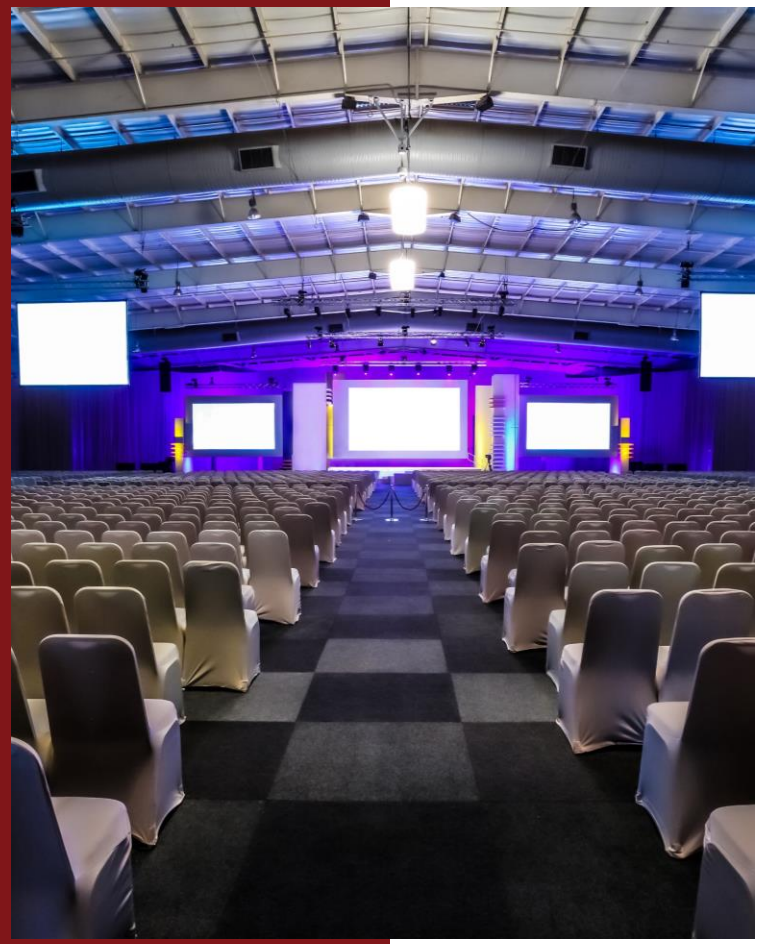
MSECB

Risk Assessment and Treatment in ISO/IEC 27001

Techniques and methodologies for conducting risk assessments and implementing risk treatments.

By Oludare Ogunkoya

MSECB



Webinar Agenda

- Overview of ISO/IEC 27001
- Understanding Risk Assessment
- Risk Assessment Steps
- Techniques and Methodologies for Risk Assessment
- Risk Treatment in ISO/IEC 27001
- Selection for Risk Treatment Options
- Utilizing Tools and Resources
- Q&A

Background of Oludare Ogunkoya

Oludare Ogunkoya is a well-breed trainer and auditor from a diverse perspective with over 20 years of industry experience across several continents. He is an astute practitioner in Governance, Risk, and Compliance (GRC) in various sectors including financial institutions, manufacturing, and the public sector, among others.

Since 2017, Mr. Ogunkoya has diligently led audits for numerous large firms on behalf of MSECB. His professionalism, impartiality, punctuality, and exceptional preparation for ISO/IEC 27001:2022, ISO/IEC 20000-1:2018, ISO 9001:2015, ISO 45001:2018, ISO/IEC 27701:2019, and ISO 22301:2019 have consistently stood out in all his audits.

Alphaedge Quodrant Africa Limited

We are a Governance, Risk, and Compliance (GRC) organization with a mission to educate, empower, and enable our clients to greater heights of assurance by partnering with them to achieve governance, risk, and compliance objectives. We have the mandate to offer all ISO training across Africa.

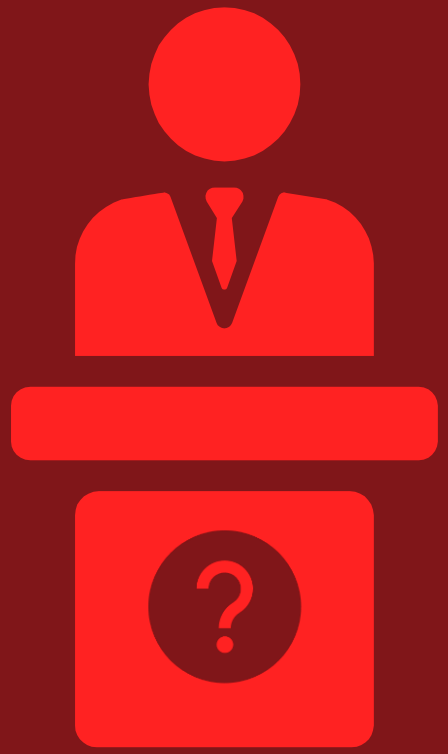
Having backed almost two decades of work experience across various sectors in over fifteen (15) African countries, we eventually established our dream child called Alphaedge Quodrant Africa Ltd on 15th October 2019. We pride ourselves on a team of diverse professionals with several years of experience in various industries including Oil & Gas, Manufacturing, Telecom, and Finance.

MSECB

Our Clients

ASACI
INLAKS own tomorrow.
workforce group
Africa Prudential
FinTrak SOFTWARE
Africa DataCentres
GTBank
Keystone Bank
Flutterwave
PROVIDUSBANK
BRD
IMPALA
Ecobank The Pan African Bank
adb agricultural development bank ...truly agric and more
BM SECURITY est.1984
AFRICAN ALLIANCE INSURANCE PLC
OAG
Training Heights
ecl Enterprise Computing Ltd
Moniepoint
eProcess International S.A.
MULTIDIGITAL NIGERIA LIMITED
MTN
CYBERSOC Incident Response and Security Services
AZA FINANCE

MSECB



Overview of ISO/IEC 27001

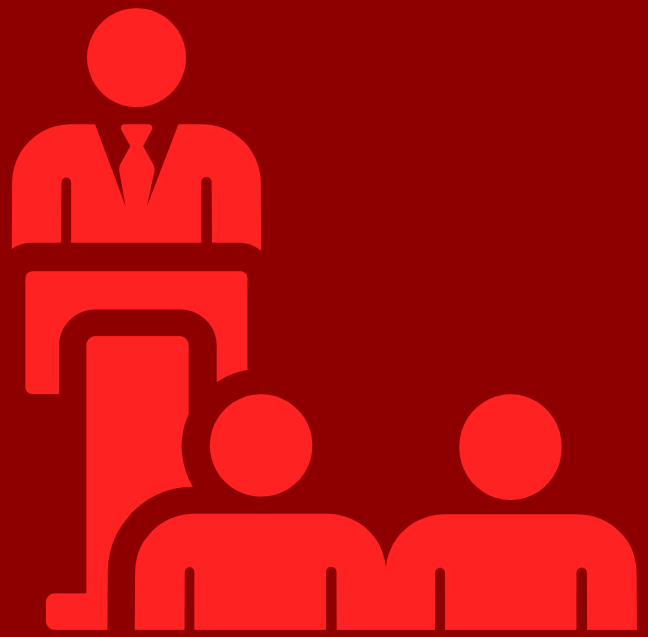
MSECB

What is ISO/IEC 27001?

- **ISO 27001**
- **ISMS**
- **Information Security Management System**

MSECB

What is ISO/IEC 27001?



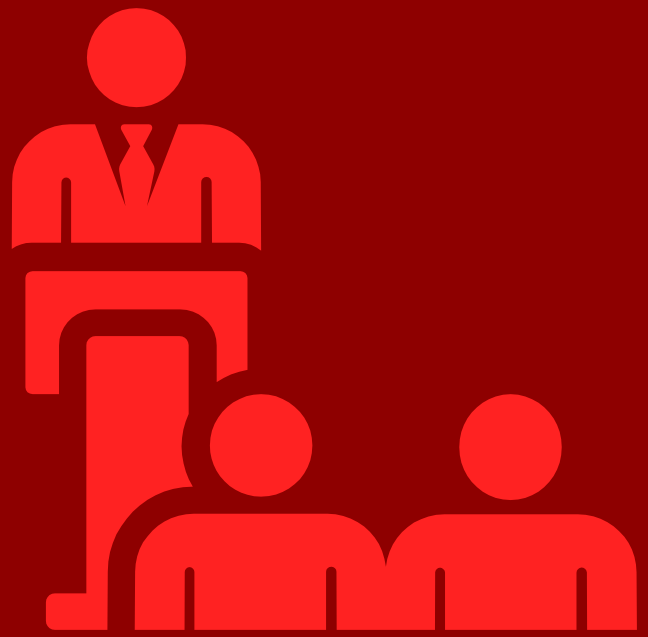
What is ISO/IEC 27001?

An international standard for information security management systems (ISMS) that focuses on protecting the confidentiality, integrity, and availability of information.

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an ISMS

Risk management is central to ISMS as it helps in identifying and mitigating potential threats and vulnerabilities that could impair information assets

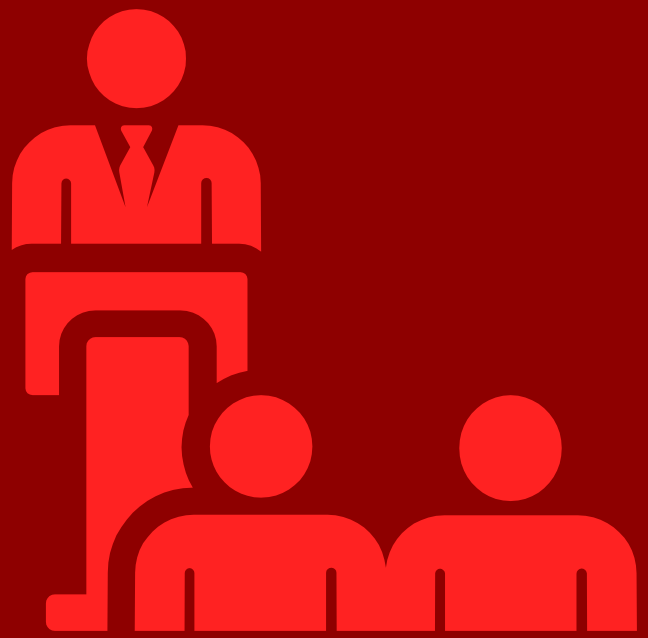
MSECB



ISO/IEC 27001 Can Mitigate

- Physical Risks
- Phishing Attacks
- Hacking & Ransomware Attacks
- System & Process Risks

MSECB



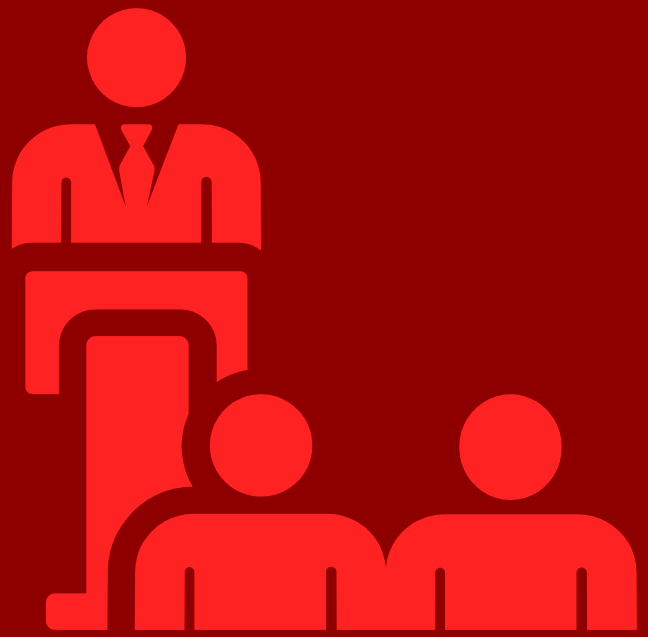
What is RISK

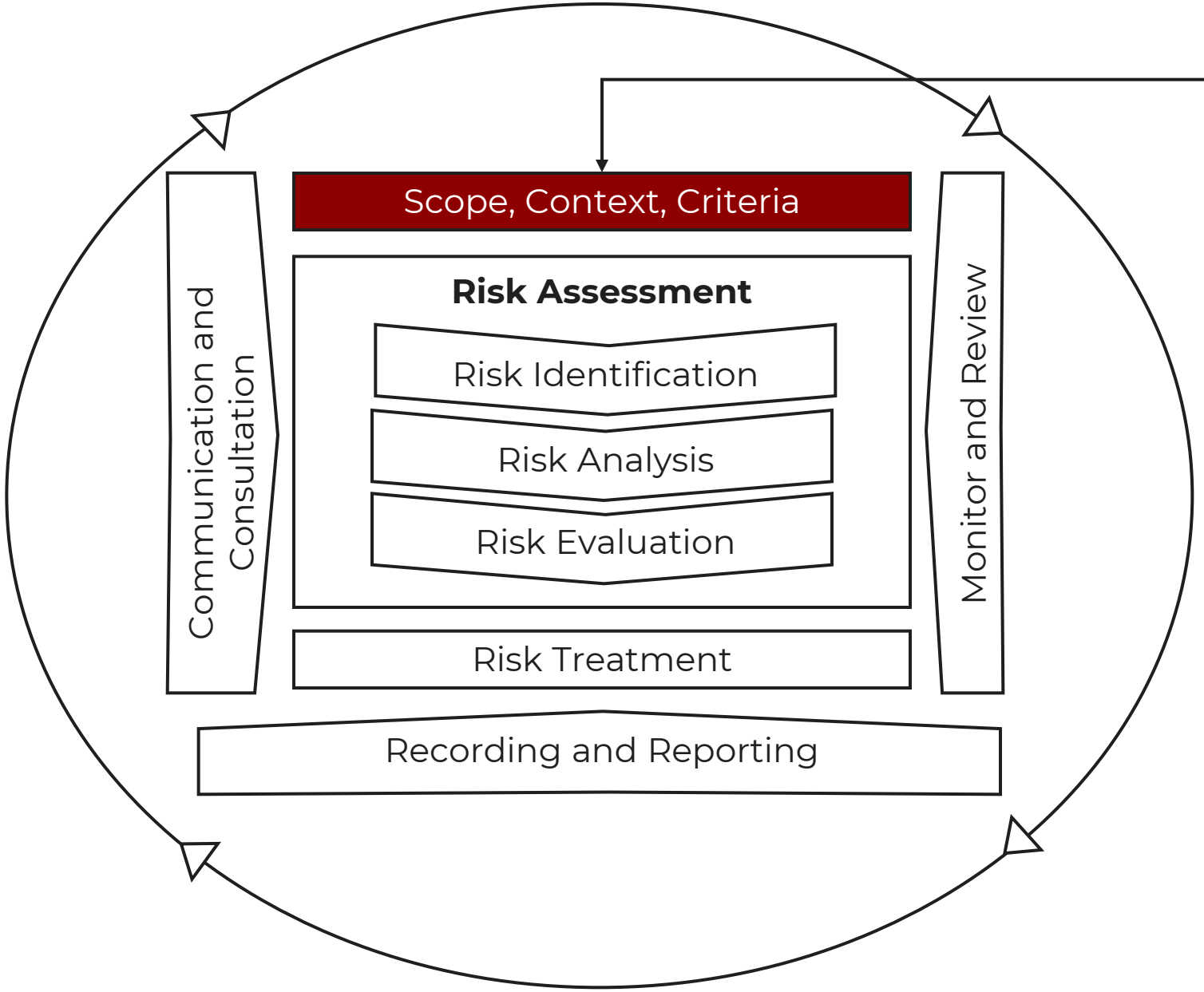
- A chance of losses
- The possibility of unfortunate occurrence
- Occurrence of economic loss
- Probability of something happening that is unwanted and unavoidable without precaution

Understanding Risk Assessment

MSECB

Scope, Context, Criteria





1.7.1 Context Establishment

ISO/IEC 27005, clause 5.1 and ISO/IEC 27000, clauses 3.22 and 3.38

Context establishment means assembling the internal and external context for information security risk management or an information security risk assessment.

External context

External environment in which the organization seeks to achieve its objectives

Note 1 to entry: External context can include the following:

- *the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;*
- *key drivers and trends having impact on the objectives of the organization;*
- *relationships with, and perceptions and values of, external stakeholders.*

Internal context

Internal environment in which the organization seeks to achieve its objectives

Note 1 to entry: Internal context can include:

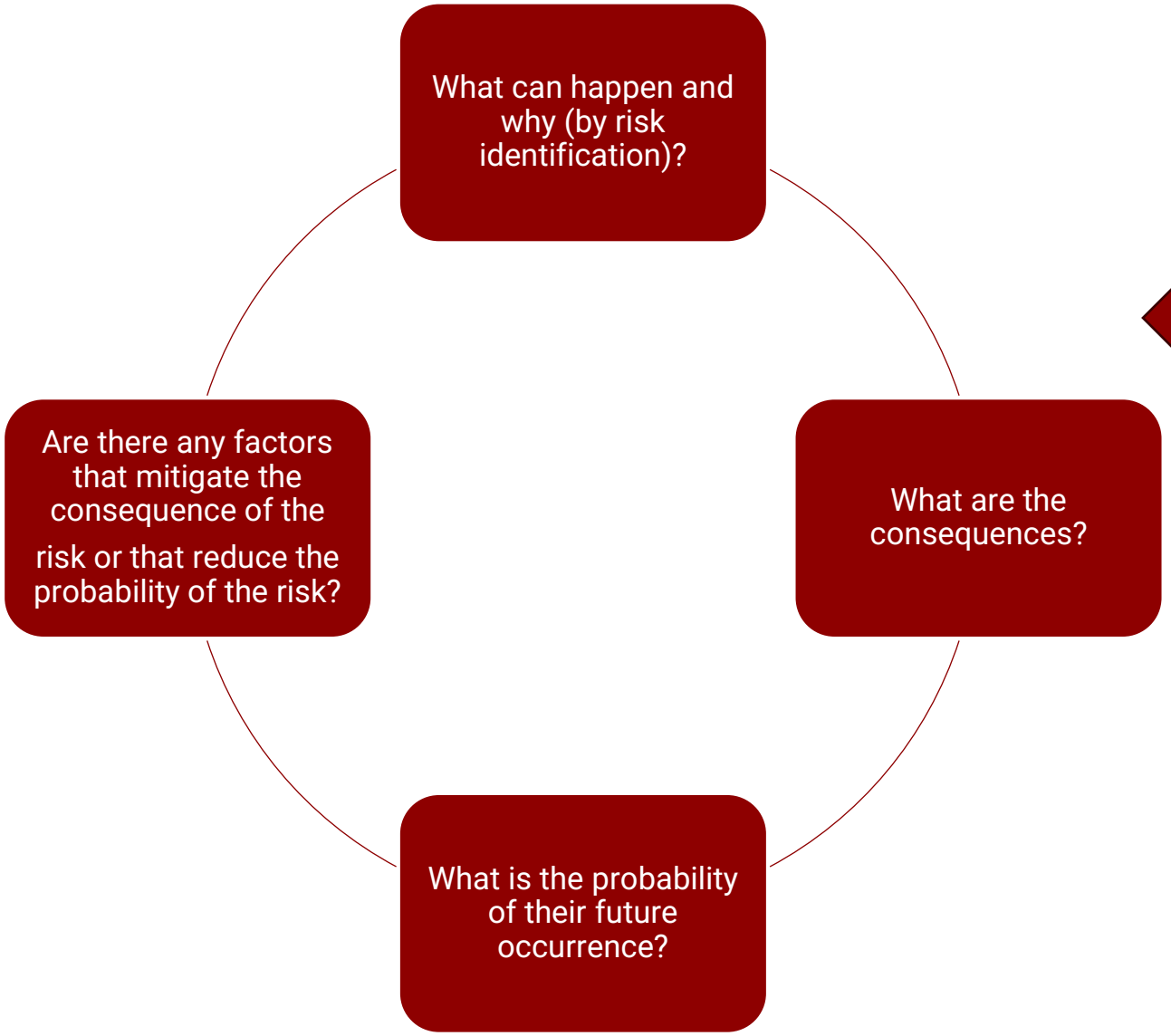
- *governance, organizational structure, roles and accountabilities;*
- *policies, objectives, and the strategies that are in place to achieve them;*
- *the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);*
- *information systems, information flows and decision-making processes (both formal and informal);*
- *relationships with, and perceptions and values of, internal stakeholders;*
- *the organization's culture;*
- *standards, guidelines and models adopted by the organization;*
- *form and extent of contractual relationships.*

Categories of Risk

Examples of Risk

MSECB

What is Risk Assessment?



Risk Assessment is the process of identifying, analyzing, and evaluating risks to the confidentiality, integrity, and availability of information within an organization. This process helps in understanding the nature and extent of risks to ensure that appropriate measures are taken to manage and mitigate these risks.

MSECB

Risk Assessment Steps

I

Risk Identification

Risk Identification is the process of finding, recognizing and recording risks

II

Risk Analysis

Risk analysis consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls. The consequences and their probabilities are then combined to determine a level of risk

III

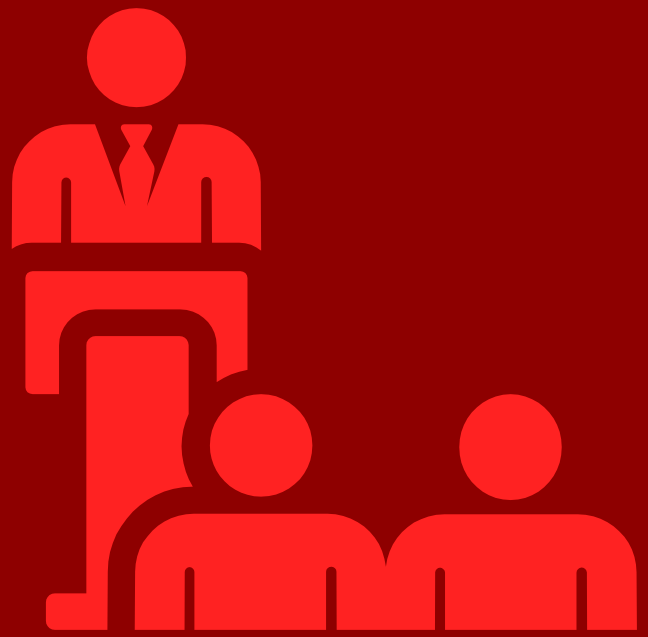
Risk Evaluation

Risk evaluation involves comparing estimated levels of risk with risk criteria defined when the context was established, in order to determine the significance of the level and type of risk

MSECB

Techniques and Methodologies for Risk Assessment

MSECB



1. Qualitative Risk Assessment

This approach uses subjective judgment to assess risks based on their likelihood and impact. It often involves categorizing risks as high, medium, or low.

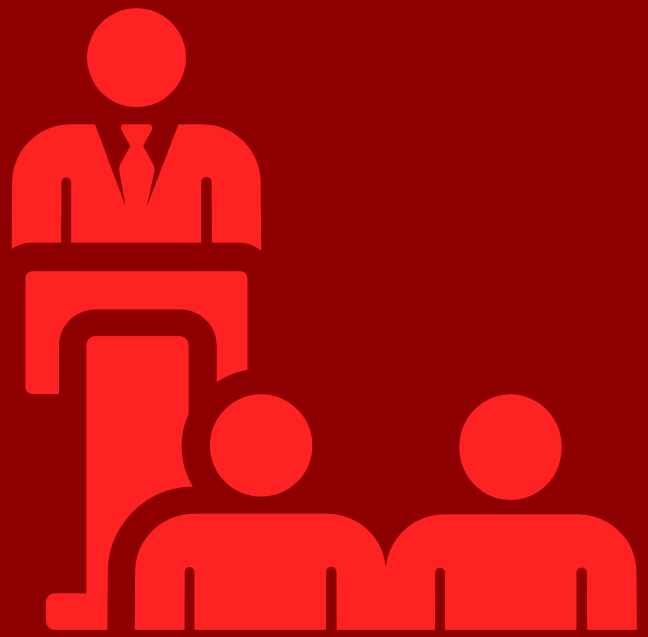
Techniques:

- **Risk Matrix:** A visual tool that helps in prioritizing risks by plotting their likelihood against their impact.
- **SWIFT (Structured What-If Technique):** A brainstorming method that systematically explores potential risks by asking "what if" questions.
- **Expert Judgment:** Leveraging the experience and insights of experts to assess risk levels.

Pros: Simple to use, quick, and useful in the early stages of risk assessment.

Cons: Less precise, dependent on the accuracy of subjective assessments.

MSECB



2. Quantitative Risk Assessment

This approach uses numerical data and statistical methods to evaluate risks, providing more objective results compared to qualitative methods.

Techniques:

- Probability-Impact Matrix
- Monte Carlo Simulation
- Fault Tree Analysis (FTA)

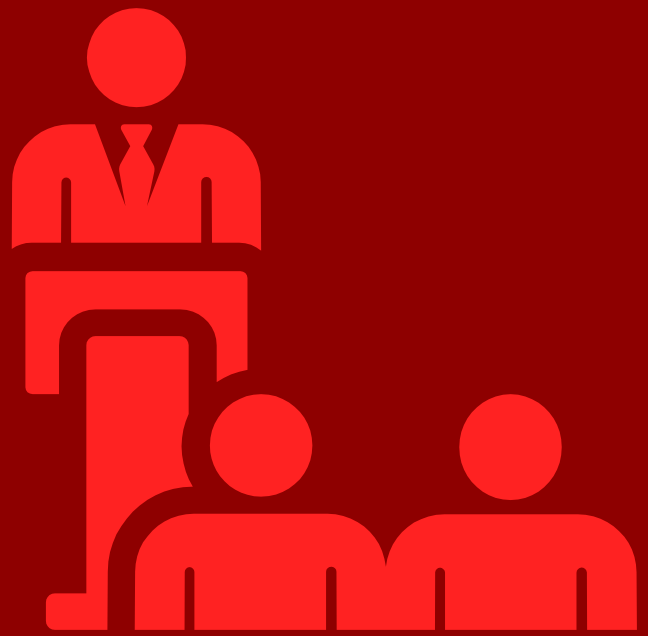
Pros:

Provides a more detailed and precise analysis, useful for making informed decisions.

Cons:

Requires significant data and can be complex to implement.

MSECB



3. Root Cause Analysis (RCA)

Focuses on identifying the underlying causes of risks and issues rather than just their symptoms.

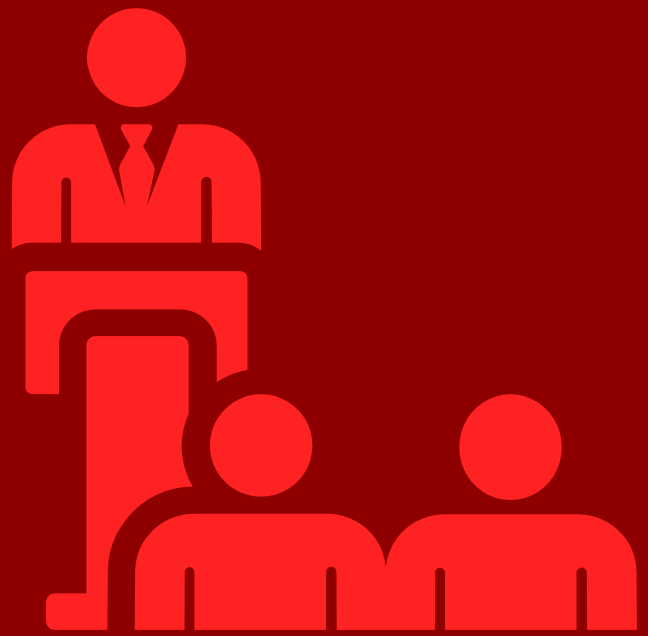
Techniques:

- **5 Whys:** A technique where you ask "why" repeatedly (usually five times) to drill down to the root cause of a problem.
- **Fishbone Diagram (Ishikawa):** A visual tool that categorizes potential causes of problems to identify the root causes.

Pros: Helps in addressing the fundamental issues rather than just surface-level problems.

Cons: May not be effective if not used systematically or if the root cause is complex.

MSECB



4. Scenario Analysis

Involves evaluating different hypothetical scenarios to understand potential risks and their impacts.

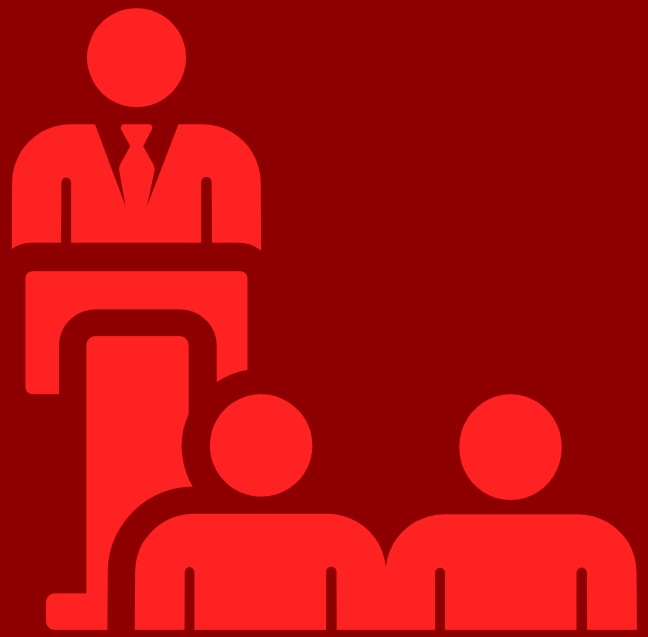
Techniques:

- **Scenario Planning:** Developing and analyzing multiple scenarios to anticipate future risks and prepare appropriate responses.
- **Stress Testing:** Assessing how extreme conditions or events might impact a system or organization.

Pros: Helps in preparing for uncertain future events and understanding potential impacts of various scenarios.

Cons: Scenarios may be based on assumptions that may not hold true.

MSECB



5. Delphi Method

A structured process for collecting and aggregating expert opinions to assess risks.

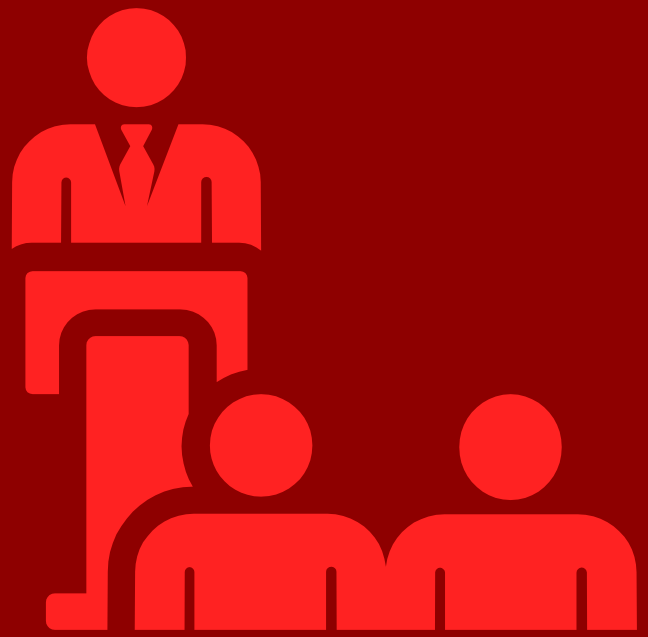
Techniques:

Round-Robin Surveys: Experts answer questionnaires in multiple rounds, with feedback provided between rounds to refine opinions.

Pros: Leverages collective expertise and provides a consensus view.

Cons: Time-consuming and dependent on the availability and expertise of participants.

MSECB



6. Bow-Tie Analysis

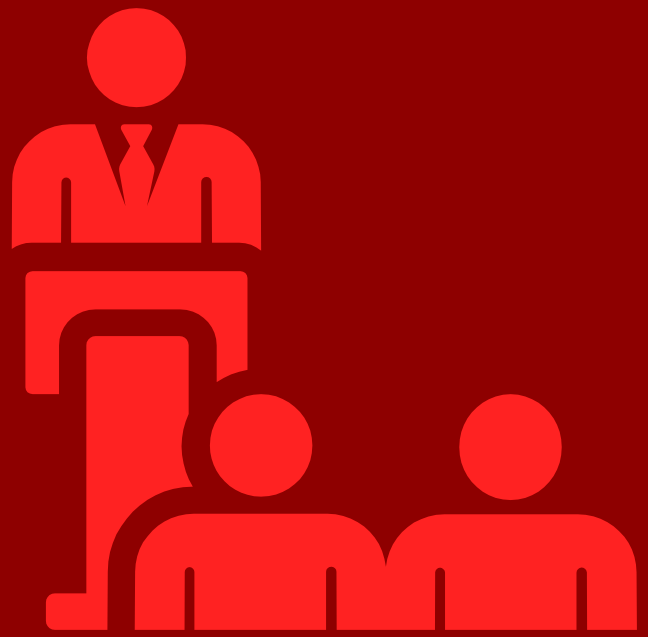
Combines elements of fault tree analysis and event tree analysis to provide a visual representation of risk management.

Techniques:

Bow-Tie Diagram: Visualizes the pathways from potential causes to potential consequences, with control measures in place to mitigate risks.

- **Pros:** Provides a clear and comprehensive view of risk scenarios and mitigation strategies.
- **Cons:** May require significant effort to develop and maintain.

MSECB



7. Hazard and Operability Study (HAZOP)

A systematic technique used mainly in industrial settings to identify hazards and operability issues.

Techniques:

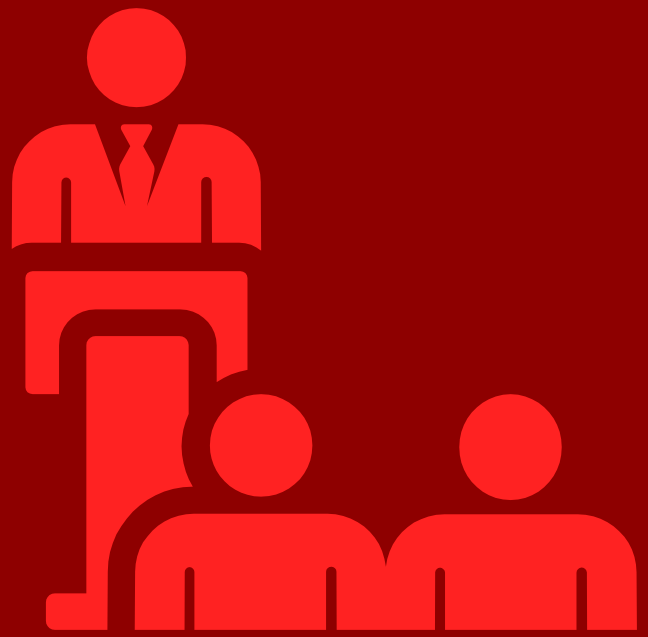
- **HAZOP Study:** A team-based method that involves systematically reviewing process design and operation to identify deviations from the intended design.

Pros: Effective for complex systems and processes, especially in engineering and manufacturing.

Cons: Can be resource-intensive and requires expertise in the process being reviewed.

MSECB

Risk Assessment in ISO/IEC 27001



Actions to Address Risks and Opportunities- General (Clause 6.1.1)

Information Security Risk Assessment (Clause 6.1.2, 6.1.3, 8.2 and 8.3)

MSECB

Different types of information security risk assessment

I

Asset-based risk assessment

This approach focuses on identifying and evaluating risks associated with specific assets within an organization, such as hardware, software, data, and infrastructure. It involves:

- Inventorying and categorizing assets
- Determining the value and criticality of each asset
- Identifying threats and vulnerabilities related to those assets
- Assessing the potential impact if the asset is compromised

II

Process-based risk assessment

This method examines risks within the context of business processes and workflows. It involves:

- Mapping out key business processes
- Identifying information assets involved in each process
- Analyzing potential vulnerabilities and threats at each step
- Assessing how a security incident could impact the process and overall business operations.

III

Context-based risk assessment

This approach takes a broader view, considering the organization's unique environment, including internal and external factors. It involves:

- Evaluating the organization's business objectives and strategy
- Considering industry-specific regulations and compliance requirements
- Analyzing the broader threat landscape and emerging risks
- Assessing how various risk factors interrelate and impact the organization as a whole.

MSECB

Risk Register

Ref	Asset	Threat	Vulnerabilities	Existing Controls	Likelihood	Impact	Risk Score	Risk Level	Treatment option chosen	Proposed control
1	**Mobile phone**	Theft of mobile phone.	Portability of the mobile phones make it susceptible to pilferage.	None	5	3	15	HIGH	Mitigate	Enforcing password protection, implementation of MDM, and remote wipe
		Staff with malicious intent can extract sensitive data.	Data can be copied from email to personal mobile device.	None	3	3	9	MEDIUM	Mitigate	Implementation of Data Loss Prevention tools
		Unathorized user can easily get access to the data contained in the device.	Mobile phones used by staff are not password protected.	None	4	4	16	HIGH	Mitigate	Implement Mobile use policy
2	**Server**	Unauthorised access to the servers	Unrestricted access to physical location of the server	None	5	4	20	HIGH	Mitigate	Implement Physical access control
		Server downtime due to power outage	No back-up power supply	SLA with power supply company	3	4	12	HIGH	Mitigate	Implement backup power supply
		Damage of server equipment due to overheating	Lack of proper cooling mechanism in place	Using fans as cooling devices for the servers	4	4	16	HIGH	Mitigate	Implement HVAC in the server room
3	**Employees**	Social engineering	Inadequate training of staff on security best practice	None	4	4	16	HIGH	Mitigate	Frequent training of staff on security best practices

Risk Assessment | Likelihood | Impact | Risk Matrix

MSECB

Risk Register

Document:	Risk Register : Sample	Project:	Pen Project	Author:	Project Manager	Date:	

This risk Register is take from the "Sample PRINCE2 Pen Project"

Project Name	Pen Project		Risk / Impact
Project No	008		High Risk > € 7,500
Project Manager	Rose Clark		Medium > € 1000
Project Executive	John King		Low Risk < € 1000

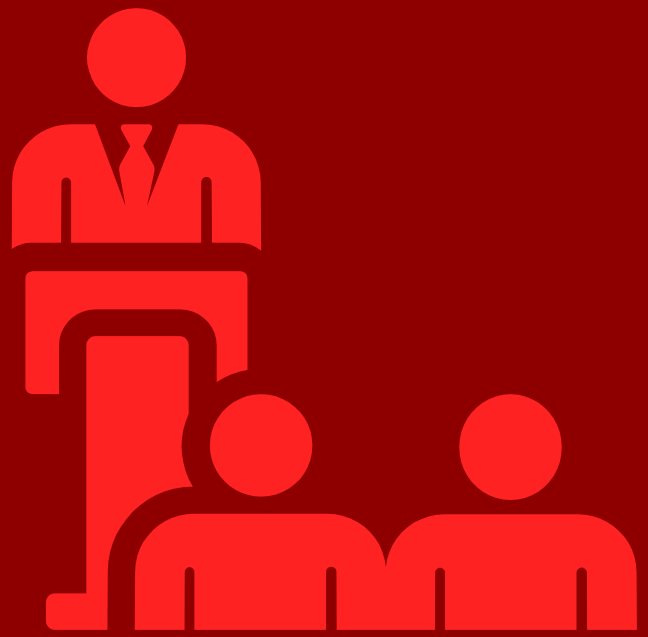
Amount is related to the value of the expected benefits
Expected gain is: €58,400

ID	Risk Author	Date Register	Risk Category	Risk Description	Probability x Impact	Proximity	Response Category	Status	Risk Owner	Risk Actionee
1	P Smith	6/3/13	Ordering	A risk that pens will be delivered 2-4 weeks later which will impact the time of the project	< €1000	Medium	Reduce	Active	P Smith	J Bell
2	S. Kelly	7/3/13	Product	50% users may not like the pens and therefore not keep using them which result in 50% less benefits	€ 29,000	Medium	Reduce	Active	S. Kelly	R Clark
3	S. Kelly	9/3/13	Product	Some sales people may not distribute the pens as intended, therefore the benefits will not be realized for these users	€ 5,600	Medium	Reduce	Active	S. Kelly	S. Kelly

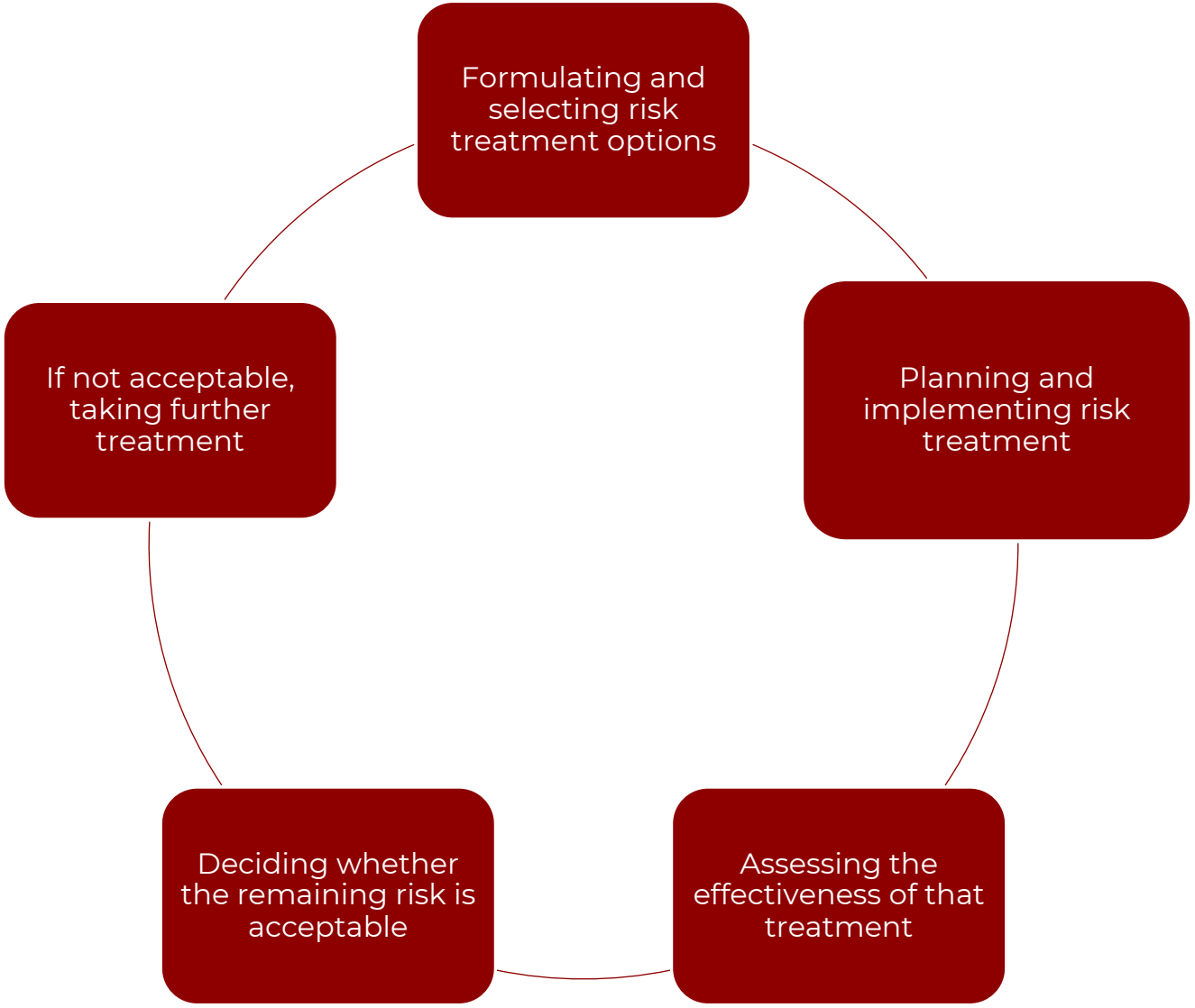
MSECB

Risk Treatment Strategies

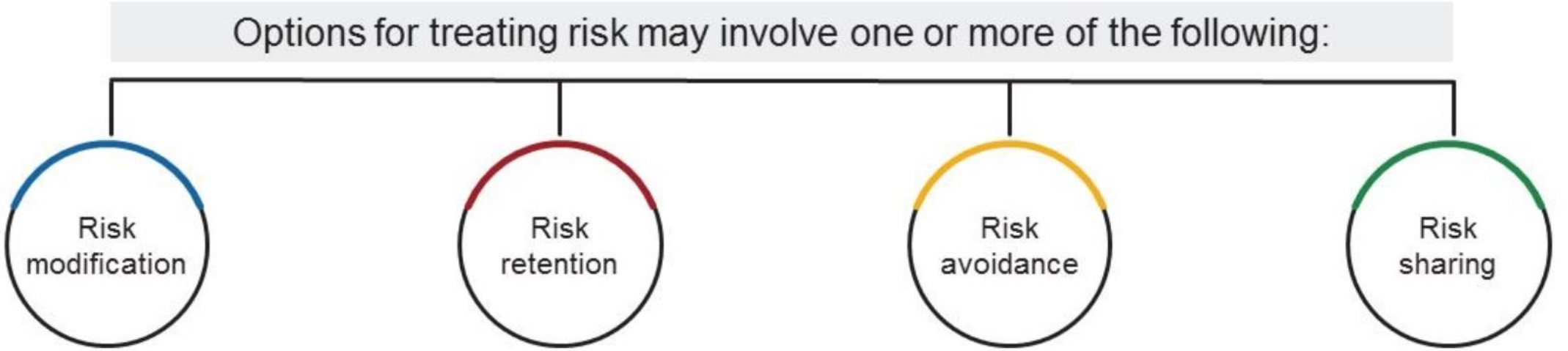
MSECB



What Is Risk Treatment?



Selection of Risk Treatment Options



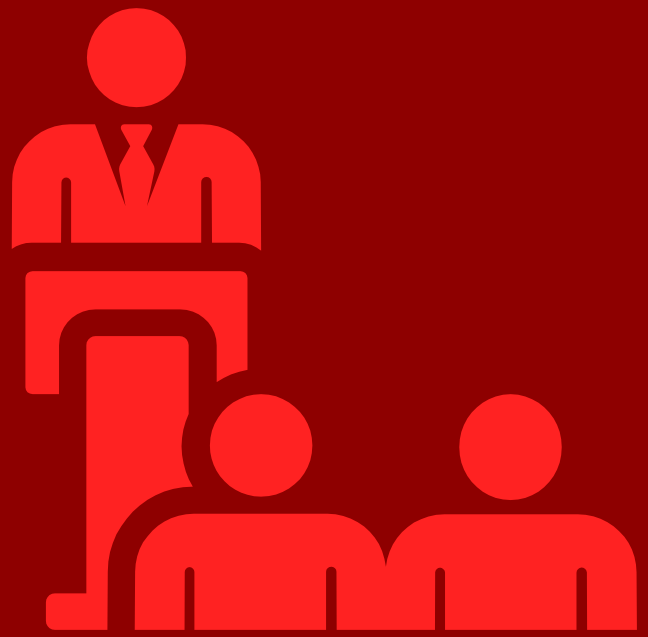
Introduction, removal, or alteration of controls so that residual risk can be considered acceptable

Decision to accept the actual level of risk

Cancellation or modification of an activity or set of activities related to risk

Decision to share risks with external parties (e.g., insurance or outsourcing)

MSECB



Risk Treatment Measures/Steps

- Identifying Risk Treatment Options

The first step in selecting risk treatment measures is to identify and evaluate all possible options, such as avoiding, sharing, modifying, or retaining the risk.

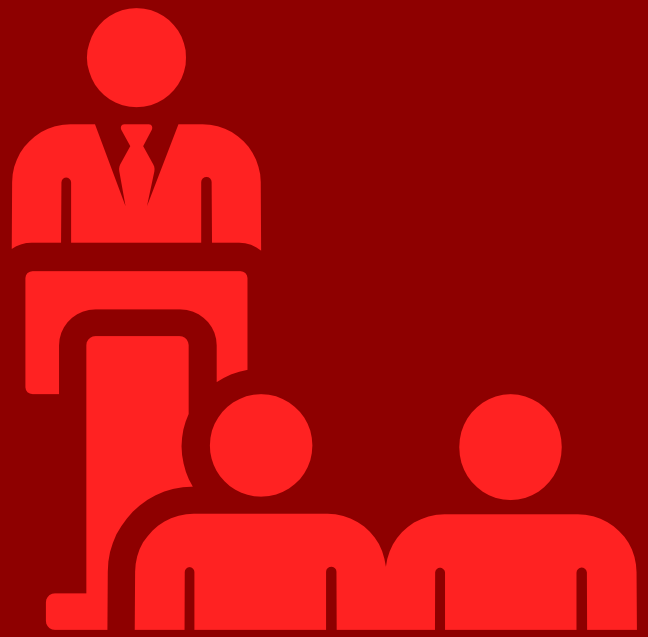
- Cost-Benefit Analysis

After identifying the risk treatment options, it's important to conduct a cost-benefit analysis to determine the most effective and efficient measures that balance the costs and benefits of each option.

- Evaluating Effectiveness

It's crucial to evaluate the effectiveness of the selected risk treatment measures on a regular basis and adjust them as necessary to ensure the continued effectiveness of the measures.

MSECB



Implementing Risk Treatment Measures

- Developing a Risk Treatment Plan

A risk treatment plan is a document that identifies the risks to be treated and outlines the measures to be taken to treat them effectively. A risk treatment plan consists of several components, including identifying risks, assigning responsibilities, setting deadlines, and determining how to measure progress.

- Assigning Responsibility

Once the risk treatment plan has been developed, it is important to assign responsibility for the implementation of each measure. Clear roles and responsibilities must be defined to ensure effective implementation.

- Risk Monitoring and Review

Regular risk monitoring and review is essential to ensure that the risk treatment measures implemented are effective and to identify any new risks that may arise in the future. It helps organizations to be proactive and to prevent risks from becoming major issues.

MSECB

Risk Assessment & Treatment Plan - template

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Risk ID	Risk Owner	Affected Asset	Applicable Threats/Impact description Threat Source: Human; Natural or Environmental	Applicable Vulnerability Description	Control Descriptions	Applicable ISO 27001 Control Clause for Existing Controls	Likelihood	Likelihood Value	C	I	A	Impact Value	Risk Value (Likelihood x Impact)	Priority	RAC	Risk Treatment Option Reduce, Avoid, Accept Transfer

Risk Assessment & Treatment Plan

A	B	C	D	E	F	G	H	I	J	K
Risk Category	Recommended Controlls/Strategies	Post Impact Value	Post Risk Value	Decision	Issue Date	Timeline	Applicable ISO 27001 Control Clause for Recommended Controls	Status	Action Taken	Remarks

MSECB

Risk Management Tools

- Freshservice
- Monday.com
- nTask
- vsRisk Manager
- Corporater
- TimeCamp
- ClickUp
- RamRisk

MSECB

Risk Management Tools

Selecting a Risk Assessment Methodology

Criteria to consider

1. Compatibility of the methodology with the requirements of ISO/IEC 27001
2. Vocabulary of the methodology
3. Software tools that facilitate the use of the methodology
4. Documentation, training, support, and competent personnel available
5. Ease and pragmatic use of the methodology
6. Cost of utilization
7. Materials for comparison (metrics, case studies, etc.)

MSECB

Q&A

MSECB

Thank you for your attention!

Stay updated!

+1 (450) 328-1227

info@msecb.com

www.msecb.com