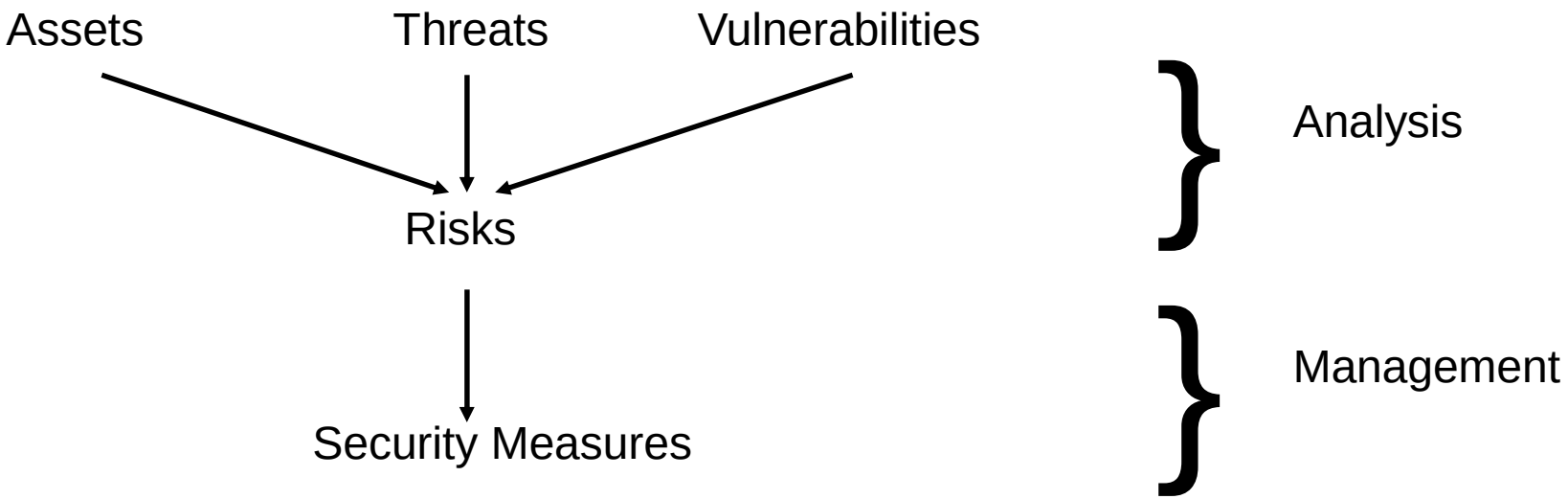
INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS OF KENYA

Credibility . Professionalism . AccountAbility

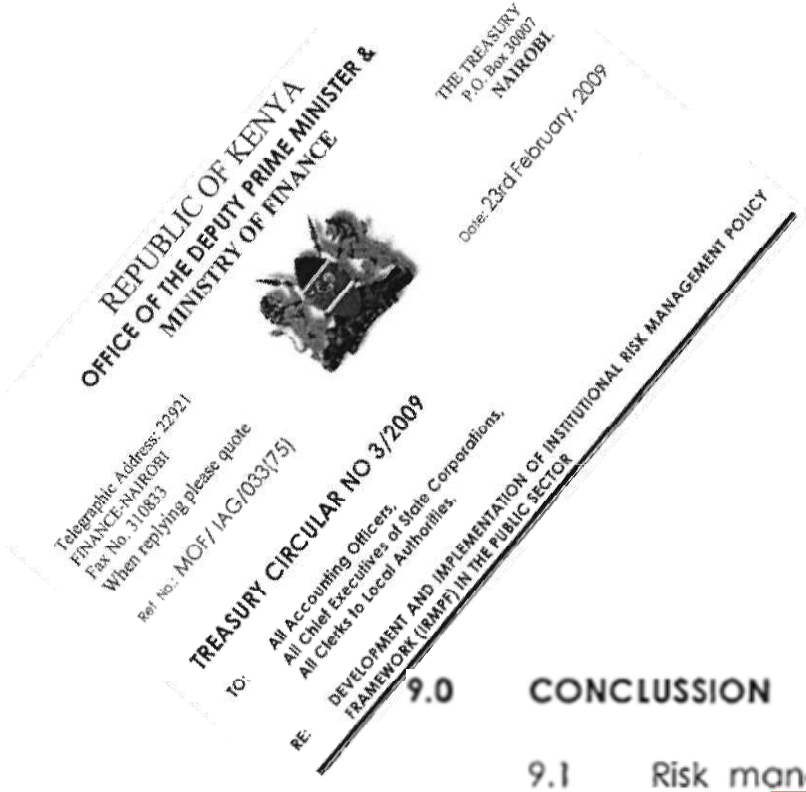
Asset – related risk

Introduction

Risk Analysis and Management Framework



Risk Management Framework



REPUBLIC OF KENYA
OFFICE OF THE DEPUTY PRIME MINISTER &
MINISTRY OF FINANCE

THE TREASURY
P.O. Box 30007
NAIROBI

Telegraphic Address: 22921
FINANCE-NAIROBI
Fax No. 310833
When replying please quote
Ref No.: MOF/ IAG/033(75)

Date: 23rd February, 2009

TREASURY CIRCULAR NO 3/2009

TO: All Accounting Officers,
All Chief Executives of State Corporations,
All Clerks to Local Authorities.

RE: DEVELOPMENT AND IMPLEMENTATION OF INSTITUTIONAL RISK MANAGEMENT POLICY FRAMEWORK (IRMPF) IN THE PUBLIC SECTOR

2.0 ELEMENTS OF AN EFFECTIVE IRMPF

3.0 RISK MANAGEMENT AS A MANAGEMENT TOOL

4.0 ROLES & RESPONSIBILITIES OF ACCOUNTING OFFICERS/CHIEF EXECUTIVES OF STATE CORPORATINS/CLERKS TO LOCAL AUTORITIES

5.0. REQUIREMENTS FOR AN EFFECTIVE RISK MANAGEMENT FRAMEWORK

6.0 FRAUD AND CORRUPTION PREVENTION MECHANISMS

7.0 SOCIAL ACCOUNTABILITY

8.0 ROLE OF INTERNAL AUDITORS IN RISK MANAGEMENT

9.0 CONCLUSSION

9.1 Risk management should be seen as an integral part of strategic and operational activities of all public institutions. In this regard the risk management philosophy must be clearly communicated in policy statements to staff and embedded in the respective strategic plans.

JOSEPH K.KINYUA, CBS
PERMANENT SECRETARY/TREASURY

Definitions - 1

The meanings of terms in this area is not universally agreed.

We will use the following

- **Threat**: Harm that can happen to an asset
- **Impact**: A measure of the seriousness of a threat
- **Attack**: A threatening event
- **Attacker**: The agent causing an attack (not necessarily human)
- **Vulnerability**: a weakness in the system that makes an attack more likely to succeed
- **Risk**: a quantified measure of the likelihood of a threat being realised

Definitions - 2

- **Risk Analysis** involves the identification and assessment of the levels of risk, calculated from the
  - Values of assets
  - Threats to the assets
  - Their vulnerabilities and likelihood of exploitation
- **Risk Management** involves the identification, selection and adoption of security measures justified by
  - The identified risks to assets
  - The reduction of these risks to acceptable levels

Overview

- The main risks that primarily contribute to an organization's failure to optimally manage their assets include:

1) not knowing what they have;
2) over or under maintenance;
3) improper operation;
4) improper risk management; and
5) sub-optimized asset management systems.

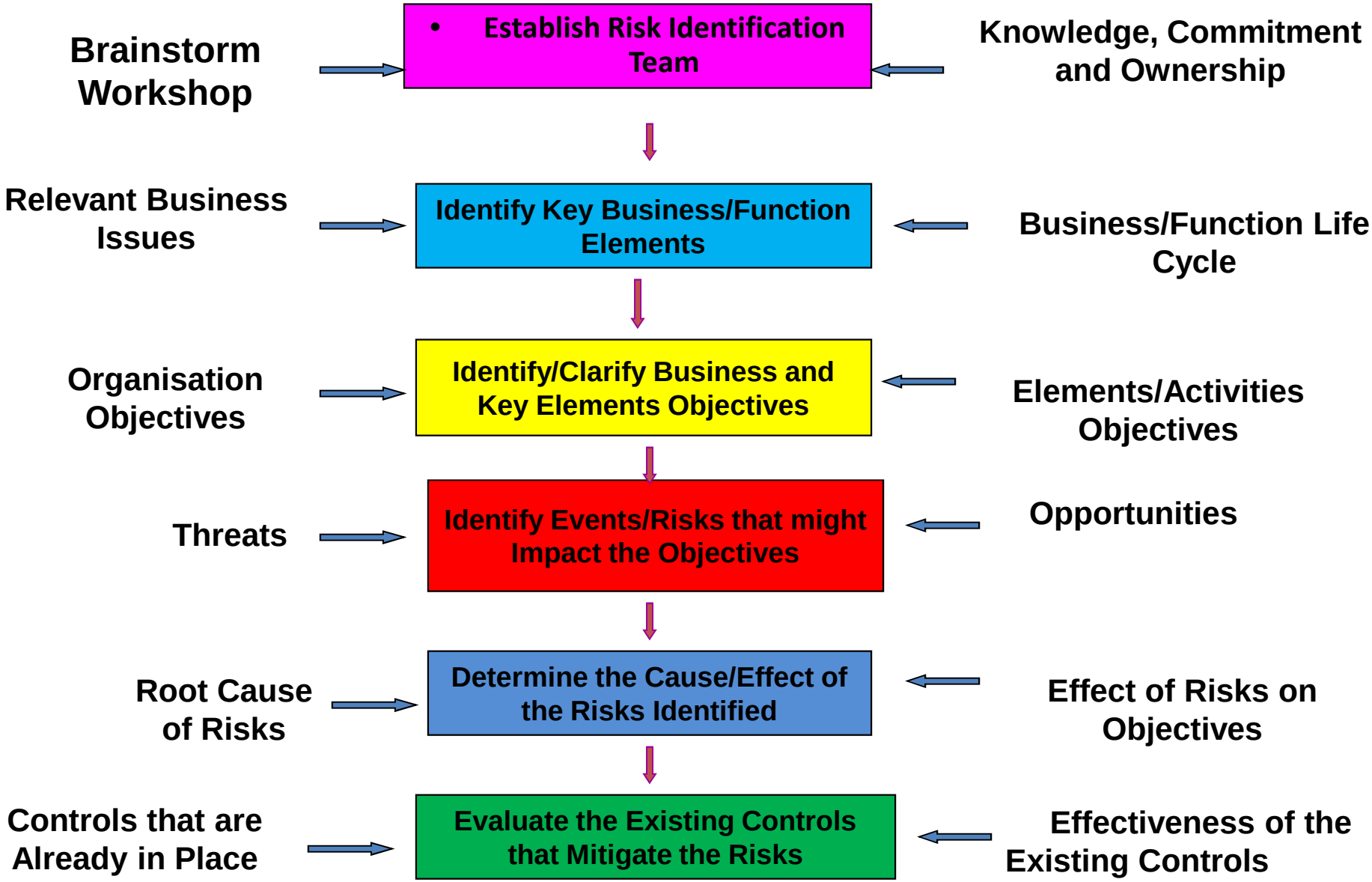
Asset management is an integrated approach to optimizing the life cycle of your assets beginning at conceptual design, through to usage, decommissioning and disposal.

Effective risk management in asset management performance does not lie only in avoiding the pitfalls, but in turning each and every one of these opportunities to fail into an opportunity to excel

Overview

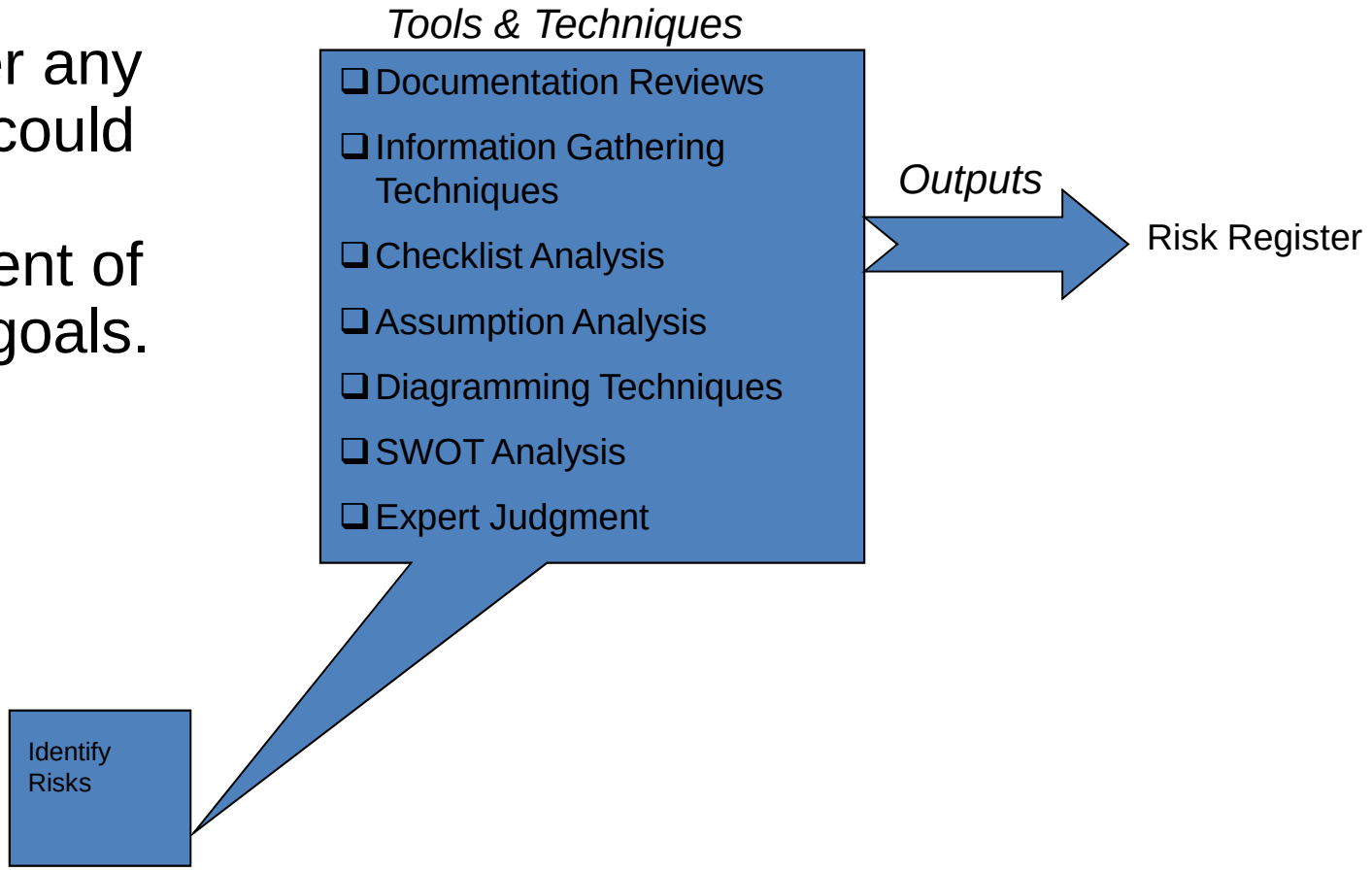
- Weather & Climate Change poses a particular risk for asset owners and operators in all sectors.
- Both have the potential to seriously affect the availability and/or reliability of assets and the goods and services that depend on them.
- In the immediate term, operations can be degraded by a range of common weather events, such as heavy rain leading to the flooding of electricity sub-stations; snow and frost preventing construction works; high winds bringing down overhead power lines and high temperatures causing rails to buckle.

THE RISK IDENTIFICATION PROCESS



Risk Identification

- To uncover any risks that could prohibit achievement of business goals.



Risk Identification

Information Gathering Techniques

- Brainstorming
- Delphi technique
- Interviewing
- Root cause identification
- Strengths, weaknesses, opportunities, and threats (SWOT) analysis

Risk Register

- The main output of the risk identification process is a list of identified risks and other information needed to begin creating a risk register.
- A **risk register** is:
  - A document that contains the results of various risk management processes and that is often displayed in a table or spreadsheet format.
  - A tool for documenting potential risk events and related information.
- **Risk events** refer to specific, uncertain events that may occur to the detriment or enhancement of the project.

Risk Register Contents

- An identification number for each risk event.
- A rank for each risk event.
- The name of each risk event.
- A description of each risk event.
- The category under which each risk event falls.
- The root cause of each risk.
- Triggers for each risk; **triggers** are indicators or symptoms of actual risk events.
- Potential responses to each risk.
- The **risk owner** or person who will own or take responsibility for each risk.
- The probability and impact of each risk occurring.
- The status of each risk.

Risk Identification

Sample Risk Register

No.	Rank	Risk	Description	Category	Root Cause	Triggers	Potential Responses	Risk Owner	Probability	Impact	Status
R44	1										
R21	2										
R7	3										

Goals of Risk Analysis

- All assets have been identified
- All threats have been identified
  - Their impact on assets has been valued
- All vulnerabilities have been identified and assessed

Problems of Measuring Risk

Businesses normally wish to measure in money, but

- Many of the entities do not allow this
  - Valuation of assets
    - Value of data and in-house software - no market value
    - Value of goodwill and customer confidence
  - Likelihood of threats
    - How relevant is past data to the calculation of future probabilities?
      - The nature of future attacks is unpredictable
      - The actions of future attackers are unpredictable
  - Measurement of benefit from security measures
    - Problems with the difference of two approximate quantities
      - How does an extra security measure affect the probability of attack?

Risk Levels

- Precise monetary values give a false precision
- Better to use levels, e.g.
  - High, Medium, Low
    - High: major impact on the organisation
    - Medium: noticeable impact (“material” in auditing terms)
    - Low: can be absorbed without difficulty
  - 1 - 10
- Express money values in levels

Risk Analysis steps

- Decide on scope of analysis
  - Set the boundary
- Identification of assets & business processes
- Identification of threats and valuation of their impact on assets (*impact valuation*)
- Identification and assessment of vulnerabilities to threats
- Risk assessment

Risk Analysis – Defining the Scope

- Draw a context diagram
- Decide on the boundary
- Make explicit assumptions about the security of assets
  - Verify them!

Risk Analysis – Impact Valuation

Identification and valuation of threats - for each group of assets

- Identify threats, e.g. for stored data
  - Loss of **confidentiality**
  - Loss of **integrity**
  - Loss of **completeness**
  - Loss of **availability** (Denial of Service)
- For many asset types the only threat is loss
- Assess impact of threat
  - Assess in levels, e.g High-Medium-Low or 1 - 10
  - This gives the valuation of the asset in the face of the threat

Risk Analysis – Process Analysis

- Every company or organisation has some processes that are critical to its operation
- The criticality of a process may increase the impact valuation of one or more assets identified

So

- Identify critical processes
- Review assets needed for critical processes
- Revise impact valuation of these assets

Risk Analysis – Risk Equation

Risk = Vulnerability x Threat x Impact
*Probability

- Vulnerability = An ***error or a weakness*** in the design, implementation, or operation of a system.
- Threat = An ***adversary*** that is motivated to exploit a system vulnerability and is capable of doing so
- Impact = the ***likelihood*** that a vulnerability will be exploited or that a threat may become ***harmful***.
- *Probability = ***likelihood*** already factored into ***impact***.

Risk Analysis – Types of risk

- **Strategic** – *Goals of the Organization*
- **Operational** – *Processes that Achieve Goals*
- **Financial** – *Safeguarding Assets*
- **Compliance** – *Laws and Regulations*
- **Reputational** – *Public Image*

Risk Analysis – Responses to risk

Severity

High	Transfer	Avoid
Low	Accept	Accept/Transfer
	Low	*High*

Frequency

Responses to Risk

Responses to risk

- **Avoid** it completely by withdrawing from an activity
- **Accept** it and do nothing
- **Reduce** it with security measures

Security Measures

Possible security measures

- Transfer the risk, e.g. insurance
- Reduce vulnerability
  - Reduce likelihood of attempt
    - e.g. publicise security measures in order to deter attackers
    - e.g. competitive approach - the lion-hunter's approach to security
  - Reduce likelihood of success by preventive measures
    - e.g. access control, encryption, firewall
- Reduce impact, e.g. use fire extinguisher
- Recovery measures, e.g. restoration from backup

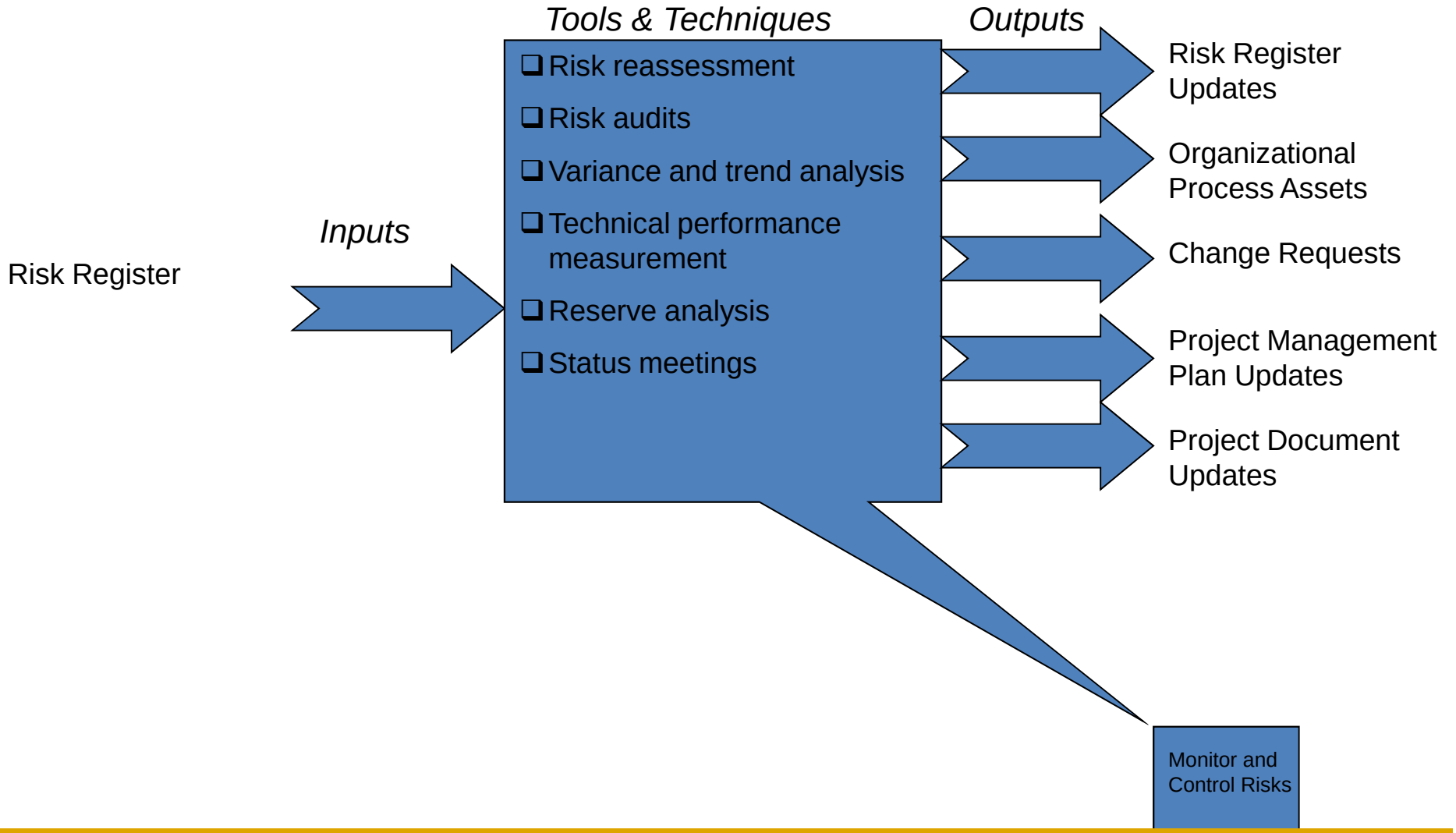
Risk Management

- Identify possible security measures
- Decide which to choose
  - Ensure complete coverage with confidence that:
    - The selected security measures address all threats
    - The results are consistent
    - The expenditure and its benefits are commensurate with the risks

Iterate

- Adding security measures changes the system
  - Vulnerabilities may have been introduced
- After deciding on security measures, revisit the risk analysis and management processes
  - e.g. introduction of encryption of stored files may remove the threat to Confidentiality but introduce a threat to Availability
    - What happens if the secret key is lost?

Monitor and Control Risks



Problems of Risk Analysis and Management

- Lack of precision
- Volume of work and volume of output
- Integrating them into a ”normal” development process

Contingency Planning & Resilience Analysis

- The resilience of any organisation or its assets is essential to its operation.
- Resilience is the ability of a system or organisation to withstand and recover from adversity.
- To become resilient to unplanned and unexpected events, it is essential that a full awareness of the critical points of an organisation and its assets is captured.

Contingency Planning & Resilience Analysis

Step 1 understand the organisation by completing a threat and vulnerability study (sometimes referred to as a Business Impact Analysis), looking at the entirety of the asset against all potential threats faced. This will need to be linked to the relevant Risk Assessment & Management processes to identify the key areas of vulnerability which need to be addressed.

Step 2 determine the strategy to be adopted, looking at the risk assessment process and deciding processes to follow.

Step 3 develop and implement the response, introducing identified mitigations where required and developing and implementing detailed Contingency Plans.

Step 4 regularly Test / Exercise, Maintain and Review the mitigations and plans and ensure that the responses are still fit for purpose and feed outcomes in the continual review process.

Conclusion

Risk Management System

Can **NOT**

- Predict future
- Identify business opportunities
- Be always right!

Risk Management System **Can**

- Predict loss, given event
- Identify most dangerous scenarios
- Recommend how to change risk profile