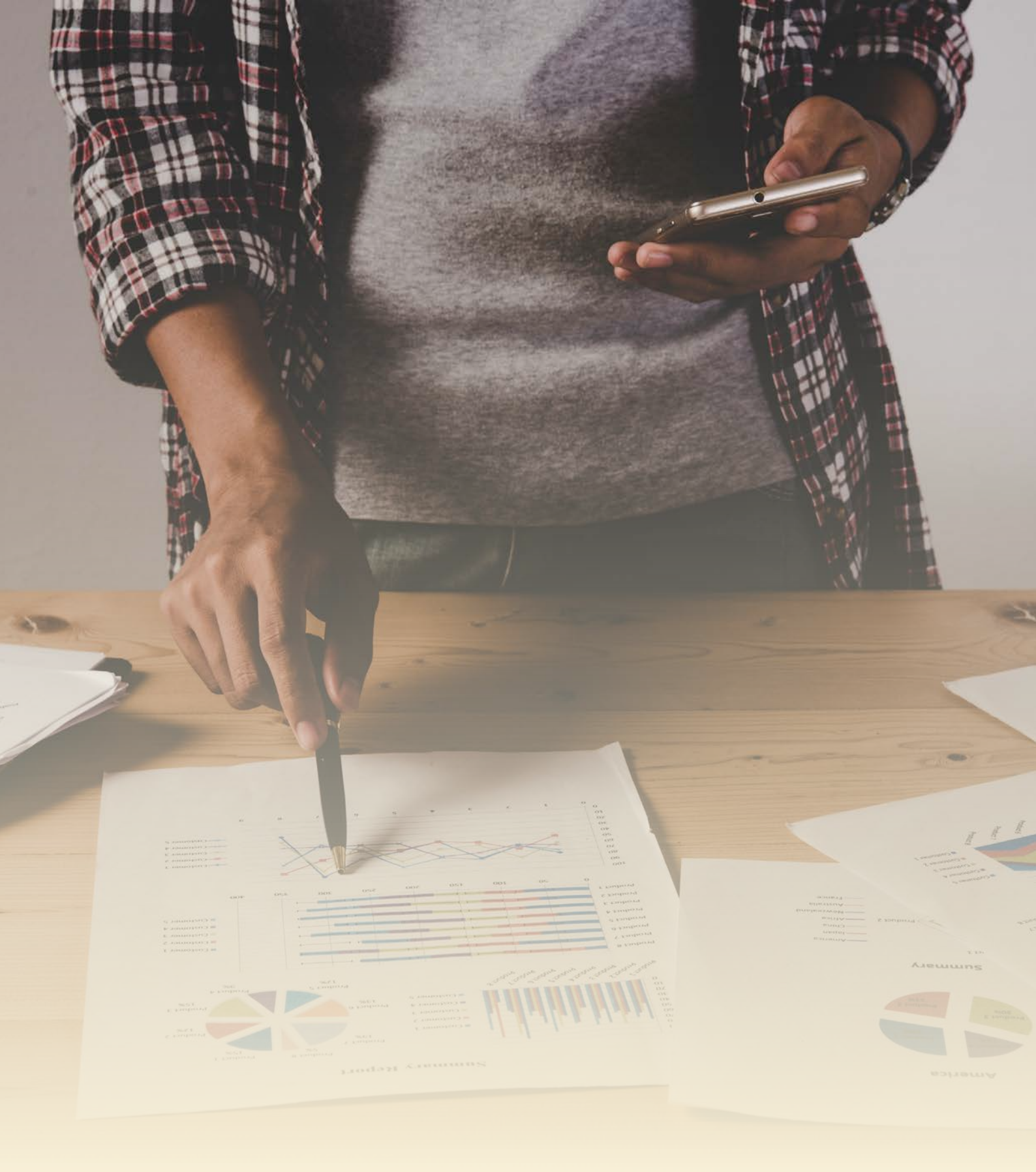
RICHARD THALER

PREFACE

Risk assessment and management is essential for the success of any business. However, many companies do not always take the necessary precautions, which leads to disaster. Successfully managing risks will prevent mistakes, which leads to a safer work environment, happier employees, and increased productivity. Following a few basic steps will place your organization on the path to success.

To win, you have to risk loss.

JEAN-CLAUDE KILLEY



CHAPTER ONE

IDENTIFYING HAZARDS AND RISKS

Every organization has both hazards and risks. Identifying hazards and risks is necessary for risk management. Hazards and risks are often confused with each other. Determining the difference between a hazard and a risk will increase the effectiveness of the risk management program.

WHAT IS A HAZARD?

A hazard is any source of harm. This includes adverse health effects or loss to the organization or employee. Hazards are varied. They include materials, substances, sources of energy, processes, practices, and conditions.

Examples of hazards:

- Sharp objects
- High temperatures
- Electricity
- Slippery surfaces
- Asbestos
- Chemicals

Once hazards are identified, you can take the opportunity to identify the risks associated with each hazard in your facility.

WHAT IS A RISK?

A risk is not a hazard. It is the chance of harm coming from a hazard. This applies to the health, bodily safety, equipment, and property. For example, prolonged exposure to chemicals in the work environment increases the risk of health problems. Noise exposure can place an employee's hearing at risk. Identifying the hazards in an environment is the first step in risk assessment. The second step is to determine who is at risk from these hazards. The third step is to evaluate the risk, and the final step is to determine the best way to control the risks and provide a safe working environment.

CONSULT WITH EMPLOYEES

Risk management is necessary to protect the company and the employees. Employees are the most valuable resource because risk management directly affects them, and they have a unique understanding of day-to-day operations. It is important to consult employees with any change in the way work is done. When consulting with employees, it is imperative that you communicate clearly and honestly. Provide ample time for the conversation to take place. Finally, it is imperative that you pay attention to everything employees have to say; do not simply pay attention to feedback that supports you current ideas.

Examples of When to Consult Employees:

- Safety inspections
- Purchasing or repairing equipment
- Workflow charts
- Internal layout
- Cleaning chemicals

LIKELIHOOD SCALE

The likelihood scale is used to determine the likelihood that an event will occur. For example, you would use it to determine the risk of an equipment malfunction. Each risk needs to be scored on the likelihood scale from 0 to 3.

- **0 – Impossible**: There is no possible way that an event can take place. This is rarely used.
- **1 – Low possibility/Remote possibility**: There is a slight risk, 2% or less, of something happening.
- **2 – Medium possibility/Possible**: The event is possible. It has between a 2 and 25% chance of occurring.
- **3 – High possibility/ Probable**: There is a greater than 25% chance that something is going to happen. The event is likely going to occur soon.

Scores should be based on the current data that you have. The reasons for your score should also be recorded.

Example:

Risk	Score	Reasoning
Hearing damage	**1**	Noise pollution is within safe parameters. The office does not have loud consistent noises.
Lab accident	**3**	Caustic chemicals are used daily, along with dangerous equipment. There is the risk of human error.

Each company will have different risks and scores. Risks with higher scores need to be addressed quickly.

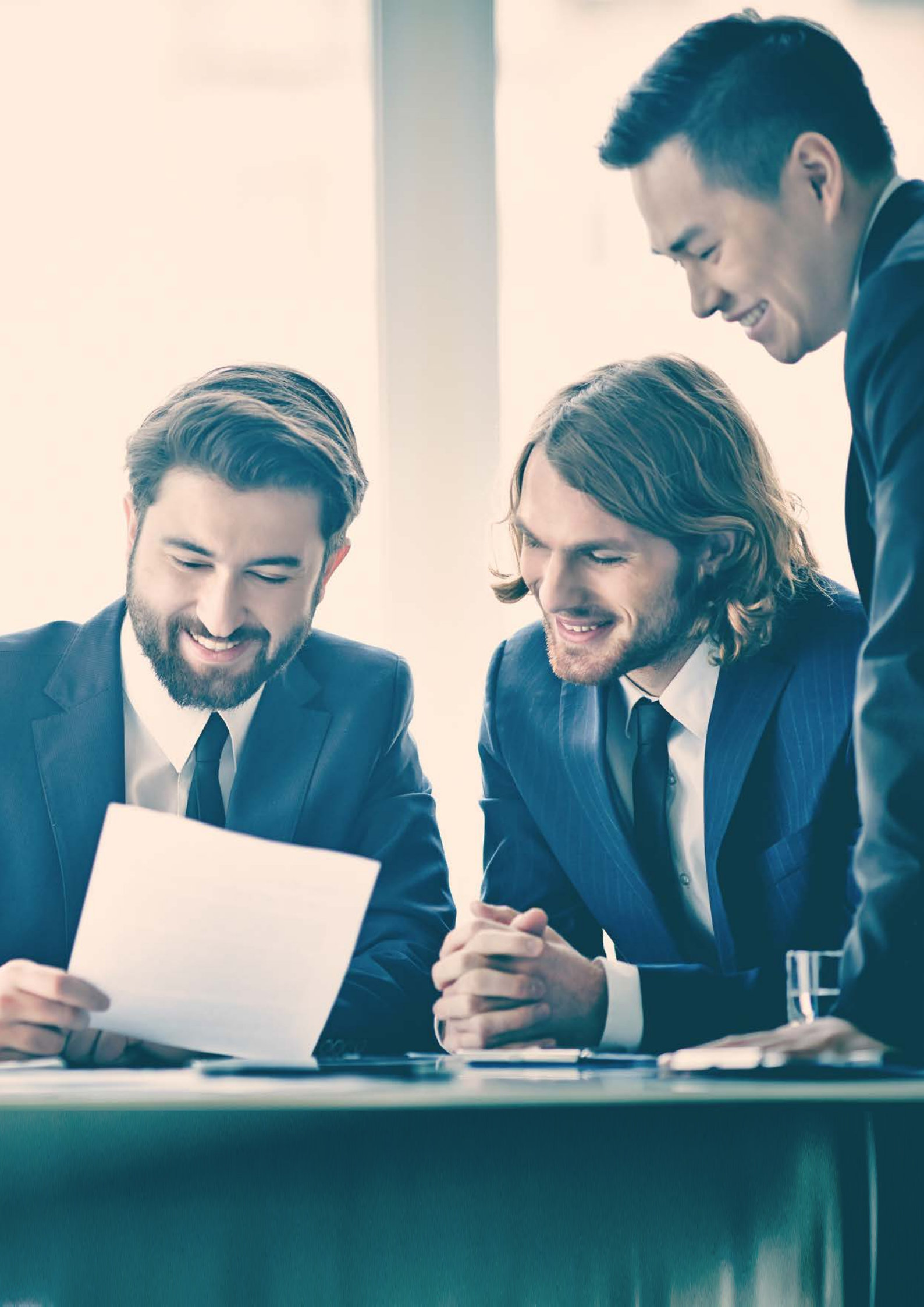
PRACTICAL ILLUSTRATION

Sean is an outside hire to his new management position. He understands that risk management is important, and he takes the time to go over the incident reports and inspect the facility. An employee tells him that one of the machines needs to be replaced. He says that several employees have come close to being injured while using it. He states the machine does not shut off properly. Sean believes that asking for new equipment this soon is not wise. He points out to the employee that there are no incident reports for the specific piece of equipment. The employee responds that the employees know to be extra careful on the machine, but it is just a matter of time before someone is injured. Sean ignored the request, and

the complaints from three other employees. He did nothing about the equipment. Two months later, an employee thought the machine was turned off and got her hand caught in it.

Take calculated risks.
This is quite different
from being rash.

GENERAL GEORGE PATTON



CHAPTER TWO

SEEKING OUT PROBLEMS BEFORE THEY HAPPEN (I)

The purpose of a risk assessment is to seek out problems before they happen. This allows you to prevent accidents and emergencies, or you can at least be better prepared when emergency situations do occur. This requires and understanding of the business and vigilance. By paying attention to potential problems, you will improve the overall health and success of your business.

UNIQUE TO YOUR BUSINESS

Each business will have its unique set of problems. For example, the risk of a retail business will be quite different from the risks that a manufacturing company would face. Pharmaceutical companies would face different risks than financial institutions. Larger organizations that cover multiple areas may find it helpful to breakdown the potential problems for each department.

There are some basic risk categories to consider when discovering what is unique to your business:

Basic Risks:

- **Physical Risks**: the building, equipment, chemicals, etc.
- **Location Risks**: Crime, natural disasters, etc.
- **Human Risks**: Intoxication, theft, fraud, human error, etc.
- **Technology Risks**: Power, hacking, telecommunications, etc.

Careful consideration will help identify unique problems so that you can address them before they happen.

WALK AROUND

Identifying potential problems requires close inspection of the work area. In order to do this, you need to look at the environment carefully. Inspect each area of the facility for hidden risks and hazards that can cause problems. This requires walking around the entire facility and making note of everything. It is essential to consider every possible use of an area, all materials used, and each tool.

Things to Consider When Walking:

- How tools are used
- Different methods used to complete tasks
- Purpose of each tool

- Materials used

Make a list of all problems as you notice them. Use this list to guide the risk assessment.

LONG TERM AND SHORT TERM

When you are identifying potential problems and issues, always keep in mind the long and short term implications. It is easy to focus on the short term problems that require immediate attention. For example, missing safety equipment is a short term problem that has immediate consequences that needs to be addressed quickly. Focusing on short term problems, however, can overshadow long term problems. Long term problems are problems that will develop over time, and because they are not immediate issues, they are easy to ignore. For example, exposure to noise pollution is a long term problem that can lead to hearing loss if it is not addressed in a timely manner. Do not allow the short term risks and problems to prevent you from addressing the long term.

COMMON ISSUES

When looking for potential problems, it is important to pay attention to common hazards and risks. Most organizations face these potential problems, regardless of the type of business they are. While each company will have its own risks and problems, beginning with the common issues will help you identify basic problems. Many common issues can be resolved by keeping the work area clean and tidy.

Examples of Common Issues:

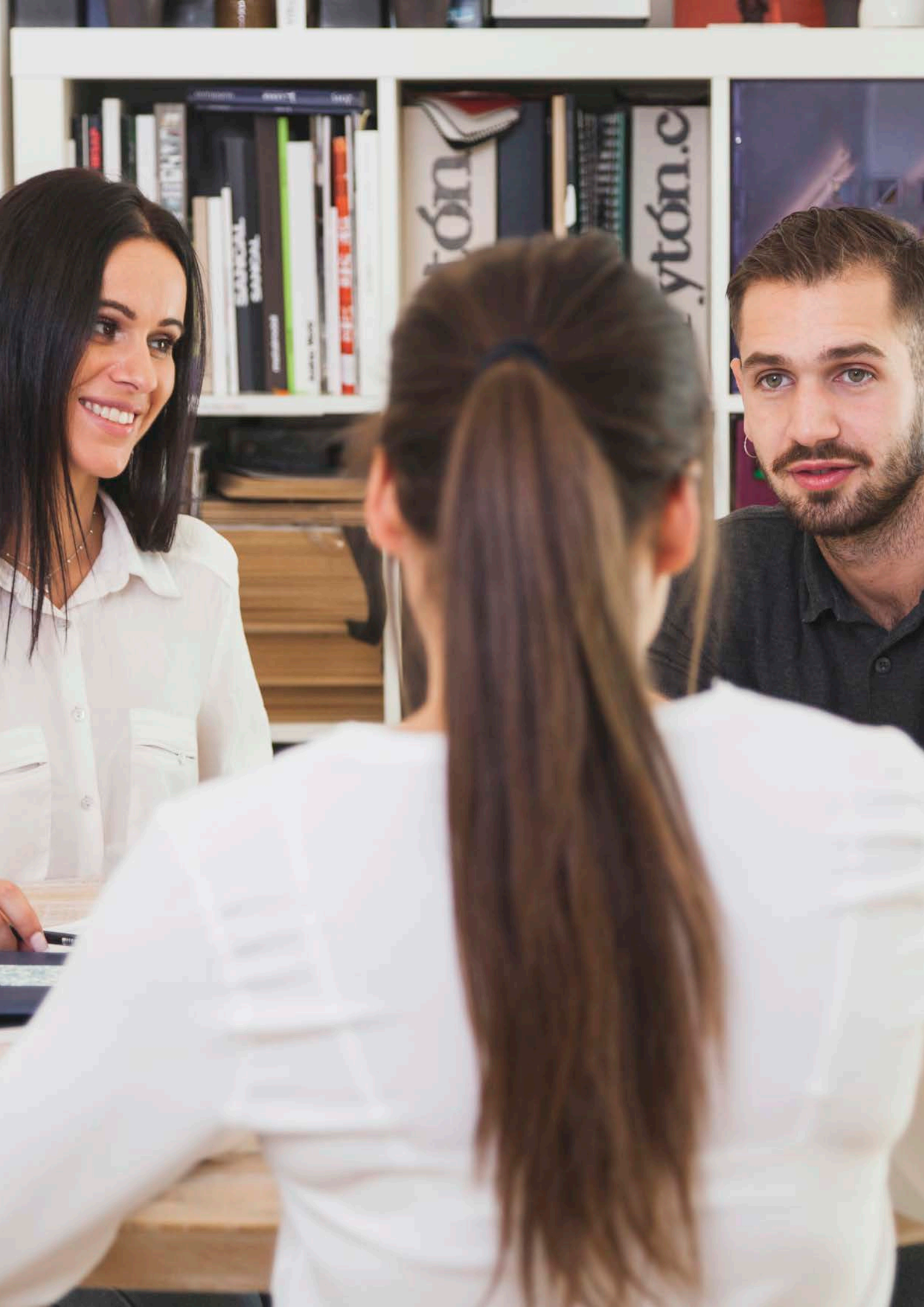
- Slip and fall areas
- Clutter
- Extension cords
- Falling objects
- Indoor pollutants

PRACTICAL ILLUSTRATION

The QRT manufacturing company was growing. Profits were high, and orders were up, but the company was still in the original space. The owner considered moving to a larger location, but he was not sure if it would be worth the cost. Workstations were placed closer together. Clutter soon developed and parts had to be stacked higher and higher on shelves. One day, an employee tripped over some debris on the floor and fell into the shelving, knocking it on top of him. The employee was injured and damaged two pieces of equipment.

If you do not actively attack risks, they will actively attack you.

TOM GILB



CHAPTER THREE

SEEKING OUT PROBLEMS BEFORE THEY HAPPEN (II)

Problems can occur at any time. This is why you must always be prepared to address them. Seeking out problems before they occur requires you to ask questions. You must pay attention to the risks of external events and preparing for the worst case scenario. The consequence scale may identify the potential problems.

ASK "WHAT WOULD HAPPEN IF … ?"

In seeking out problems, you need to consider every aspect of risks. The key is to look at a situation and ask, *"What would happen if…"* For example, you may ask, *"What would happen if the electricity went out in the middle of the workday?"* Once you ask what would happen, you will be able to determine what type of impact it would have on the organization. Each possible problem can be assigned a different level of impact. Only assign a possible impact if you have all the information. Assign these as: need more information or needs to be determined.

Levels of Impact:

- **Low Impact**: If a problem occurs, it will have little impact on the business and can be easily remedied.
- **Medium Impact**: The problem is not critical, but it will have an impact on the organization.
- **High Impact**: This is a critical problem will disrupt the business.

Determining the level of impact will establish which problems need to be addressed first.

EXTERNAL EVENTS

No matter how prepared you are, problems are not always easy to predict. This is especially true of external events. You have more control over internal events, but external events are more unpredictable. With external events, you need to be prepared for every possible problem. These events are, basically, anything around the office that is not internal.

Types of External Events:

- **Suppliers**: Suppliers bring external events with their own risks
- **Customers**: Customers bring external events with their own risks
- **Visitors**: Visitors bring external events with their own risks
- **Traffic**: Traffic affects schedules and the ability to make deadlines
- **Parking**: Drivers and car maintenance affect parking

- **Environment**: Weather and other environmental factors are external events

WORST CASE SCENARIOS

Part of risk management is preparing for the worst case scenario in every situation. Discovering the worst case scenario goes beyond asking *"what if."* You need to ask, *"What is the worst that could happen?"* For example, you should ask, *"What is the worst that could happen if the computers were hacked?"* The worst case scenario is essentially what happens if everything were to go wrong. The worst case scenario will vary according to the unique risks of each organization. A company that manufactures fertilizer, for example, will have a different worst case scenario than a call center. Once the worst case scenarios are defined, you will be able to anticipate them and develop the appropriate back up plans.

CONSEQUENCE SCALE

Once you identify the risks and potential problems that the organization faces, you need to understand the severity of the consequences. The consequence scale can be used for every potential problem that you identify. Using the consequence scale allows you assess severity and determine what the outcome of each risk will be.

Consequence Scale

- **Insignificant**: Little impact on the organization; no injuries
- **Minor**: A small impact; first aid is necessary

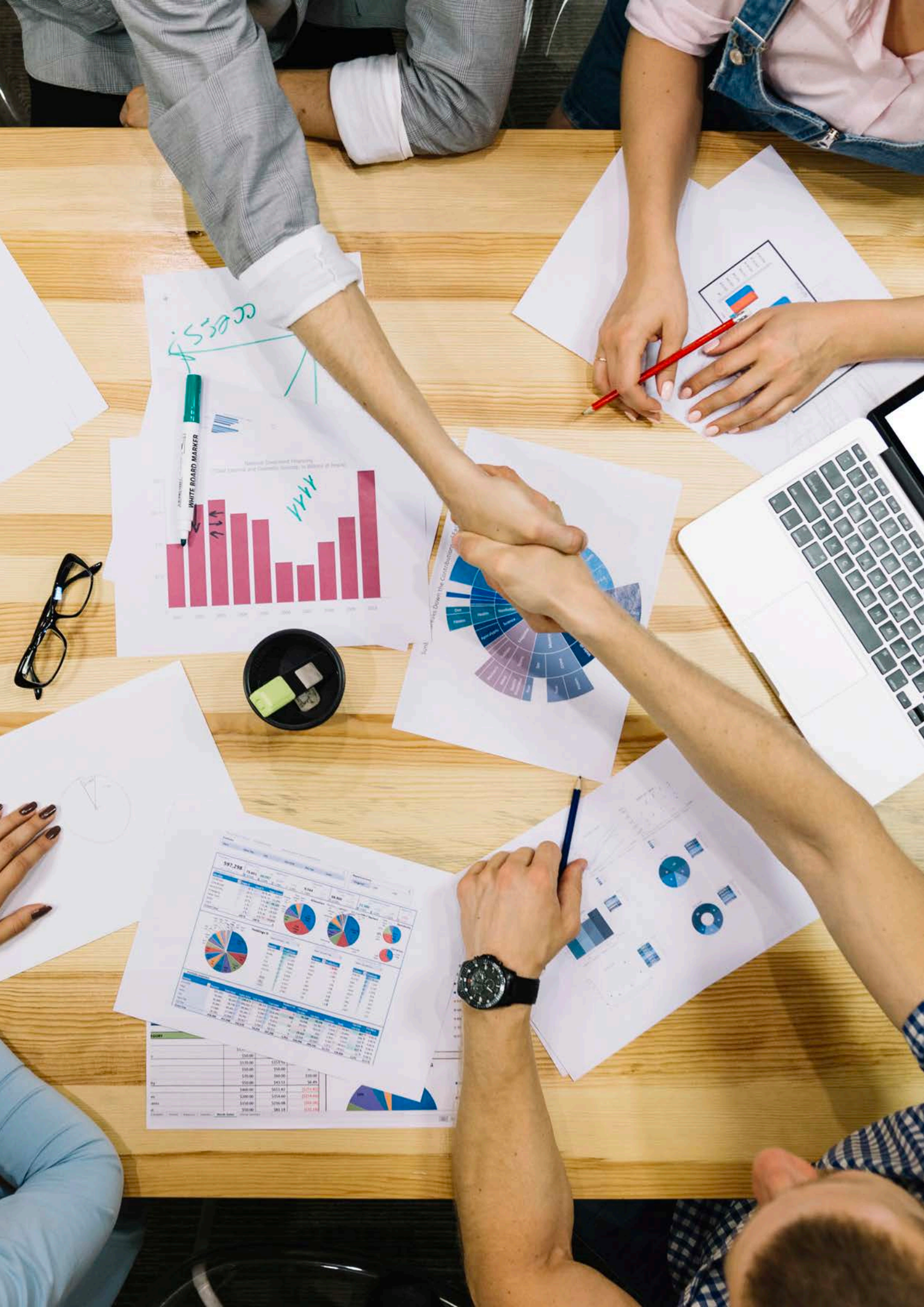
- **Moderate**: A definite impact; involves hospitalization
- **Major**: A large impact; may involve 1 to 3 deaths
- **Catastrophic**: A crisis; multiple deaths reported

PRACTICAL ILLUSTRATION

Jane carefully planned her risk assessment for every internal aspect of the business. She was certain that nothing would catch her off guard. One day, a supplier delivered an order and stacked it in the hallway. The boxes were not stacked securely, and they fell over. Part of the order included cleaning supplies that broke and spilled in the fall. As the cleaning supplies mixed, they created a chemical reaction that produced noxious fumes. Several employees and customers became sick from the smell, and people soon fled the building. Jane had no plan in place for the problem, and she spent the next few days handling the damage from the accident.

You cannot escape the responsibility of tomorrow by evading it today.

ABRAHAM LINCOLN


WHITE BOARD MARKER

CHAPTER FOUR

EVERYONE'S RESPONSIBILITY

Managing risks does not stop with the management team. Everyone is responsible for the safety of the business environment. The risks and potential problems that an organization faces must be clear to employees at all levels. If everyone works to prevent problems before they begin, everyone will enjoy a safe and smoothly run work environment.

SEE IT, REPORT IT!

When everyone takes responsibility for risk management, it is necessary that all employees know to report potential problems. A system should be in place to make reporting problems simple, and everyone must be aware of how the system works. Employees should be actively encouraged to report risks and potential problems. There should be no confusion about this expectation. Create a visual reminder by posting lists of risks that employees should watch out for along with emergency contact information throughout the workplace.

Common safety risks employees should report:

- Unauthorized individuals
- Leaks

- Smells
- Broken locks
- Broken equipment
- Slippery floors

IF IT'S NOT SAFE, DON'T DO IT

Safety is a primary concern for organization. A common mantra is, "If it's not safe, don't do it." This rule must extend to all employees. Safety standards and risk management programs are only effective if they are properly implemented, and leaders need to be an example of safety standards. Do not perform a task without the appropriate safety equipment and expect your employees to use theirs. Any leader who violates safety rules is sending the message that they are not important.

Additionally, listen to employees who believe that a work environment is not safe. Provide employees with stop work authority (the authority to stop working if the environment becomes dangerous). Employees should not feel pressured to work in dangerous situations just to keep their jobs. Make sure that employees are taught the safety rules and that the rules are consistently followed.

TAKE APPROPRIATE PRECAUTIONS

When you have identified the risk and problems, it is essential to take the appropriate precautions. The precautions that you need to take will be determined by the organization. Precautions will be based on the risks

identified in each company. There are, however, basic safety precautions that every organization needs to take.

Common Precautions:

1. Safety equipment
2. Accessible exits
3. Fire alarms
4. Safety training
5. Ergonomic work stations
6. Security
7. Ventilation

COMMUNICATING TO THE ORGANIZATION

Risks and safety precautions need to be communicated to the entire organization. Everyone needs to be informed. The communication needs to inform, educate, and prevent problems. When communicating, it is important to create a plan and follow it.

Communication Strategy:

- **Identify the information you need to communicate**: Sift through the information and highlight everything that needs to be communicated.

- **Consider the audience**: Identify what the audience does and does not know about the topic and communication barriers.
- **Create the communication**: Tailor the communication to the needs of the audience.
- **Choose communication methods**: Choose the communication methods for your audience. You may use more than one method of communication.

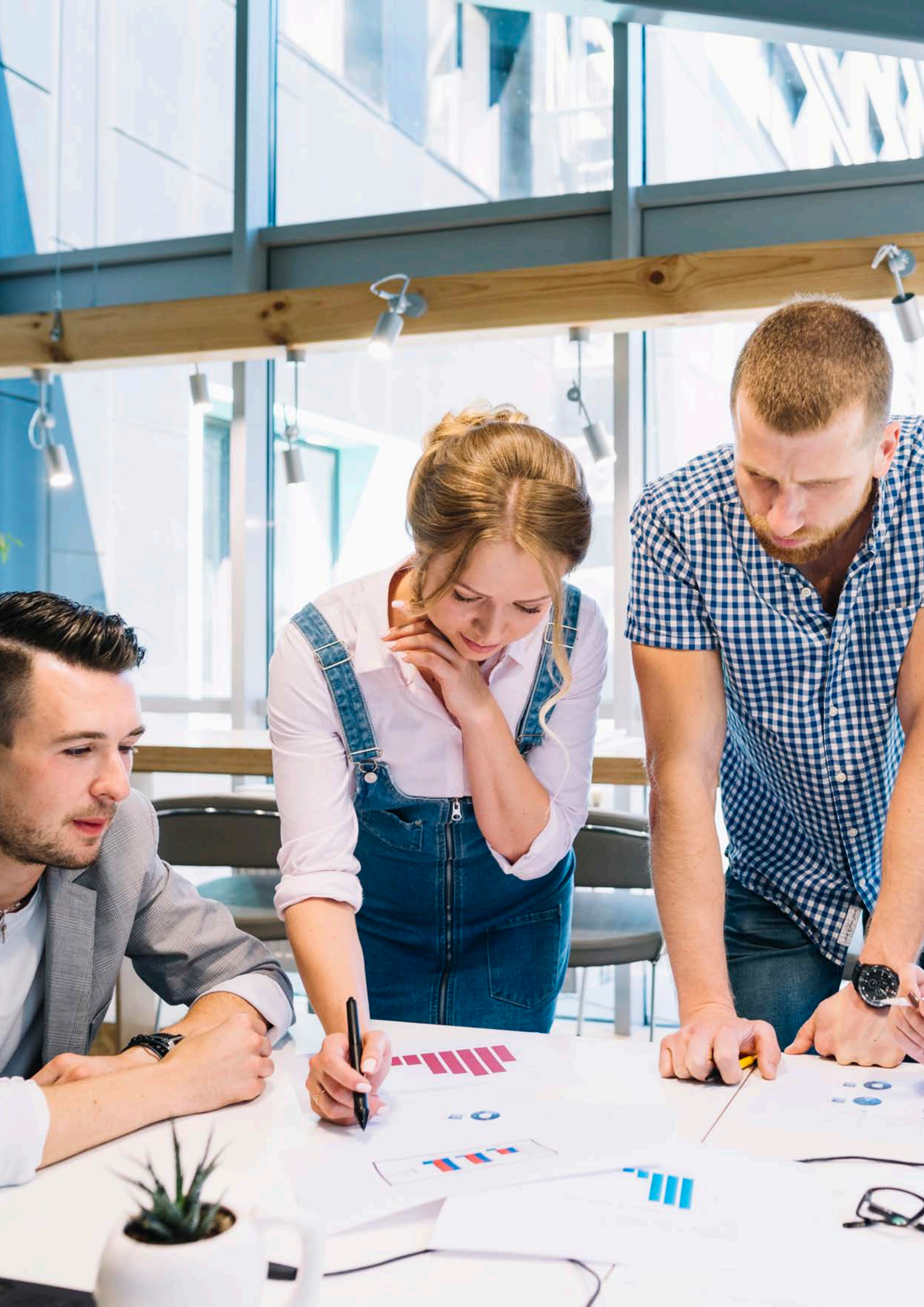
Communication is ongoing. Once you communicate the information, evaluate its effectiveness, and determine if any changes need to be made.

PRACTICAL ILLUSTRATION

Jake was in charge of implementing new safety standards in the repair company. The standards include wearing safety glasses and aprons as well as proper ergonomics when working on jewelry. Additionally hair needs to be covered to prevent accidents in the workroom. One day, a customer required a quick repair, and Jake was in a hurry. He walked into the workroom and completed the repair without following the safety guidelines. There was no accident, and he occasionally broke the rules to save time. Employees soon followed his example. Soon, an employee forgot to cover her hair and got it stuck in the polish wheel.

In God we trust;
all others bring data.

W. Edwards Deming



CHAPTER FIVE

TRACKING AND UPDATING CONTROL MEASURES

Control measures are essential to risk management. The risk assessment allows you to effectively track control measures. By tracking control measures, you will be able to update them as necessary. Updated control measures ensure that the work environment is safe for everyone and that it remains safe as changes occur within the organization.

WHAT IS A CONTROL MEASURE?

Most organizations have control measures in place. Control measures are actions or activities that are in place to limit or prevent risks. There are six basic types of control measures. The measures used depend on the risk that is involved and how easily than can be avoided. There is a basic hierarchy to control measures, with the top measures being the most desirable. Some risks will require multiple control measures.

Control Measure Hierarchy:

- **Eliminate**: Remove the hazard.
- **Substitute**: Trade for a lesser risk.

- **Isolate**: Limit access to the risk.
- **Engineered controls**: Designs to prevent access to risks and hazards.
- **Administrative controls**: Safe work practices and procedures
- **Protective equipment**: Personal protective equipment is worn around hazards.

YOUR BUSINESS PROCEDURES

Every business has different needs. The needs of the business determine how you develop your business procedures and your control measures. Remember that every company is unique and must develop procedures independently; you cannot rely on common procedures and control measures. You need to determine what is best for your organization.

Many business procedures are based on specific control measures. For example, inspecting equipment is a control measure. The policy and procedure for the inspection process will vary according to each organization. A busier organization will require more frequent an in-depth inspections. Additionally, certain pieces of equipment may require more frequent inspections than others.

ARE THEY ADEQUATE?

Control measures and procedures will need to change as the organization does. Measures that are necessary one year may not be necessary the next, or they may no longer be adequate to fill the company's needs.

Determining if the established control measures and procedures are adequate requires frequent evaluation.

When to Conduct Evaluations:

- At least once a year
- After new procedures are implemented
- After any change in the organization

There are common methods of evaluation, but it is important that each company identify the most effective methods for the organization.

Common Methods of Evaluation:

- Surveys and checklists
- Employee interviews
- Changes in the number of incidents
- Performance indicators
- Performance standards

As control measures are evaluated, determine what, if any, changes need to be made to the controls or procedures.

UPDATING AND MAINTAINING

It is important to update control measures as necessary and maintain them once they are established or updated. Evaluating whether a control measure is adequate will determine what needs to be updated and when

it needs to be updated. Changes in the external work environment will also require updating. For example, changes to government regulations would require updating the control measures.

Once control measures are implemented or updated, they need to be maintained carefully. If control measures and procedures are not maintained, it is not possible to determine whether they are effective. Establishing basic quality assurances can do this. Identify key activities for control measures and create checklist to determine that the measures are being maintained.

Example:

Key Activity	**Checklist**
Understanding of expectations	Training available Written procedures are available Documentation of completed training

The checklists provide consistency and routine. They also make it easier to identify when the measures are not being maintained.

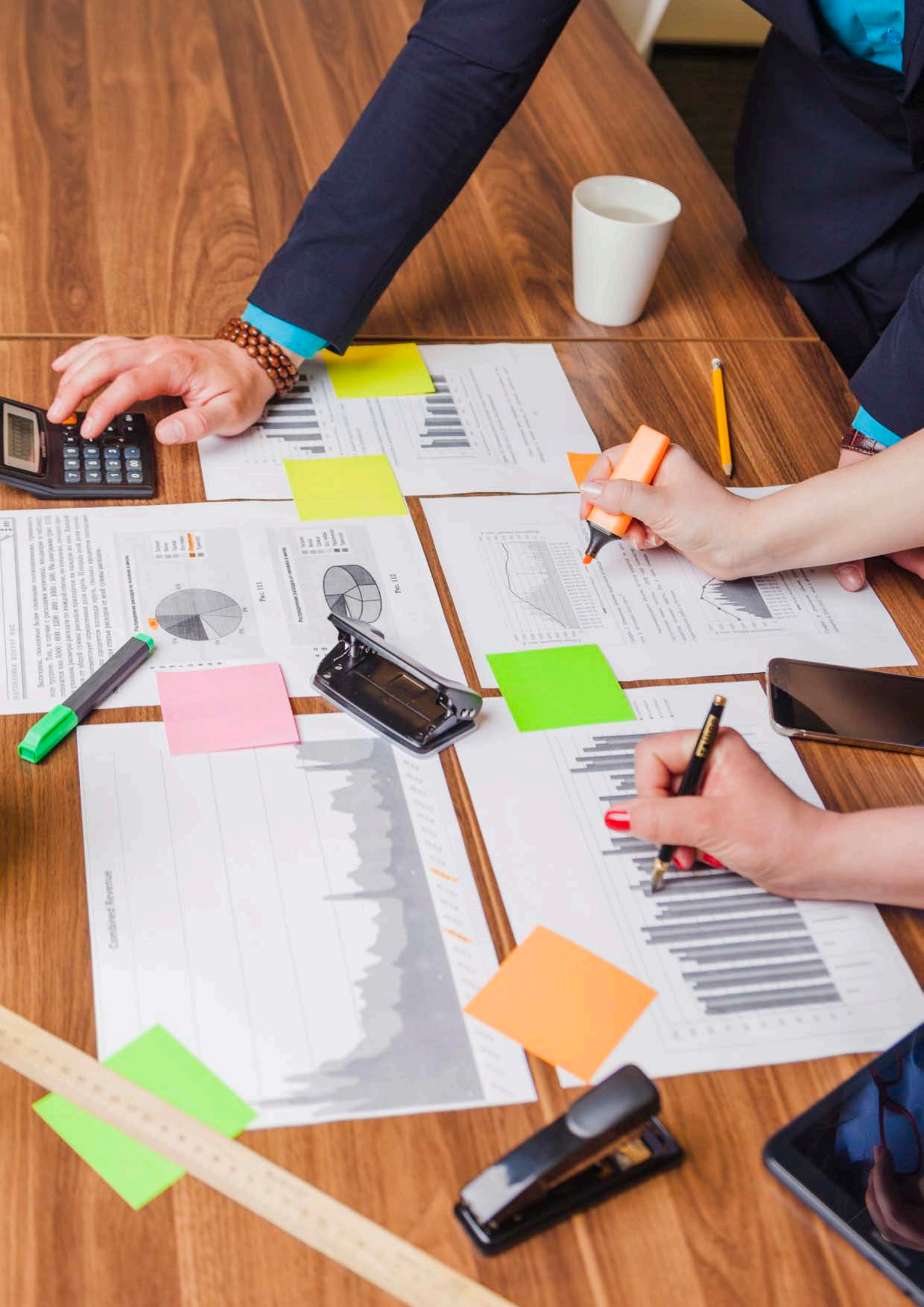
PRACTICAL ILLUSTRATION

The BCD Corporation established control measures based on government regulations and current evaluations. The initial company reports after initiation showed a decrease in injuries and other unwanted events. Over the next few months, the company saw massive growth due to

increased sales. The control measures and procedures remained in place for the organization. Soon, there was an increase in missing inventory, and employees began to report the theft of personal items. The security measures remained in place, but they were obviously ineffective.

It's important to take risks, but it's idiotic to take them blindly.

TERRY LEVINE



CHAPTER SIX

RISK MANAGEMENT TECHNIQUES

Once the risks are assessed, they must be managed carefully. There are four basic risk management techniques, and your company probably uses all of them. The management technique that you use will vary according to the severity of the risk and the current stability of the organization. You will choose between reducing the risk, transferring the risk, avoiding the risk, and accepting the risk when determining which technique to use.

REDUCE THE RISK

Risk reduction is a common technique used in business. It is necessary when there is no possibility of removing the risk such as in using machines. When you reduce the risk, you limit the severity of the risk and the likelihood of the risk occurring. When determining how to best reduce the risk, it is necessary to establish which method of reduction will be the most effective. For example, one risk reduction technique may reduce the risk of loss more than others, but it could also be more expensive to implement.

Examples of Risk Reduction:

- Retrofit a building to for severe weather
- Sprinkler systems with fire alarms
- Training programs
- Security system
- Machine maintenance

TRANSFER THE RISK

The act of transferring a risk is also called risk sharing. This is often done in business relationships. For example, working with contracting labor or vendors may require a transfer of risk. The transfer of risk does not remove all risk from you, but it does offer some protection. The most common method used to transfer the risk is insurance. The insurance company takes on the risk from the policyholder.

When working with other parties, insurance is not enough to cover the liability. It is necessary to review contractual obligations. You do not want to take all of the risk in a contractual relationship. There are different ways to transfer the risk:

- **Indemnification**: Place the legal responsibilities on an established party.
- **Certificates of insurance**: Require specific levels insurance. Certificates are proof of specific coverage.

- **Additional insurance status**: A business is added on to another company's policy. It offers protection if indemnification is lost and prevents subrogating.

AVOID THE RISK

Avoiding risks is not always possible. When avoiding risks, however, the purpose is to eliminate the risk or simply not engage it. Risk avoidance occurs regularly. It occurs when you decide against a business proposition or refuse to expand the company. Eliminating risk by avoiding may seem like the safe route, but it is not always practical. If you avoid every risk that comes along, you will also avoid great business opportunities.

Always consider both the risks and rewards that a new situation brings. For example, expanding the business may be costly. There is always the chance, however, that the expansion will pay for itself and increase profits. Before avoiding a risk, make sure that you are not overlooking and opportunity. The severity of the risk will help you determine if it is something that you truly need to avoid.

ACCEPT THE RISK

There are times when it is necessary to accept risks. When you accept risks, it is necessary to choose small risks that will not have a large impact on the organization, and they can include reduced risks. The cost of the risk should be smaller than insuring or avoiding the risk. A common act of risk acceptance is refusing insurance. When accepting a risk, you are

accepting full responsibility if something goes wrong. This includes legal and financial responsibility.

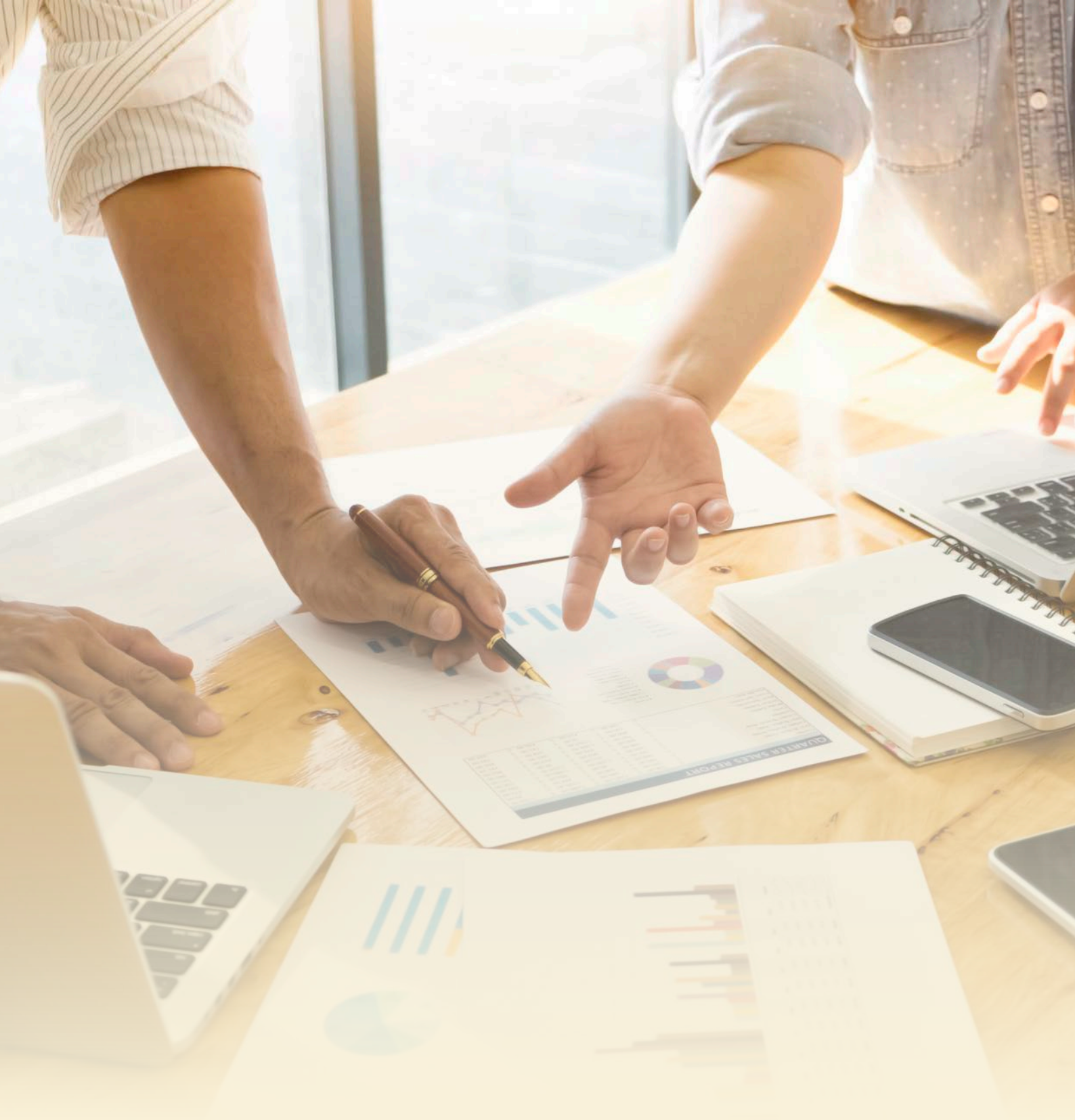
There are two different types of acceptance. Active acceptance occurs when a risk is identified and a plan is established should you need to face the consequences of the risk. Creating a plan of action helps you determine the best plan of action without the emotional impact that comes with facing the consequences. Passive acceptance occurs when there is no plan in place for an accepted risk. Passive risk occurs when the risk is so small that it is not worth the time and energy to plan a course of action.

PRACTICAL ILLUSTRATION

Kara was known for her successful business strategies. She never walked into any situation blindly, and managed to grow every company that she worked for over the past ten years. Kara was careful about every decision she made in her personal and professional life. After she started her own company, Karen was offered the chance to expand by buying out her main competitor. She refused because of the financial risk. Someone else made the purchase. After six months, Kara was having trouble meeting her projected goals. Her competition, however, saw exponential growth.

Safety doesn't
happen by accident.

ANONYMOUS


QUARTER SALES REPORT

CHAPTER SEVEN

GENERAL OFFICE SAFETY AND REPORTING

It is important not to overlook the importance of safety in the office setting. A large number of accidents occur in the seemingly safe office environment. While it is important to try and prevent accidents in the office, it is equally important to be prepared in the event that accidents occur. Planning and reporting are essential to risk management. Preparation will help create a safe working environment.

ACCIDENT REPORTS

Accidents are inevitable in every workplace, and they need to be reported immediately, or within 24 hours of the accident. Make sure that all accidents are reported, even if the employee does not believe that they are injured. It is possible for injuries to become apparent after the initial incident. Accident reports must follow local guidelines. Regardless of the local regulations, the report must include why the report is being filed and how the incident occurred. The accident report is essential if the employee needs worker's compensation or develops medical work restrictions.

There are three different sections of the accident report:

- Employee
- Supervisor
- Medical Provider

The employee and supervisor must complete their portions of the report, regardless of whether medical treatment is sought. In the event that an employee requires medical treatment, the provider must fill out the accident report. A doctor's note should be provided along with the completed accident report.

ACCIDENT RESPONSE PLANS

Accident response plans are put in place to help prevent accidents from happening again. An accident report requires an investigation. The results of an investigation will provide information to improve the safety of the work environment. When creating an accident response plan it is essential that everything that needs to be done in the event of an accident is outlined.

Plan Elements:

- Establish the chain of command.
- Determine procedures for different level of accidents (from minor to catastrophic).

- Collect evidence/information (including witness statements, reports, and photographs). Make sure that the scene of the accident is secure.

Analyze the evidence and draft a report explaining the incident. The report will be used to determine the exact cause and which changes are necessary to prevent repeat occurrences.

EMERGENCY ACTION PLAN

Every office building requires an emergency action plan. Emergency action plans are implemented in case of an emergency such as a fire or major machine malfunction. Emergency action plans need to be written and accessible to employees. In small groups (under 10), the action plan may be communicated to employees verbally.

What to Include in an Emergency Action Plan:

- Procedures to report emergency
- Evacuation procedures
- Critical employee procedures
- Accounting for employees after evacuation
- Rescue and medical procedures
- Title of the employee who informs others of their duties in the plan

Each employee must be trained to evacuate and assist other employees. The employer must review the action plan with employees when they are hired, when there are changes, when employee roles change.

TRAINING AND EDUCATION

Everyone in the office needs to be educated about safety risks and trained to avoid them. The education and training needs to begin with new hires. Make all risk that employees face in the office clear from the beginning, and add new training programs when new risks are identified. The needs of the organization will determine which safety topics require further training. There are, however, typical safety topics that most office employees need to know about.

Typical Safety Topics for Training:

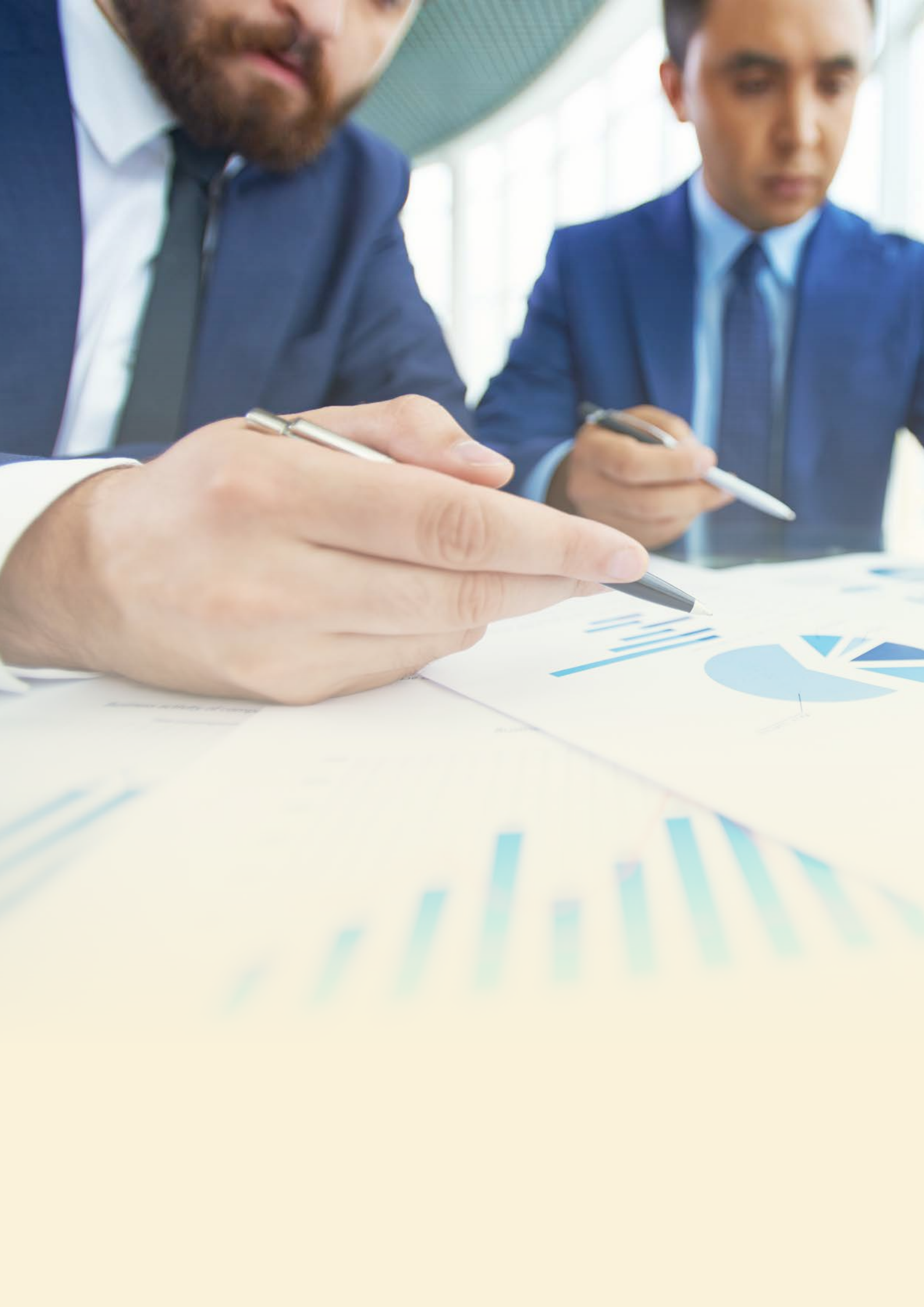
- Electrical safety
- Housekeeping
- Falls
- Awareness
- Ergonomics
- Fire Safety

PRACTICAL ILLUSTRATION

Sharon worked in a safe office environment that was free of incidents and injuries, which is why she was surprised when a box fell off of a shelf in the supply closet and on her shoulder. Her manager panicked and made her sit down for a few minutes. Sharon decided that she suffered no serious damage because there was only a small bruise on her shoulder, but it hardly hurt. Her manager asked if they "needed to bother with an accident report." Sharon decided that a report was not necessary. Two days later, Sharon woke up to discover that she had trouble moving her shoulder and neck. The doctor told her that she had whiplash and needed treatment.

In the last analysis, sound judgement will prevail.

JOSEPH CANNON



CHAPTER EIGHT

BUSINESS IMPACT ANALYSIS

The business impact analysis is used to calculate the consequences of potential disruptions, and it determines what is necessary for a company to recover. The risk assessment identifies the potential losses that the organization faces as well as severe risks. Combining the information of the risk assessment with the business impact analysis will allow you to prepare for risk and overcome the impact that they have on the organization.

GATHER INFORMATION

Conducting a business impact analysis requires gathering information. The information gathered must be very specific about a chosen critical function. For example, the data for a sales department would focus on the selling process, roles, responsibilities, etc. The typical methods for gathering information are used in the business impact analysis:

- Reports
- Research
- Interviews
- Questionnaires
- Conference calls

Interviews and questionnaires are the main sources of information because they provide you with the opportunity to create questions specific to the topic you are researching. When creating questions for interviews and questionnaires, you may want to consult an expert in the critical area. For example, you could consult an IT expert to gather data about internet security.

IDENTIFY VULNERABILITIES

Every organization has threats and vulnerabilities. The risks identified in the risk assessment will facilitate the identification of threats. The threats to the company that can affect the operations of the organization become vulnerabilities. Vulnerabilities are potential emergencies.

The process of identifying vulnerabilities requires listing threats and considering how your critical processes are vulnerable to these threats.

Once the vulnerabilities are identified, you can determine how they can affect the organization and plan accordingly.

ANALYZE INFORMATION

Once you have gathered information and identified vulnerabilities, you may analyze information to determine your priorities. The first step to analyzing information is validating it. You can validate the data you gathered by conducting face-to-face interviews with the participants who provided the information.

After the information is verified, use it to prioritize your actions. Ask the following questions:

- How would losing this function affect the business?
- What would losing this function cost?
- Do other systems rely on this function?

The answers to these questions will reveal which functions are priorities.

IMPLEMENT RECOMMENDATIONS

Once the information is analyzed, draft a report based on your findings. The report should include the recommendations. In order for the recommendations to be implemented, you need to buy in of superiors. Successful implementation requires the a few basic steps:

- Identify the best venue for implementation.
- Review recommendations.
- Confirm commitment from participants.
- Schedule the implementation process.

After implementing the recommendations, you need to communicate with everyone involved and review the results as scheduled.

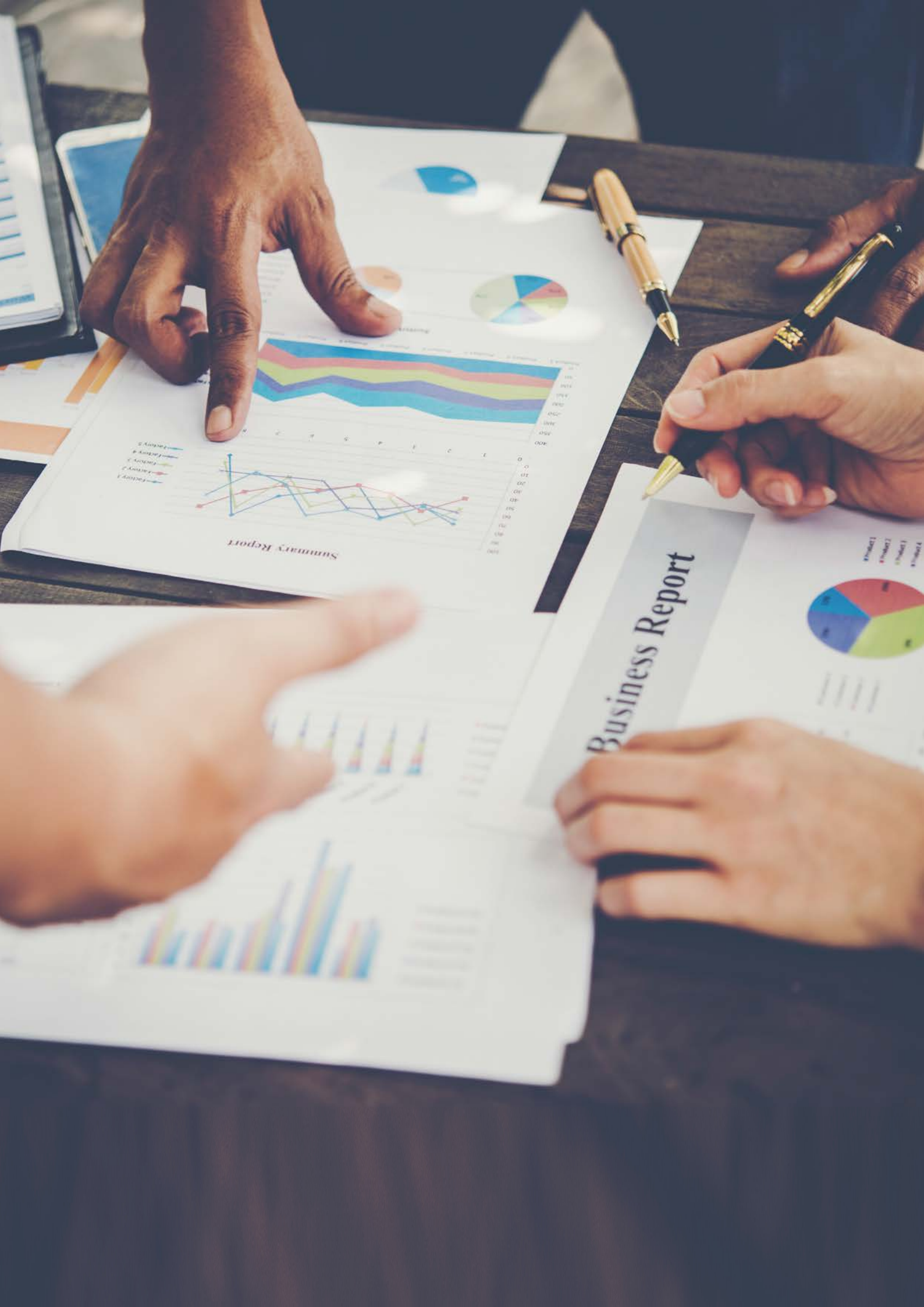
PRACTICAL ILLUSTRATION

Alec had a business in an area prone to severe weather. He realized that the weather was a threat but he never established the ways that

his business was vulnerable. A large tornado swept through the city, but missed the Alec's business. He was relieved, but damage to city's infrastructure led to flooding. A foot of water stood in the building for two days while Alec could not reach it. Soon mold was growing in the walls. Alec never considered the possibility of flooding, and was not sure what to do. He did not have flood insurance or a plan. He was not sure what to start working on first.

I always try to turn every disaster into an opportunity.

JOHN D. ROCKEFELLER


Business Report

CHAPTER NINE

DISASTER RECOVERY PLAN

Every organization needs a disaster recovery plan. The disaster recovery plan outlines the procedures that need to be followed in the event of a disaster to protect it. By considering the consequences of disasters ahead of time, the recovery plan will mitigate their effects. The disaster recovery plan is established for different disasters, including natural and manmade disasters such as severe weather or technology crashes.

MAKE IT BEFORE YOU NEED IT

Disaster recovery plans are not easy to make. They take time and commitment, but they are essential to success in a disaster. Remember that 10% of businesses do not recover from disaster situations. The disaster recovery plan needs to be written ahead of time. You need to make it before you need it. By making the disaster recovery plan before it is necessary, you will be aware of the factors necessary for the company's survival.

Necessary Factors:

- People
- Facilities

- Technology
- Data
- Suppliers
- Policies and procedures

All of these factors need to be considered when establishing strategies to create a disaster recovery plan.

TEST, UPDATE, AND REPEAT

Once a disaster recovery plan is created, the aspects of it need to be tested. For example, you may want to test your IT security. After testing the plan, make the necessary update and adjustments. Repeat this process regularly because both the business and the potential disasters will change over time.

Establishing a Testing System:

- Choose the purpose of the test and what is being evaluated.
- Determine objectives and measurements.
- Collect results
- Evaluate results
- Update the plan

Always record the tests and updates that you make to the plan. Be sure that you have the most current plan recorded.

HOT, WARM, AND COLD SITES

There are three basic disaster recovery sites for IT and technology. They are hot, warm, or cold sites. Hot sites are very similar the pre disaster site. They are coordinated with the existing site and fully stocked. They allow business to continue practically without interruption. Cold sites are the sites nothing like hot sites. They are minimal back up sites that do not resemble the normal work sites. They are simply locations used for emergencies. There are also warm sites, which are between the hot and cold sites. Warm sites are not as Spartan as cold sites, but the transition to the warm site is not seamless.

The disaster recovery needs of an organization will help determine which type of site is chosen. Many, companies, however, choose warm sites because they offer more protection than cold sites, but they are less expensive than hot sites.

KEEP DOCUMENTATION SIMPLE AND CLEAR

It is important to thoroughly document the disaster recovery plan. When creating the document, keep the formatting and wording simple. Make the message of the plan very clear. There is a basic outline that can be used to guide documenting a disaster recovery plan.

Information to document:

- Objective
- Assumptions

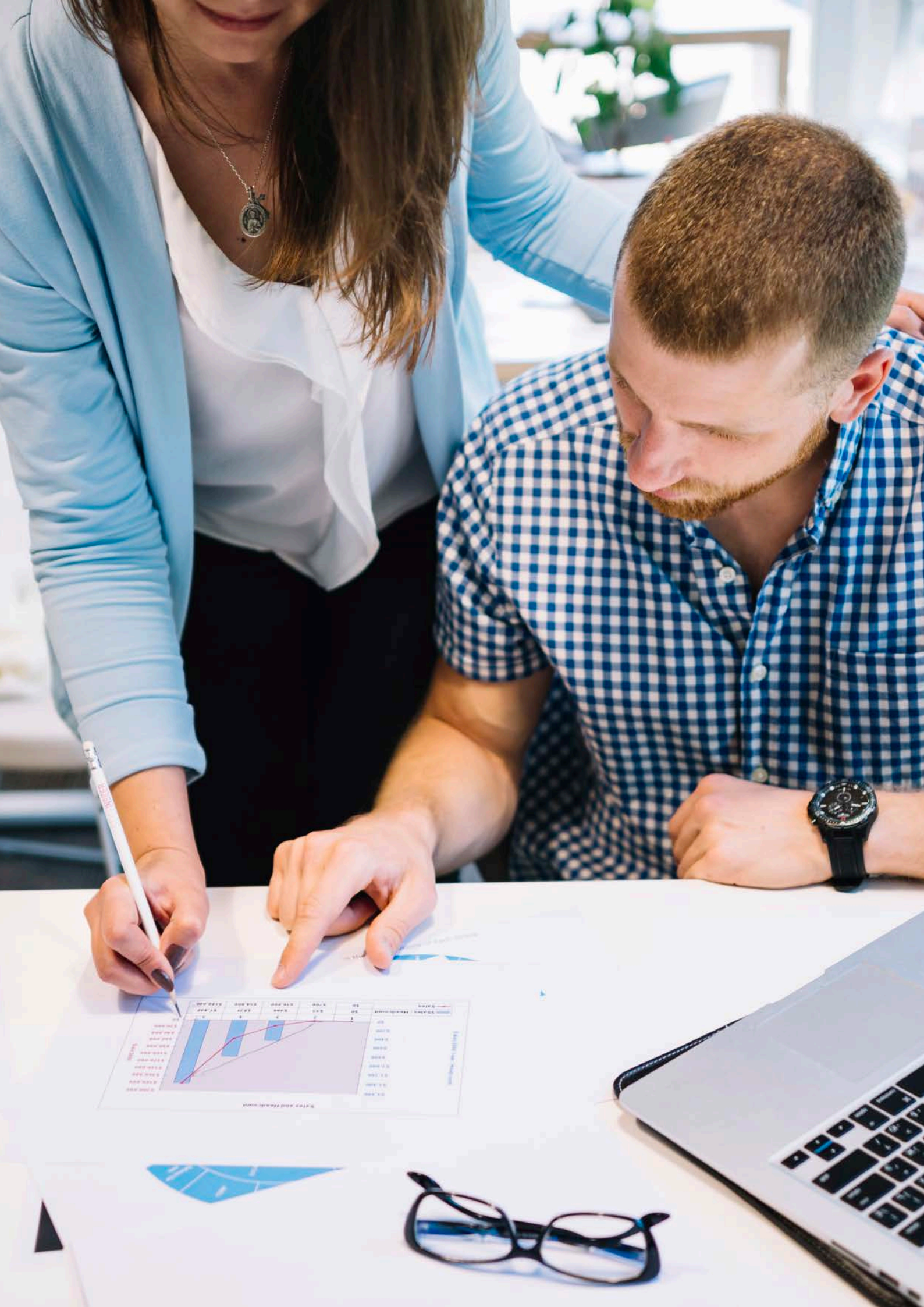
- Criteria to invoke the plan
- Roles and responsibilities
- Contingency procedures
- Resource plan
- Procedures for returning to the original space
- Procedure for information recovery

PRACTICAL ILLUSTRATION

Sean transferred the client lists, ordering system, and inventory to the computer. He was so focused on the transition that he neglected to plan for potential disasters. He was sure that the transition to electronic data would provide him with added protection as long as he installed virus software and chose useful passwords, which he did. A month after the transition, Sean discovered that he was the victim of a hacker. The entire computer system was taken offline. When Sean turned it back on, the letters were Cyrillic. Sean had no way to work after the cyber-attack, and the information was compromised.

If you treat risk management as a part-time job, you may soon find yourself looking for one.

DELOITTE



CHAPTER TEN

SUMMARY OF RISK ASSESSMENT

The risk assessment is essential to risk management and many other strategies. This requires an understanding of risk assessment and risk assessment strategies. The ability to apply risk assessment techniques in the office will improve safety for employees and the organization.

WHAT ARE THE HAZARDS?

The first step in a risk assessment is identifying hazards. Each organization will face its own unique set of hazards. Different methods are used to identify hazards, and many have already been introduced.

Methods of Identification:

- Talk to employees
- Walk around the workplace
- Evaluate operations
- Read operation manuals
- Examine company records
- Consider long-term and short-term hazards

Keep a list as you identify different hazards. Review the list for any overlap and to evaluate the hazards you identified.

WHO MIGHT BE HARMED?

Once hazards are identified, it is important to identify who might be harmed by the hazard. You must be aware of customers, employees, vendors, etc. Employees may be directly harmed by a hazard, or indirectly harmed. For example, handling chemicals can cause direct harm. Inhaling the fumes from another room is indirect harm. Additionally, you must be aware of people who may be at increased risk:

- Pregnant women
- The elderly
- Children
- People with disabilities
- Inexperienced employees

After determining who might be harmed, you need to consider how they could be harmed by the hazards.

ARE CURRENT CONTROL MEASURES SUFFICIENT?

Control measures are necessary for the risk assessment, and they will depend on the hazard of the organization. Each hazard will have its own control measure. For example, chemical hazards would have a control measure of personal protective equipment. Evaluating the control measures will determine if they are sufficient. Evaluations need to be done

when there are any changes in the organization or each year. Sufficient control measures will provide control over hazards, and they will meet government regulations.

IF NOT, CHANGE CONTROL MEASURES

Control measures are not always sufficient. In fact, you may find that some hazards do not even have the control measures. For example, a new piece of equipment has a hazard of flying debris. It requires a PPE (personal protective equipment) control measure. When you discover that control measures are not sufficient, you must change them. Once you determine how to alter the control measures, you must communicate the measures and implement them. Monitor the measures for their effectiveness and evaluate the results to determine if they are sufficient. They will need to meet government regulations and provide the safest environment possible.

PRACTICAL ILLUSTRATION

Jean took the time to identify hazards in the department. She made a list of the hazards and how they could cause damage. This information was used to create control measures. The measures were created with well-trained, young, and strong employees in mind. Jean forgot to consider people who have a higher risk of injury and members of the public such as customers and vendors. Eventually, an elderly customer with limited mobility had difficulty navigating slippery floors. She fell and injured her arm.

Every day is a journey, and the journey itself is to home.

MASTUO BASHO

CLOSING THOUGHTS

- **Theodore Roosevelt**: Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you.
- **Max Bazerman**: When our leaders accept the status quo, we run the risk of disaster.
- **Cicero**: To make a mistake is only human; to persist in a mistake is idiotic.
- **George Santayana**: Those who cannot remember the past are doomed to repeat it.

Rick Chisholm made history when he single-handedly changed the professional Audio Visual industry by breaking all the rules and capitalised over 50% market share in Australia with very little capital, no partners, mergers or lenders and set up the first franchise operation of its kind in the world in the late 1990's and early 2000's.

As a 7x founder of companies and 30x businesses such as Innovest, AI Machine, Lightsounds, LSW, Light Emotion with revenue in excess of $300 million and having employed more than 1,000 staff over the last 35 years. Rick is known as the Start-Up and SME Guru and is Author of a number of books including Business Success for Life. Unlike many mentors, he actually walks the talk and has a number of businesses under management in such areas as Automation, Events management, Importing, Distribution, Retailing and E-commerce.

His BIG passion is Business Education empowering Businesses Owners through knowledge and skills. Whilst Rick has experienced great success, he has also endured many failures. Rick has faced and overcome the exact same challenges you are facing now.

Tala Chisholm is an SME specialist who has owned and managed several small to medium sized businesses in the last 20 years, several of which were eventually sold. She has extensive experience in the fields of retail, franchising, licensing, dealerships, education, importing, distribution and consulting.

Her expertise lies in building and implementing customised cross-platform database and software solutions for businesses, automation, IT, web marketing, advertising, graphic design, business administration, process refinement and implementation. Her business experience ranges from bricks-and-mortar Giftware retailing to highly technical fields such as Security, CCTV, Entertainment Lighting and Audio sales, hire and installations as well as e-commerce.

Throughout her career she also trained and mentored Franchise business owners as well as internal division managers. Some areas of training included retail operations, management practices, business strategy, accounting, cash-flow, marketing, customer service and IT. She has also headed up the drafting of Operating Compliance Manuals for Franchise operations and implementation of all the elements involved.

Phone: +61 2 8007 2907
E-mail: admin@innovestsme.com.au
Website: www.innovestsme.com.au