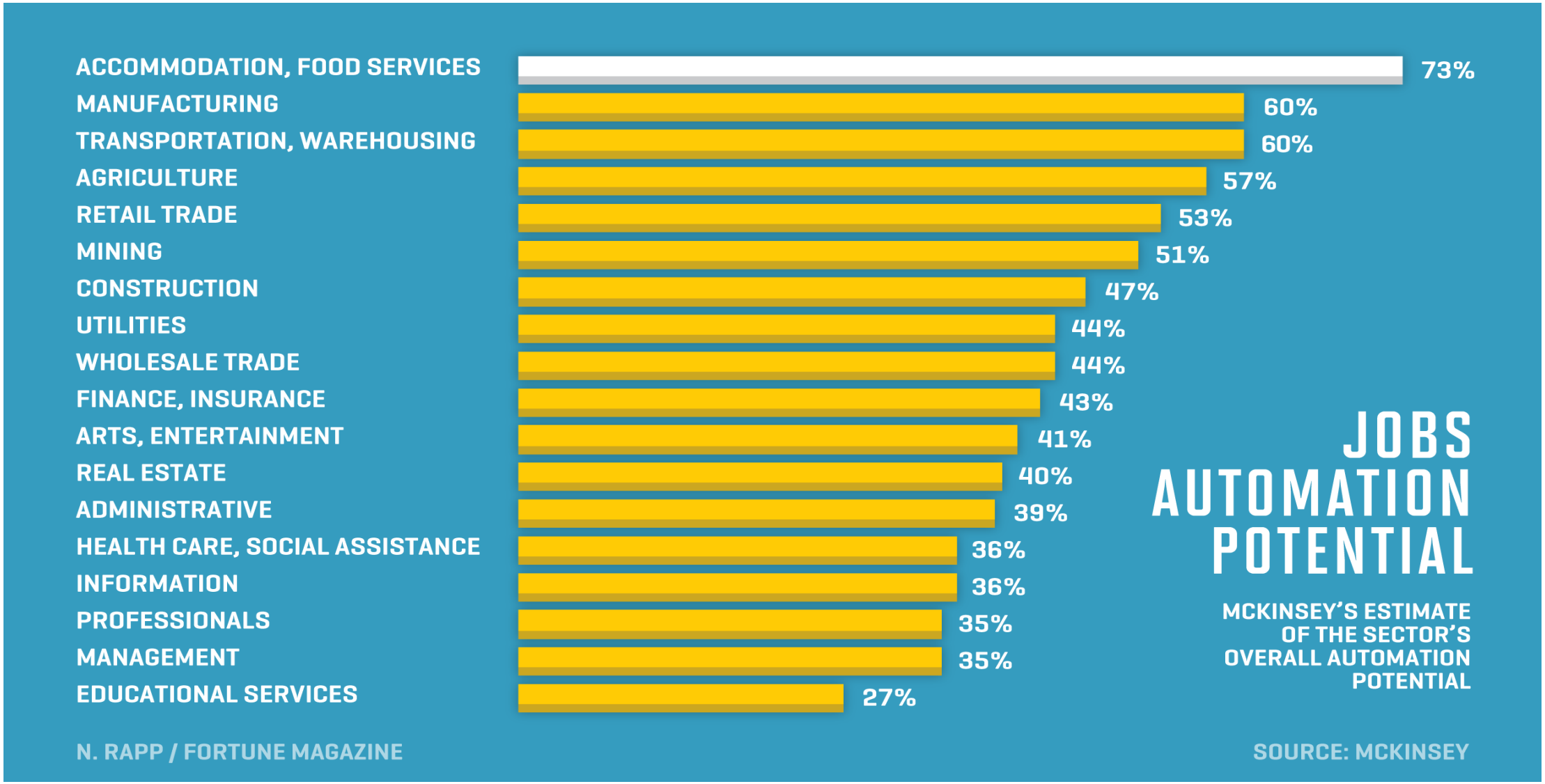
The Institute of Internal Auditors Kenya

How Risk Management Program Supports Controls And Governance Effectiveness

Internal Audit in a disruptive environment

Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

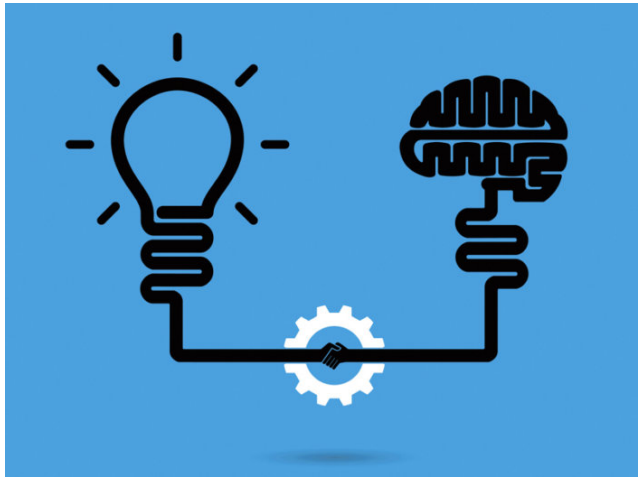


Sentinel Africa
Risk Management Consultants

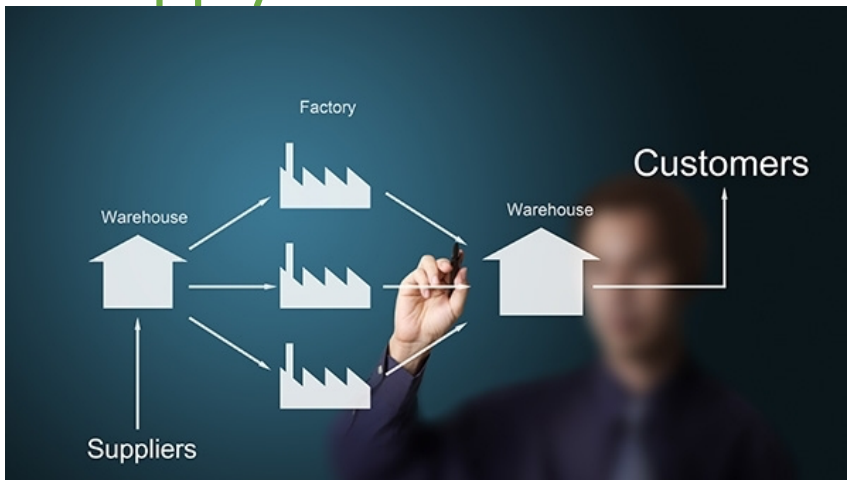
ISO/IEC 27001 CERTIFIED PECB

Our World Today: Why risk management?

Innovation

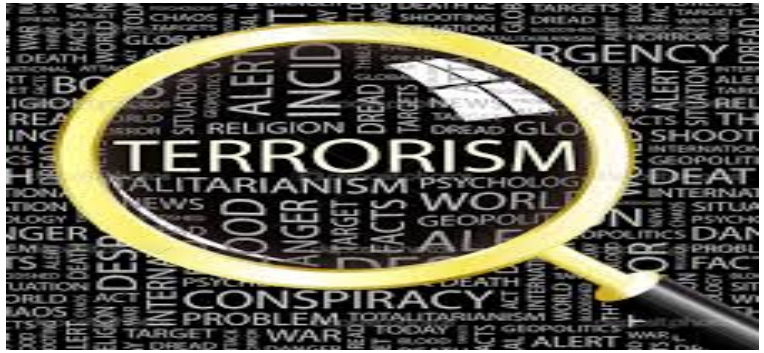


Supply Chain



Cyber Security

Terrorism



Regulation

Climate Change

Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED
PECB

What is a risk?

Objective — To win an Olympic world record

How
- Departments
- IT tools

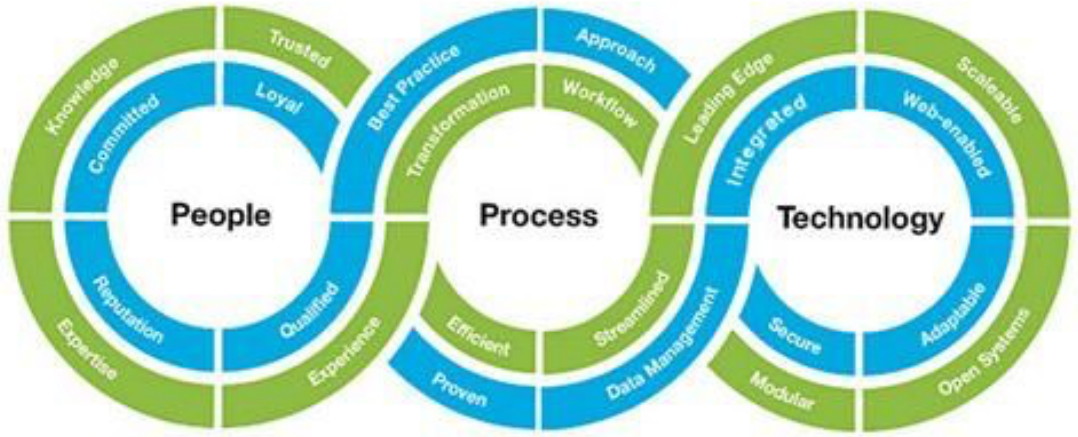
Processes

Expected Result

Brand recognition

1 Million dollars

Endorcements



Risk- Effect of uncertainty on objectives

- Risk Management -Coordinated activities to direct and control an organization with regard to risk
- Risk Framework- Policy, Objectives, Processes to manage risk

Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

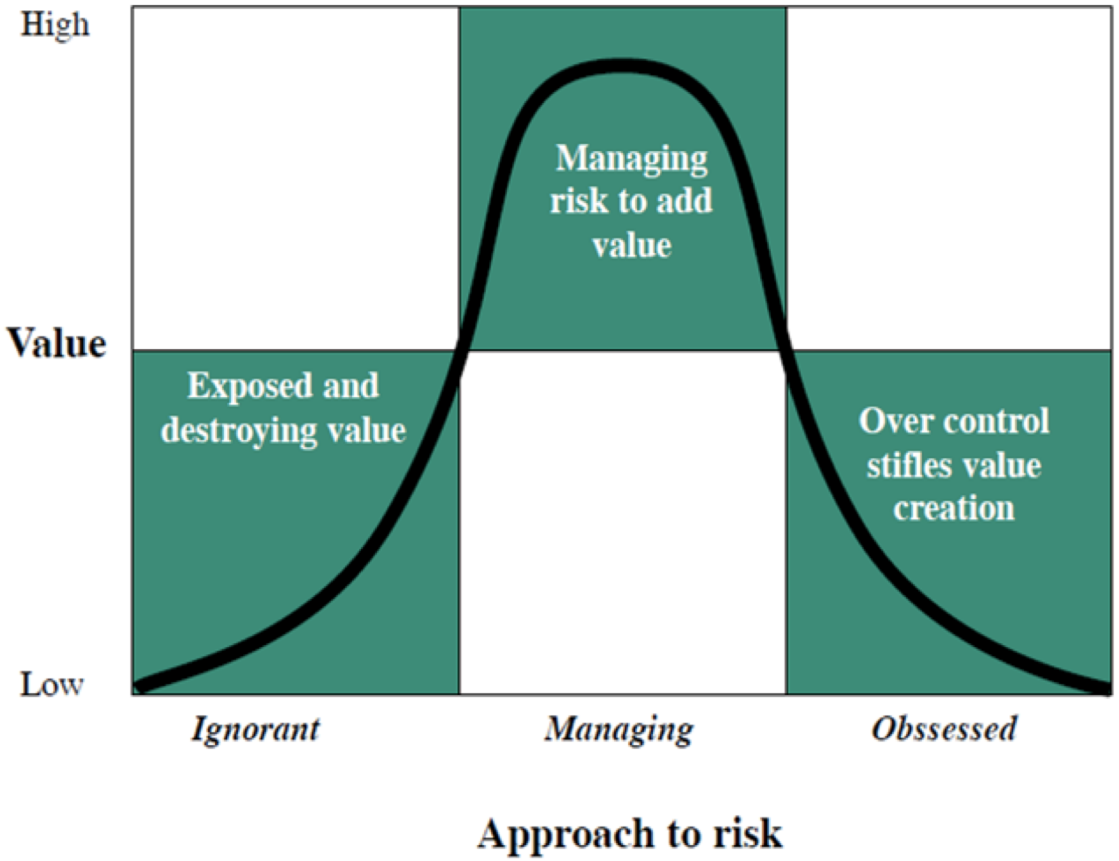
Risk Appetite vs Risk capacity

- Risk appetite- Amount and type of risk an organization is willing to accept in pursuit of its business objectives/value
- Risk capacity- The amount and type of risk an organization is able to support in pursuit of its business objectives
- Residual risk- Risk remaining after the implementation of controls
- Risk acceptance- Knowingly accept the risk as it falls within the organization's "risk tolerance", in other words management deem the risk acceptable, compared to the cost of implementing or improving controls to mitigate it;

Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

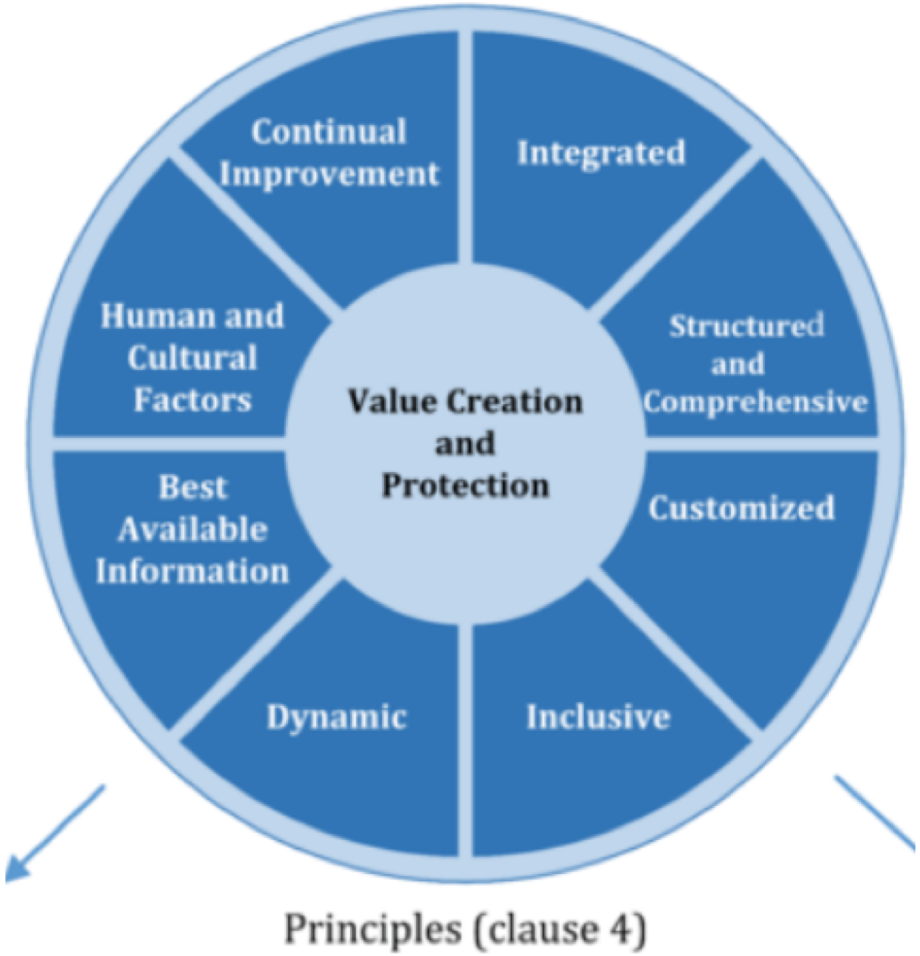
Managing Risk to add value



Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

ISO 31000:2018
Risk Management Framework



COSO. "COSO Enterprise Risk Management—Integrated Framework"

Sentinel Africa
Risk Management Consultants

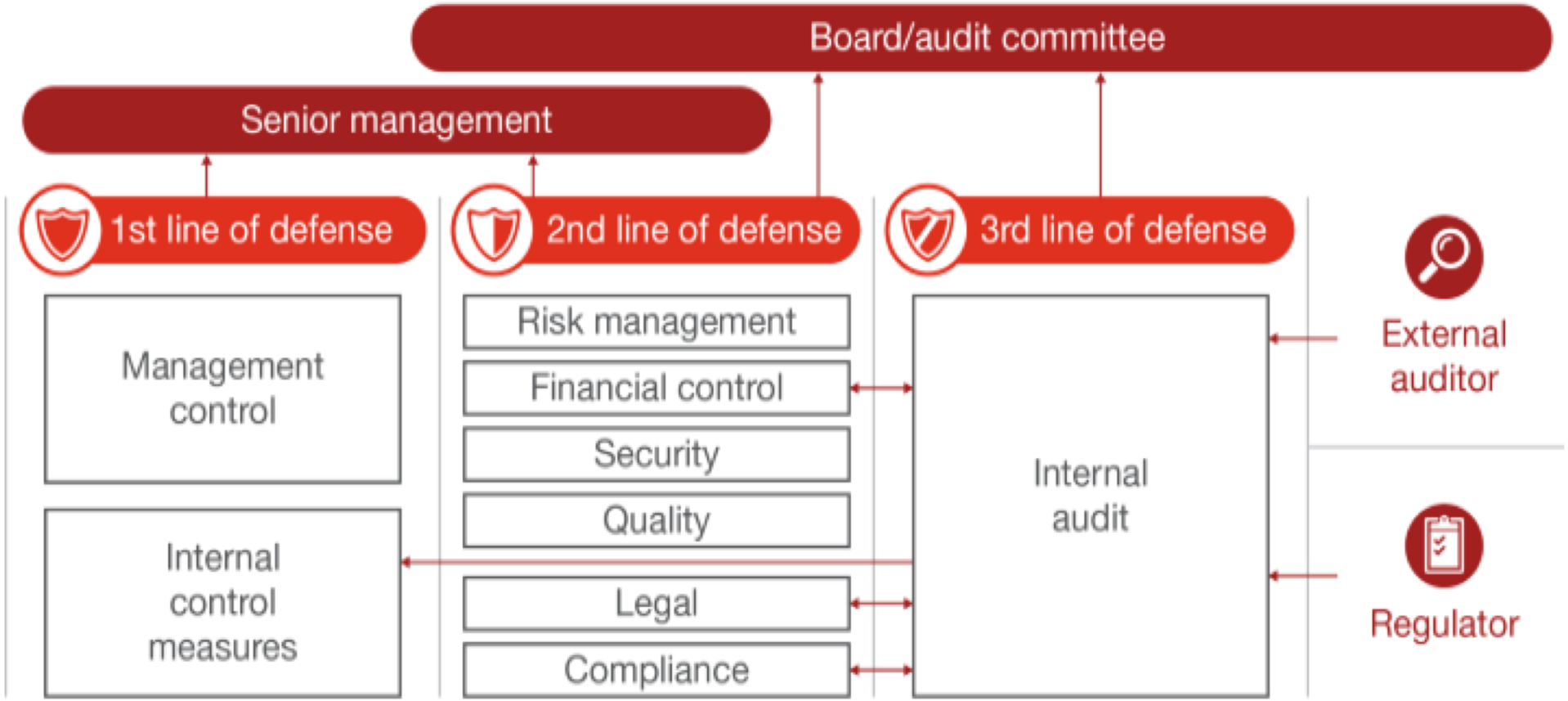
ISO/IEC 27001 CERTIFIED PECB

Living on shaky ground

Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED
PECB

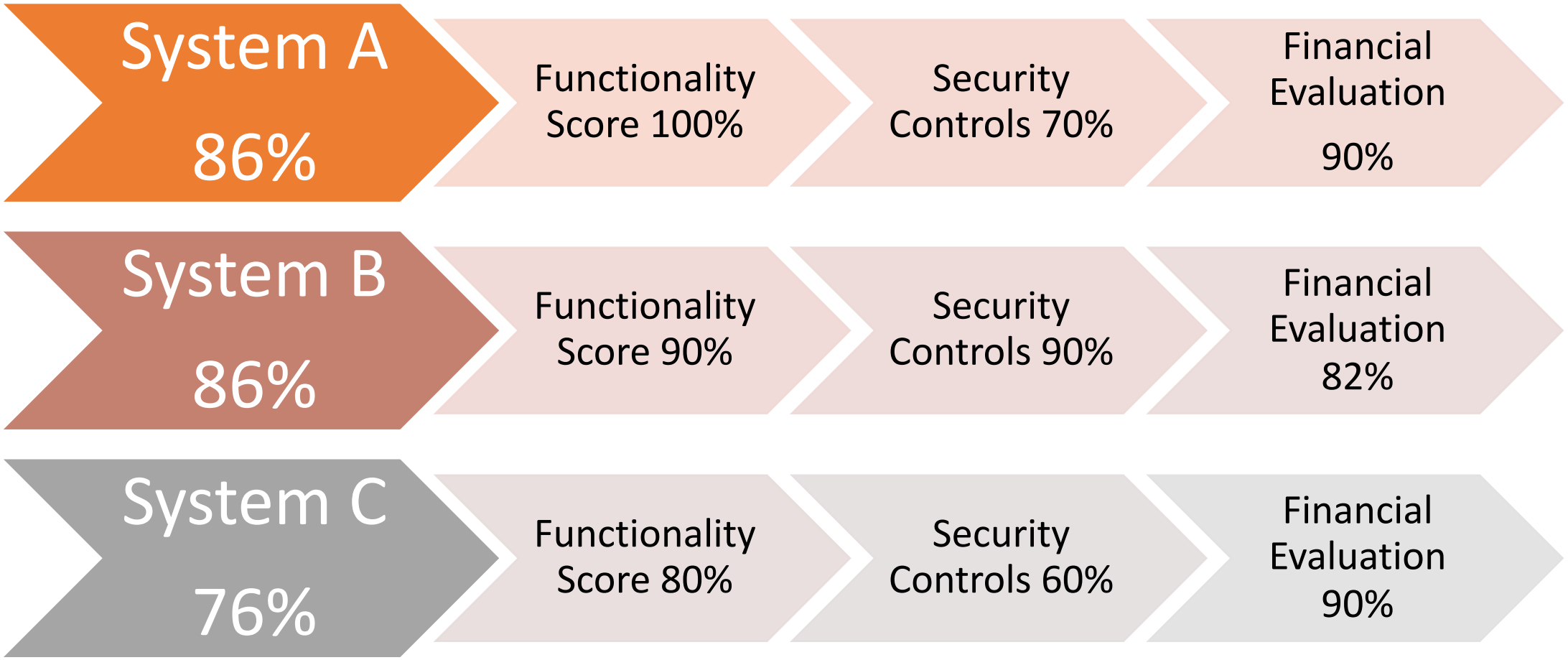
The Three Lines of Defense Model for Managing Risk



Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

Payroll System Evaluation



Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

Biases in risk management

Anchoring bias- People are over reliant on the 1st piece of information they hear

Availability heuristic- People overestimate the importance of information available to them

Bandwagon effect-

the probability of one person adopting a belief increases based on the number of people who hold that belief

Choice – supportive bias-

When you choose something you tend to feel positive about it, even if that choice has flaws

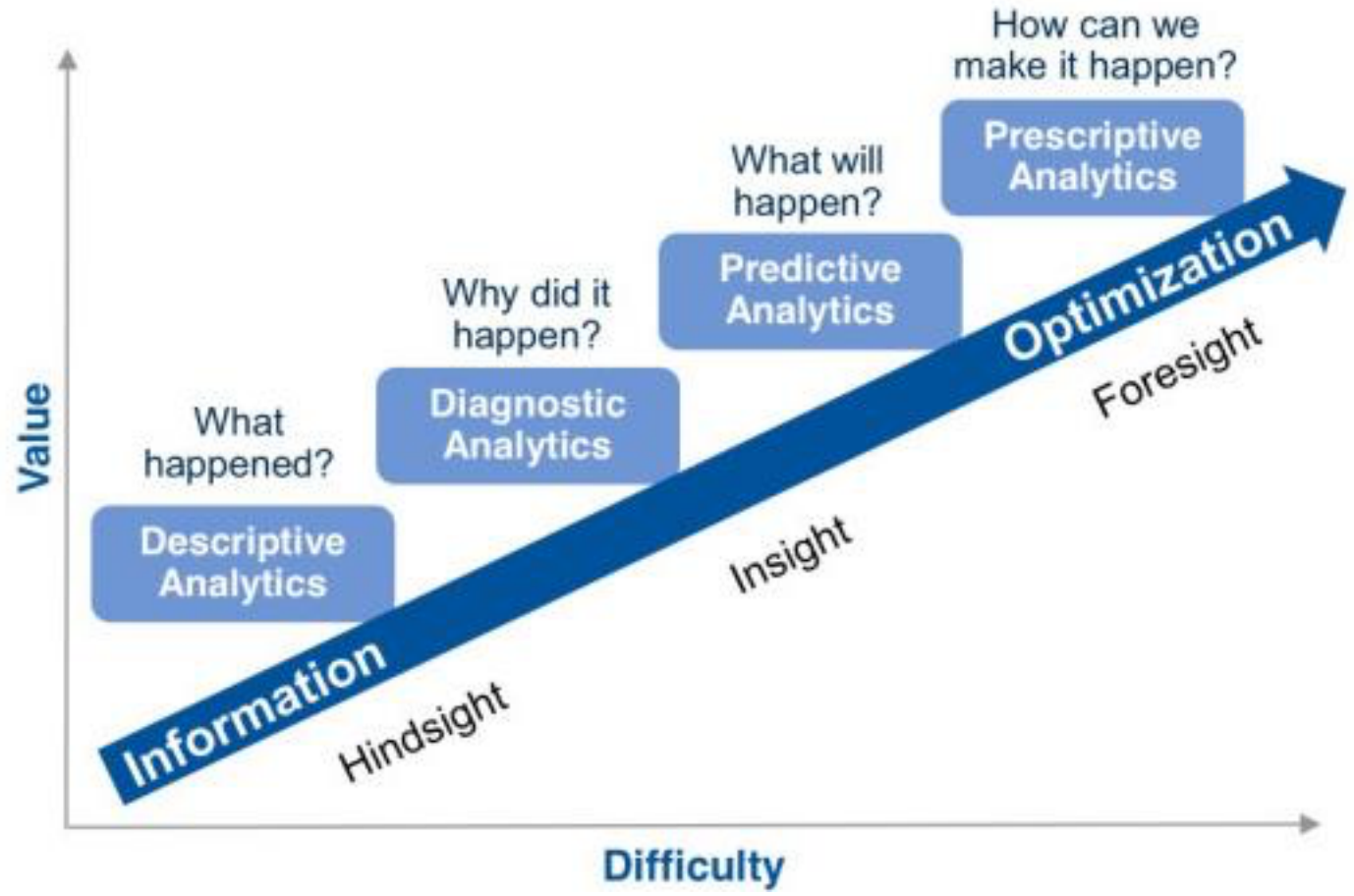
Confirmation Bias-

We tend to listen only to information that confirms our preconceptions

Conservatism bias-

People favor prior evidence over new evidence

Risk management vs Control Assurance



Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

Enterprise risk management is not….

“ERM is not a function or department. It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in ”

“ERM is more than a risk listing. Requires more than inventory of all the risks within the organization.

ERM addresses more than internal control. It also addresses other topics such as strategy-setting, governance, communicating with stakeholders, and measuring performance..

ERM is not a checklist. It is a set of principles on which processes can be built or integrated for a particular organization, and it is a system of monitoring, learning, and improving performance.

ERM can be used by organizations of any size.

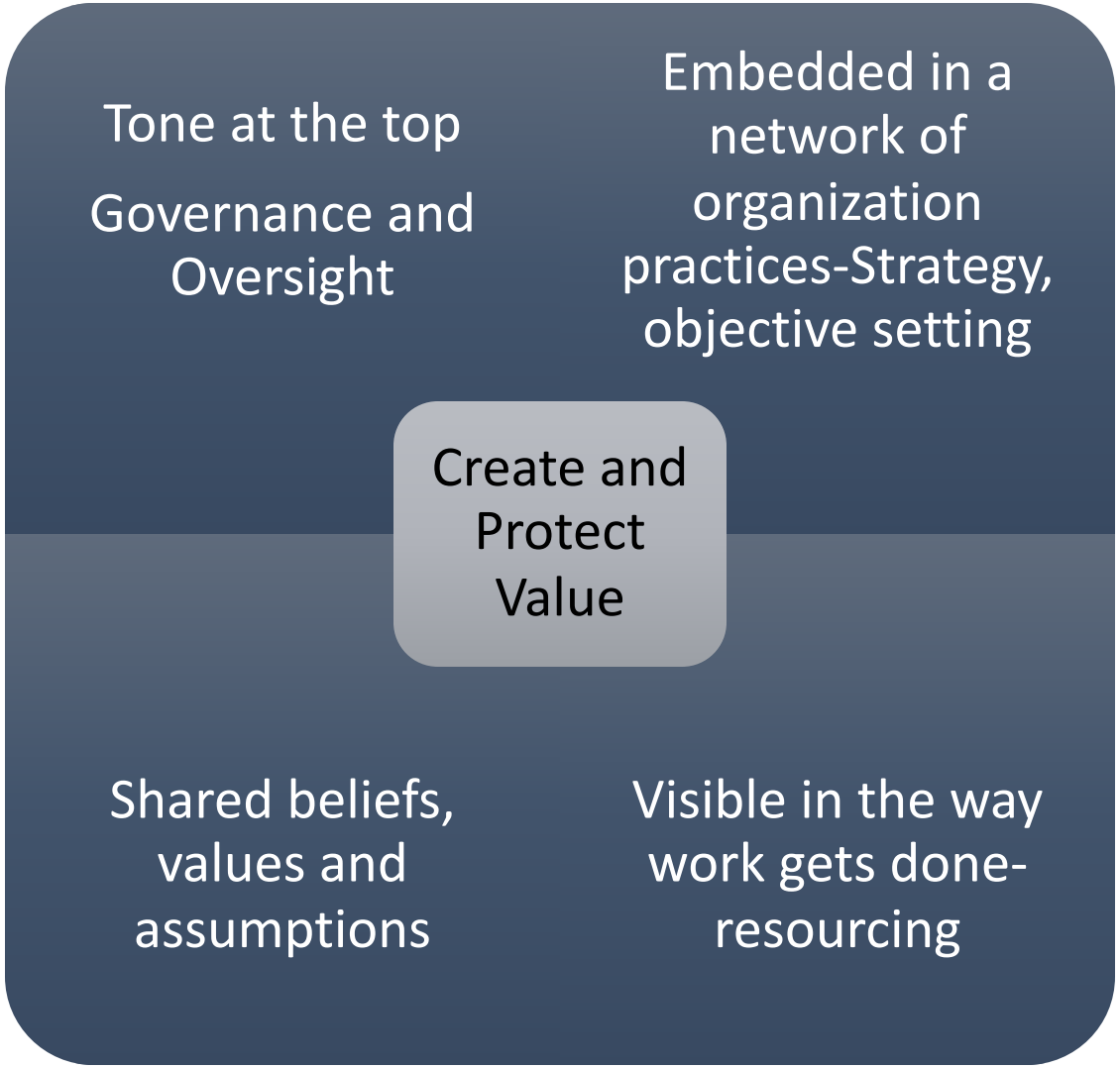
Excerpt From: COSO. “COSO Enterprise Risk Management—Integrated Framework”. Apple Books.

Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

How to access the effectiveness of your risk management

- **Awareness**-Risk Management must be communicated to all
- **Devolved**- RM must be implemented on an operational, tactical and strategic level
- **Practical**- RM must be customized to your orgnisation
- **Improvement**- Management should endeavor to increase data and statistics to manage risks better



Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

Understand. Tailor. Embed

Denial of risk

"I imagine no circumstance that could cause the sinking of the ship. I do not want to imagine a life threatening disaster that could affect that ship"

Captain of the Titanic, 1912

Source: Institute for Governance of Information Systems
ISACA, 2004

Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

Sentinel Africa Consulting Limited

We are an ISO 27001 certified firm based in Nairobi, supporting organizations **Grow** and **Protect** their **Value;**

IMPLEMENTATION

- Business Management processes
- Policy & Process Development

AUDIT AND ADVISORY

- System Audits
- Risk Audits
- Advisory on Risk, Information Security & Business Continuity

DEPLOYMENT OF TOOLS

- Cyber Security Tools (Antivirus, Firewall, Phishing application)
- Business Process Automation

TRAINING

- Information Security
- Cyber Security
- Risk Management
- Business Continuity
- Quality Management

Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

Speaker Contacts

Stella Simiyu
Chief Operating Officer
Sentinel Africa
+254722969874
Stella.Simiyu@sentinelafrica.co.ke
Linkedin: https://www.linkedin.com/in/stella-makona-simiyu-48313215/

Sentinel Africa
Risk Management Consultants

ISO/IEC 27001 CERTIFIED PECB

Understand. Tailor. Embed