LEARNER GUIDE

Unit Standard Title:	**Manage Risk in Own Work Environment**
Unit Standard No:	**119265**
Unit Standard Credits:	**2**
NQF Level:	**4**

This outcomes-based learning material was developed by Masifunde Training Centre with funding from INSETA in July 2014. The material is generic in nature and is intended to serve as a minimum standard for the industry.

Manage Risk in Own Work Environment

Introduction

In everyday usage, risk means ‘the danger (or uncertainty) of injury, damage or loss’. In a financial services environment, *risk* refers to the uncertainty of achieving the expected rate of return on an investment, or of suffering a physical or financial loss – quantified in terms of the probability of these outcomes.

The short-term insurance sub-sector addresses the risk of damage to, or loss of physical assets, and the financial consequences. However, insured parties cannot gain from short-term insurance contracts, which only indemnify them against loss. Investors may gain (more than they expect) from risky investments, but they may also suffer a serious loss, perhaps even losing their capital. (Substantial gains or losses are most likely in high-risk investments.)

Module 1

The Risks associated with Life and Work

This Module deals with:

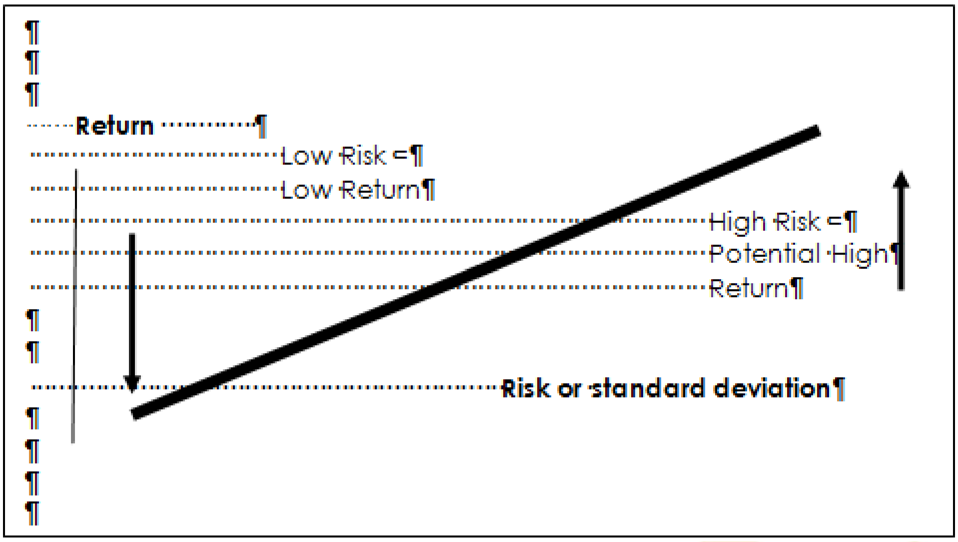
- Work responsibilities for a selected position analysed and listed as outputs.
- The measurable quality requirements for each work responsibility/output in terms of legislation and/or industry standards.
- The implications of not performing to required standards with reference to the organisation and the individual.
- The implications of exceeding quality requirements with reference to the organisation and the individual.

1.1 Risk or return?

The objective of an investor is to obtain the largest possible rate of return without placing invested funds at more risk than the investor can bear. The investor’s reluctance to assume risk limits his or her ability to maximize returns. Remember: The aim is to maximize return and minimize risk. However, the higher the return, the greater the risk. Investors must therefore find and optimal balance, or trade-off, between high returns and low risk.
We can also call the risk or return trade-off ‘the ability-to-sleep-at-night test’. While some people can handle the financial equivalent of cliff climbing without batting an eye, others are terrified of climbing the financial ladder without a secure harness.

Risk implies that you may lose some or even all of your original investment. Investors should decide how much risk they can take on to remain comfortable with their investments. Low levels of uncertainty (low risk) are associated with low potential returns. High levels of uncertainty (high risk) are associated with high potential returns. The risk or return trade-off is the balance between the desire for the lowest possible risk and the highest possible return. This principle is demonstrated graphically in Figure 1.

In an investment context, risk increases with the chance that the actual return on an investment will be different from the expected. Standard deviation is a measure of this difference.



High–return investments require that you risk your principal, that is, you could lose all the money that you invest. Most people are averse to risk. We call this risk aversion. For instance, when you buy a publicly traded stock, you can lose your entire investment. If you are risk averse, you will avoid such a high level of risk. However, you will have to sacrifice some returns. If you don't invest in the stock market during certain periods, you may sacrifice huge profits. (This is also called profit aversion.) Can you see that being totally risk averse is not a good investment strategy? At the other end of the scale, being totally risk tolerant is a very high-risk strategy.

A common approach to evaluating the risk associated with an asset involves estimating:

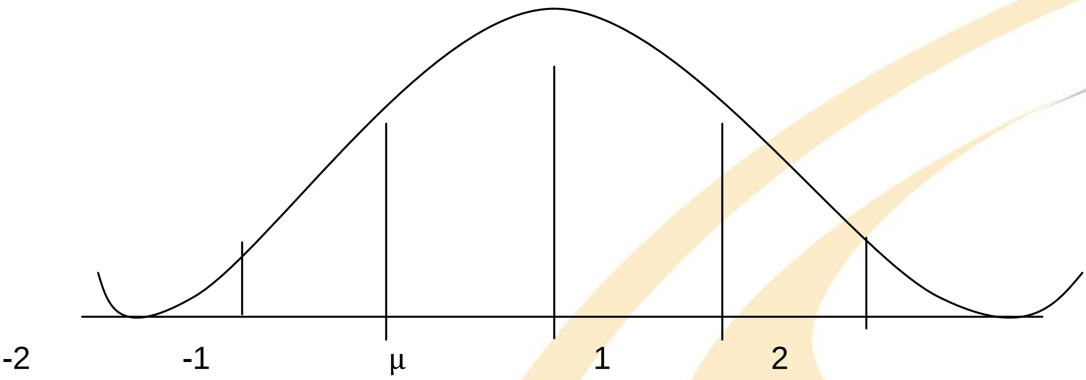
- the pessimistic (worst);
- the most likely (expected); and
- the optimistic (best) return, associated with a given asset.

If you take a group of investments and plot the estimated risk against the return, return usually increases with risk. Take another look at Figure 1.
An investor might tell you that he or she expects the investment to yield a rate of return of 10%. However, this is the investor's most likely estimate. Pressed further the investor would probably acknowledge that the estimated rate of return is uncertain. He or she would probably also admit that it is possible that the annual rate of return on this investment might go as low as – 10% or as high as 25% under certain conditions. The admission that there might be a large range of possible returns on an investment reflects the investor's uncertainty regarding the actual rate of return. A larger range of expected returns makes an investment riskier. You can

determine how likely the expected rate of return on an investment is by analysing estimates of expected returns. To do this, you assign probability values to all possible returns.

We often estimate risk in business decisions by using a distribution of outcomes such as a normal distribution. The aim of estimating risk is to minimize (or at least take account of) risk as measured by the standard deviation from the mean (average) outcome within the normal distribution. What is a normal distribution? Normal distributions are a very important class of statistical distributions. All normal distributions are symmetric and have bell-shaped density curves with a single peak. Figure 2 will help you to understand this concept. The bell-shaped curve represents a normal distribution with a mean u and standard deviations from the mean marked -1, +1 and so on.

What does the standard deviation tell us? If a share price has a mean of 15 and a standard deviation of 5 it means that most historical prices occurred between 10 and 20 (the mean plus or minuses the standard deviation)



We can divide financial instruments into the following broad categories:

- Fixed-income investments, including bonds and preferred stocks;
- equity investments; and
- special equity instruments such as warrants and options.

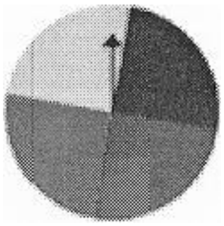
A broad range of factors influences the price of securities issued by for example, companies (stocks), and government agencies or municipalities (bonds). These factors include the following:

- Financial fundamentals - fluctuations in profits, earnings and cash flow affect security prices;
- Market psychology - perceptions often influence the markets as much as reality. Optimism leads prices higher, while uncertainty and negativism can cause a decline in a sector or the entire market;
- Economic factors - economic indicators (for example, gross domestic product, employment, inflation), housing statistics, oil prices and industry-specific factors all affect investors;
- Major events - acquisitions, product innovations, corporate scandals, natural disasters and political changes can have a major influence on a company, industry or entire market.

On average, bonds tend to be less volatile than stocks but bonds may also experience price variations from year to year. Factors that affect bond and equity prices include changing interest rates, shifting supply and demand dynamics and the level of perceived risk in the stock market. You can ask yourself the following question to help you determine the level of risk associated with a financial instrument - which factors will reduce earnings and the subsequent pay-off potential of the issuing company, forcing them to default on the payment obligations?

The concept of probability
We'll explain the concept of probability using historical examples.
Probability: We can define probability as a measure of the likelihood that an event in the future will actually happen. Let's look at an experiment. A spinning wheel has four equal sectors, yellow, blue, green and red. What are the chances that the wheel will stop on blue after being spun? What are the chances of the wheel stopping on red?

Yellow Blue



Green Red

- The chances of stopping on blue are 1 in 4, or one fourth;
- The chances of stopping on red are 1 in 4, or one fourth;
- The chances of stopping on yellow are 1 in 4, or one fourth;
- The chances of stopping on green are 1 in 4, or one fourth.

In the experiment, the probability of each outcome is always the same, that is, the outcomes are all equally likely to occur. The outcomes in life are not always equally likely to occur.

1.2 Risk Exposure

A problem when you have a number of possible risks is that it can be difficult to decide which risks are worth putting effort into addressing. Risk Exposure is a simple calculation that gives a numeric value to a risk, enabling different risks to be compared.
Risk Exposure of any given risk = Probability of risk occurring x total loss if risk occurs
A limitation of this calculation is that it will give the same scores to high-probability/low loss risks and low-probability/high loss risks. If you are concerned with these differences, a Risk Matrix may be a better way of evaluating risks.

Risk analysis consists out of a few steps. They are as follows:

Risk Identification
Risk identification sets out to identify an organisation's exposure to uncertainty. This requires an intimate knowledge of the organisation, the market in which it operates, the legal, social, political and cultural environment in which it exists, as well as the development of a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

- Strategic - These concern the long-term strategic objectives of the organisation. They can be affected by such areas as capital availability, sovereign and political risks, legal and regulatory changes, reputation and changes in the physical environment.
- Operational - These concern the day-to-day issues that the organisation is confronted with as it strives to deliver its strategic objectives.
- Financial - These concern the effective management and control of the finances of the organisation and the effects of external factors such as availability of credit, foreign exchange rates, interest rate movement and other market exposures.
- Knowledge management - These concern the effective management and control of the knowledge resources, the production, protection and communication thereof. External factors might include the unauthorised use or abuse of intellectual property, area power failures, and competitive technology. Internal factors might be system malfunction or loss of key staff.
- Compliance - These concern such issues as health & safety, environmental, trade descriptions, consumer protection, data protection, employment practices and regulatory issues.

Risk Description
The objective of risk description is to display the identified risks in a structured format, for example, by using a table. The risk description table overleaf can be used to facilitate the description and assessment of risks. The use of a well-designed structure is necessary to ensure a comprehensive risk identification, description and assessment process. By considering the consequence and probability of each of the risks set out in the table, it should be possible to prioritise the key risks that need to be analysed in more detail.

High	Financial impact on the organisation is likely to exceed Rx Significant impact on the organisation's strategy or operational activities Significant stakeholder concern
Medium	Financial impact on the organisation likely to be between Rx and Ry Moderate impact on the organisation's strategy or operational activities Moderate stakeholder concern
Low	Financial impact on the organisation likely to be less that Ry Low impact on the organisation's strategy or operational activities Low stakeholder concern

Risk Evaluation
When the risk analysis process has been completed, it is necessary to compare the estimated risks against risk criteria which the organisation has established. The risk criteria may include associated costs and benefits, legal requirements, socio-economic and environmental factors, concerns of stakeholders, etc. Risk evaluation therefore, is used to make decisions about the significance of risks to the organisation and whether each specific risk should be accepted or treated.

Risk Treatment
Risk treatment is the process of selecting and implementing measures to modify the risk. Risk treatment includes as its major element, risk control/mitigation, but extends further to, for example, risk avoidance, risk transfer, risk financing, etc.

NOTE: In this standard, risk financing refers to the mechanisms (e.g. insurance programmes) for funding the financial consequences of risk.

Risk financing is not generally considered to be the provision of funds to meet the cost of implementing risk treatment. Effectiveness of internal control is the degree to which the risk will either be eliminated or reduced by the proposed control measures.

One method of obtaining financial protection against the impact of risks is through risk financing which includes insurance. However, it should be recognised that some losses or elements of a loss will be uninsurable e.g. the uninsured costs associated with work-related health, safety or environmental incidents, which may include damage to employee morale and the organisation's reputation. The risks that need to be addressed in the individuals life is dependent on the life stage the individual is in.

As a newly employed single person just starting a career, the basic risks are as follows:

- Risk of not being able to pay debt;
- Risk of becoming sick;
- Risk of being unable to earn an income.

In the next life stage, living together, the individual is now earning more income but also has more financial responsibilities.
Risks are as follows:

- Risk of not being able to pay debt;
- Risk of becoming sick;
- Risk of being unable to earn an income;
- Risk of dying and your partner losing your income.

The Family life stage.
Risks are as follows:

- Risk of not being able to pay debt;
- Risk of becoming sick;
- Risk of being unable to earn an income;
- Risk of dying and your partner losing your income;
- Risk of not being able to pay for education.

Mature Stage
- Risk of becoming sick;
- Risk of being unable to earn an income;
- Risk of living too long and not having enough money.

1.3 Risk management

What is a risk? Definition: An undesirable future event. It is also uncertain whether it will occur, which actually includes all future events. There are several types of risks you can consider, including:
- Things that are likely to happen;
- Things that will have a big impact, should they happen;
- Things outside of your control. So you just have to manage your way around them;
- Things you know very little about, including not knowing how likely they are to occur (in this case, you can only use the potential impact of the risk as a guide to whether prior action is of value).

Risk management includes:
- Risk identification: Identifying potential risks and prioritizing them for action. This means sorting out the risks that are worthy of up-front action on reduction, contingencies and/or monitoring from those that you will 'manage on the fly' (i.e. you won't bother with them until they hit you in the face).

For example using Risk Exposure or a Risk Matrix
- Risk reduction: Acting to reduce the probability of targeted risks occurring and/or the impact, should they happen. (If you're lucky, you'll be able to eliminate the risk altogether or possibly reduce it to a 'manage on the fly' risk.
- Contingency planning: Where you cannot reduce risks to 'manage on the fly' status, you may want to prepare people, equipment, actions and processes to 'put on the shelf' in case the risk occurs.
- Risk monitoring: Setting up measurement and other monitoring to spot risks coming so you have time to respond proactively. Note that setting up process measures through risk management is a very good way of ensuring that the things you are measuring are the right things and will lead to actions.

The opposite of risks are opportunities, and many risk management techniques can also be used for opportunity management. Risk Management is increasingly recognised as being concerned with both positive and negative aspects of risk. It should address methodically all the risks surrounding the organisation's activities past, present and in particular, future.

Potential risk treatments

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:
- Avoidance (aka elimination);
- Reduction (aka mitigation);
- Retention;
- Transfer (aka buying insurance).

Ideal use of these strategies may not be possible. Some of them may involve trade-offs that are not acceptable to the organization or person making the risk management decisions. Another source, from the US Department of Defence, Defence Acquisition University, calls these ACAT, for Avoid, Control, Accept, or Transfer. The ACAT acronym is reminiscent of the term ACAT (for Acquisition Category) used in US Defence industry procurements.

Risk avoidance
Includes not performing an activity that could carry risk. An example would be not buying a property or business in order to not take on the liability that comes with it. Another would be not flying in order to not take the risk that the airplane was to be hijacked. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning profits.

Risk reduction
Involves methods that reduce the severity of the loss or the likelihood of the loss from occurring. Examples include sprinklers designed to put out a fire to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable. Halon fire suppression systems may mitigate that risk, but the cost may be prohibitive as a strategy. Modern software development methodologies reduce risk by developing and delivering software incrementally. Early methodologies suffered from the fact that they only delivered software in the final phase of development; any problems encountered in earlier phases meant costly rework and often jeopardized the whole project. By developing in iterations, software projects can limit effort wasted to a single iteration. Outsourcing could be an example of risk reduction if the outsourcer can demonstrate higher capability at managing or reducing risks. In this case companies outsource only some of their departmental needs. For example, a company may outsource only its software development, the manufacturing of hard goods, or customer support needs to another company, while handling the business management itself. This way, the company can concentrate more on business development without having to worry as much about the manufacturing process, managing the development team, or finding a physical location for a call centre.

Risk retention
Involves accepting the loss when it occurs. True self-insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured are retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

Risk transfer
Means causing another party to accept the risk, typically by contract or by hedging. Insurance is one type of risk transfer that uses contracts. Other times it may involve contract language that transfers a risk to another party without the payment of an insurance premium. Liability among construction or other contractors is very often transferred this way.

On the other hand, taking offsetting positions in derivatives is typically how firms use hedging to financially manage risk. Some ways of managing risk fall into multiple categories. Risk retention pools are technically retaining the risk for the group, but spreading it over the whole group involves transfer among individual members of the group.

This is different from traditional insurance, in that no premium is exchanged between members of the group up front, but instead losses are assessed to all members of the group.

Create a risk management plan
Follow all of the planned methods for mitigating the effect of the risks. Purchase insurance policies for the risks that have been decided to be transferred to an insurer, avoid all risks that can be avoided without sacrificing the entity's goals, reduce others, and retain the rest. Risk Quantification imparts a sound understanding of the tools available for assessing exposure to risk: quantifying both the probability of the event, frequency of the event or the likeliness of it occurring.

1.4 The Role of the Insurance Broker

The broker has a broad advisory role in helping the organization to determine its insurance requirements as well as placing the insurance on their behalf.
This evolution has been evidenced even more so in many regions of the world, most notably continental Europe, where risk managers have little or no reliance on their brokers, preferring to place their coverage directly with insurers.

1.4.1 Advisory
The insurance broker can provide the internal risk manager with information that assists the risk manager in determining the risk transfer strategy for their organization. This information can include exposure and claims analysis, best practices within its own industry and business in general and information on insurance markets.

1.4.2 Transactional
In order to efficiently access the worldwide insurance markets, many commercial insurance buyers utilize the services of insurance brokers. The extent and modalities of such use is extremely variable by country, industry, individual organization, and even by line of coverage. In many jurisdictions, such as North America the use of intermediaries is still prevalent; however in other countries, such as continental Europe, the traditional brokerage intermediation is less and less common. Insurance brokers also might be asked to provide expertise in the "marketing" of the account. This should include the development of comprehensive,

effective underwriting submissions, identifying potential insurance partners and designing and organizing presentations by clients.

1.4.3 Servicing and Administration:
Once the insurance policy is placed, regardless of the extent of involvement of the broker in such placement, a significant amount of servicing and administration work remains to be done, and continues from the inception of the policy throughout its expiration. This can include checking of policy wordings, premium payments administration, issuing of certificates, routine claims administration, among other activities. Through economies of scale achieved in supplying similar services to numerous clients, the broker can often provide such services more efficiently than the internal risk management department. These services should be clearly listed in a comprehensive servicing agreement.

Many insurance brokers describe their role as purchasing the most coverage possible at the lowest price. This is not necessarily true. The role of the broker is to execute the insurance management strategy that is determined by its client, to the extent indicated by its client. For most organizations, that strategy will include the development of strong, long-term relationships with its insurance transfer partners. It is important that the risk manager build personal and corporate relationships with the underwriters on his or her account. While the broker might provide additional specific services, no individual can present the risk of an organization better than an internal professional. It is up to the risk manager to determine the risk financing strategy and then to direct the efforts relating to the presentation of the risk and the negotiation of the terms of the insurance policies.

While the influence of large insurance brokers with insurance companies is an important asset, it should in no way change the nature of this relationship. As the insured's representative, the broker must provide professional services to its clients with transparency and integrity.

1.5 Risk Perception Factors

Dread
What’s worse, being eaten by a shark or dying of a heart disease? Both kill you, and heart problems are far more likely to do you in. But the dreadful death often evokes more concern. Despite the fact that heart disease kills roughly 25 percent more Americans each year, cancer evokes more fear in most people because cancer is perceived as a dreadful way to die. This helps explain why hazards that might cause cancer, such as radiation and industrial chemicals, evoke strong fears. Dread is a clear example of the more general way we think about risk in terms of our intuitive feelings, a process that has been labelled The Affect Heuristic.

Control
Do you feel pretty safe when you drive? Most people do. Having the wheel in your hand gives you the feeling that you can control what happens. But switch to the passenger seat and you’re a little more nervous because you are no longer in control. This also applies to process. If you feel as though you have some control of the process of determining a risk you will face, the risk probably won’t seem as big as if it was decided by a process over which you felt you had no control.

Is the risk natural or is it human-made?
Anthropogenic sources of radiation like nuclear power, mobile phones, or electrical and magnetic fields frequently evoke greater concern than radiation from the sun, which is a vastly greater risk (1.3 million skin cancer cases, 7,800 melanoma deaths per year in the U.S.) but less worrisome to many because it is natural. This factor helps explain widespread concern about many technologies and products, and offers important insights into one key factor in the debate over the Precautionary Principle.

Choice
A risk we choose seems less risky than if that risk is imposed on us. If you use a mobile phone while driving, you may have on occasion noticed a driver next to you, using his or her mobile, and felt upset about the risk that the other driver was imposing on you, even while you voluntarily took the same risk, albeit with less concern. (Of workshop, you have control over your car, so that factor of control also contributes in this example.)

Children
In addition to the genetic imperative to survive (which is, after all, the underlying impetus of our risk perceptions and responses) humans are genetically driven to reproduce. Survival of the species depends on survival of our progeny. So it is not surprising that research has found that a risk to children, like asbestos in a school or the abduction of a youngster, seems worse than the same risk to adults, such as asbestos in a workplace or the abduction of an adult. During last year's sniper attacks in Washington D.C., after five adults had been murdered, the sniper wounded a 13 year-old boy. The local police chief, tears in his eyes, declared of the sniper "He's really getting personal now!"

Is the risk new?
At the time bovine spongiform encephalopathy first showed up in Germany, an opinion survey found that about 85% of the public thought mad cow disease was a serious threat to public health. But the same poll done at the same time in the U.K., where it had been around for years and killed many for animals and more than 100 humans, found that only around 40% of the public thought mad cow disease was a serious threat. New risks, including everything from SARS and West Nile virus to new technologies or products tend to be more frightening that the same risk after we've lived with it for a while and our experience has helped us to put the risk in perspective.

Awareness
The more aware of a risk we are, the more available it is to our consciousness, and the more concerned about it we are likely to be. SARS is currently evoking far more new coverage, attention and concern than influenza, which kills an estimated 36,000 people a year. In the Washington D.C. area last fall, fear of being shot by a sniper was much higher than the greater risks of heart disease cancer or stroke. The other risks weren't gone, but conscious concern about them was lower, because awareness of them had been reduced.

Can it happen to me?

Any risk seems larger if you think you or someone you care about could be a victim. Consider terrorism in the United States. Prior to September 11, 2001, the American's were the victims of terrorism were "someone else". Yes, they were American's. But they were in foreign embassies, or on foreign military assignment. After 9/11/01, however, Americans at home felt they too were possible targets, and fear of terrorism grew.

This helps explain why statistically probability is often irrelevant to people and ineffective form of risk communication. Imagine what someone hands out 1 million bottles of water, one of which contains a poison. You get one of those bottles. Now imagine taking a drink from that bottle. Your risk of dying is only one in a million, but it still feels risky to drink it, because you could be that one. This helps explain why the acceptable level of risk to many people is zero.

1.6 The Risk-Benefit trade-off

Some risk perception researchers and many risk analysts believe that the risk-benefit trade-offs the major factor that makes us more or less afraid of a given threat. If we perceive a benefit from a behaviour or choice, the risk associated with it seems smaller. If there is no perceived benefit, the risk seems larger. When measles and polio were prevalent, the benefits of vaccination were perceived to outweigh the risk of the side effects. But no, with these diseases rare, the perception of some parents is that the risks of those side effects, as low as they are, outweigh the benefits of vaccines. Many American health care workers, "first providers", are refusing a smallpox vaccination because of the risk of the treatment, low though it may be, seems larger than the benefit, which is protection from a disease they aren't convinced is a threat at all.

1.7 Trust

Research has found that the less we trust the people who are supposed to protect us, or the people or government or corporate institutions exposing us to the risk in the first place, or the people communicating to us about the risk, the more afraid we'll be. The more we trust, the less concern we'll feel. Imagine you're in a desert, nearly dead of thirst, and someone appears to you and offers you two glasses of clear liquid. She won't tell you what is in either glass, only that one comes from Pope John Paul and the other comes from a tobacco company. Which one would you take?

1.8 The Implications

But what of all this? What is the utility of understanding the underpinnings of our fears? We suggest that by realizing and respecting the realities of affect and other heuristic processes, and but accepting that they are apparently deeply rooted and reflect intrinsic human techniques for survival, policy makers can incorporate these values, as well as fact-based analysis, into their risk management decision making. Further, by understanding the reasons people perceive risk as they do, policy makers can communicate with various audiences about these issues in terms of language relevant to people's concerns.

Risk communication which acknowledges and respects the affective motivators which underlie people's concerns, rather than dismissing such perceptions as 'irrational' because they are not solely fact-based, is likely to be more successful in helping people make more informed choices about the risks they face. This is directly a matter of public health. People, who are either too afraid of relatively low risks, or not afraid enough of relatively big ones, make dangerous choices. People afraid of flying choose instead to drive, a much riskier behaviour. People afraid of terrorism or other crimes take the risk of acquiring firearms. In 2001 people afraid of anthrax took antibiotics prophylactically increasing the proliferation of drug-resistant bacteria. Further, chronic stress, by altering blood levels of adrenaline and cortisol, impairs the immune system. Worrying too much about getting sick may actually increase the likelihood that you will get sick, or sicker, or stay sick longer, or die, from any infectious disease. Chronic stress is also associated with the likelihood of type-II diabetes, accelerated osteoporosis, and cause decrements in learning and long term memory. Fear is, in itself, a risk.

Not enough fear can also be dangerous. People unafraid of natural risks like solar radiation, or risks that they think they can control like driving, or risks that are associated with benefits, such as smoking or alcohol consumption or fat and calorie-rich diets, fail to take adequate precautions, and they too face a greater likelihood of premature death. Lack of appropriate caution can be dangerous too.

As a societal level, elevated concern about relatively low risks, and too little concern about relatively big ones, is also potentially harmful. People afraid of a risk that triggers their intuitive fears demand government protection from that risk, though it may not actually be as much of a threat as they feel. Conversely, if a threat is indeed high but does not trigger affective alarm, demand for protection will be low. This drives allocation of resources that is suboptimal form public health. Time and money spent protecting people from greater risks. As a result, some of the people left unprotected from those higher risks will suffer. Some will surely die.

1.9 Possible Solutions

One solution to the dangers that arise when the analytic and affective sides of our risk perception don't agree is effective risk communication, informed and empowered by an understanding of risk perception. This must become a priority at the highest levels of policy making in government, in business, and in international affairs. More must be done to help people keep their sense of risk in perspective. Decision-makers must realize, and accept, that the dangers of misperception of risk are reasonable, and pose both a threat to public health and an impediment to policy making that will provide the greater benefit to public health.

Effective risk communication requires recognition by policy makers that there are risk perception implications in what they do, that communication is not just what they say and how they say it. Setting a threshold for acceptable exposure to a pollutant, allowing or disallowing a product or process, requiring or not requiring labelling – indeed all risk management decisions – have risk communication mean and impact. At the most senior level, government agencies must consider the risk perception and communication implications of their actions as policy choices are being made. Risk communication must be thought of as more than just press releases, news conferences, and public service campaigns. It is substance, not just spin.

Some call this pandering to irrationality and emotion, and suggest instead that a benevolent technocracy should be empowered to manage the societal risk in order to ensure intelligent, rational and effective policies. But this fails to recognize the sensitive and pivotal issues of trust and control. Even the most benevolent process, if removed from the input of citizen values, will feel like one overt which the public has too little control and will not likely be trusted. The policies of such a process are more likely to provoke resistance than support. Further, the very idea of such a rationality-based technocracy fails to accept that risk perception is at least as much an effective and intuitive process as it is analytical, and that fear itself, either too much or not enough is a significant risk that also must be factored into decisions about the public and environmental protection.

Risk communication, informed by the insights of risk perceptions, is a powerful yet neglected tool in helping people make more informed and ultimately healthier choices for themselves. More informed individual decision making will in turn free the leaders of social institutions to make reasoned risk management choices that will maximize the public and environmental health with the most efficient use of limited resources.

1.10 Short term insurance as a means of reducing financial risk in own life

First, let’s understand the concept of short term insurance:
Short term insurance describes a number of different categories of cover, such as commercial insurance (on commercial or industrial properties, for instance) personal insurance (on private property or assets, or corporate insurance (in respect of multinational assets or interests). For the purposes of this programme we will focus on personal insurance. Personal indemnity insurance or short term insurance as it is more commonly known is insurance which covers: the actual loss that the policy holder has suffered. It is insurance for uncertain events, the timing of which is uncertain

The nature of the subject matter of insurance is facts, which the insured knows. Insurers generally are not aware of facts unless the insured tells them. While the insured may examine a copy of the policy before accepting the insurer’s terms, the insurer cannot examine all aspects of the insurance offer which may be material to his decision on terms and conditions. The questions set out in a proposal form do not only define the limits of what is material information. The duty of full disclosure of all relevant or material facts rests with both parties. Facts which are material, and must be disclosed, include:

- Those which would indicate that the risk is greater than would be expected from its class;
- Those which may tend to make the amount of any loss greater than normal;
- Previous loss and claims history;
- Penalty terms or restricted cover applied by previous insurers;
- The fact that the insured had absolved a third party form normal legal liabilities, which would affect subrogation rights;

- Facts which are not material and do not need to be disclosed include:
- Facts which are known under any law;
- Facts which reduce the risk or hazard;
- Facts which are advised but which the insurer does not further investigate;
- Facts which all insurers should know from his normal business operations;
- Facts, which a survey would reveal.

Short term policies operate on the indemnity principle, meaning the insured is only paid for the actual losses suffered.

Therefore you would want to be insured for as close to possible, the exact amount of the items being insured. The insured can never be paid for a claim for more than the actual value of an item. Since you pay for the value and nature of risk of the insured event or item, and cannot claim for more than the actual losses you have incurred, there is no benefit to over insuring and events or items. Similarly, there can be no benefit to the insured to insure for a value that is less than the actual value. If it is going to cost you R100 000 to replace the items in your home that are lost due to theft or acts of God (e.g. flooding), and you have only insured the contents for R80 000, you will experience a shortfall of R20 000 in replacing the goods if a claim arises. Furthermore, if an assessor finds that tat you have been paying a premium for insurance that is disproportionate to the risk, you can be penalised in your claim by the amount of the underinsurance. (E.g. you originally insured your household contents for R75 000. Over the years you have acquired new assets and have not advised your insurance company that the value of your household contents have increased. You experience a theft, where you lose goods that would cost R30 000 to be replaced. An assessor is sent from the insurance company and finds that the value of your household contents is actually R90 000. You were under insured by R15 000. The insurance company can reduce / penalise your claim by the R15 00 and only pay out R15 000.

As has been established above, it is pointless to be over insured, because the insurer will only pay you for the actual losses incurred. Under insurance creates a deficit to the amount you need to replace the lost items and can result in penalties from your insurer when there is a claim. This means that you need to review and change your insurance cover periodically. We will discuss short term insurance in detail in the next module.

1.11 Risk management and you

Compliance is one aspect of risk management. It is defined as the process of minimizing regulatory risk (the risk of not adhering to legislative requirements) and, as a result, its impact on reputational risk (the risk of damage to the company's reputation in the market place and the loss of business as a result). Organizations have an obligation to their employees, customers and the government to undertake to manage regulatory risk in order to minimize exposure that could negatively impact the reputation of the organization.

This includes ensuring that every aspect of the business:

- conforms to industry standards;
- complies with legislative requirements;

- has the correct policies and procedures in place to guide employees in terms of carrying out their responsibilities;
- as well as, to protect the rights of customers, employers and employees.

It is impossible to ensure that there is a policy and procedure in place to ensure that everything runs smoothly and that no mistakes are made that could negatively affect the business in one way or another.

1.12 The analysis of work responsibilities and risk management

One way of documenting your responsibilities is to list them as outputs. An output describes the end result rather than specific activities or tasks. For example if one of your responsibilities is to 'administer contracts', some the outputs may be written down as:

- Answered telephone queries;
- Updated biographical details e.g. address, contact details, etc.;
- Maintained benefits, contribution payments, credit control process, etc.

Listing responsibilities as outputs is useful because there are many ways to produce an output even though the standards that need to be maintained are the same. By listing outputs you encourage a process of continuous improvement because you create a certain amount of freedom, to whoever is producing the outputs, to experiment with different ways of doing the work in an attempt to improve the way the outputs are produced.

1.13 Quality Requirements

"Quality is meeting or exceeding expectations".

Quality requirements provide guidelines in terms of standards that need to be met to make sure that the outputs are produced according to requirements. This would include the fact that customers expect businesses to observe and obey regulatory items that affect the business e.g. legislative and/or industry standards and also include the fact that businesses expect their employees to comply with company policies and procedures. For example, if the output is 'answered telephone queries' then some of the quality requirements may be 'phone answered within 3 rings, client is provided with information according to XYZ policy guidelines, procedure XYZ is followed, information is extracted off XYZ system, written responses are dispatched within 24 hours, etc.'

It is particularly important to pay attention to legislation and/or industry standards. Customers expect all businesses to do their homework in terms of ensuring that they are buying a product or paying for a service that complies with the above mentioned standards. Whilst customers are able to comment on the service provided or the end product produced according to their expectations, they are not always familiar with the standards that govern the running of a business and the products / services provided. This means that when developing quality requirements, businesses should ask input from customers in terms of service provided and / or product design but the responsibility to ensure that legislation and/or industry standards are observed lies with the company. Policies and Procedures are developed, amongst other things, as a result of interpreting industry standards and/or legislation and form part of the risk management process in that they provide guidelines to ensure that the company adheres to Industry standards and legislative requirements.

1.14 The Cost of Quality

When outputs are produced according to quality requirements, the employee, company and customers benefit. The business stays profitable and attracts more customers.
When outputs are not produced according to quality requirements a lot of time is wasted fixing up errors, re-doing work which ultimately costs money and could even result in the business having to close down, customers being dissatisfied, employees being dismissed for poor ratings, etc. There is always a price to pay for not doing the job correctly.

In order to manage quality we need to measure it. The measure is called 'Cost of Quality'.

"Cost of Quality is the total of all the costs incurred in meeting or failing to meet customer expectations the first time"

Cost of quality is obtained by adding together two important costs i.e. the Cost of Compliance (meeting quality requirements) and the Cost of Non-Compliance (cost of not meeting quality requirements). Cost of compliance is the cost of meeting customer expectations the first time. This is also referred to as Quality Management Costs, or 'the cost of doing things right the first time'. Cost of non-compliance is the cost of not meeting customer expectations the first time. This is also referred to as Quality failure costs, or 'the cost of doing things wrong the first time'. If we add together all the quality management costs and the quality failure costs we get the cost of quality.

1.15 Cost of Compliance

Quality management costs can be divided into two categories: Prevention Costs and Appraisal Costs. Prevention costs are sometimes referred to as 'Quality Creation' costs. Appraisal costs are also known as 'Inspection', 'Evaluation', or even 'detection' costs. No matter what we call them, they all have to do with managing quality and meeting customer expectations the first time.

Prevention costs are the costs of trying to ensure that things are done right the first time. Examples of activities that are involved in prevention costs include the following:

- Planning for Quality;
- Setting quality standards;
- Reporting on quality;
- Quality training and education;
- Quality improvement projects;
- Developing a work profile with quality requirements;

- Making sure staff have the tools to do their work;
- Making sure that there are policies and procedures in place.

Appraisal costs are the costs of checking to see if things were done right the first time. They include all the initial costs of checking whether or not a product or service meets the customer's expectations. Examples of appraisal costs include the following:

- Testing products;
- Proof reading letters;
- Inspecting materials;
- Analysis of test results;
- Monitoring of suppliers;
- Audits to ensure that policies and procedures are being adhered to;
- Performance reviews with employees to ensure that quality requirements are being adhered to and making plans to provide coaching where necessary;
- Gathering feedback from customers in the form of surveys, etc.

The cost of compliance is the total of all the quality management costs.

1.16 The implications of not performing

Quality failure costs are the costs of failing to meet customer expectations the first time. They are the costs of doing things wrong the first time, which results in correction costs – the costs of having to do things over in order to meet and exceed customer expectations.

Examples of failure costs include:

- Downtime;
- Rejects;
- Repairs;
- Rework;
- Complaints;
- Returns;
- Disruption;
- Fines imposed by not adhering to regulations;
- For employees, it could mean no annual increase.

In service industries, rework could include things like resubmitting a computer run because of input errors or correcting errors on invoices in accounts payable.
By expressing poor quality in money terms the cost of non-compliance serves three purposes:

- It highlights the need for quality improvement;
- It produces an objective measure of quality improvement efforts;
- It helps to pinpoint areas where improvement will be most profitable;

Most of the costs of non-compliance are hidden costs and difficult to measure, e.g.:

- Loss of goodwill;
- Loss of market share;
- Loss of capacity;

- Loss of failure sales;
- Loss of potential customers.

The table below outlines different scenarios with regards to non-compliance, to give an indication to what possible affects it could have for the individual as well as for the company.

Scenario	**Implications for Judy**	**Implications for the company**
The company rules say that all press queries must be referred to the Public Relations Department or the Legal Department. Judy works in a call centre and receives a call from a reporter to ask why Company X did not pay a claim for Mrs. Rondo. She decides to answer the query as the reporter says it is off the record, and after all Judy dealt with the query.	Disciplinary action for ignoring company regulations which could lead to dismissal. Could be misquoted by the press as she has no skills in Public Relations and does not understand the big picture and legal ramifications	Possible negative publicity as the reporter is unlikely to keep the information off the record. Also Judy is not skilled to answer the question correctly.

1.17 Prevention versus Cure

By investing appropriately in prevention efforts, the cost of non-compliance can be drastically reduced with a consequent reduction in the cost of quality. A small increase in prevention costs leads to a large decrease in failure costs. By working smarter and making better use of the time available to eliminate errors it is possible to reduce the cost of non-compliance and the overall cost of quality. Reducing costs by focusing on prevention (ensuring that things are done right the first time) adds directly to the 'bottom-line' of the business without having to sell anything to a single extra customer. Hence prevention is the name of the game in quality-conscious companies.

1.18 The implications of exceeding quality requirements

The table below gives two examples of exceeding quality requirements with regards to the organization and the individual.

Incident	**Implication to Judy**	**Implication to the company**
A client asks Judy for a refund that is owing to her.	Upside Risk: The client is impressed with Judy's service and advises her supervisor – Judy is recognized for her customer service. Judy feels good	Upside Risk: The client tells other people about the service & this leads to increased business.

Incident	Implication to Judy	Implication to the company
The client needs the refund by close of business today. To assist the client Judy decides to drop the cheque off at the client's home on the way home from work as she sees it is on route.	because the client is very thankful and desperately needed the money. Downside Risk: Judy does not know the client and could put herself at risk by going to a stranger's house. If anything happened to Judy on the way to the client and at the client, after working hours, the company may not compensate her because it is not part of her job to personally drop off cheques at clients houses.	Downside Risk: If anything happened to Judy – the company may be liable to compensate because Judy was acting in the best interest of the client
Judy is able to answer 10 calls a day more than her colleagues due to her efficiency and because she knows her products well	Upside risk: Judy could get better performance reviews than her peers, resulting in increased responsibilities and possible benefits, pay and perhaps promotion (if this is available for the company) Downside risk: Judy's supervisor may begin giving Judy more work because she knows Judy will do it better than other staff that don't perform so well – Judy may become overloaded. This is known as performance punishment i.e. good performers get more work and the poor performers don't. A supervisor can manage the situation by exploring reasons for non-performance and taking steps to correct the gaps.	Upside risk: Increased productivity – good reputation for efficient service Downside risk: Judy may feel that she is being taken advantage of and may leave the company or become demotivated – this will affect her productivity

Module 2

Work Procedures in the Workplace and the risk of Non-Compliance

This Module deals with:

- Procedures required in predictable situations with reference to a particular organisation or scenario.
- Information sources in unusual or unpredictable circumstances.
- The risk associated with non-compliance with organisation procedures.
- Reasons why it is important to authenticate sources of information.
- The risk to the organisation associated with acting on or repeating unverified or unsubstantiated information as to whom to trust as a source.

In the previous exercise you documented the implications of not performing to quality standards. By doing this, you documented items that could pose a negative risk to the organisation. Non-compliance always poses a risk of some sort or another to an individual and/or the company but the extent of risk varies. In some cases the risk is minimal and will have a minimum impact on either an individual and/or company and in some cases the risk is a large one and could have a huge impact on the organisation to the extent that it could result in a close down of the business. Part of the risk management process involves identifying risk items and assessing the extent of risk so that risk items can be prioritised and appropriate plans put in place to manage the risk so that it is minimised.

2.1 Assess Risk associated with Non-compliance

Once the risk has been identified, you need to assess each item in order to determine the extent of the risk in terms of its potential impact on the individual and/or the company. This is done by analysing each item identified according to whether it is a high, medium or low risk to the business according to set criteria, i.e. a list of what low, medium or high risk will mean. For example if non-compliance to a procedure will place the life or lives of employees at risk, then it will be prioritised as a high risk. If non-compliance to a procedure will result in wasted time of 15 minutes then you would probably rate it as a low risk.

2.2 Legislation available to support work procedures

Occupational Health and Safety Act, 1993

2.2.1**. Section 8 (1) General duties of employers to their employees**

- Every employer shall provide and maintain, as far as is reasonably practicable, a working environment that is safe and without risk to the health of his employees.
- Without derogating from the generality of an employer's duties under subsection (1), the matters to which those duties refer include in particular --

a) The provision and maintenance of systems of work, plant and machinery that, as far as is reasonably practicable, are safe and without risks to health;

b) taking such steps as may be reasonably practicable to eliminate or mitigate any hazard or potential hazard to the safety or health of employees, before resorting to personal protective equipment;
c) making arrangements for ensuring, as far as is reasonably practicable, the safety and absence of risks to health in connection with the production, processing, use, handling, storage or transport of articles or substances;
d) establishing, as far as is reasonably practicable, what hazards to the health or safety of persons are attached to any work which is performed, any article or substance which is produced, processed, used, handled, stored or transported and any plant or machinery which is used in his business, and he shall, as far as is reasonably practicable, further establish what precautionary measures should be taken with respect to such work, article, substance, plant or machinery in order to protect the health and safety of persons, and he shall provide the necessary means to apply such precautionary measures;
e) Providing such information, instructions, training and supervision as may be necessary to ensure, as far as is reasonably practicable, the health and safety at work of his employees;
f) as far as is reasonably practicable, not permitting any employee to do any work or to produce, process, use, handle, store or transport any article or substance or to operate any plant or machinery, unless the precautionary measures contemplated in paragraphs (b) and (d), or any other precautionary measures which may be prescribed, have been taken;
g) Taking all necessary measures to ensure that the requirements of this Act are complied with by every person in his employment or on premises under his control where plant or machinery is used;
h) Enforcing such measures as may be necessary in the interest of health and safety;
i) ensuring that work is performed and that plant or machinery is used under the general supervision of a person trained to understand the hazards associated with it and who have the authority to ensure that precautionary measures taken by the employer are implemented; and
j) Causing all employees to be informed regarding the scope of their authority as contemplated in section 37(1) (b).

2.2.2 Section 13 Duty to inform

Without derogating from any specific duty imposed on an employer by this Act, every employer shall --

a) as far as is reasonably practicable, cause every employee to be made conversant with the hazards to his health and safety attached to any work which he has to perform, any article or substance which he has to produce, process, use, handle, store or transport and any plant or machinery which he is required or permitted to use, as well as with the precautionary measures which should be taken and observed with respect to those hazards;
b) inform the health & safety representatives concerned beforehand of inspections, investigations or formal inquiries of which he has been notified by an inspector, and of any application for exemption made by him in terms of section 40; and
c) Inform a health and safety representative as soon as reasonably practicable of the occurrence of an incident in the workplace or section of the workplace for which such representative has been designated.

2.2.3 Section 17 (1) Health and Safety Representatives

Subject to the provisions of subsection (2), every employer who has more than 20 employees in his employment at any workplace, shall, within four months after the commencement of this Act or after commencing business, or from such time as the number of employees exceeds 20, as the case may be, designate in writing for a specified period health & safety representatives for such workplace, or for different sections thereof.

a) An employer and the representative of his employees recognized by him or, where there are no such representatives, the employees shall consult in good faith regarding the arrangements and procedures for the nomination or election, period of office and subsequent designation of health and safety representatives in terms of subsection (1): Provided that if such consultation fails, the matter shall be referred for arbitration to a person mutually agreed upon, whose decision shall be final: Provided further that if the parties do not agree within 14 days on an arbitrator, the employer shall give notice to this effect in writing to the President of the Industrial Court, who shall in consultation with the chief inspector designate an arbitrator, whose decision shall be final.
b) Arbitration in terms of subsection (2) shall not be subject to the provisions of the Arbitration Act, 1965 (Act No. 42 of 1965), and a failure of the consultation contemplated in that subsection shall not be deemed to be a dispute in terms of the Labour Relations Act, 1956 (Act No. 28 of 1956): Provided that the Minister may prescribe the manner of arbitration and the remuneration of the arbitrator designated by the President of the Industrial Court.
c) Only those employees employed in a full-time capacity at a specific workplace and who are acquainted with conditions and activities at that workplace or section thereof, as the case may be, shall be eligible for designation as health and safety representatives for that workplace or section.
d) The number of health and safety representatives for a workplace or section thereof shall in the case of shops and offices be at least one health and safety representative for every 100 employees or part thereof, and in the case of all other workplaces at least one health and safety representative for every 50 employees or part thereof: Provided that those employees performing work at a workplace other than that where they ordinarily report for duty, shall be deemed to be working at the workplace where they so report for duty.
e) If an inspector is of the opinion that the number of health and safety representatives for any workplace or section thereof, including a workplace or section with 20 or fewer employees, is inadequate, he may by notice in writing direct the employer to designate such number of employees as the inspector may determine as health and safety representatives for that workplace or section thereof in accordance with the arrangements and procedures referred to in subsection (2).
f) All activities in connection with the designation, functions and training of health and safety representatives shall be performed during ordinary working hours, and any time reasonably spent by any employee in this regard shall for all purposes be deemed to be time spent by him in the carrying out of his duties as an employee.

2.2.4 Section 26 Victimization forbidden

a) No employer shall dismiss an employee, or reduce the rate of his remuneration, or alter the terms or conditions of his employment to terms or conditions less favourable to him, or alter his position relative to other employees employed by that employer to his disadvantage, by reason of the fact, or because he suspects or believes, whether or not the suspicion or belief is justified or correct, that that employee has given information to the Minister or to any other person charged with the administration of a provision of this Act which in terms of this Act he is required to give or which relates to the terms, conditions or circumstances of his employment or to those of any other employee of his employer, or has complied with a lawful prohibition, requirement, request or direction of an inspector, or has given evidence before a court of law or the industrial court, or has done anything which he may or is required to do in terms of this Act or has refused to do anything which he is prohibited from doing in terms of this Act.

b) No employer shall unfairly dismiss an employee, or reduce the rate of his remuneration, or alter the terms or conditions of his employment to terms or conditions less favourable to him, or alter his position relative to other employees employed by that employer to his disadvantage, by reason of the information that the employer has obtained regarding the results contemplated in section 12(2) or by reason of a report made to the employer in terms of section 25.

2.3 Occupational Health and Safety Act, 1993

Definitions

<u>Approved inspection authority</u>
An inspection authority approved by the chief inspector: Provided that an inspection authority approved by the chief inspector with respect to any particular service shall be an approved inspection authority with respect to that service only.
<u>Biological monitoring</u>
A planned programme of periodic collection and analysis of body fluid, tissues, excreta or exhaled air, in order to detect and quantify the exposure to or absorption of any substance or organism by persons.
<u>Building</u>
Any structure attached to the soil;
Any building or such structure or part thereof which is in the process of being erected; or Any prefabricated building or structure not attached to the soil.
<u>Chief executive officer</u>
In relation to a body corporate or an enterprise conducted by the State, means the person who is responsible for the overall management and control of the business of such body corporate or enterprise.
<u>Chief Inspector</u>
The officer designated under section 27 as chief inspector, and includes any officer acting as chief inspector.
<u>Council</u>
The Advisory Council for Occupational Health and Safety established by section 2.
<u>Danger</u>
Anything which may cause injury or damage to persons or property.
<u>Department</u>
The Department of Manpower.
<u>Employee</u>
Subject to the provisions of subsection (2), any person who is employed by or works for an employer and who receives or is entitled to receive any remuneration or who works under the direction or supervision of an employer or any other person.

<u>Employer</u>
Subject to the provisions of subsection (2), any person who employs or provides work for any person and remunerates that person or expressly or tacitly undertakes to remunerate him, but excludes a labour broker as defined in section 1(1) of the Labour Relations Act, 1956 (Act No. 28 of 1956).
<u>Employers' organization</u>
An employers' organization as defined in section 1 of the Labour Relations Act, 1956 (Act No.28 of 1956).
<u>Employment or employed</u>
Means employment or employed as an employee.
<u>Explosives</u>
Any substance or article as listed in Class I: Explosives in the South African Bureau of Standards Code of Practice for the Identification and Classification of Dangerous Substances and Goods, SABS 0228.
<u>Hazard</u>
A source of, or exposure to danger.
Health and Safety Committee
A committee established under section 19.
<u>Health and safety equipment</u>
Any article or part thereof which is manufactured provided or installed in the interest of the health or safety of any person.
<u>Health and safety representative</u>
A person designated in terms of section 17(1).
<u>Health and safety standard</u>
Any standard, irrespective of whether or not it has the force of law, which, if applied for the purposes of this Act, will in the opinion of the Minister promote the attainment of an object of this Act.
<u>Healthy</u>
Free from illness or injury attributable to occupational causes.
<u>Incident</u>
An incident as contemplated in section 24(1).
<u>Industrial court</u>
The industrial court referred to in section 17 of the Labour Relations Act, 1956 (Act No. 28 of 1956).
<u>Inspection authority</u>
Any person who with the aid of specialized knowledge or equipment or after such investigations, tests, sampling or analyses as he may consider necessary, and whether for reward or otherwise, renders a service by making special findings, purporting to be objective findings, as to -
The health of any person; the safety or risk to health of any work, article, substance, plant or machinery, or of any condition prevalent on or in any premises; or the question of whether any particular standard has been or is being complied with, with respect to any work, article, substance, plant or machinery, or with respect to work or a condition prevalent on or in any premises, or with respect to any other matter, and by issuing a certificate, stating such findings, to the person to whom the service is rendered.
<u>Inspector</u>
A person designated under section 28.
<u>Listed work</u>
Any work declared to be listed work under section 11.

Local authority
Any institution or body contemplated in section 84(1) (f) of the Provincial Government Act, 1961 (Act No. 32 of 1961);
Any regional services council established under section 3 of the Regional Services Councils Act, 1985 (Act No. 109 of 1985);
Any other institution or body or the holder of any office declared by the Minister by notice in the Gazette to be a local authority for the purposes of this Act.
Machinery
Any article or combination of articles assembled, arranged or connected and which is used or intended to be used for converting any form of energy to performing work, or which is used or intended to be used, whether incidental thereto or not, for developing, receiving, storing, containing, confining, transforming, transmitting, transferring or controlling any form of energy.
Major hazard installation
Mans an installation where any substance is produced, processed, used, handled or stored in such a form and quantity that it has the potential to cause a major incident;
Major incident
Means an occurrence of catastrophic proportions, resulting from the use of plant and machinery, or from activities at a workplace;
Mandatory
Includes an agent, a contractor or a subcontractor for work, but without derogating from his status in his own right as an employer or a user.
Medical surveillance
A planned programme of periodic examination (which may include clinical examinations, biological monitoring or medical tests) of employees by an occupational health practitioner or, in prescribed cases, by an occ. medicine practitioner.
Minister
The Minister of Manpower.
Occupational health
Includes occupational hygiene, occupational medicine and biological monitoring.
Occupational health practitioner
An OCC medicine practitioner or a person who holds a qualification in occupational health recognized as such by the South African Medical and Dental Council as referred to in the Medical, Dental and Supplementary Health Service Professions Act, 1974 (Act No. 56 of 1974), or the South African Nursing Council as referred to in the Nursing Act, 1978 (Act No. 50 of 1978).
Occupational hygiene
The anticipation, recognition, evaluation and control of conditions arising in or from the workplace, which may cause illness or adverse health effects to persons.
Occupational medicine
The prevention, diagnosis and treatment of illness and adverse health effects associated with a particular type of work.
Occupational medicine practitioner
A medical practitioner as defined in the Medical, Dental and Supplementary Health Service Professions Act, 1974 (Act No. 56 of 1974), who holds a qualification in occupational medicine or an equivalent qualification which qualification or equivalent is recognized as such by the South African Medical and Dental Council referred to in the said Act.
Office

An office as defined in section 1(1) of the Basic Conditions of Employment Act, 1983 (Act No. 3 of 1983).

Officer

An officer or employee as defined in section 1(1) of the Public Service Act, 1984 (Act No. 111 of 1984).

Organism

Any biological entity which is capable of causing illness to persons.

Plant

Includes fixtures, fittings, implements, equipment, tools and appliances, and anything which is used for any purpose in connection with such plan

Premises

Includes any building, vehicle, vessel, train or aircraft.

Prescribed

Prescribed by regulation.

Properly used

Used with reasonable care, and with due regard to any information, instruction or advice supplied by the designer, manufacturer, importer, seller or supplier, as the case may be.

Reasonably practicable

Practicable having regard to - The severity and scope of the hazard or risk concerned;

the state of knowledge reasonably available concerning that hazard or risk and of any means of removing or mitigating that hazard or risk;

the availability and suitability of means to remove or mitigate that hazard or risk; and the cost of removing or mitigating that hazard or risk in relation to the benefits deriving there from.

Regulation

A regulation made under section 43.

Remuneration

Any payment in money or in kind or both in money and in kind, made or owing to any person in pursuance of such person's employment.

Shop

A shop as defined in section 1(1) of the Basic Conditions of Employment Act, 1983 (Act No. 3 of 1983).

Standard

Any provision occurring in a specification, compulsory specification, code of practice or standard method as defined in section 1 of the Standards Act, 1993 (Act No. 29 of 1993); or

In any specification, code or any other directive having standardization as its aim and issued by an institution or organization inside or outside the Republic which, whether generally or with respect to any particular article or matter and whether internationally or in any particular country or territory, seeks to promote standardization.

Substance

Any solid, liquid, vapour, gas or aerosol, or combination thereof.

This Act

Includes any regulation

Trade union

A trade union as defined in section 1 of the Labour Relations Act, 1956 (# 28 of 1956).

<u>User</u>
In relation to plant or machinery, means the person who uses plant or machinery for his own benefit or who has the right of control over the use of plant or machinery, but does not include a lessor of, or any person employed in connection with, that plant or machinery.
<u>Work</u>
Work as an employee or as a self-employed person, and for such purpose an employee is deemed to be at work during the time that he is in the course of his employment, and a self-employed person is deemed to be at work during such time as he devotes to work as a self-employed person.
<u>Workplace</u>
Any premises or place where a person performs work in the course of his employment.
The Minister may by notice in the Gazette declare that a person belonging to a category of persons specified in the notice shall for the purposes of this Act or any provision thereof be deemed to be an employee, and thereupon any person vested and charged with the control and supervision of the said person shall for the said purposes be deemed to be the employer of such person.

This Act shall not apply in respect of:
A mine, a mining area or any works as defined in the Minerals Act, 1991 (Act No. 50 of 1991), except in so far as that Act provides otherwise; any load line ship (including a ship holding a load line exemption certificate), fishing boat, sealing boat and whaling boat as defined in section 2(1) of the Merchant Shipping Act, 1951 (Act No. 57 of 1951), or any floating crane, whether or not such ship, boat or crane is in or out of the water within any harbour in the Republic or within the territorial waters thereof, or in respect of any person present on or in any such mine, mining area, works, ship, boat or crane.

2.4 Policy on Non-compliance

All identified or suspected breaches in compliance, arising from any source including monitoring activities or complaints must be reported at the earliest opportunity to both Department Management and the Compliance Department. The Compliance department may assist the Department in addressing non-compliance issues, in accordance with priorities relating to minimizing regulatory risk and its consequential impact on reputation risk for the Company. Corrective action in cases of non-compliance remains the accountability of the relevant Department's Management unit, who should agree their plan of corrective action with the Compliance Department. The relevant Department Head, together with the Compliance Department should sign off identified or suspected breaches and corrective action to be taken.

The Compliance department may escalate any disputes. Breaches in compliance or failure to report any breach or suspected breach will be seen in a serious light and may result in action being taken.

Should staff members have any queries regarding this policy or regarding suspicious and unusual transactions, they should contact the Compliance department.

2.5 Financial Intelligence Centre Act

2.5.1 Background

The Financial Intelligence Centre Act sets up a regulatory anti-money laundering regime, which is intended to break the cycle used by organized criminal groups to benefit from illegitimate profits. By doing this, the Act aims to maintain the integrity of the financial systems. The Financial Intelligence Centre Act imposes, amongst others, ‘know your client’, record-keeping and reporting obligations on this organisation

This document is aimed at creating awareness with respect to obligations relating to the reporting of suspicious and unusual transactions. The suspicious and unusual transaction reporting requirement, within Financial Intelligence Centre Act came into operation on 3 February 2003’. What is every staff member’s obligation with respect to reporting suspicious and unusual transactions?

It is the duty of every member of management and staff who becomes aware of suspicious and unusual transactions to report their suspicion to the Compliance Department. All members of management and staff must be aware of the policy on reporting Money Laundering Suspicious and Unusual Transactions, which sets out how reports are to be submitted. Once a member of management and staff has reported in terms of the policy, all personal legal obligations with respect to reporting have been met.

2.5.2 What constitutes money laundering suspicious and unusual transaction?

As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious and unusual transaction. Suspicion is personal and subjective and falls far short of proof based on firm evidence. However, the suspicion must at least have some foundation and not just be based on mere speculation. Financial Intelligence Centre Act sets out the criteria to be used when determining whether a transaction is suspicious or unusual.

These include:

- A person who knows or suspects business has been received is likely to receive, facilitate, proceeds unlawful activities
- Transaction has no apparent business or lawful purpose
- Conducted purpose of avoiding giving rise to reporting duty
- Relevant investigation of evasion or attempted evasion of duty to pay any tax or levy imposed by legislation administered by SARS
- Business used or likely to be used in any way for money laundering purposes.

2.5.3 A suspicious transaction will often be:

Any transaction where the amount, duration or other specific feature is inconsistent with the customer’s professional or business activities, standard of living or normal movements on the account.
A transaction that is not logical from an economic, financial or commercial point of view with respect to reporting. Based on having enough knowledge about a customer to be able to recognize what is abnormal / unusual and what might be suspicious

2.5.4 Period for report submission

The company has fifteen (15) days, excluding weekends and public holidays, to submit a report to the Financial Intelligence Centre. An overview, objectives and overall architecture of the Financial Intelligence Centre are highlighted below.

"If you are in doubt, report!"

Therefore, in order to ensure compliance, all reports must immediately be reported to the Compliance department for analysis, investigation and reporting once the staff member develops a suspicion.

When the Compliance department receives reports from staff members, which after analysis and investigation by the Compliance department are deemed to be suspicious and unusual transactions, the Compliance department will forward such reports to the Financial Intelligence Centre.

2.5.5 Protection of staff members making a report

Persons reporting in terms of the policy are protected from civil or criminal action. However, reports must be made in good faith and in accordance with the criteria highlighted in the company handbook. No evidence concerning the identity of a person reporting is admissible in criminal proceedings unless the person testifies. Testimony is, however, optional.

2.5.6 About the Financial Intelligence Centre

The Financial Intelligence Centre is established in order to identify the proceeds of unlawful activities and to combat money laundering activities. It aims to do so by making information collected by it available to investigating authorities (the Police Service, the Scorpions, the Special Investigating Unit and the Asset Forfeiture Unit), the intelligence services and the Revenue Service. In order to fulfil its objectives, the Centre will collect, process, analyse and interpret information reported to it in terms of various statutory reporting obligations. The Centre will also monitor compliance with the Financial Intelligence Centre Act and give necessary guidance.

Further reading in own time – Regulatory Acts: Financial Intelligence Centre Act, 38 of 2001, including the regulations and exemptions Prevention of Organised Crime Act, Act 121 of 1998

Module 3

Ways of Managing Risk

This Module deals with:
- Upside and downside risk for a particular position in an organisation.
- Potential risk associated with a specific procedure and measures to minimize the risk with reference to a specific organization.
- Measures to minimize risk for a particular situation and innovative recommendations to help minimize the risk.

This module looks at the different ways of managing risk. We need to first understand the negative and positive impact of risk. To explain we are going to look at a scenario where we might have to relocate to a different city to be promoted.

3.1 Negative implications could include:

- Financially we may be worse off because of the costs associated with moving – conveyancing and transfer fees; transportation expenses; costs associated with refurbishment and repair; compliance fees; new deposits for electricity and rates and taxes; maybe extended travel costs; area defined schooling and education costs; additional security costs; new furnishing costs; insurance.
- The emotional effects of the stress of relocating.
- The additional time and effort needed to get everything in place.

3.2 Positive implications could include:

The following are considered positive aspects of the risk attached to relocating:
- There is a sense of achievement when all is in order.
- Pride in the extent of the new property, and how it reflects your success.
- A new closeness to the family unit as result of this achievement.
- Perhaps a sense of financial success in terms of savings made, if downgrading.
- A new drive engendered by new surroundings.

So we see that every situation or ensuing actions have both positive and negative consequences. The trick is to plan for the potential negative implications and to manage the risk of such implications impacting the process beyond acceptable levels.

3.3 A framework for developing a risk management plan

Whilst it is impossible to totally eliminate any possibility of risk, it is possible to minimize risk through developing and implementing a risk management plan. The plan should include:

3.3.1 Action items for managing risk in order of priority

You need to priorities your action items according to the prioritised risk items e.g. deal with the high risk items first, then the medium and then the low. Suggest ways of managing the risk. These will include steps, actions or control measures that need to be taken in order to minimize the risk, e.g.:

- General compliance awareness;
- Specific training relating to industry regulatory items;
- Training relating to business processes / control measures to meet requirements of provisions;
- Review, update or develop procedures for employees to follow ;
- Review update systems to report on errors;
- Develop a check list;
- Arranging training sessions for employees;
- Arrange education workshops;
- Conduct awareness workshops;
- Implement regular audits;
- Provide coaching to staff;
- Recruit workplace safety officers ;
- Conduct regular performance checks, etc.

The name of the person who is responsible for carrying specific steps or actions needs to be documented next to applicable actions. The target date for finalizing and implementing the steps or actions that needs to be taken needs to be defined. Make sure that you have allocated reviews at regular intervals and/or when items or control measures change and how the reviews will be conducted

3.3.2 Develop Monitoring Plans

The actions that were implemented to minimize risk need to be monitored on an ongoing basis for the following reasons:

- To ensure that the cost of implementing the controls does not exceed the expected benefit i.e. the reason why they were implemented in the first place;
- Human error due to carelessness, negligence, distractions, misunderstanding of instructions, etc.;
- Abuse of internal controls, e.g. overriding of internal controls by management;
- Possibility of controls becoming inadequate due to changes in conditions.

Monitoring – What:

- The control measures and not the requirement;
- The sufficiency and effectiveness of control measures;
- Identify which control measures must be monitored – based on risk assessment;
- How will the control measures be monitored?

Monitoring – When:

- Plan when the monitoring will take place;
- Avoid duplication wherever possible;
- Focus on the prioritised items;
- Identify the frequency;
- Daily, Weekly, Monthly, Bi-annually, annually.

Monitoring – Who:

- Whose responsibility is it to perform the monitoring exercise?

- Management;
- Compliance Officer;
- External auditor.

Types of Monitoring
- Regular ongoing monitoring, e.g. transactional, exception reports;
- Adhoc monitoring / sampling;
- Complaints.

3.3.3 Implement Monitoring Plans
Identify where requirements are being complied with – determine whether controls are working effectively and identify where requirements are not being complied with.
Corrective Action based on Monitoring Findings includes:
- Identify control breakdowns and actual breaches;
- Prioritize based on risk assessment of seriousness;
- Identify corrective action/s required;
- Set target dates for corrective action;
- Manage corrective action activities;
- Appropriate signing off of corrective action – nature;
- Appropriate escalation of breaches – nature;
- Facilitating and assisting where necessary.

3.3.4 Compliance Reporting
How will you report on findings and what will the report include? Consider:
- At what level will you report?
- Status and activities of risk management plan;
- Report on findings; Report on corrective action; Who will you report your findings to?; Complaints and breaches to be reported to nominated persons;
- Management; Compliance Officer; Regulatory reporting e.g. Financial Intelligence Centre Act or OHASA e.g. injuries.

Module 4

Behaviours and attitudes versus Risk Management

This Module deals with:

- Personal behaviour to determine behaviour risk to an employment contract.
- Personal behaviour that could be construed as an upside risk to the organisation.
- Own behaviour to determine how well own values and attitudes contribute to positive work relationships.
- Behaviours and attitudes most valued by co-workers or colleagues and own behaviour is compared to the perceived dominant value system and own experiences in workplace relationships.
- A personal action plan to manage both positive and negative risk associated with own behaviour and attitudes.

How well do your own values and behaviours measure against this common set of the organisation? How will you ensure that you uphold the values and attitudes for the benefit of positive relationships in the work place? You need to assess yourself against these standards, identify any risk behaviours and develop a plan to minimize the risk associated with non-conformance to these standards.

4.1 Attitudes and Behaviours in the workplace

Attitudes reflect how one feels about something. When you say ‘I like my job’, you are expressing your attitude about work. Attitudes are evaluative statements or judgments concerning objects, people, or events. Values are not the same as attitudes but the two are interconnected. A value can be defined as ‘beliefs about what is desirable or good, e.g. free speech, and what is undesirable or bad, e.g. dishonesty’. What you believe will influence your attitude and reflect in your behaviour. Behaviour is a component of an attitude and refers to an intention to behave in a certain way toward someone or something. When someone doesn’t like another person, it may be obvious in their behaviour toward that person e.g. ignores them when they are around, says negative comments about the person, etc. Research shows that people seek consistency between their attitudes and their behaviour. When someone’s attitude towards something or someone changes, their behaviour will reflect the changes in attitude. E.g. Sally never liked John and so behaved in a hostile way toward him. When Sally got to know John and began to like him, her behaviour toward him reflected her new attitude. Our attitudes in the work place affect the way we do our work, how we behave towards our colleagues and our leaders and the contribution we make in terms of team-work and overall contribution to the company.

4.2 Aligning own values and behaviours

People behave differently as a result of their values / attitudes and their different experiences throughout their lives. In your individual reflection of positive and negative work relationships you discussed your experiences regarding the down side of negative relationships in the work place in terms of impact to you as a person, commitment to colleagues, your work, the company and spin-off in terms of your personal life as well as the benefits associated with positive relationships. We spend a huge amount of time in the workplace and if we are not happy it has a negative spin-off not only in terms of the abovementioned criteria but also the impact are felt in our personal lives as well. We do not switch off at the end of the day; we take our negative or positive feelings home with us. The spin-off is felt by our families, friends and the way we feel about ourselves too. One way to promote positive relations in the workplace, especially among team members is to establish a common set of operating guidelines. Operating guidelines help to ensure effective team member interactions. They provide a common vision of how team members should act and the common rules to follow so those interactions between team members are highly efficient and effective. The operating guidelines essentially consist of a set of agreed behaviours that the team commonly feels will contribute to and promote positive relationships and are usually guided by values and attitudes that are important to the team. For example, if the team values free speech, then some of the behaviours defined may be:

- Seek first to understand the speaker's position before responding; No interruptions or side conversations while a speaker is speaking;
- Acknowledge what people are saying and don't judge; Seek to find common ground when there are disagreements;
- No staff member to be penalized for speaking; Keep things safe and confidential.

Team members need to consciously choose the operating guidelines by which they will operate. If these guidelines are not set, certain norms will emerge over time. Often these 'norms' are not constructive. In some groups, for example, it is acceptable to start meetings late or for group members to frequently interrupt one another during discussions. By setting operating guidelines the team determines what it's preferred 'norms' for operating will be. Operating guidelines typically define such things as acceptable behaviour during meetings, how decisions are made, how accountability for assignments is maintained and how feedback is given. Operating guidelines can be used to compliment the value and behaviour statements defined by the team.

Bibliography

INSETA & IMFUNDO Learning Materials, 2003/8