COMMON FRAMEWORKS OF ERM (the how of ERM)

Presentation by:

Gilbert Mwalili *CA,CPRM,MRiskMgt*

ENTERPRISE RISK MANAGEMENT SEMINAR
5-7 July 2017

Risk Management Source of Competitive Advantage

Presentation agenda

- Common Frameworks for ERM
- A comparison of ERM Frameworks – differences and similarities
- Practical application of the Frameworks

Common ERM Frameworks

Most widely used frameworks:

- ✓ ISO 31000: 2009 - Risk Management - Practices and Guidelines
- ✓ COSO: 2004 - Enterprise Risk Management - Integrated Framework

Other used frameworks:

- ✓ Basel III
- ✓ Solvency II:2012
- ✓ FERMA: 2002
- ✓ BSI 31100:2008 etc

COSO Framework

COSO's structure and mission

COSO is a joint initiative of five sponsoring organisations

- American Accounting Association (AAA)
- American Institute of Certified Public Accountants (AICPA)
- Financial Executives International (FEI)
- Institute of Management Accountants (IMA)
- Institute of Internal Auditors (IIA)

COSO's mission is…

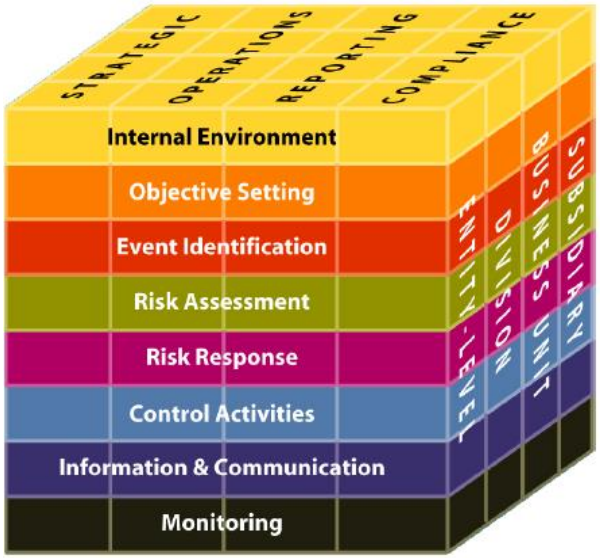
"…to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations."

www.coso.org/aboutus.htm

COSO Framework

- First published in 1992
- Gained wide acceptance following financial control failures of early 2000's
- Most widely used framework in the US
- Also widely used around the world

COSO Cube (Original 1992)



COSO Cube (2004 Edition)

COSO Cube (2013 Edition)

COSO 2013 Internal control

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

COSO ERM 2004

- Starts with objectives:
  - strategic
  - operations
  - reporting
  - compliance
- Applies to activities at all levels of the organization
- Has eight interrelated components

INTERNAL ENVIRONMENT	What is the internal philosophy and culture?
OBJECTIVE SETTING	What are we trying to accomplish?
EVENT IDENTIFICATION	What could stop us from accomplishing it?
RISK ASSESSMENT	How bad are these events? Will they really happen?
RISK RESPONSE	What are the options to stop those things from happening?
CONTROL ACTIVITIES	How do we make sure they don't happen?
INFORMATION & COMMUNICATION	How (and from/with whom) will we obtain information and communicate?
MONITORING	How will we know that we've achieved what we wanted to accomplish?

About ISO 31000

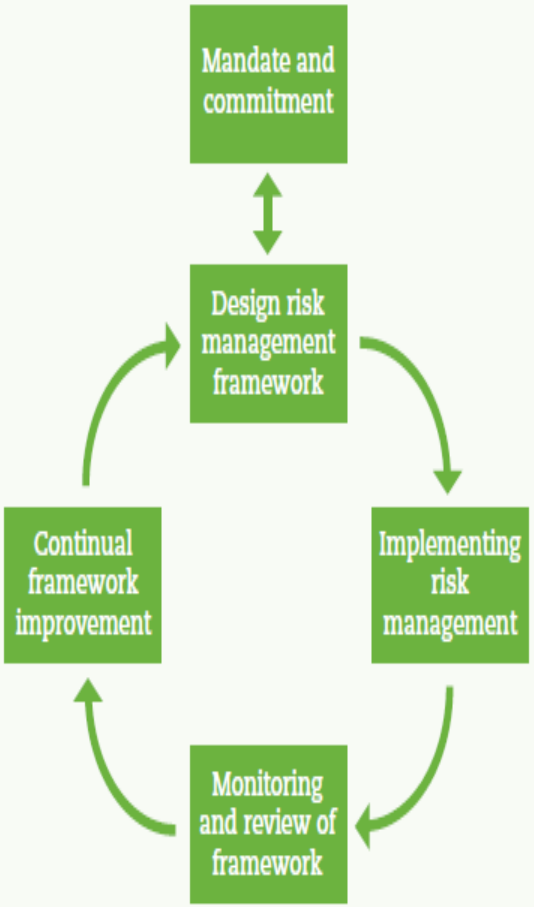
- ✓ International consensus
- ✓ Developed by risk experts from all parts of the world
- ✓ Single global reference for stakeholders
- ✓ Developed in consideration of all existing standards – AS/NZS 4360/1994/1999/2004, AIRMI/ALARM/IRM 2002, COSO2004
- ✓ 164 out of 206 countries are members of ISO
- ✓ World-wide recognition as national risk management standard

ISO 31000:2009

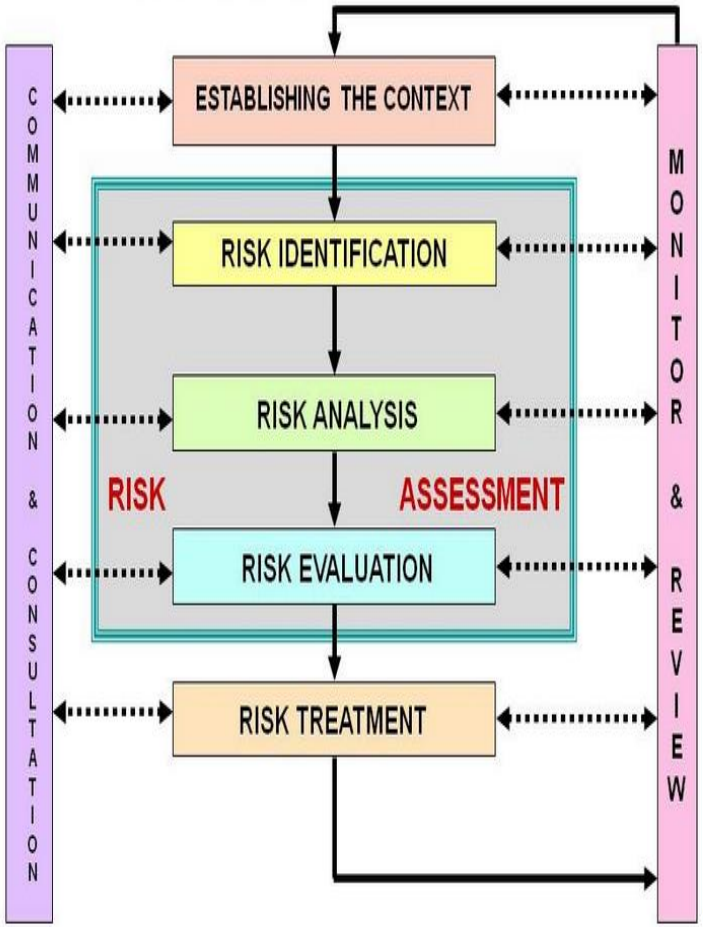
PRINCIPLES

a) *Creates value*
b) *Integral part of organizational processes*
c) *Part of decision making*
d) *Explicitly addresses uncertainty*
e) *Systematic, structured and timely*
f) *Based on the best available information*
g) *Tailored*
h) *Takes human and cultural factors into account*
i) *Transparent and inclusive*
j) *Dynamic, iterative and responsive to change*
k) *Facilitates continual improvement and enhancement of the organization*

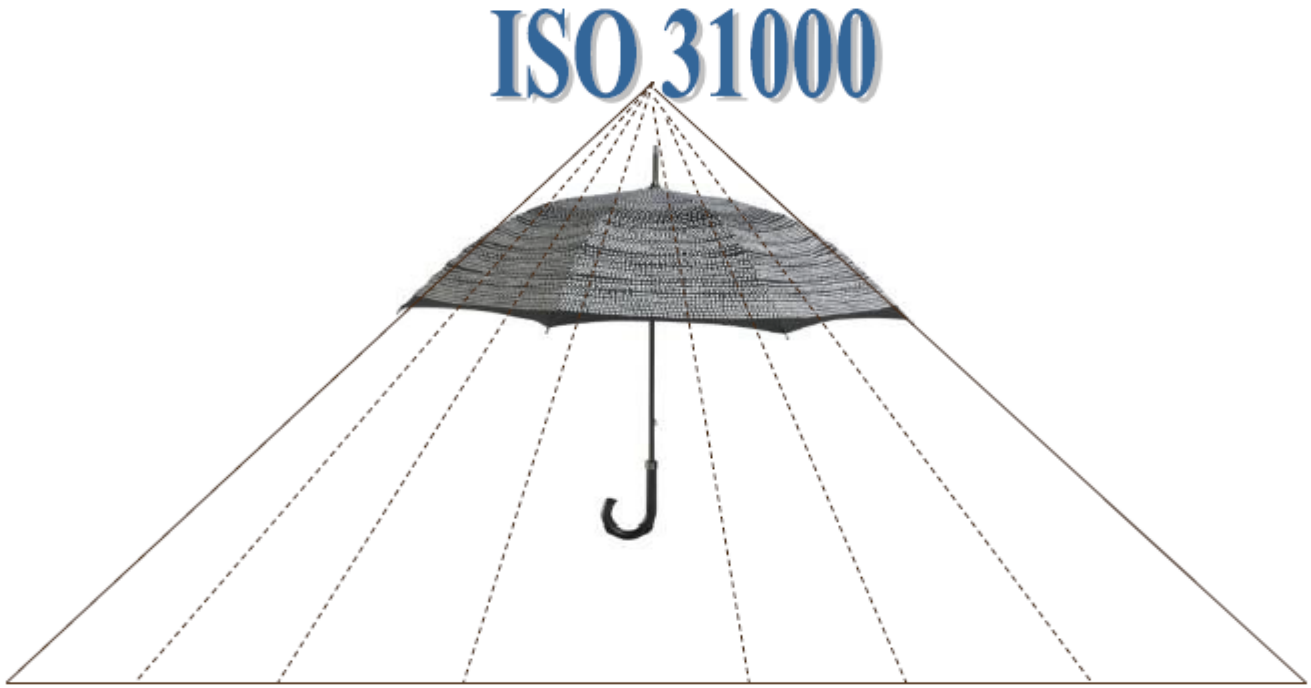
FRAMEWORK



PROCESS



ISO 31000 as umbrella standard



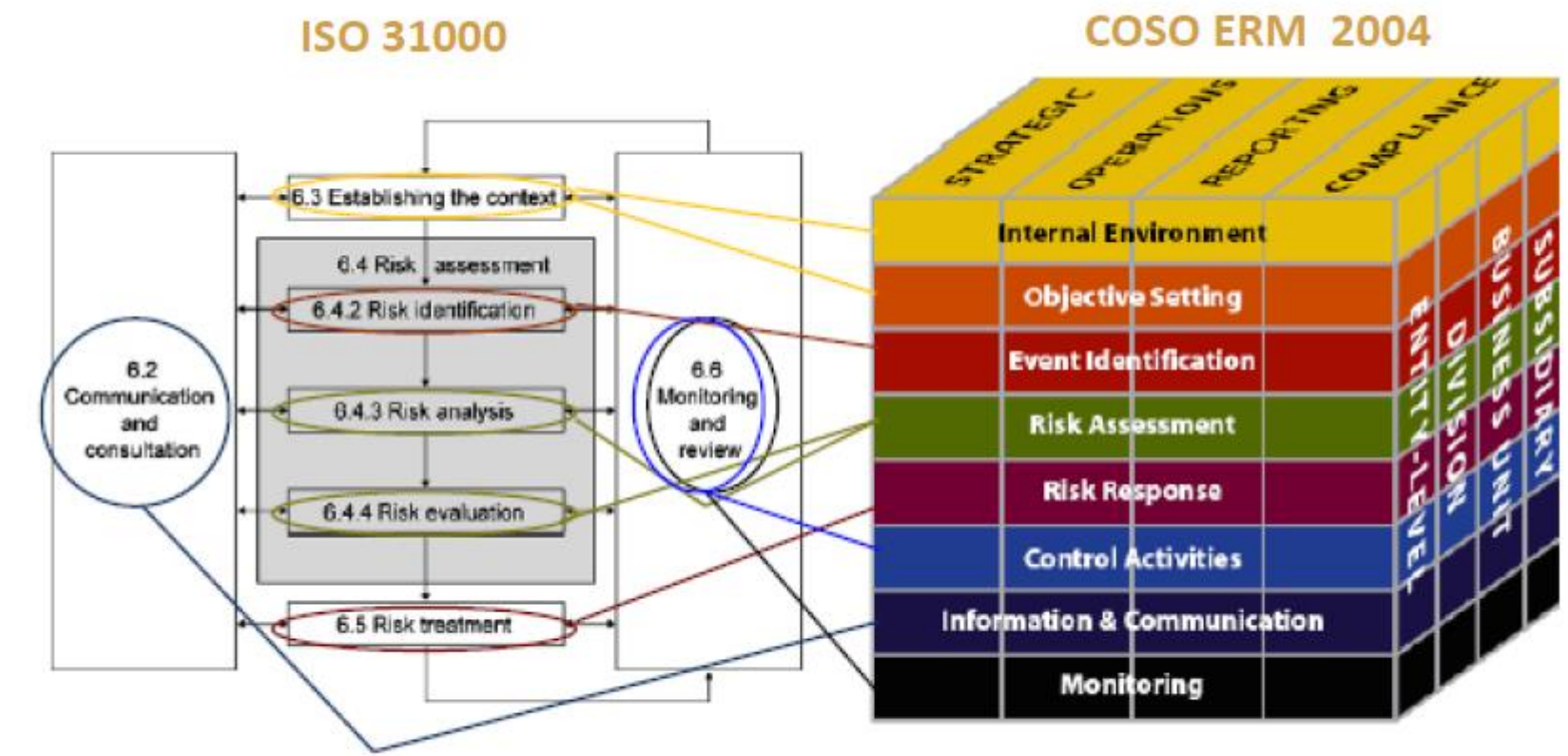
Quality OH&S Finance IT security Project

Environment Food safety Equipment Supply chain

Why ISO 31000

- ✓ Links risk, performance and service delivery
- ✓ Links risk and objectives
- ✓ Cover all types of risks
- ✓ Cover all types of activity and sectors
- ✓ Input from all countries
- ✓ Input from all existing risk standards and guidelines
- ✓ Guideline for all existing standards

Comparison



Source: Aon Risk Solutions, White Paper on Risk Management Committee, 2011

Comparison of ERM Framework

Key aspects similarities:

- Enterprise-wide approach
- A structured Risk Management process
- Formality of Risk Management
- Monitoring of risks and application in decision making
- Continuous improvement of the Risk Management process

Practical application

Key aspects of the frameworks:

- ❑ Define the Policy Framework
- ❑ Define the Risk Appetite/Tolerance
- ❑ Conduct Risk Assessments
- ❑ Set up Risk Monitoring
- ❑ Implement tools for ERM
- ❑ Integrate with Management processes
- ❑ Set up assurance function

Practical application

Steps: Define the Policy Framework

- ❑ Defines scope
- ❑ Defines risk and common terminologies
- ❑ Defines the principles of ERM
- ❑ Defines the methodology to be applied
- ❑ Addresses the governance structure and assigns responsibility

Practical application

Steps: Define the Risk Appetite/Tolerance

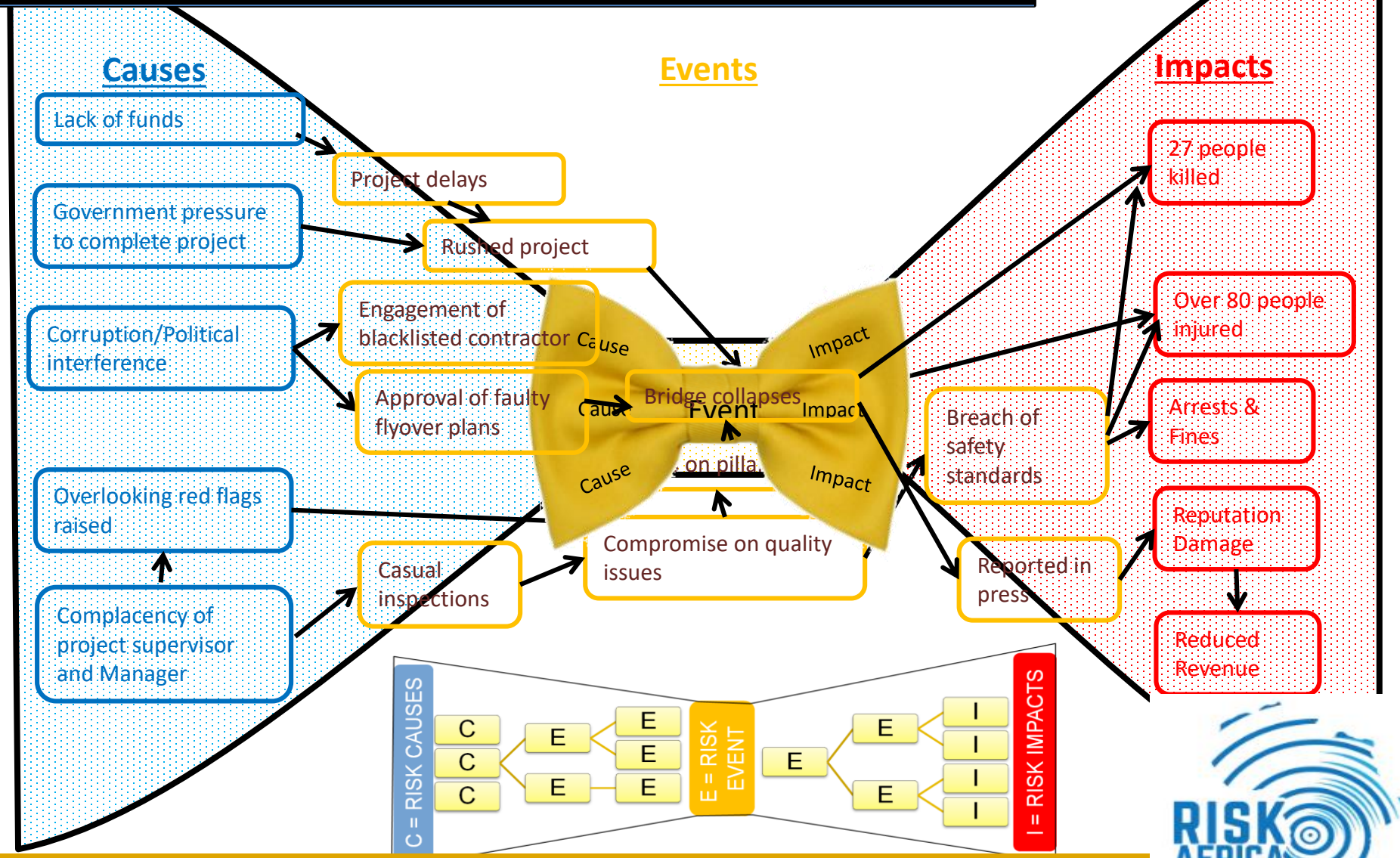
- Defining comprehensive measures of appetite/tolerance for Board to exercise oversight role.
- Going beyond Likelihood/Consequence matrices

Practical application

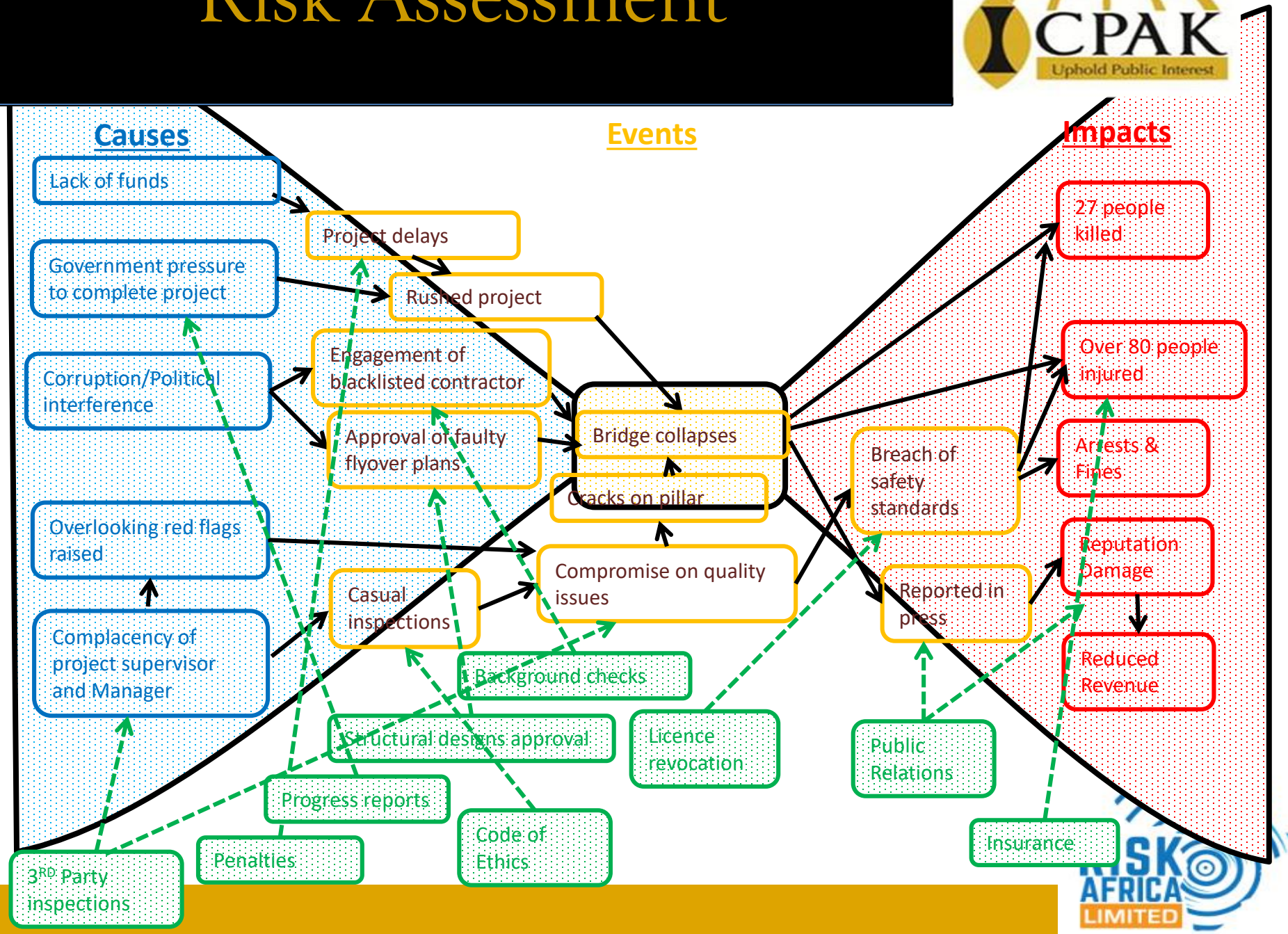
Steps: Conduct Risk Assessments

- The process of:
  - Identifying a risk
  - Analyzing the risk (causes, sources, factors, effects, controls, likelihood, consequence)
  - Measuring the risk against predetermined criteria considering controls
  - Treating the risk where not tolerable or not within risk appetite.

Risk Assessment



Risk Assessment

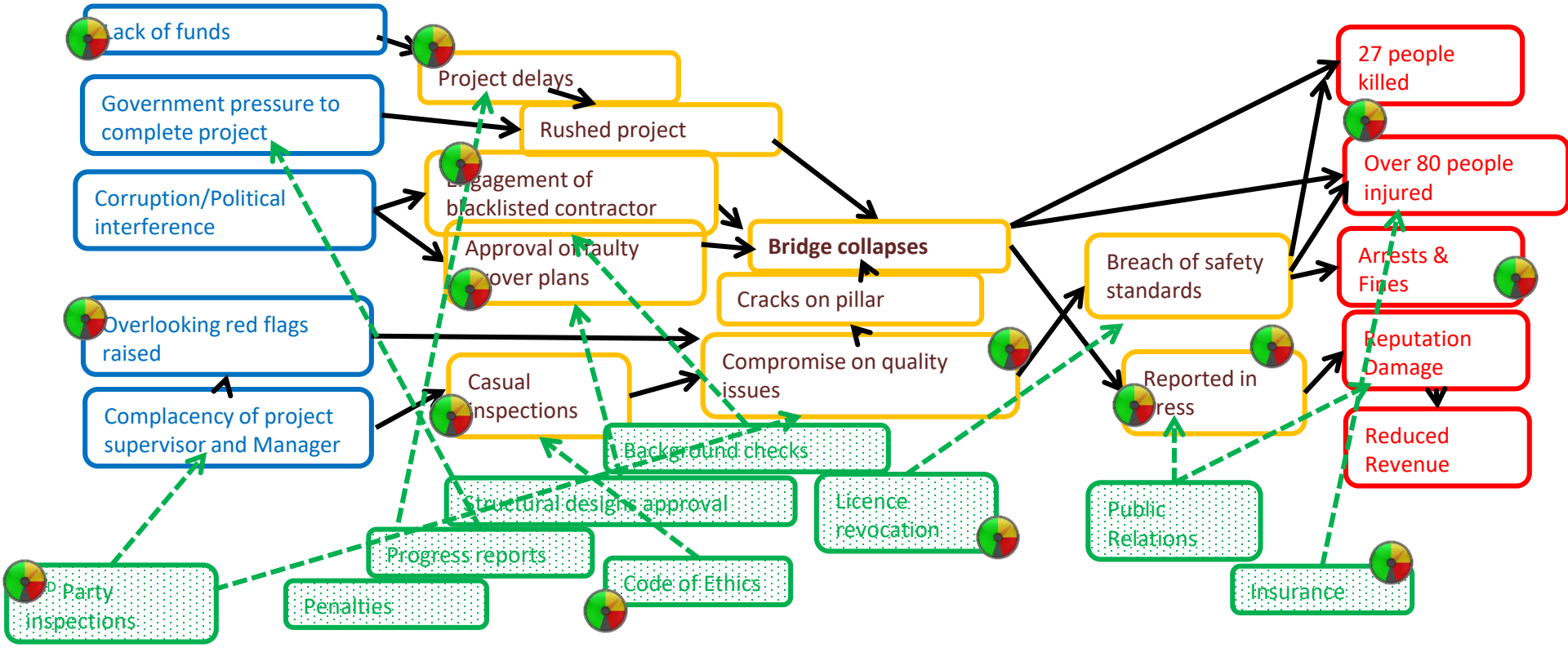


Practical application

Steps: Set up Risk Monitoring

- ❑ Key risk indicators
- ❑ Incident management
- ❑ Compliance monitoring
- ❑ Action tracking
- ❑ Escalation and workflow

Risk Monitoring - KRIs



%ge outstanding GoK disbursement

Constructi on project completion rate

# of missed inspections

%ge of contracts with alterations from the original scope

Fraud cases

Number of non-compliance issues notified

Number of negative press articles

# of deaths/in jury incidents

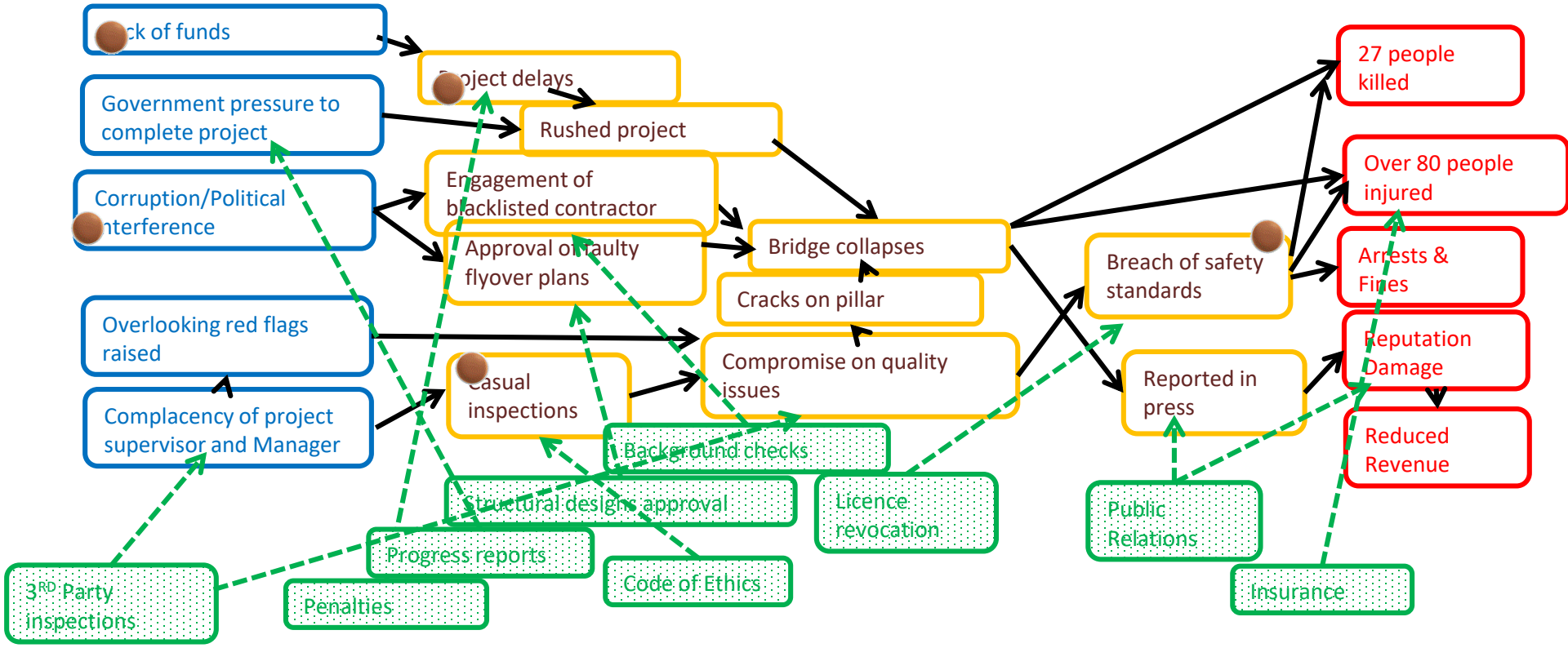
# of inspections

# of trainings

# of breaches

$ recovered by insurance / $ lost

Risk Monitoring – Incidents & Actions



Incidents

- Accumulation of unpaid contracts
- Projects overdue
- Inspections overdue
- Alteration of construction plans
- Construction accidents

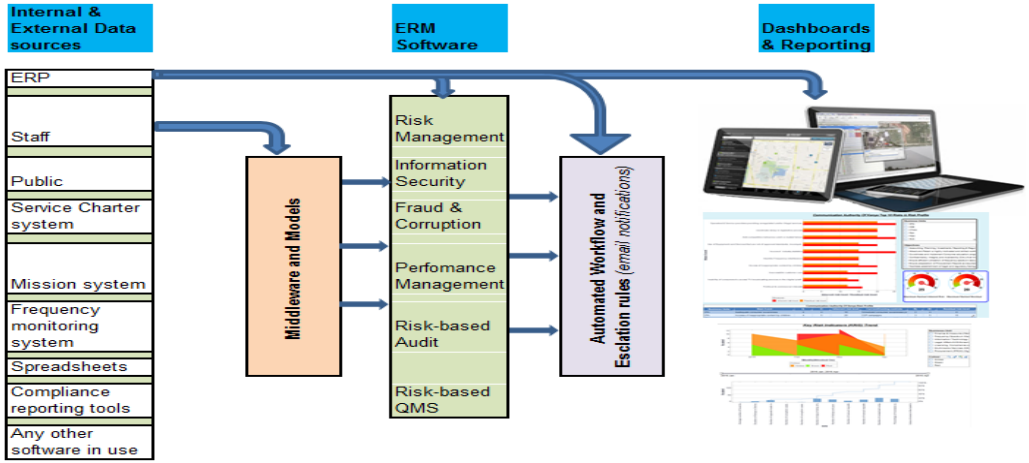
Improvement actions

- Put in place thorough due diligence procedures
- Intensive inspections (Cross checking) throughout the project life

Practical application

Steps: Implement tools for ERM

- ❑Manual systems vs Automated systems
- ❑Analytical tools
- ❑Risk models
- ❑Reporting tools - Dashboards



Practical application

Steps: Integrate with Management processes

Among others, integrate ERM with:

- ❑ Performance Management
- ❑ Strategic planning
- ❑ Projects
- ❑ Fraud & Corruption
- ❑ Business Continuity
- ❑ Information Security
- ❑ Security
- ❑ Legal/Regulatory Compliance
- ❑ Financial Management
- ❑ Quality Management etc

Practical application

Steps: Set up assurance function

- Assurance to the Board that the Management is managing risks to be within the Boards risk appetite.
- The essence of Risk-Based Internal Audit (RBIA)

Practical application

Conclusion

The wealth of available standards describing ERM demonstrates that it is an emerging and essential business discipline.

You will agree with me that:

- ✓ Standards and guidelines tend to be conceptual with little guidance on practical implementation
- ✓ There are more similarities than differences among the standards and guidance documents
- ✓ Institutions need a harmonizing tool regarding the more practical attributes and behaviors that most of the standards are attempting to address as per **RiskAfrica.ERM** Model.
- ✓ Elements in each of the standards and/or guidelines may be useful or adaptable for specific organizations

The fact that all the standards share more characteristic similarities than differences demonstrates that ERM is also an evolving discipline that has meaningful applications to all sectors, whether organizations are structured for profit, not for profit, governmental or non-governmental purposes.

Since ERM is not about certification, what really matters is its application to the institution.

The End

Thank You

Presented by

Gilbert Mwalili
gilbert.mwalili@riskafrica.co.ke
www.riskafrica.co.ke
0716-216-451