Concepts & Principles and Process of HIRA

QCTO: Occupational Health, Safety Quality Practitioner Qualification – NQF Level 5

226302001-KM 03 KT 07

ISO NET (Pty) Ltd

Learner Guide

We believe our Clients are unique
Website: https://iso-net.co.za Address: 15 Porter Avenue Brakpan 1541 Cell: 03

Course Content:

The difference and interrelationship between hazards and risks
What is the difference between a 'hazard' and a 'risk'?
Definition of a Hazard
Definition of a Risk
Describe the process of hazard identification and risk assessment
Hazard identification, risk assessment and risk control
Using the Think Safe steps
Spot the hazard
Assess the risk
Make the changes

- **Elimination**
- **Substitution**
- **Isolation**
- **Safeguards**
- **Instructing workers in the safest way to do something**
- **Using personal protective equipment and clothing (PPE)**

Steps for identifying hazards
What are workplace hazards?
What are the most common workplace hazards?

- **physical hazards**
- **ergonomic hazards**
- **chemical hazards**
- **biological hazards**

Common health risks
How to prevent workplace hazards
Different processes of classifying hazards
What is a hazard?
Harm
Hazard
What are examples of a hazard?
What is risk?
What is a risk assessment?
What is an adverse health effect?
Will exposure to hazards in the workplace always cause injury, illness or other adverse health effects?
What types of hazards are there?

- **biological**
- **chemical**
- **ergonomic**
- **physical**
- **psychosocial**
- **safety**

Typical process for identifying the related risks
The key elements of a risk management program include:

1. **Process**

2. **Integration**
3. **Culture**

Infrastructure.

Step One: Identify Risk

1. **Impact**
2. **Likelihood**
3. **Velocity**
4. **Persistence**

Step Two: Source Risk

Step Three: Measure Risk

1. **Risk rating or scoring**
2. **Claims exposure and cost analysis**
3. **Sensitivity analysis**
4. **Stress testing**
5. **Tracking key variables relating to an identified exposure**
1. **Earnings at risk**
2. **Rigorous analytics that are proprietary to the company**
3. **Risk-adjusted performance measurement**
4. **Examining value at risk**

Step 4: Evaluate Risk

1. **Avoid**
2. **Accept**
3. **Reduce**
4. **Share**

Step 5: Mitigate Risk

Step 6: Monitor Risk

Methods of classifying and describing significant risks

Introduction

Exhibit 1 – Risk Management Process

Risk Management Framework

Risk Management Plan

Risk Identification

Risk Sources

Exhibit 2 – Risk Sources

Risk Category

Exhibit 3 – Organization-Provided Standard Risk Categories

Risk Analysis

3. Probability of Risk Occurrence

4. Risk Impact

Exhibit 4 – Impact classification guideline

5. Risk Exposure

Exhibit 5 – Impact-Probability Matrix

6. Risk Occurrence Timeframe

Exhibit 6 – Risk occurrence timeframe

7. Risk Classification Examples:

Exhibit 7 – Risk Classification Examples

Risk Response Planning

1. Risk Response Plans

Exhibit 8 – Risk response - Examples

2. Risk Triggers

Exhibit 9 – Risk Trigger Examples
3. Risk Ownership
Exhibit 10 – Risk Owner Examples
Risk Monitoring and Control
Risk reporting
Risk Threshold
Risk Efficiency measurement
Risk Metrics
Risk Audit
Scope (stakeholders, techniques and area)
What is Scope Risk?
What is Scope Creep in Project Management?
Scope Risk Examples
Tip: Project Risk Categories
Ways to Identify Scope Risks
Interviews
Brainstorming
Checklists
Assumption Analysis
Cause and Effect Diagrams
Nominal Group Technique (NGT)
Affinity Diagrams
Work Breakdown Structure (WBS)
The Six-Step Assessment Process
The Six Steps of Assessment
Important questions to ask when conducting assessment:
Monitoring and reporting process
Introduction to Implementation and Monitoring
Refinement of the action plan
Monitoring
An effective monitoring and reporting system ideally includes the following elements:
Collecting Data
“Pressures – state - impact – response”
Systematic data collection
Corrective measures
Communication and involvement

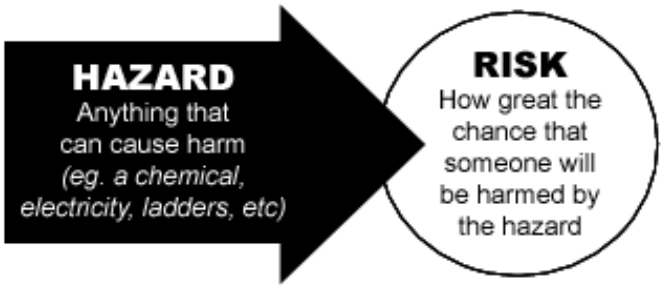
The difference and interrelationship between hazards and risks

What is the difference between a 'hazard' and a 'risk'?

A **hazard** is something that can cause harm, e.g. electricity, chemicals, working up a ladder, noise, a keyboard, a bully at work, stress, etc.

A **risk** is the chance, high or low, that any hazard will actually cause somebody harm.

For example, working alone away from your office can be a hazard. The risk of personal danger may be high. Electric cabling is a hazard. If it has snagged on a sharp object, the exposed wiring places it in a 'high-risk' category.



Note: This content is provided as general background information and should not be taken as legal advice or financial advice for your particular situation. Make sure to get individual advice on your case from your union, a source on our free help page or an independent financial advisor before taking any action.

Definition of a Hazard

“Hazard” means a source of or exposure to danger.

Definition of a Risk

“Risk” means the probability that injury or damage will occur.

Describe the process of hazard identification and risk assessment

Hazard identification, risk assessment and risk control

There are three steps used to manage health and safety at work.

- Spot the Hazard (Hazard Identification)
- Assess the Risk (Risk Assessment)
- Make the Changes (Risk Control)

At work you can use these three ThinkSafe steps to help prevent accidents.

Using the Think Safe steps

Spot the hazard

Key point: A hazard is anything that could hurt you or someone else.

Examples of workplace hazards include:

- frayed electrical cords (could result in electrical shock)
- boxes stacked precariously (they could fall on someone)
- noisy machinery (could result in damage to your hearing)

During work experience, you must remain alert to anything that may be dangerous. If you see, hear or smell anything odd, take note. If you think it could be a hazard, tell someone.

Assess the risk

Key point: Assessing the risk means working out how likely it is that a hazard will harm someone and how serious the harm could be.

Whenever you spot a hazard, assess the risk by asking yourself two questions:

- how likely is it that the hazard could harm me or someone else?
- how badly could I or someone else be harmed?

Always tell someone (your employer, your supervisor or your health and safety representative) about hazards you can't fix yourself, especially if the hazard could cause serious harm to anyone.

For example:

- ask your supervisor for instructions and training before using equipment
- ask for help moving or lifting heavy objects
- tell your supervisor if you think a work practice could be dangerous

If you are not sure of the safest way to do something on work experience, always ask your work experience supervisor.

Make the changes

Key point: It is your employer's responsibility to fix hazards. Sometimes you may be able to fix simple hazards yourself, as long as you don't put yourself or others at risk.

For example, you can pick up things from the floor and put them away to eliminate a trip hazard.

The best way to fix a hazard is to get rid of it altogether. This is not always possible, but your employer should try to make hazards less dangerous by looking at the following options (in order from most effective to least effective):

- **Elimination** - Sometimes hazards - equipment, substances or work practices - can be avoided entirely. (e.g. Clean high windows from the ground with an extendable pole cleaner, rather than by climbing a ladder and risking a fall.)
- **Substitution** - Sometimes a less hazardous thing, substance or work practice can be used. (e.g. Use a non-toxic glue instead of a toxic glue.)
- **Isolation** - Separate the hazard from people, by marking the hazardous area, fitting screens or putting up safety barriers. (e.g. Welding screens can be used to isolate welding operations from other workers. Barriers and/or boundary lines can be used to separate areas where forklifts operate near pedestrians in the workplace.)
- **Safeguards** - Safeguards can be added by modifying tools or equipment, or fitting guards to machinery. These must never be removed or disabled by workers using the equipment.
- **Instructing workers in the safest way to do something** - This means developing and enforcing safe work procedures. Students on work experience must be given information and instruction and must follow agreed procedures to ensure their safety.

- **Using personal protective equipment and clothing (PPE)** - If risks remain after the options have been tried, it may be necessary to use equipment such as safety glasses, gloves, helmets and ear muffs. PPE can protect you from hazards associated with jobs such as handling chemicals or working in a noisy environment.

Sometimes, it will require more than one of the risk control measures above to effectively reduce exposure to hazards.

Steps for identifying hazards

Every workplace has hazards. As an employer, you have a legal responsibility to look after your employees' safety and protect them against health and safety hazards at work.

In order to manage workplace health and safety and help prevent accidents and sickness absence, it's important to identify, monitor and reduce the risk associated with workplace hazards.

What are workplace hazards?

Simply put, workplace hazards are any aspect of work that cause health and safety risks and have the potential to harm.

Some hazards are more likely to be present in some workplaces than others, and depending on the work that you do, there will be hazards that are more or less relevant to your business.

What are the most common workplace hazards?

There are many types of workplace hazards, which tend to come under four main categories:

- **physical hazards** – the most common workplace hazards, including vibration, noise and slips, trips and falls;
- **ergonomic hazards** – physical factors that harm the musculoskeletal system, such as repetitive movement, manual handling and poor body positioning;
- **chemical hazards** – any hazardous substance that can cause harm to your employees;
- **biological hazards** – bacteria and viruses that can cause health effects, such as hepatitis, HIV/AIDS and Legionnaire's disease.

Common health risks

Some of the most common health risks associated with workplace hazards include:

- breathing problems;
- skin irritation;
- damage to muscles, bones and joints;
- hearing damage;
- reduced wellbeing.

How to prevent workplace hazards

The best way to protect yourself and your employees from workplace hazards is to identify and manage them and take reasonable steps to prevent their potential to harm.

In order to control workplace hazards and eliminate or reduce the risk, you should take the following steps:

- identify the hazard by carrying out a workplace risk assessment;
- determine how employees might be at risk;
- evaluate the risks;
- record and review hazards at least annually, or earlier if something changes.

Different processes of classifying hazards

What is a hazard?

The meaning of the word hazard can be confusing. Often dictionaries do not give specific definitions or combine it with the term "risk". For example, one dictionary defines hazard as "a danger or risk" which helps explain why many people use the terms interchangeably.

There are many definitions for hazard but the most common definition when talking about workplace health and safety is:

A **hazard** is any source of **potential** damage, harm or adverse health effects on something or someone.

Hazard identification and elimination and risk assessment and control" uses the following terms:

Harm - physical injury or damage to health.

Hazard - a potential source of harm to a worker.

Basically, a hazard is the potential for harm or an adverse effect (for example, to people as health effects, to organizations as property or equipment losses, or to the environment).

Sometimes the resulting harm is referred to as the hazard instead of the actual source of the hazard. For example, the disease tuberculosis (TB) might be called a "hazard" by some but, in general, the TB-causing bacteria (Mycobacterium tuberculosis) would be considered the "hazard" or "hazardous biological agent".

What are examples of a hazard?

Workplace hazards can come from a wide range of sources. General examples include any substance, material, process, practice, etc. that has the ability to cause harm or adverse health effect to a person or property. See Table 1.

Table 1
Examples of Hazards and Their Effects

Workplace Hazard	Example of Hazard	Example of Harm Caused
Thing	Knife	Cut
Substance	Benzene	Leukemia
Material	Mycobacterium tuberculosis	Tuberculosis
Source of Energy	Electricity	Shock, electrocution
Condition	Wet floor	Slips, falls
Process	Welding	Metal fume fever
Practice	Hard rock mining	Silicosis
Behaviour	Bullying	Anxiety, fear, depression

Workplace hazards also include practices or conditions that release uncontrolled energy like:

- an object that could fall from a height (potential or gravitational energy),
- a run-away chemical reaction (chemical energy),
- the release of compressed gas or steam (pressure; high temperature),
- entanglement of hair or clothing in rotating equipment (kinetic energy), or
- contact with electrodes of a battery or capacitor (electrical energy).

What is risk?

- **Risk** is the chance or probability that a person will be harmed or experience an adverse health effect if exposed to a hazard. It may also apply to situations with property or equipment loss, or harmful effects on the environment.
- Hazard identification and elimination and risk assessment and control" uses the following terms:
- **Risk** – the combination of the likelihood of the occurrence of a harm and the severity of that harm.
- **Likelihood** – the chance of something happening.

Note: In risk assessment terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (e.g., a probability or a frequency over a given time period).

For example: the risk of developing cancer from smoking cigarettes could be expressed as:

- "cigarette smokers are 12 times (for example) more likely to die of lung cancer than non-smokers", or
- "the number per 100,000 smokers who will develop lung cancer" (actual number depends on factors such as their age and how many years they have been smoking). These risks are expressed as a probability or likelihood of developing a disease or getting injured, whereas hazard refers to the agent responsible (i.e. smoking).
- Factors that influence the degree or likelihood of risk are:
- the nature of the exposure: how much a person is exposed to a hazardous thing or condition (e.g., several times a day or once a year),
- how the person is exposed (e.g., breathing in a vapour, skin contact), and
- the severity of the effect. For example, one substance may cause skin cancer, while another may cause skin irritation. Cancer is a much more serious effect than irritation.

What is a risk assessment?

Risk assessment is the process where you:

- Identify hazards and risk factors that have the potential to cause harm (hazard identification).
- Analyze and evaluate the risk associated with that hazard (risk analysis, and risk evaluation).
- Determine appropriate ways to eliminate the hazard, or control the risk when the hazard cannot be eliminated (risk control).

The OSH Answers document on Risk Assessment has details on how to conduct an assessment and establish priorities.

What is an adverse health effect?

A general definition of adverse health effect is "any change in body function or the structures of cells that can lead to disease or health problems".

Adverse health effects include:

- bodily injury,
- disease,
- change in the way the body functions, grows, or develops,
- effects on a developing fetus (teratogenic effects, fetotoxic effects),
- effects on children, grandchildren, etc. (inheritable genetic effects)
- decrease in life span,
- change in mental condition resulting from stress, traumatic experiences, exposure to solvents, and so on, and
- effects on the ability to accommodate additional stress.

Will exposure to hazards in the workplace always cause injury, illness or other adverse health effects?

Not necessarily. To answer this question, you need to know:

- what hazards are present,

- how a person is exposed (route of exposure, as well as how often and how much exposure occurred),
- what kind of effect could result from the specific exposure a person experienced,
- the risk (or likelihood) that exposure to a hazardous thing or condition would cause an injury, or disease or some incidence causing damage, and
- how severe would the damage, injury or harm (adverse health effect) be from the exposure.

The effects can be acute, meaning that the injury or harm can occur or be felt as soon as a person comes in contact with the hazardous agent (e.g., a splash of acid in a person's eyes). Some responses may be chronic (delayed).

For example, exposure to poison ivy may cause red swelling on the skin two to six hours after contact with the plant.

On the other hand, longer delays are possible: mesothelioma, a kind of cancer in the lining of the lung cavity, can develop 20 years or more after exposure to asbestos.

Once the hazard is removed or eliminated, the effects may be reversible or irreversible (permanent). For example, a hazard may cause an injury that can heal completely (reversible) or result in an untreatable disease (irreversible).

What types of hazards are there?

A common way to classify hazards is by category:

- **biological** - bacteria, viruses, insects, plants, birds, animals, and humans, etc.,
- **chemical** - depends on the physical, chemical and toxic properties of the chemical,
- **ergonomic** - repetitive movements, improper set up of workstation, etc.,
- **physical** - radiation, magnetic fields, pressure extremes (high pressure or vacuum), noise, etc.,
- **psychosocial** - stress, violence, etc.,
- **safety** - slipping/tripping hazards, inappropriate machine guarding, equipment malfunctions or breakdowns

Typical process for identifying the related risks

What are the key elements of the risk management process? It's a great question — and an important one — since crafting an effective risk management program protects a company's reputation and can even give it a competitive edge in the marketplace.

Like any other worthwhile business activity, risk management requires a process with a clear purpose, reliable inputs, well-designed activities and value-added outputs. Here's what *to consider when evaluating your company's enterprise risk management (ERM).*

The key elements of a risk management program include:

4. **Process**
5. **Integration**
6. **Culture**
7. **Infrastructure.**

These elements of a risk management program are flexible. They have to be, because strategies, organizational structures, operating philosophies and risk profiles vary in complexity across industries and firms.

This article describes the steps in the process — your job is to put them into action as soon as possible.

Step One: Identify Risk

An enterprise risk assessment process identifies and prioritizes a company's risks, providing quality inputs to decision makers to help them formulate effective risk responses, including information about the current state of capabilities around managing the priority risks.

Risk assessment spans the entire organization, including critical business units and functional areas. Effectively applied using business strategy as a context, risk assessment considers attributes such as:

5. **Impact**
6. **Likelihood**
7. **Velocity**
8. **Persistence**

Step Two: Source Risk

Once priority risks are identified, they are traced to their root causes. If management understands the drivers of risk, it is easier to design risk metrics and proactive risk responses at the source. Will this step present challenges?

Almost certainly. Overcoming them is key to success.

Step Three: Measure Risk

There is an old adage that says, "If you can't measure something, you can't manage it." Because not all risks are quantifiable, increasing transparency by developing quantitative and qualitative risk measures is common practice.

Measurement methodologies may be simple and basic. Here are some examples of how to measure risk:

6. **Risk rating or scoring**
7. **Claims exposure and cost analysis**
8. **Sensitivity analysis**
9. **Stress testing**
10. **Tracking key variables relating to an identified exposure**

More complex methodologies for companies with more advanced capabilities could differ — and might be more complicated.

But remember: ignoring risk won't make it go away. Other risk management methodologies might include analyzing these complex factors:

5. **Earnings at risk**
6. **Rigorous analytics that are proprietary to the company**
7. **Risk-adjusted performance measurement**
8. **Examining value at risk**

Step 4: Evaluate Risk

Based on the priority risks identified, their drivers or root causes and their susceptibility to measurement, the next step requires that management choose the appropriate risk response.

There are four categories of risk responses:

5. **Avoid**
6. **Accept**
7. **Reduce**
8. **Share**

These responses can be applied to groups of related risks consisting of natural families of risks that share fundamental characteristics (like common drivers, positive or negative correlations, etc.) consistent with a portfolio view.

The organization first decides whether to accept or reject a risk based on an assessment of whether the risk is desirable or undesirable. A desirable risk is one that is inherent in the entity's business model or normal future operations and that the company believes it can monitor and manage effectively.

An undesirable risk is one that is off-strategy, offers unattractive rewards or cannot be monitored or managed effectively.

If an entity chooses to accept a risk, it can accept it at its present level, reduce its severity and/or its likelihood of occurrence (typically through internal controls), or share it with a financially capable, independent party (typically through insurance or a hedging arrangement).

Step 5: Mitigate Risk

Depending on the risk response selected, management identifies any gaps in risk management capabilities and improves those capabilities as necessary to implement the risk response. Over time, the effectiveness of risk mitigation activities should be monitored.

Step 6: Monitor Risk

Models, risk analytics and web-enabled technologies make it possible to aggregate information about risks using common data elements to support the creation of a risk management dashboard or scorecard for use by risk owners, unit managers and executive management.

Dashboard and scorecard reporting should be flexible enough to enable the design of reports to address specific needs, including reporting to the board of directors.

Examples of dashboard reporting, which often features "heat maps" or "traffic light" indicators, are provided in the Application Techniques of the COSO Enterprise Risk Management Integrated Framework. Monitoring also includes activities of an internal audit function.

The purpose of the risk management process varies from company to company, e.g., reduce risk or performance variability to an acceptable level, prevent unwanted surprises, facilitate taking more risk in the pursuit of value creation opportunities, etc.

Regardless of purpose, the good news is that a large body of knowledge on the risk management process is readily available so that companies can adopt a process view that best fits their circumstances.

Methods of classifying and describing significant risks

Risk Analysis and Management is a key project management practice to ensure that the least number of surprises occur while your project is underway. While we can never predict the future with certainty, we can apply a simple and streamlined risk management process to predict the uncertainties in the projects and minimize the occurrence or impact of these uncertainties.

This improves the chance of successful project completion and reduces the consequences of those risks.

This paper presents the structured Risk Management process followed at Nokia Siemens Networks that helps avoid crisis situations and incorporate learning from past mistakes.

It highlights that effective and early risk identification and management secures the achievement of project objectives, leading to reduced rework costs.

Introduction

Project team members at various levels identify and handle risks in different flavours. However, this will be ineffective without a structured risk management framework, as this leads to:

- Incomplete impact evaluation, leading to loss of:
    - Knowledge of the overall impact on the project objectives, like scope, time, cost, and quality
    - Identification of secondary or new risks arising from the already identified risks
- Lack of transparency and a communication gap within and outside the team
- Thus, it is very important for any project organization to set up an effective risk management framework. Instituting such a practice as a project team culture ensures:
- Conscious and focused risk identification and management
- Project progress as desired, with the least amount of deviations or surprise, and in line with project and organizational objectives
- Early and effective communication of project issues to organization and project stakeholders
- An effective team building tool, as team buy-in and acceptance is assured

Exhibit 1 shows that risk management is an iterative process and each facet of risk management should be planned and followed during each phase of the project.

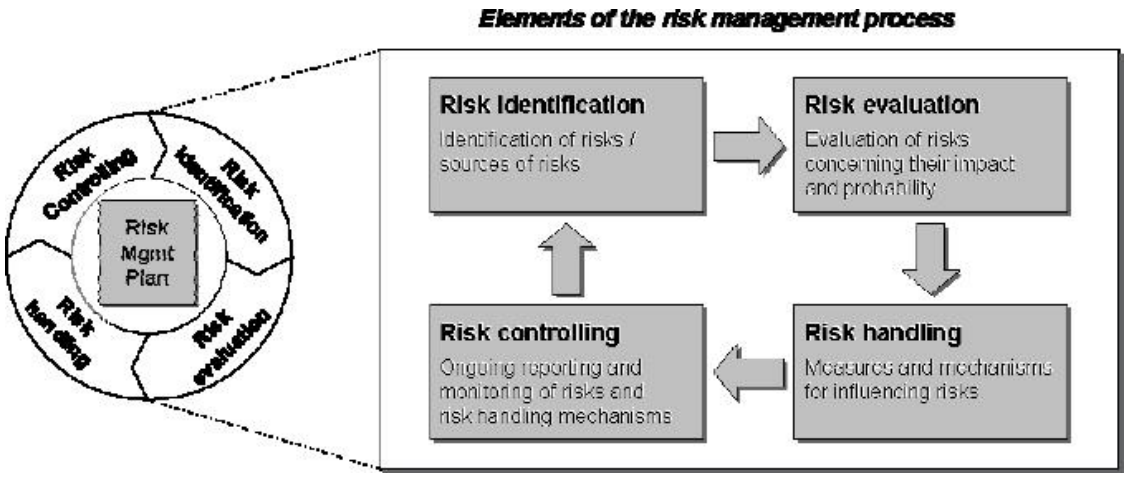


Exhibit 1 – Risk Management Process

The risk management framework followed at Nokia Siemens Networks provides guidelines for:

- Continuous risk identification
- Risk evaluation
- Risk mitigation and contingency measure definition
- Risk monitoring and control
- Risk identification efficiency measurement

The risk management framework also provides templates and tools, such as:

- A risk register for each project to track the risks and issues identified
- A risk checklist, which is a guideline to identify risks based on the project life cycle phases
- A risk repository, which is all the risks identified across projects so far

Risk Management Framework

Risk Management Plan

The organization-mandated risk management framework is reviewed and tailored to define the project risk management plan when the project is initiated. The risk management plan includes these definitions and guidelines:

- List of possible risk sources and categories
- Impact and probability matrix
- Risk reduction and action plan
- Contingency plan
- Risk threshold and metrics

Risk Identification

Risks are to be identified and dealt with as early as possible in the project. Risk identification is done throughout the project life cycle, with special emphasis during the key milestones.

Risk identification is one of the key topics in the regular project status and reporting meetings. Some risks may be readily apparent to the project team—known risks; others will take more rigor to uncover, but are still predictable.

The medium for recording all identified risks throughout the project is the risk register, which is stored in the central project server.

The following tools and guidelines are used to identify risks in a structured and disciplined way, which ensures that no significant potential risk is overlooked.

Risk Sources

Risk Source	Description
Risk repository	The risk repository is the history data containing the list of risks identified for completed projects. The risk repository can be used to arrive at a list of potential risks for the project. This risk repository can also be filtered based on risk sources, categories, and projects.
Checklist analysis	The risk identification checklist is a questionnaire that helps identify gaps and potential risks. It is developed based on experience and project type.
Expert judgement	Risk identification is also done by brainstorming with or interviewing experienced project participants, stakeholders, and subject matter experts.
Project status	The project status includes project status meeting reports, status reports, progress reports, and quality reports. These reports provide the current project progress, issues faced, and threshold violations. These provide insight into the status of the project and potential new risks.

Exhibit 2 – Risk Sources

Risk Category

Risk category provides a list of areas that are prone to risk events. The organization recommends high-level, standard categories, which have to be extended based on the project type.

Risk Category	Extended categories
Technical	Requirements, Technology, Interfaces, Performance, Quality, etc.
External	Customer, Contract, Market, Supplier, etc.
Organizational	Project Dependencies, Logistics, Resources, Budget, etc.
Project Management	Planning, Schedule, Estimation, Controlling, Communication, etc.

Exhibit 3 – Organization-Provided Standard Risk Categories

Risk Analysis

Risk analysis involves examining how project outcomes and objectives might change due to the impact of the risk event.

Once the risks are identified, they are analysed to identify the qualitative and quantitative impact of the risk on the project so that appropriate steps can be taken to mitigate them. The following guidelines are used to analyse risks.

3. Probability of Risk Occurrence

a. High probability – (80 % ≤ x ≤ 100%)
b. Medium-high probability – (60 % ≤ x < 80%)
c. Medium-Low probability – (30 % ≤ x < 60%)
d. Low probability (0 % < x < 30%)

4. Risk Impact

a. High – Catastrophic (Rating A – 100)
b. Medium – Critical (Rating B – 50)
c. Low – Marginal (Rating C – 10)

As a guideline for Impact Classification the following matrix is used:

Project Objective	C Rating 10	B Rating 50	A Rating 100
Cost	Cost increase > 0 % or > 0 €	Cost increase 5 - 10% or > 50.000 €.	Cost increase > 10 % or > 100.000 €.
Schedule	overall project schedule delay > 0 days	overall project schedule delay > 1 week	overall project schedule delay > 2 weeks *
Scope	Scope decrease barely noticeable	Minor areas of scope are affected	Major areas of scope are affected; scope reduction unacceptable to the client
Quality	Quality reduction barely noticeable	Quality reduction does not affect vital functionality	Quality reduction requires client approval

Exhibit 4 – Impact classification guideline

The score represents bottom thresholds for the classification of risks assuming "normal" conditions. An upgrade of the score to the next or even next + 1 level is necessary, if the risk is impacted by critical factors such as:

- How important the specific customer is

- Whether the project is critical for the further development of the relationship with the customer
- The risk is already in the focus of the customer
- Specific penalties for deviations from project targets are agreed in the contract with the customer

5. Risk Exposure

Risk Exposure or Risk Score is the value determined by multiplying the Impact Rating with Risk Probability as shown in Exhibit 5.

		Probability			
		1 = high (80% ≤ x ≤ 100%)	2 = medium high (60% ≤ x < 80%)	3 = medium low (30% ≤ x < 60%)	4 = low (0% < x < 30%)
Impact	A=high (Rating 100)	(Exposure – Very High) (Score 100)	(Exposure – Very High) (Score 80)	(Exposure – High) (Score 60)	(Exposure – Moderate) (Score 30)
	B=medium (Rating 50)	(Exposure – High) (Score 50)	(Exposure – Moderate) (Score 40)	(Exposure – Moderate) (Score 30)	(Exposure – Low) (Score 15)
	C=low (Rating 10)	(Exposure – Low) (Score 10)	(Exposure – Low) (Score 8)	(Exposure – Low) (Score 6)	(Exposure – Low) (Score 3)

Exhibit 5 – Impact-Probability Matrix

The colours represent the urgency of risk response planning and determine reporting levels.

6. Risk Occurrence Timeframe

The timeframe in which this risk will have an impact is identified. This is classified into one of the following:

Timeframe	Description
Near	Now- until one month
Mid	next 2-6 months
Far	>6 months

Exhibit 6 – Risk occurrence timeframe

In addition to classifying risks according to the above guidelines, it is also necessary to describe the impact on cost, schedule, scope, and quality in as much detail as possible based on the nature of the risk.

7. Risk Classification Examples:

Risk event	Probability	Impact rating	Score
The hardware will be delivered 10 days late, leading to an overall project delay of 10 days in a project that is of minor importance to the customer	100%	B (50)	50
The hardware will be delivered 10 days late, leading to an overall project delay of 10 days. Delivery on time is important to the customer. High penalties for each day of delayed delivery are agreed.	100%	B (50)	50, but because of special circumstances is upgraded to 100
The acceptance test scope of work is not confirmed by the customer by integration test completion. From experience, it may be expected that the customer will require a certain number of additional test cases, leading to schedule delay and additional costs.	70%	B (50), because a risk of 6% cost increase and 10 days project schedule delay are expected	40
At C130 the customer has confirmed half the features described in the R-Spec, but informs Nokia Siemens Networks that the other half, as well as some additional requirements, are still under discussion. The final scope of the project is therefore very unclear. Major changes are to be expected.	80%	A (100), because a risk of more than 10% cost increase and more than 2 weeks project schedule delay, as well as major changes in scope, are expected	100

Exhibit 7 – Risk Classification Examples

Risk Response Planning

There may not be quick solutions to reduce or eliminate all the risks facing a project. Some risks may need to be managed and reduced strategically over longer periods. Therefore, action plans should be worked out to reduce these risks. These action plans should include:

- Risk description with risk assessment
- Description of the action to reduce the risk
- Owner of the risk action
- Committed completion date of the risk action

All risk action plans should be allotted to the person identified to carry out the action plan.

1. Risk Response Plans

For each risk, a risk response must be documented in the risk register in agreement with the stakeholders. This should be ensured by the project manager.

Risk response plans are aimed at the following targets:

1. Eliminating the risk
2. Lowering the probability of risk occurrence
3. Lowering the impact of the risk on the project objectives

Risk response plans usually impact time and costs. It is therefore mandatory that the time and cost for the defined response plan are calculated as precisely as possible. This also assists in selecting a response plan from the alternatives, and in verifying whether the response plan is costlier or has more impact on one of the project objectives than the risk itself.

After successfully implementing a set of response plans, the score of a risk could be lowered in consultation with the stakeholders.

Examples:

Risk event	Risk Response
Schedule delay to be expected if the hardware is delivered late.	Agree on penalties with the hardware supplier for delayed delivery. • Evaluate ways to shorten the timeline for onsite activities like installation, commissioning, etc. • Shorten the acceptance phase by reducing acceptance test cases or inviting the customer to a joint system test before customer release.
Time, cost, and scope deviation to be expected if requirements not final at project kick-off.	• Make sure that the requirements specification has been internally reviewed by all concerned parties and is internally agreed as complete and feasible. • Inform the customer about the latest possible date for input into the final version of the requirements specification and about the version that is to be used as basis for the development if no further input is available until then. • Open a claim against the customer. • Agree with the customer that all issues not clarified until project kick-off will be treated as change requests with possible impacts on time and cost.

Exhibit 8 – Risk response - Examples

2. Risk Triggers

For each risk a trigger must be documented in the risk register. The trigger identifies the risk symptoms or warning signs. It indicates that a risk has occurred or is about to occur. The risk trigger also gives an indication of when a certain risk is expected to occur.

Examples:

Risk Event	Risk Trigger
Schedule delay to be expected if the hardware is delivered late.	Confirmed hardware delivery dates not available at project initiation.
Time, cost, and scope deviation to be expected if requirements will not be final at project kick-off.	R-Spec is not ready for customer review 1 week before project kick off.

Exhibit 9 – Risk Trigger Examples

3. Risk Ownership

The ground rule is that responsibility for managing all risks in the project lies with the project manager.

Based on this ground rule a Risk Owner (who is not necessarily the project manager) must be determined and named in the Risk Register. The Risk Owner is normally the one who can best monitor the risk trigger, but can also be the one who can best drive the defined countermeasures.

The Risk Owner is responsible for immediately reporting any changes in the risk trigger status and for driving the defined countermeasures.

Examples:

Risk event	Risk owner
Schedule delay to be expected if the hardware is delivered late.	Technical Order Manager and Service Account Manager
Time, cost, and scope deviation to be expected if requirements will not be final at project kick-off.	Project Manager
Overall project schedule delay to be expected if customer release will not be reached in time.	System Test leader

Exhibit 10 – Risk Owner Examples

Risk Monitoring and Control

Risk monitoring and control includes:

- Identifying new risks and planning for them
- Keeping track of existing risks to check if:
  - Reassessment of risks is necessary
  - Any of risk conditions have been triggered
  - Monitor any risks that could become more critical over time
  - Tackle the remaining risks that require a longer-term, planned, and managed approach with risk action plans
  - Risk reclassification

For the risks that cannot be closed, the criticality has to go down over a period of time due to implementing the action plan. If this is not the case then the action plan might not be effective and should be re-examined.

Risk reporting

The risk register is continuously updated, from risk identification through risk response planning and status update during risk monitoring and control. This project risk register is the primary risk reporting tool and is available in the central project server, which is accessible to all stakeholders.

Risk monitoring and controlling or risk review is an iterative process that uses progress status reports and deliverable status to monitor and control risks. This is enabled by various status reports, such as quality reports, progress reports, follow-up reports, and so forth.

Risk Reviews are a mandatory item of milestone meetings and/or regular project meetings, but they can also be executed during separately planned risk review meetings. These risk reviews must be held regularly. The frequency could also be determined based on the overall risk level of a project.

Risk Threshold

The risk priorities have to be set to direct focus where it is most critical. The risks with the highest risk exposure rating are the highest priority.

Risks with Exposure Low can be dropped from the mitigation plans, but may need to be revisited later in the project.

The organizational mandate is that if the projects have at least one “Very High” risk or more than 3 “High” risks, guidance should be sought from management and stakeholders, as the project may be at high risk of failure.

This is the recommended risk threshold. Projects can customize the threshold based on project needs.

Risk Efficiency measurement

Risk Metrics

The efficiency of risk analysis and management is measured by capturing the following metrics during project closure. The analysis results are used to decipher lessons learned, which is updated in the organization's lessons learned database.

- Number of risks that occurred / Number of risks that were identified
- Was the impact of the risks as severe as originally thought?
- How many risks recurred?
- How do the actual problems and issues faced in a project differ from the anticipated risks?

Risk Audit

This is an independent expert analysis of risks, with recommendations to enhance maturity or effectiveness of risk management in the organization. This evaluates:

- How good are we at identifying risk?
- Exhaustiveness and granularity of risks identified
- Effectiveness of mitigation or contingency plan
- Linkage of project risks to organizational risks

This is not a “process adherence” audit, but an aid to enhance the quality of risk identification and risk analysis. This is also used as a forum to benchmark and identify good practices of risk management among various projects in the organization.

The risk audit is done by a group of independent domain or technical experts through documentation review and interviews. The key deliverables of this risk audit are:

- Customized checklist to evaluate the risks of a project
- Identify areas of importance for risk analysis for a project (risk taxonomy)
- Risk radar – risk-prone areas of the product group
- Potential additional risks identified based on the review
- Top 10 risks in the organization from key projects, which requires management attention

Scope (stakeholders, techniques and area)

If you wish to be a successful project manager, you must manage scope risks. In this article, let's define scope risks, look at some examples, and explore eight ways to identify scope risks.

What is Scope Risk?

Risk is "an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives" (PMBOK® Guide—6th Edition, Page 720). Scope risks are uncertain events or conditions that are related to the project scope.

What do we mean when we say something is out of scope? It should not be included in the project. Things have a way of sneaking in, don't they?

Keep in mind, product scope includes the features and functions of the products, services, and results. And project scope is the work required to create the deliverables.

- scope. WORD ORIGIN. Scope Root Word Definition
- indicating an instrument for observing, viewing, or detecting: microscope, telescope

What is Scope Creep in Project Management?

Have you ever started a project with two deliverables and midway you have five? Or perhaps you have a well-defined list of key software features. New stakeholders started adding to the list. In agile projects, the additional requirements/features (i.e., unplanned work) were added during an iteration.

Scope Risk Examples

Scope tends to be a vague concept. Allow me to clarify with examples:

- Individuals may add features to the product that were not approved.
- The project team may not identify all the deliverables, requiring changes later.
- Scope changes may not be processed through the change control process.
- Requirements may not be properly analyzed and understood.
- Requirements may not be properly prioritized.
- Traceability structure may not be developed resulting in requirements not being managed through the design, development, and testing processes.
- The project team may fail to identify all the activities required to create the deliverables.

Tip: Project Risk Categories

Here's a tip: specify risk categories when identifying risks. And the typical risk categories include:

- Schedule
- Scope
- Cost
- Quality

Now, we can filter our risk register to scope risks. You and your team can review the scope risks and develop appropriate risk response plans. Wise project managers look for high leverage responses. A single response may address two or more risks.

Lastly, project managers can use risk categories to compare the amount of risk exposure between risk categories. You can invest your limited time and budget on the risk categories that matter most.

Ways to Identify Scope Risks

What tools and techniques can we use to identify scope risks? For most projects, you will only need a few methods. Pick the ones that make the most sense.

Interviews

Select key stakeholders. Plan the interviews. Define specific questions related to the project scope — deliverables, assumptions, constraints, exclusions. Additionally, document the results.

Brainstorming

Plan your brainstorming questions. Here are questions I like to use: What are the most significant risks related to the project deliverables? What are the most significant risks related to the project work? For instance, requirements, coding, testing, training, and implementation.

Checklists

See if your company has a list of the most common risks. Look for scope-related risks. If not, create a checklist. After each project, conduct a post-review where you capture the most significant risks. This list may be used for subsequent projects.

Warning – checklists are great, but no checklist contains all the risks.

Assumption Analysis

The PMBOK® Guide defines an assumption as “factors that are considered to be true, real, or certain without proof or demonstration." Assumptions are sources of risk.

Project managers should ask stakeholders, “What assumptions do you have concerning this project?” Document these assumptions and associated risks.

Cause and Effect Diagrams

Cause and Effect diagrams are powerful. Project managers can use this simple method to help identify causes of risks. If we address the cause, we will reduce the risk.

Nominal Group Technique (NGT)

Many project managers are not familiar with the Nominal Group Technique. It is brainstorming on steroids. Input is collected and prioritized. The output of NGT is a prioritized list; for risk identification, the result is a prioritized list of risks.

Affinity Diagrams

Creating affinity diagrams is a fun, creative, and beneficial exercise. Participants are asked to brainstorm risks. I ask participants to write each risk on a sticky note. Then participants sort the risks into groups or categories. Lastly, each group is given a title.

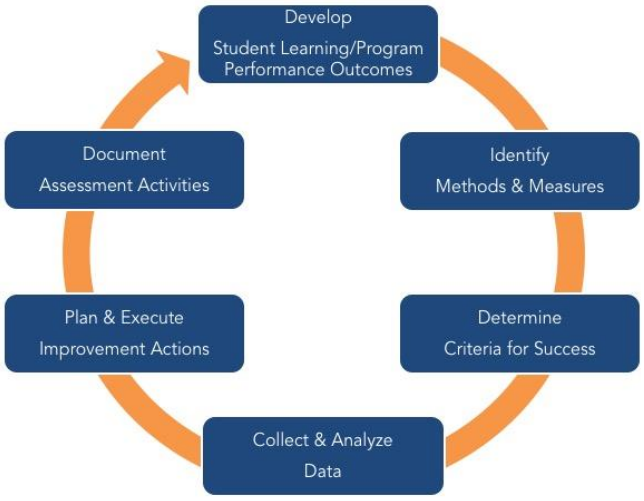
Work Breakdown Structure (WBS)

One of the most powerful tools for identifying scope risks is to facilitate a WBS with your project team. Then walk through each of the lowest elements — commonly referred to as work packages — and ask the participants to identify risks.

Various process steps for conducting the assessment

The Six-Step Assessment Process

Assessment is an ongoing process aimed at continuous improvement of student learning. At CSUF, assessment follows a 6-step cycle:



The Six Steps of Assessment

- Develop student learning outcomes that align with the university's mission, the university's student learning goals, and (if applicable) the accreditation requirements of the respective discipline
- Develop and implement methods of assessment involving direct and indirect and measures
- Determine criteria for success
- Collect and analyze data
- Plan (and execute) improvement actions
- Document assessment and improvement activities.

Important questions to ask when conducting assessment:

- What do we want our students to learn - at the course level, program level, and the university level?
- How are our students doing? How do we know?
- What evidence do we need to know to determine how well our students are learning?
- How do we use the data to confirm or improve our teaching and learning practices?
- What impacts do our improvement actions have on student learning?
- How are we documenting the assessment and improvement activities and outcomes?

Monitoring and reporting process

Introduction to Implementation and Monitoring

With the implementation of the strategic programme and the action plan, the management cycle reaches its very core: all the preceding assessment and planning has the overall objective of improving the way the city functions in terms of sustainable development.

The implementation is where it shows. The implementation is a demanding task in terms of organisation and coordination of all the parallel actions that will take place.

A crucial condition is a solid communication and involvement approach and the organisational setup. Cooperation with and between various stakeholders assures that the different actors buy in to the implementation process.

Therefore, implementation is based on the “foundation” which is a combination of the action plan, the organisational setup and above all – communication and involvement. The approval of the action plan by the city council may be a determining success factor, as it legitimises actions and gives them a required priority.

In parallel, and for the purpose of being able to measure and report the results, the implementation of the strategic programme and its action plan should be monitored in an appropriate way and fed back to the politicians.

It allows for being able to see if actions are implemented with good results. If not, it allows for taking corrective measures while implementation is in progress. In order to be able to engage in monitoring, the actions need to rely on targets based on indicators defined in the strategic programme.

Refinement of the action plan

With the strategic programme and action plan approved by the city council, an important step has been taken towards improvement of the sustainability performance. The action plan serves as a basis for the implementation of the strategic programme, but needs to be further refined.

Outline and segment the objectives and targets to concretise measures and projects to be realised by the relevant departments and stakeholders involved. In order to serve as a good basis for day-to-day work, ensure that the action plan answers the following questions:

- What is to be done? (title, short description of measure)
- Who is responsible? (person, department or stakeholder, contact details)
- Who should support implementation and how (person, department, contact details)

- By what time should the measures be completed? (timetable, date of realisation)
- Which personnel and financial resources are assigned? (staff, budget)
- Is public information legally required? (which information? to whom? through which instruments? when? how often?)
- Are green procurement procedures in place in case of a call for tender or purchase by the local government? (yes/no (*If not in place yet, green procurement procedures should be introduced.*)/under development)

For the majority of measures, stakeholder involvement will be necessary for realisation. This requires substantial and formal agreements with stakeholders. Describe the measures taken by stakeholders in the same way as the actions worked out by the municipal departments.

Concrete measures could also include the training of personnel in specific aspects and/or new legislation. Further information regarding staff training – for example, the responsibilities for training and an analysis of training needs – is provided in the "Organisational Setup" section.

The heads of the department and the involved stakeholder organisations are responsible for the concretisation of measures. The coordinator is responsible for compiling the information on the refined measures and to document them in the "refined action plan".

The responsible department documents and completes the refined action plan and makes it available at one spot for all actors involved. It serves as a basis for the monitoring of realisation of activities through the coordinator and responsible persons assigned.

Monitoring

Good management practises include regular monitoring on both a short- and long-term basis. An effective monitoring process provides ongoing, systematic information that strengthens project implementation. The monitoring process provides an opportunity to:

a) compare implementation efforts with original goals and targets,
b) determine whether sufficient progress is being made toward achieving expected results, and,
c) determine whether the time schedule is observed.

Monitoring is not an "event" that occurs at the end of a management cycle, but rather is an ongoing process that helps decision-makers to better understand the effectiveness of the action or system. An effective monitoring and evaluation programme requires collecting and analyzing important data on a periodic basis throughout the management cycle of a project.

This process often involves collecting baseline data on existing conditions, reporting on progress toward environmental/sustainability improvements, making connections between actions and intended outcomes, and making mid-course changes in program design.

An effective monitoring and data management system records the performance of all institutions with implementation responsibilities. It provides a system of accountability for all responsible parties on how well they are achieving the goals and targets established in the IMS.

The responsibility of appropriate application of the monitoring system lies with the responsible persons/organisations/authorities assigned to this activity and has to follow the reporting

duties as outlined during the “organisational setup” phase.

Implementation together with monitoring show how important it is to work with indicators and SMART targets from the very beginning of the system implementation. The work with indicators and measurable data has to start with the baseline review.

Key data based on indicators have to be mapped in addition to analysis and recognition of missing indicators on the occasion of the baseline review of the existing situation.

Within the next step of the system, these key data and indicators are used to formulate SMART targets in the strategic programme and as a result will form the basis for the action programme and therefore the basis for implementation processes.

Finally, the implementation can be further controlled and monitored, referring to the clearly defined indicators and thus SMART targets. Effectiveness monitoring is thus very much dependent on a baseline recognition and reference to selected indicators.

It is important to have a look at the current situation of monitoring to adapt the monitoring system as much as possible to the structures in place and to avoid duplication of work. Several of the EU based legislations require monitoring (e.g., Strategic Environmental Assessment, Clean Air Directive, etc.).

Very often, monitoring activities are very dispersed and not linked with each other. It would, however, be very useful if one unit could make use of data collected in another unit. As an example, the monitoring results of the traffic control department could provide useful insights for the health department. The IMS delivers a platform to connect the various data sources.

An effective monitoring and reporting system ideally includes the following elements:

- Clearly articulated targets and a set of indicators to measure performance;
- A schedule and set of guidelines for all responsible parties to report to each other;
- An opportunity for responsible parties and stakeholders to periodically meet to coordinate actions and review each other’s performance
- A link between the evaluation reports and relevant statutory planning cycles of the municipality, such as annual budgeting and capital planning, so that the municipality can adjust its plans as based on the actions taken by other sectors.

Collecting Data

In preparing the monitoring setup, it is good to check the following questions:

- For which indicators are data currently being collected?
- What are key information sources? Are representatives from these information sources already involved in the IMS process?
- How valid and accurate are the data?
- Are the data easily accessible and available?
- Are there any costs associated with acquiring the data?
- For those indicators where no data currently exists, which steps should be taken to collect new data?
- How expensive would a new data collection effort be?

Ideally, most monitoring processes include collecting both quantitative and qualitative data.

Quantitative data is information that can be counted and measured. Quantitative environmental data focuses on actual environmental improvements, such as the amount of waste reduced or energy saved.

Mechanisms for collecting quantitative environmental data are usually programme-specific, such as using water meters to measure actual water consumption.

Qualitative data is a more difficult measurement of programme success. It includes assessments of problems encountered, stakeholder satisfaction, and unanticipated benefits. Qualitative data can give a real understanding of the actual impact the actions are making on people's lives.

It is usually collected through instruments such as surveys and personal interviews. In order to have a better understanding of the successes and challenges, it is advisable to collect both types of data.

For example, to address persistent water shortages, a town may decide to implement a pilot water conservation programme to install low-flow showerheads in residences.

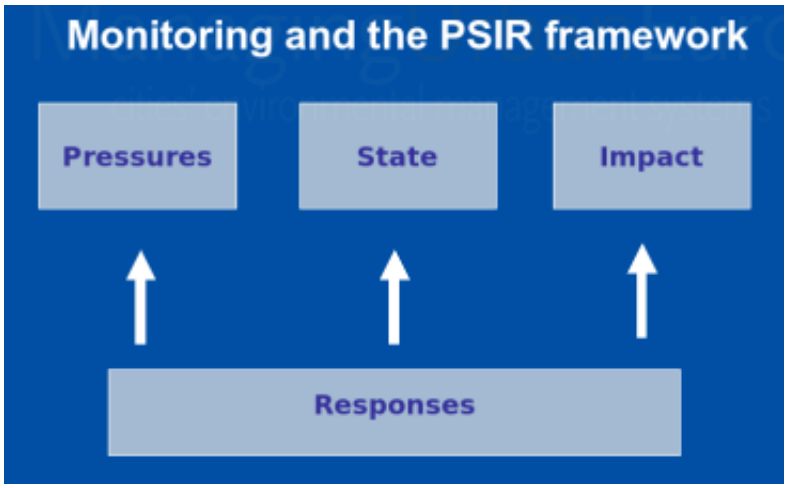
A quantitative data collection effort would focus on how much water has actually been saved, while qualitative data would reveal how satisfied consumers were with the performance of the new showerheads.

Both types of information are imperative to determine whether the program was successful.

"Pressures – state - impact – response"

When applying the analytical framework of "pressures – state - impact – response" to monitoring, it becomes obvious that all of the four areas need to be monitored. Ideally, this has already been taken into account when choosing the indicators.

If not, the indicators can still be sorted at this point according to the schematic to facilitate the analysis:



To take a concrete example, if you want to monitor the effectiveness of an action, say a noise protection wall, you need to measure

- whether the wall has been erected (response),
- whether the noise level has been reduced as a result of the wall (state),
- or if the source of the noise has decreased (independently of this action, maybe due to related measures in the action plan) (pressure),
- and finally, if the affected people living there are less disturbed now (impact).

In collecting data, it is also important to distinguish between *compliance monitoring* versus *effectiveness monitoring* — both types of monitoring are important.
Compliance monitoring measures whether the implementing institution did what it said it was going to do (e.g., install 5,000 low-flow showerheads, or to use the above example, the noise protection walls have been installed), while *effectiveness monitoring* measures whether the actions achieved their intended result (e.g., reducing water usage by 20% per household, or the decibels behind the wall are a certain rating lower).
Of course, the real measure of success is effectiveness, i.e., how well conditions are improving.
However, compliance monitoring is a critical piece of the evaluation process to help determine whether implementing institutions have fulfilled their commitments, and it helps to analyse why goals were not reached where this is the case.

Systematic data collection

This system can be as simple as using standardized reporting forms to facilitate the collection and compilation of data up to an entirely computerized data-sharing system.

Nevertheless, what counts is not the level of high-tech computer application that is installed to manage your data, but whether the indicators chosen and the items monitored accurately reflect the progress of implementation and allow for an analysis of deviation from targets and goals.

Data management

Observe	Set up a system and tools that allow keeping track of changes (based on the indicators and targets, considering PSIR). Set time intervals for measuring
Record	Organise the way you store data in a logical way

Be sure to collect data on the indicators prior to beginning the implementation of the strategic programme. Ideally, you used the same set of indicators already for the collection of data for the baseline review, upon which the impacts of implementing selected actions will be measured.

In practical terms, data collection is less troublesome if it is organised systematically and in a reproducible way, i.e.,:

- Establish overviews of existing data sources in the form of inventories and a meta-database;
- Prepare templates and guidelines on data handling, technical documentation of the data and analytical methods used;
- For each dataset and indicator (diagrams, tables and maps), maintain a paper or electronic fact-sheet with description of data source, data quality, methods for data compilation, other relevant information and its graphical draft.

Each institution submits information to the responsible coordinator, who is responsible for assuring the system and who compiles this information into a report.

The more specifically the coordinator formulates what he/she expects the different departments to monitor, the easier it will be to systematically store and later retrieve this information, to make it accessible to a larger audience and to evaluate the results.

- Example: A monitoring form for a specific action

A good monitoring and evaluation process engages all stakeholders and is useful to those ultimately responsible for improving the project.

Evaluation is also an important public awareness and educational tool.

The objective is to use synergies, avoid double work and report as efficiently as possible. Please consult the section “organisational setup”, which has further information on reporting routines.

To monitor the realisation of the action in accordance with the action plan is easier than monitoring their effects. The coordinator needs to receive feedback from the responsible persons regarding the

- realisation of the activity - yes/no?
- agreed timetable
- assigned resources
- modifications

With this information, the coordinator is able to control the compliance of the implementation process with the action plan and to elaborate one part of the interim report or internal audit report.

Corrective measures

A well-organised monitoring system is able to detect deviations from the set direction promptly. The mistake can be analysed immediately, corrective measures taken as soon as possible, and damage or loss minimised.

Communication and involvement

The effectiveness of implementation is very much dependent on the partnerships developed and the involvement and cooperation of various stakeholders. This is the step of actual action, which most often creates lots of challenges, mainly due to the fact that it requires the cooperation of different sorts of groups with various stakes.

Planning is usually much less complicated than the actual implementation of the action plan.

At this stage, questions about cross-sectoral cooperation and multi-stakeholder involvement and cooperation appear.

- Is the organisational set-up cross-sectoral enough?
- Are those to implement working together for a common objective? Is the common objective of sustainability clear?
- Are departments cooperating with each other and are the relevant stakeholders involved?
- Are the targets SMART?
- Are indicators available and measurable?
- Is the timetable realistic?
- In order to make things happen, address all these issues in line with the development of the integrated management system in the city.

The public needs to know what is ongoing. To inform the public about the implementation of the action plan may play the decisive role as to whether the implementation will be successful or not happen at all.

Very often the effectiveness of the implementation depends on citizens' involvement.

In this case, combine information about the ongoing implementation processes with the call for cooperation and involvement.

The examples are various: waste separation, rational energy use (decreasing energy consumption in households) or water-saving measures, to name just a few.