# Risk Management Basics - ISO 31000 Standard

**Louis Kunimatsu, CRISC**
IT Security & Strategy,
Ford Motor Company

**Risk Management Basics - ISO 31000 Standard**

1. Risk Management Basics
2. ISO 31000 – Risk Management Principles and Guidelines

# Risk Management Basics

Organizational objectives are influenced by internal and external factors which create uncertainty in achieving those objectives. The effect of this uncertainty is "risk" to the organization's objectives.

Unlike *Risk Elimination* (approach of military and law enforcement) which seeks to remove all risk; *Risk Management* is the coordinated activities to direct and control an organization with regard to risk.

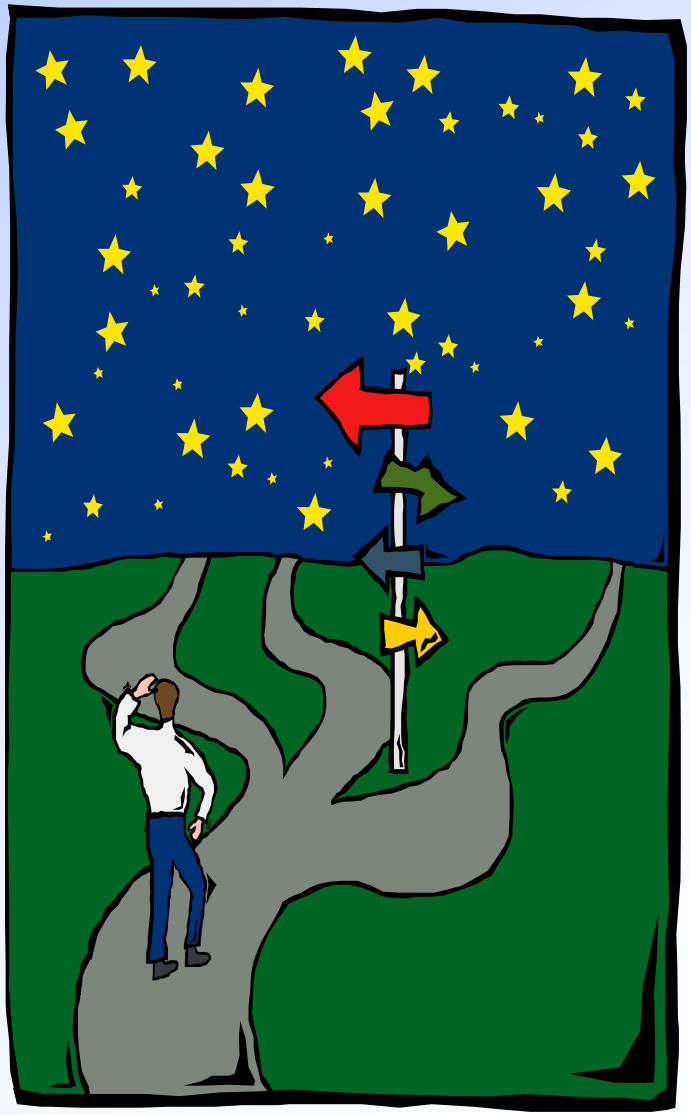
Risk Management allows for multiple risk responses dependent upon evaluation and analysis of risk.

**RISK = Negative IMPACT to objectives X LIKELIHOOD of occurrence.**

# Risk Management Basics

**Risk Responses:**

1. **MITIGATE** - corrective action to eliminate or reduce IMPACT or LIKELIHOOD
2. **AVOID** - Cease activity to eliminate risk
3. **TRANSFER** - Shift IMPACT to another entity
4. **ACCEPT** - No corrective action. Document acceptance decision and monitor



# ISO 31000: Risk management — Principles and guidelines

- Published in 2009, to provide "principles & generic guidelines on risk management"
- "…can be applied to any type of risk, whatever its nature, whether having positive or negative consequences"
- "…not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes,.."
- "…not intended for the purpose of certification"

# ISO 31000: Principles, Framework & Process

**PRINCIPLES**

a) Creates value

b) Integral part of organizational processes

c) Part of decision making

d) Explicitly addresses uncertainty

e) Systematic, structured & timely

f) Based on the best available information

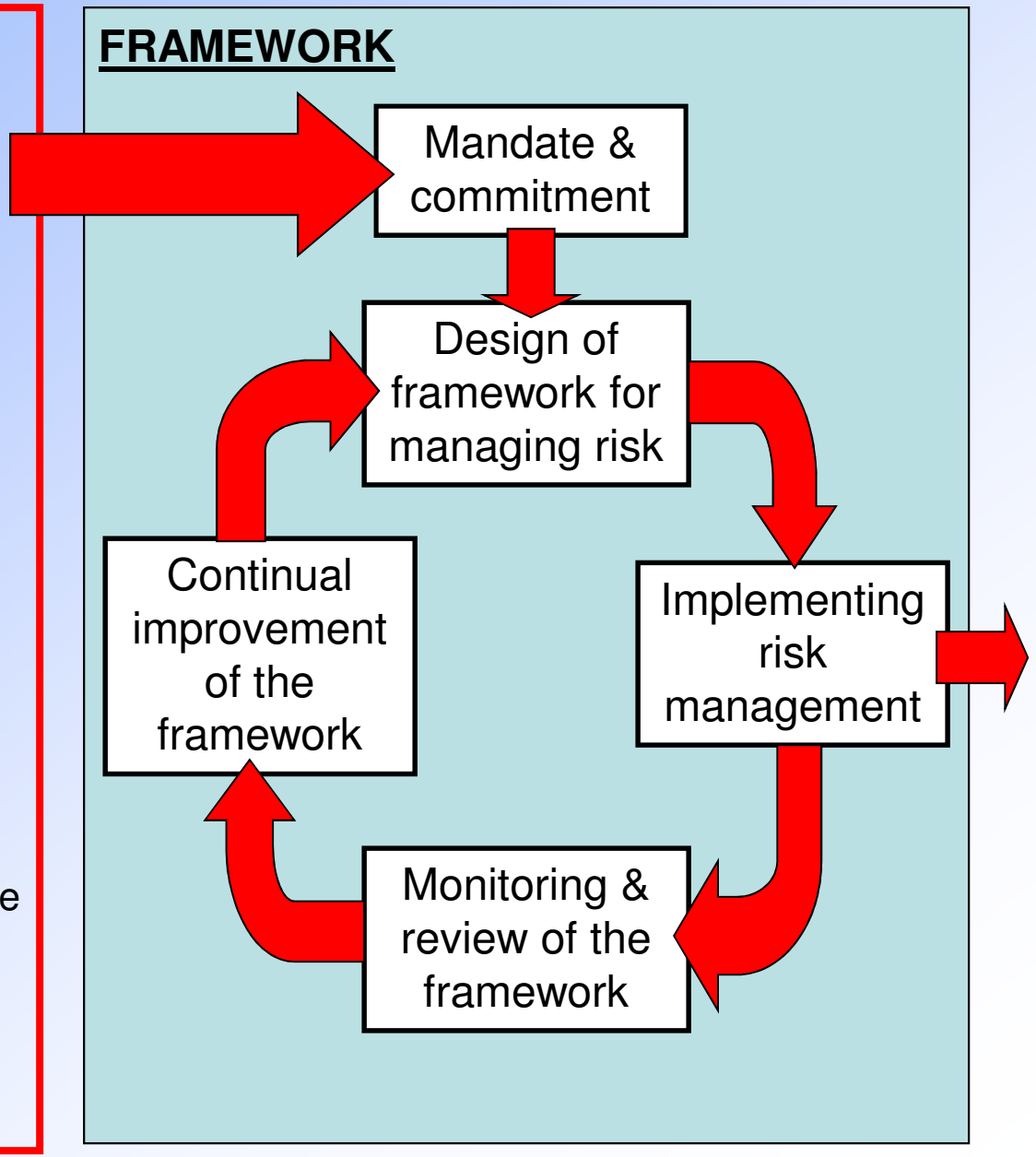
g) Tailored

h) Takes human & cultural factors into account

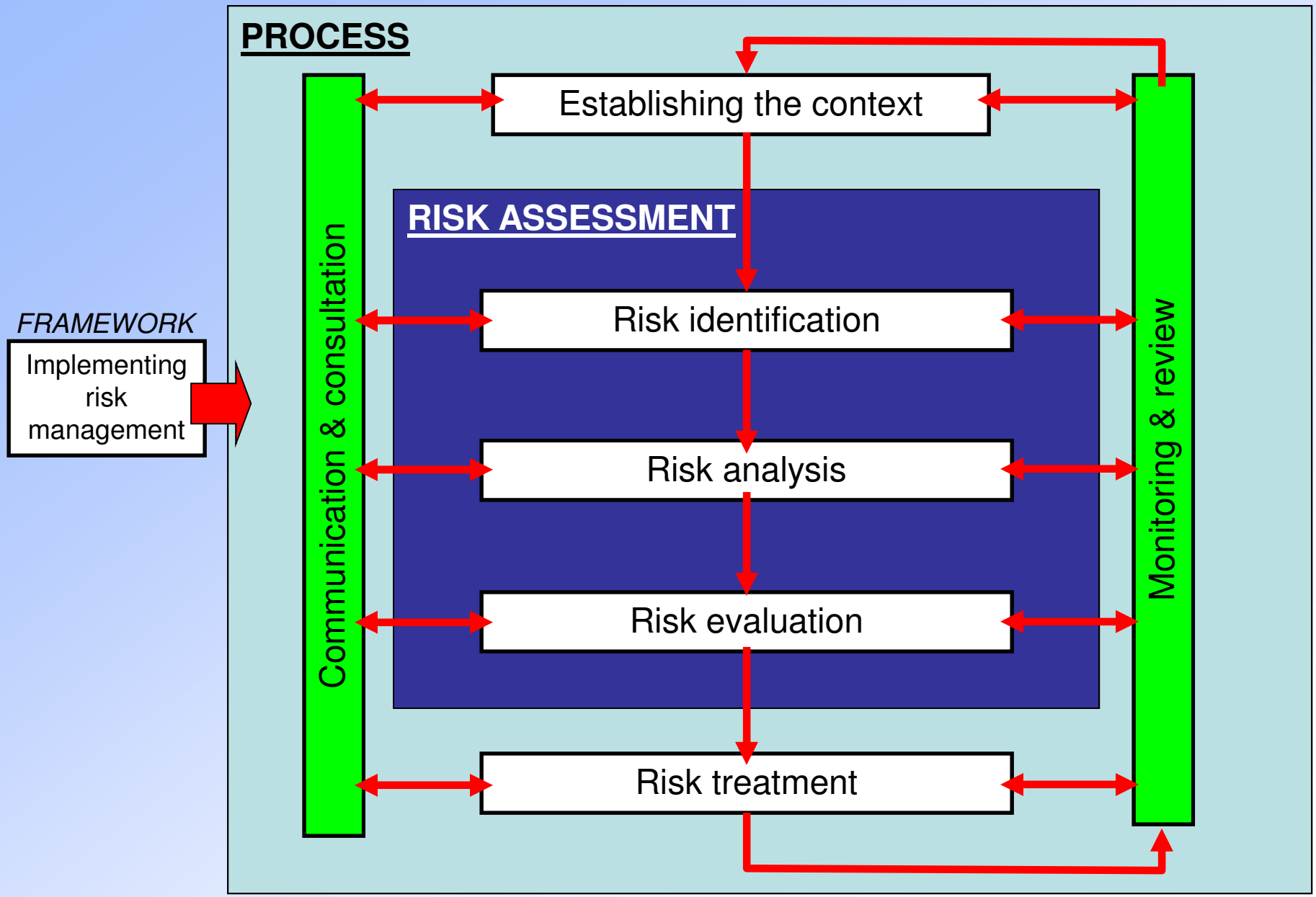
i) Transparent & inclusive

j) Dynamic, iterative and responsive to change

k) Facilitates continuous improvement & enhancement of the organization



# ISO 31000: Principles, Framework & Process



# Risk Management: Establish the context

## External context

- Legal, Regulatory, Financial
- International, national, regional or local
- Relationships with, perceptions and values of external stakeholders

## Internal context

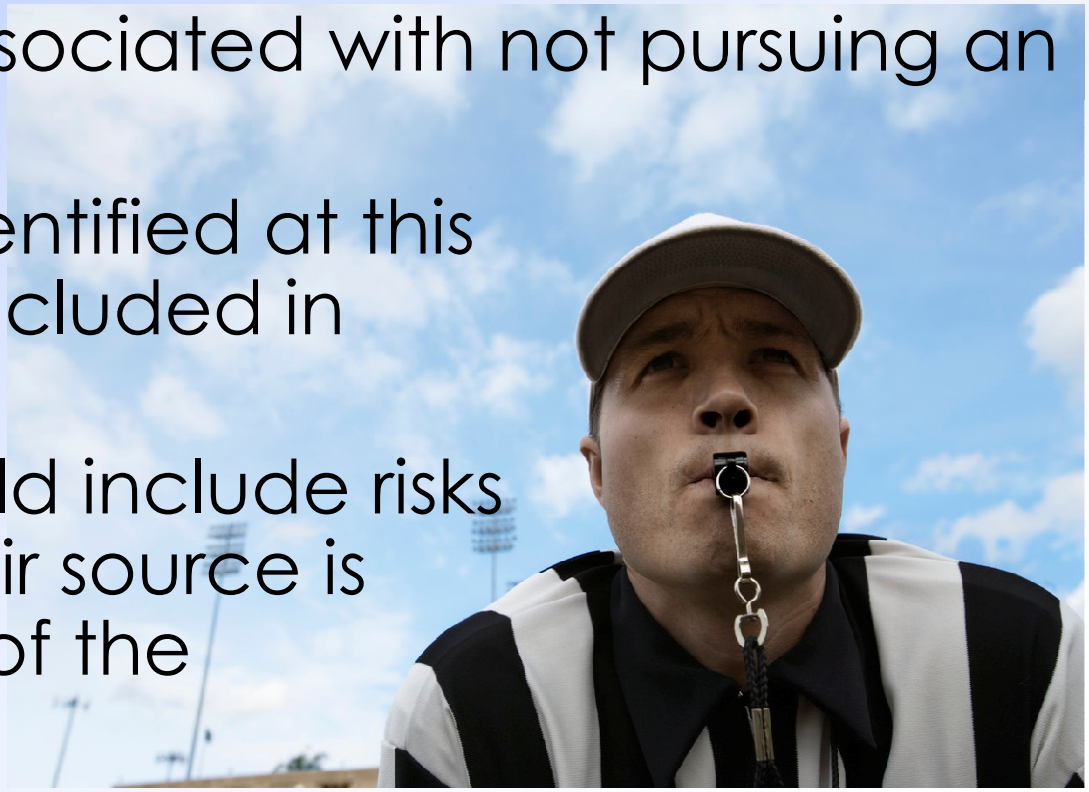
- Organizational objectives
- Project, process, or activity objectives
- Policy, standards, guidelines and models adopted by the organization
- Contractual relationships

## Risk Management process context

- Objectives, scope, responsibilities, methods
- Defining risk criteria – measures, tolerance levels, views of stakeholders

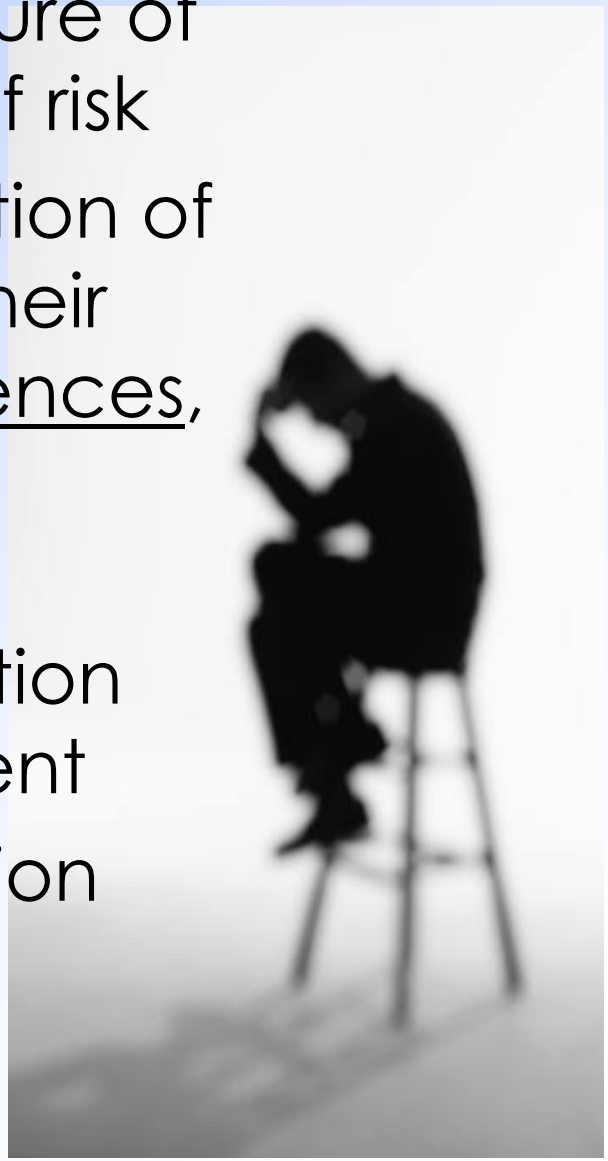
# ISO 31000: Risk Identification

- Process of finding, recognizing and describing risks
- Comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.
- Identify the risks associated with not pursuing an opportunity
- A risk that is not identified at this stage will not be included in further analysis
- Identification should include risks whether or not their source is under the control of the organization



# ISO 31000: Risk Analysis

- Process to comprehend the nature of risk and to determine the level of risk
- "Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur."
- Provides the basis for risk evaluation and decisions about risk treatment
- Risk analysis includes risk estimation



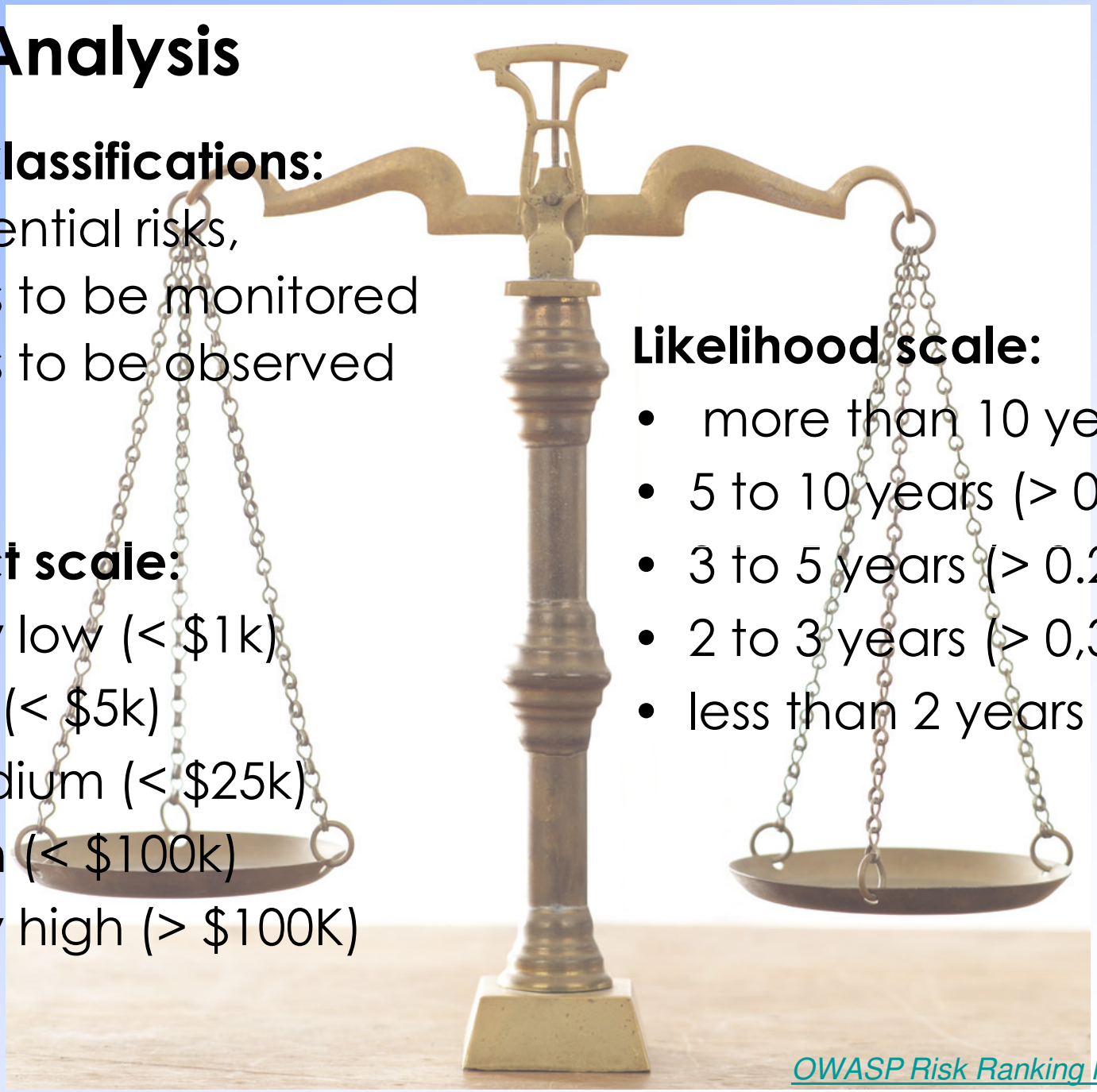
# Risk Analysis

**Risk Classifications:**

- essential risks,
- risks to be monitored
- risks to be observed

**Impact scale:**

- very low (< $1k)
- low (< $5k)
- medium (< $25k)
- high (< $100k)
- very high (> $100K)



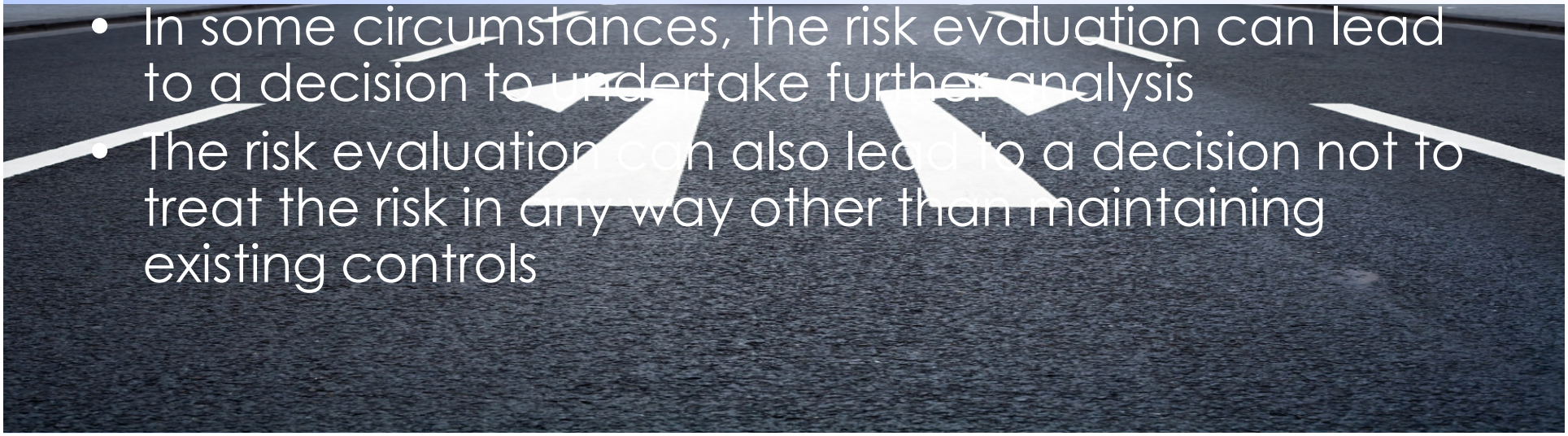
**Likelihood scale:**

- more than 10 years
- 5 to 10 years (> 0.1 )
- 3 to 5 years (> 0.2 )
- 2 to 3 years (> 0,33 )
- less than 2 years (> 0.5 )

OWASP Risk Ranking Methodology

# ISO 31000: Risk Evaluation

- The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation
- Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefits from the risk
- Decisions should be made in accordance with legal, regulatory and other requirements
- In some circumstances, the risk evaluation can lead to a decision to undertake further analysis
- The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls



# ISO 31000: Risk Evaluation

- The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation
- Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefits from the risk
- Decisions should be made in accordance with legal, regulatory and other requirements
- In some circumstances, the risk evaluation can lead to a decision to undertake further analysis
- The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls

# ISO 31000: Risk Treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options.

Risk treatment options are not necessarily mutually exclusive. The options can include the following:

**TRANSFER**

- Sharing the risk with another party or parties (including contracts and risk financing)

**AVOID**

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Removing the risk source

**MITIGATE**

- Changing the likelihood
- Changing the consequences (impact)

**ACCEPT**

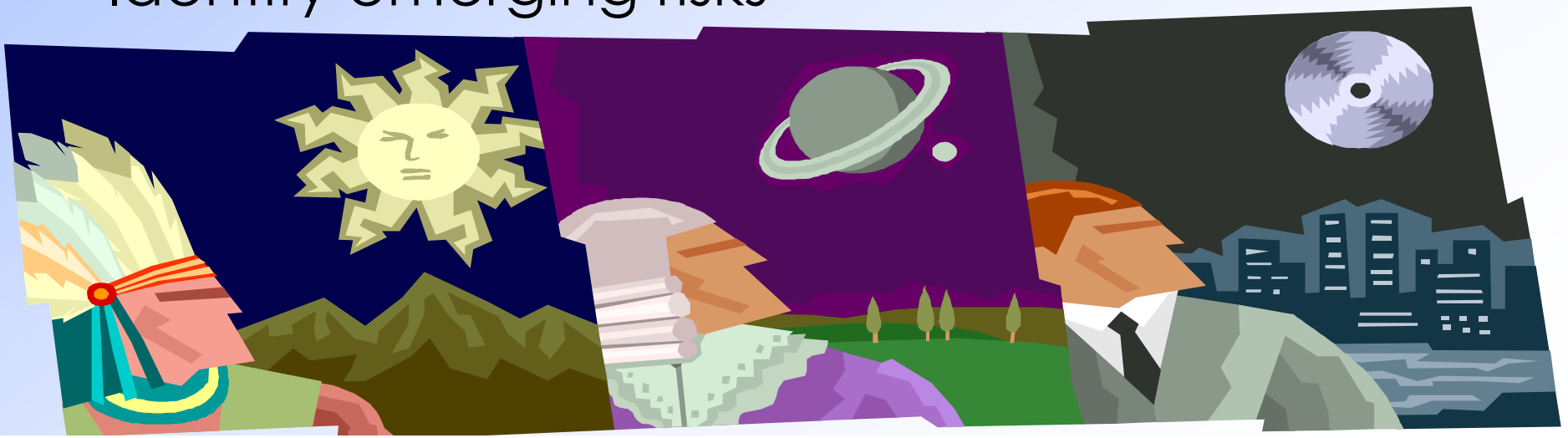
- Retaining the risk by informed decision
- Taking or increasing the risk in order to pursue an opportunity

# ISO 31000: Risk Treatment

- Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment.
- A number of treatment options can be considered and applied either individually or in combination.
- Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the risk treatment plan to give assurance that the measures remain effective.

# ISO 31000: Monitoring & Review

- An integral part of the risk management process involving regular checking or surveillance
- Ensure controls are effective & efficient
- Detect change in external or internal context
- Analysis, lessons learned, continuous improvement
- Identify emerging risks



# Risk Management Basics - ISO 31000 Standard

*THANKS for attending!*

*ENJOY the conference!*

**Louis Kunimatsu, CRISC**
IT Security & Strategy,
Ford Motor Company