

The Risk Management Process

ISO 31000:2018



Day 2: Session 2

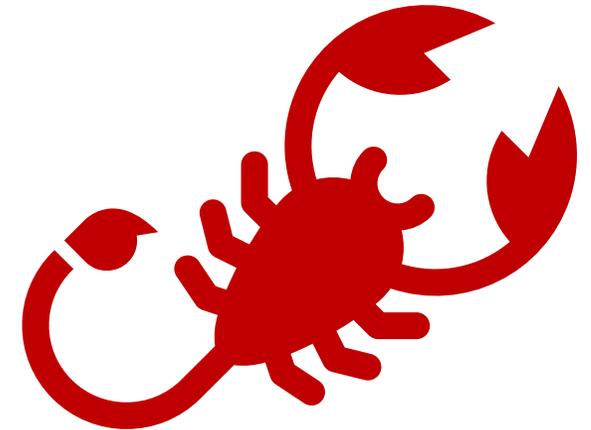
Mustapha B Mugisa, Mr. Strategy



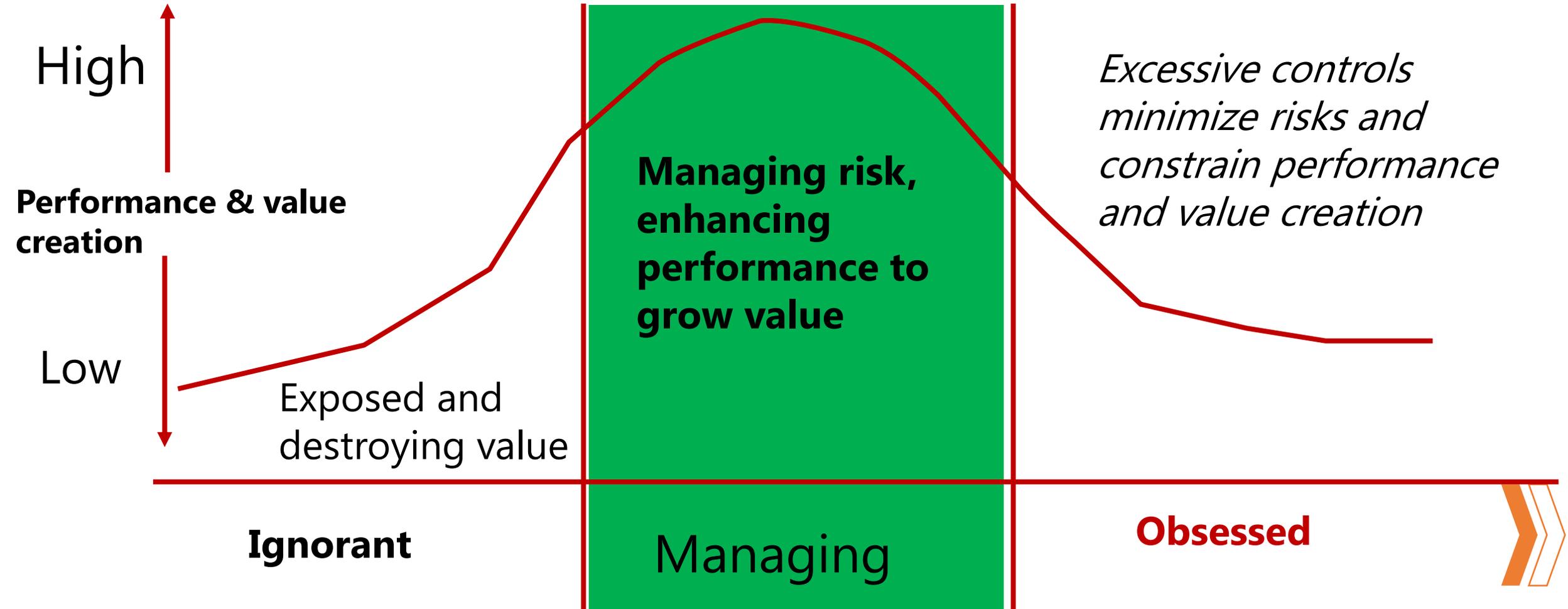
What is “Risk”?

In ISO 31000:2018, risk is defined as:

**The effect of
uncertainty on your
objectives.**



The essence of risk management



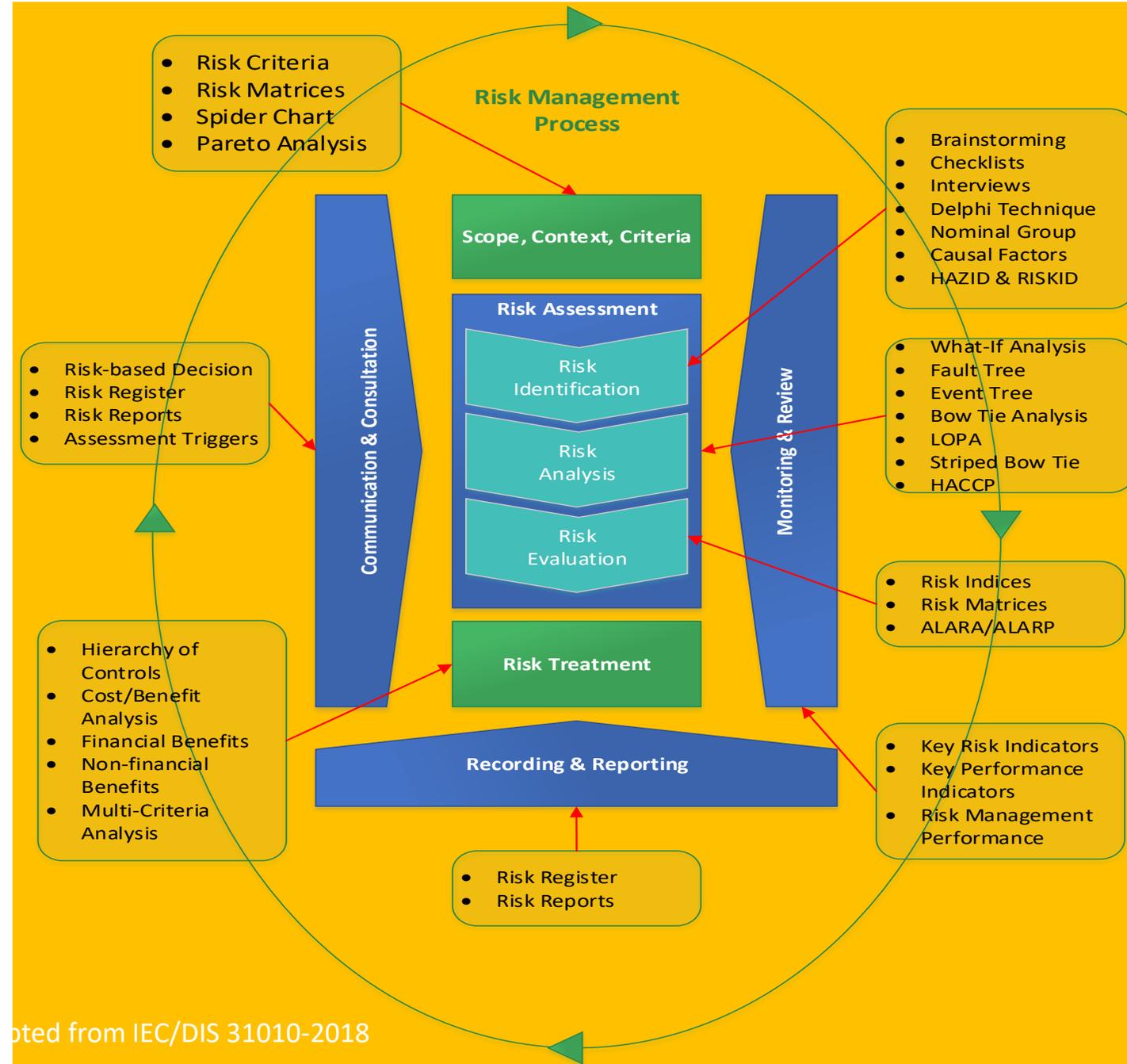
Test your knowledge... give brief answers...

1. What is risk management? What factors of risk are addressed by managing risk?
2. What is risk avoidance? Give an example.
3. Describe the reduction of risk.
4. Describe risk minimization?
5. Describe transfer of risk?



The ISO 31000 Risk Management Process

- It's a continuous process
- There is a logical flow to the process
- An organization can implement risk management at any part of the organization and at any part of the cycles a continuous process



Step 1: Establish scope, context & criteria



01

Outcome:

- 1.1 Risk universe (scope)
- 1.2 Objectives at risk (context)
- 1.3 Risk appetite (risk criteria)
- 1.4 Risk matrix (impact x likelihood)
- 1.5 Risk classification (H, M, L)



Step 2: Risk assessment – 2.1) Risk identification



2.1



Outcome – identify events that could happen...

2.1.1 What could happen? To what? E.g Fire outbreak

2.1.3 How could it happen? E.g Electrical malfunction

2.1.3 Where could it happen? E.g Stores

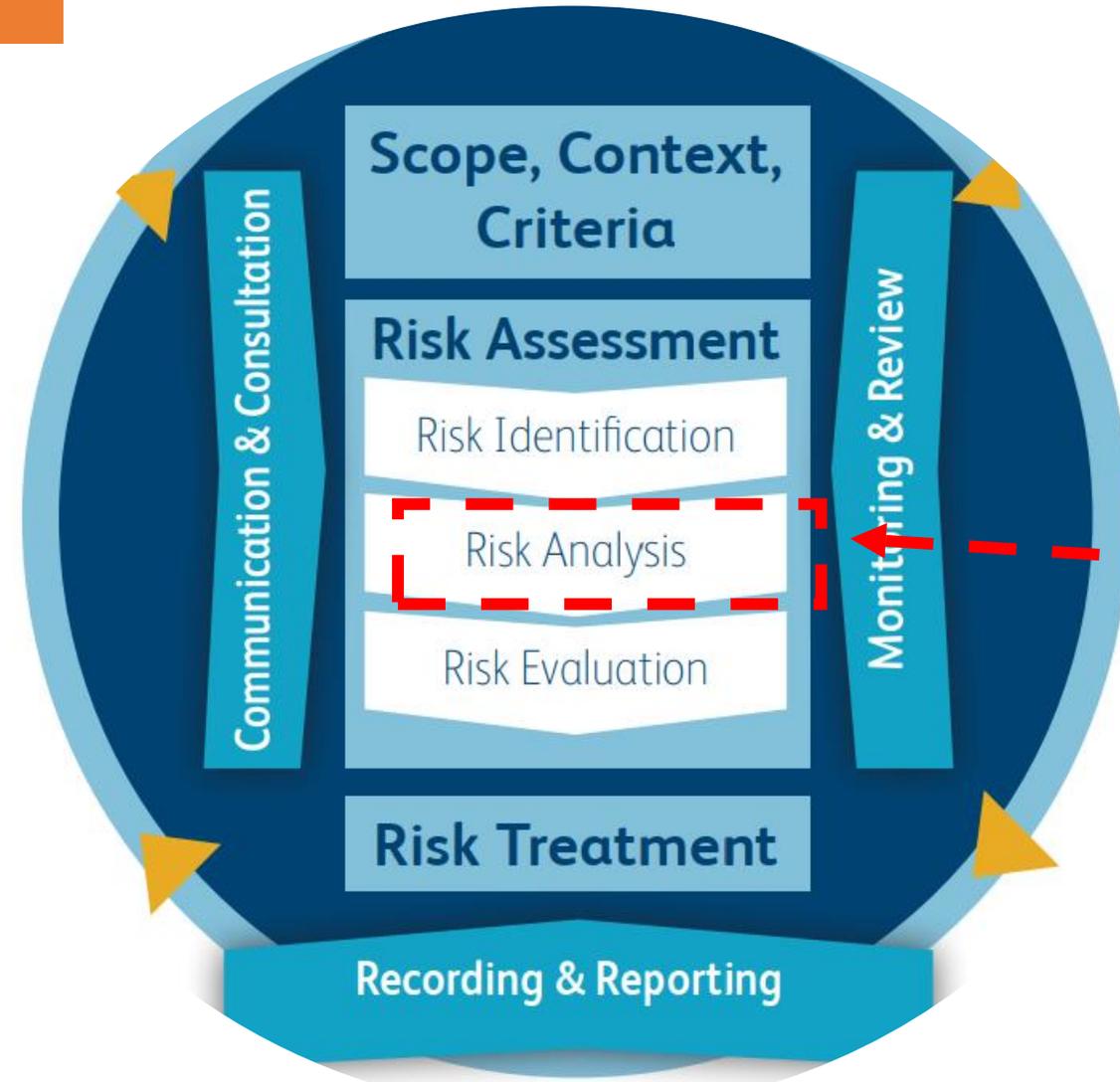
2.1.4 Why might it happen? E.g Unattended kettle left on

2.1.5 Who can influence this event? E.g Stores Manager

2.1.6 What can we do to prevent it? E.g No unattended kettles !



Step 2: Risk assessment – 2.2) Risk analysis



2.2



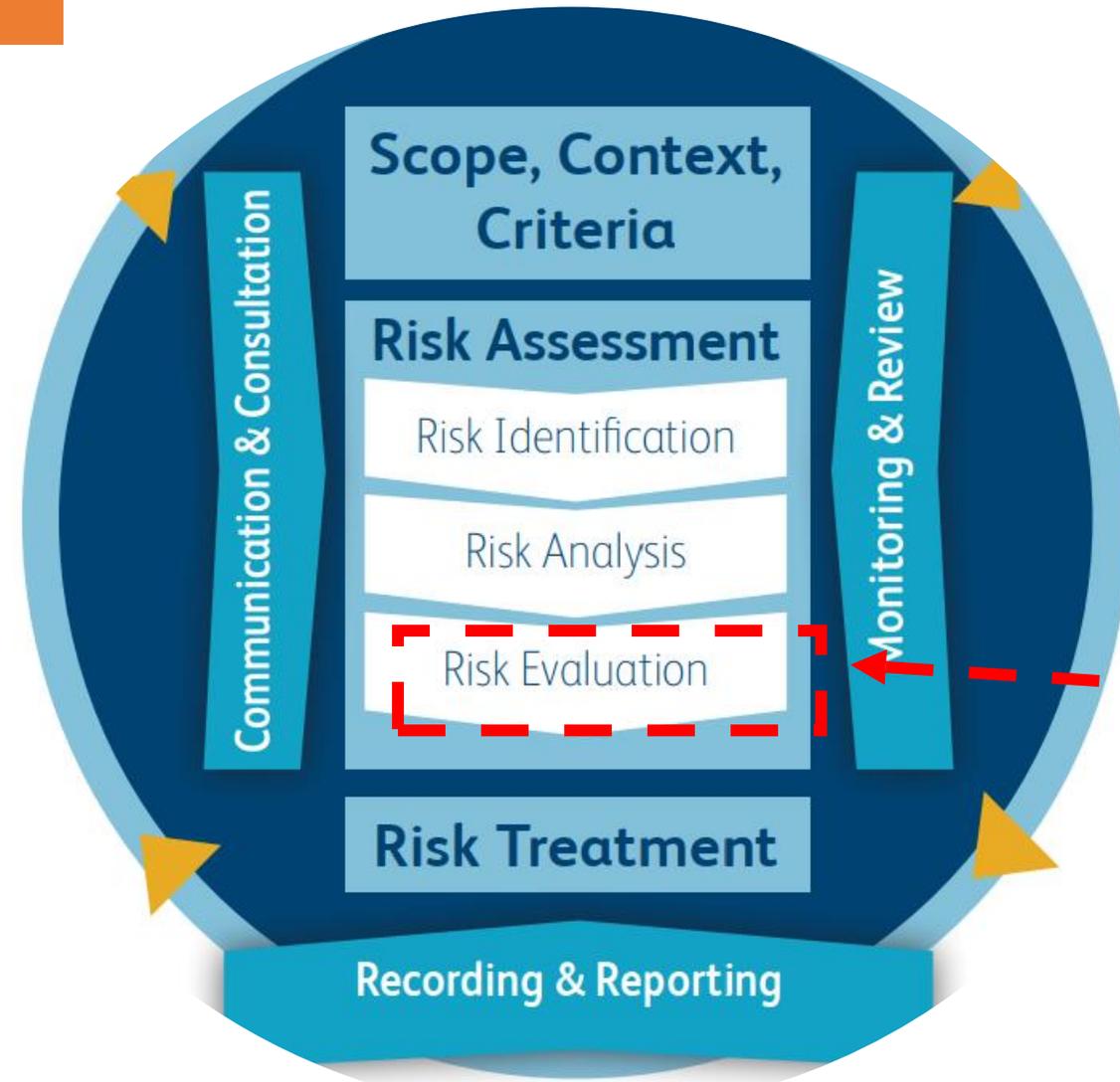
Outcome – the likelihood and impact of events

2.2.1 What might be the impact? E.g Loss of all records

2.2.2 What is the likelihood of the event? E.g Almost certain, more than 75% chances of occurring

2.2.3 How effective are existing controls? E.g  Not effective. More controls needed...

Step 2: Risk assessment – 2.3) Risk evaluation



2.3



Outcome – Which risk is bigger?

2.3.1 Which are our top risks? (rank risks)

2.3.2 Are risks within our established risk appetite? Yes or No?



Step 3: Risk treatment



3

Outcome



- 3.1 What are risk treatment strategy?
- 3.2 Are controls effective?
- 3.3 Is the risk adequately managed?
- 3.4 On-going risk monitoring (what are KRIs)
- 3.5 Do we need further risk treatment?
- 3.6 Responsibilities for risk treatment?



Step 4: Risk recording and treatment



4

Outcome

- 4.1 Risk register
- 4.2 Risk map
- 4.3 Risks after controls report
- 4.4 Risk implementation plan
- 4.5 On-going risk assurance plan



Test your knowledge...

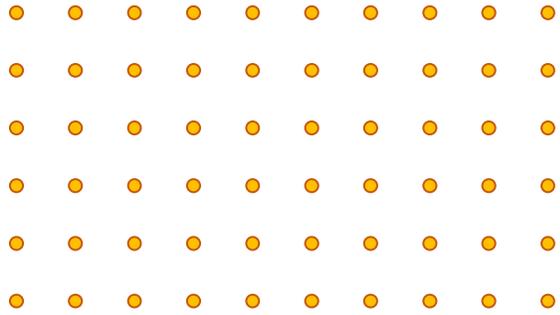
6. Describe risk elimination.
7. Discuss the relationship between avoidance and elimination.
8. Give one reason why do we do not transfer all risks by using insurance.
9. Name one way in which the Government is involved in risk reduction.
10. Name one way to manage the risk to items that are susceptible to water damage.
11. How does the risk management process start?
12. Name two items covered in a risk management statement



Test your knowledge...

13. Name two items covered in a risk management statement.
14. Who is responsible for compiling the risk management statement?
15. How do you decide on items of priority? What factors are taken into account when deciding priority?
16. What is the cost of insurance called?
17. How is risk reduction or minimisation used in the process of risk management?
18. What is a risk management statement?





Ends...

summitFORENSICS
Know the Truth. Transform.

