

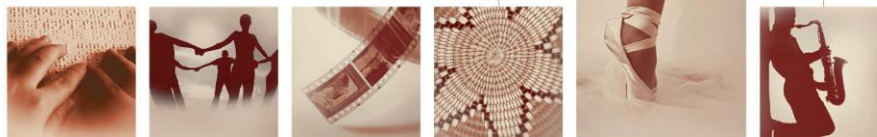


arts & culture

Department:
Arts and Culture
REPUBLIC OF SOUTH AFRICA

“The Value of Risk Management”
IDI Municipal Forum on Risk Management
24th August 2017

LAYING THE FOUNDATION FOR GREATNESS



1. Overview

1. Objective

Deliberate on the value of risk management .

2. Focus Areas

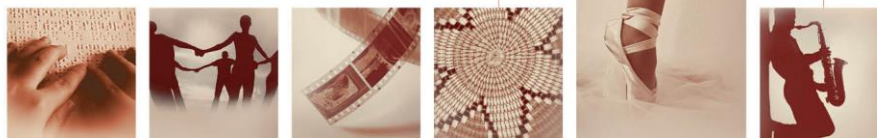
Expected domestic Risk Management Structures .
Avenues which you have by now as risk managers?

3. Limitations

What are the strengths and limitations in demonstrating the value of risk management? What have challenges have you been exposed to?

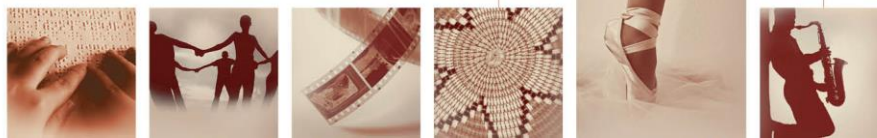
4. Key Take-Always

What can you as a Risk Practitioner do in the short-term to initiate processes to demonstrate value on risk management?



2. Acknowledgements

- *Corporate Executive Board*
- *Salim Ismail “Exponential Organizations”*
- *Reference : Constitution*
- *Reference : Municipal Finance Management Act*



3. Generic Scope of Services at Municipal Level

1. Constitution-Section 152 - Objects of local government

The objects of local government are:

- Provide democratic and accountable government of local communities
- Ensure provision of services to communities in a sustainable manner
- Promote social and economic development;
- Promote a safe and healthy environment; and
- Encourage the involvement of communities and community organizations in the matters of local government.

2. Constitution Section 156- Powers and functions of municipalities

A municipality has executive powers authority in respect of; and has the right to administer:

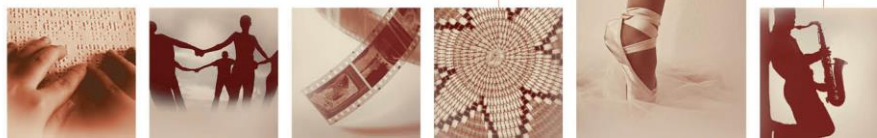
- The local government matters listed in [Part B of Schedule 4](#) and [Part B of Schedule 5](#)
- [Part B Schedule 4](#) [Air pollution; Building Regulations; Firefighting Service; Local Tourism; Municipal airports; Municipal health services; Municipal planning; Municipal transport ; Trading Regulations etc]
- [Part B of Schedule 5](#)[Cemetery; Burial of animals; local sport facilities; Noise Pollution; Refuse Removal; Street Lighting; Traffic & Parking]
- Any other matter assigned to it by national or provincial legislation

3. Support Function

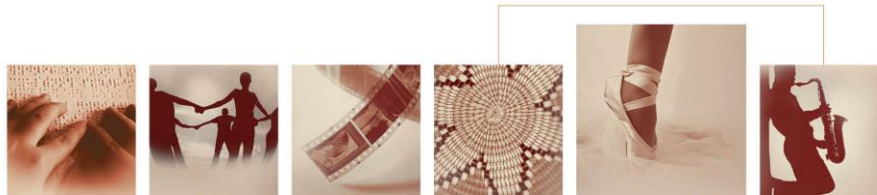
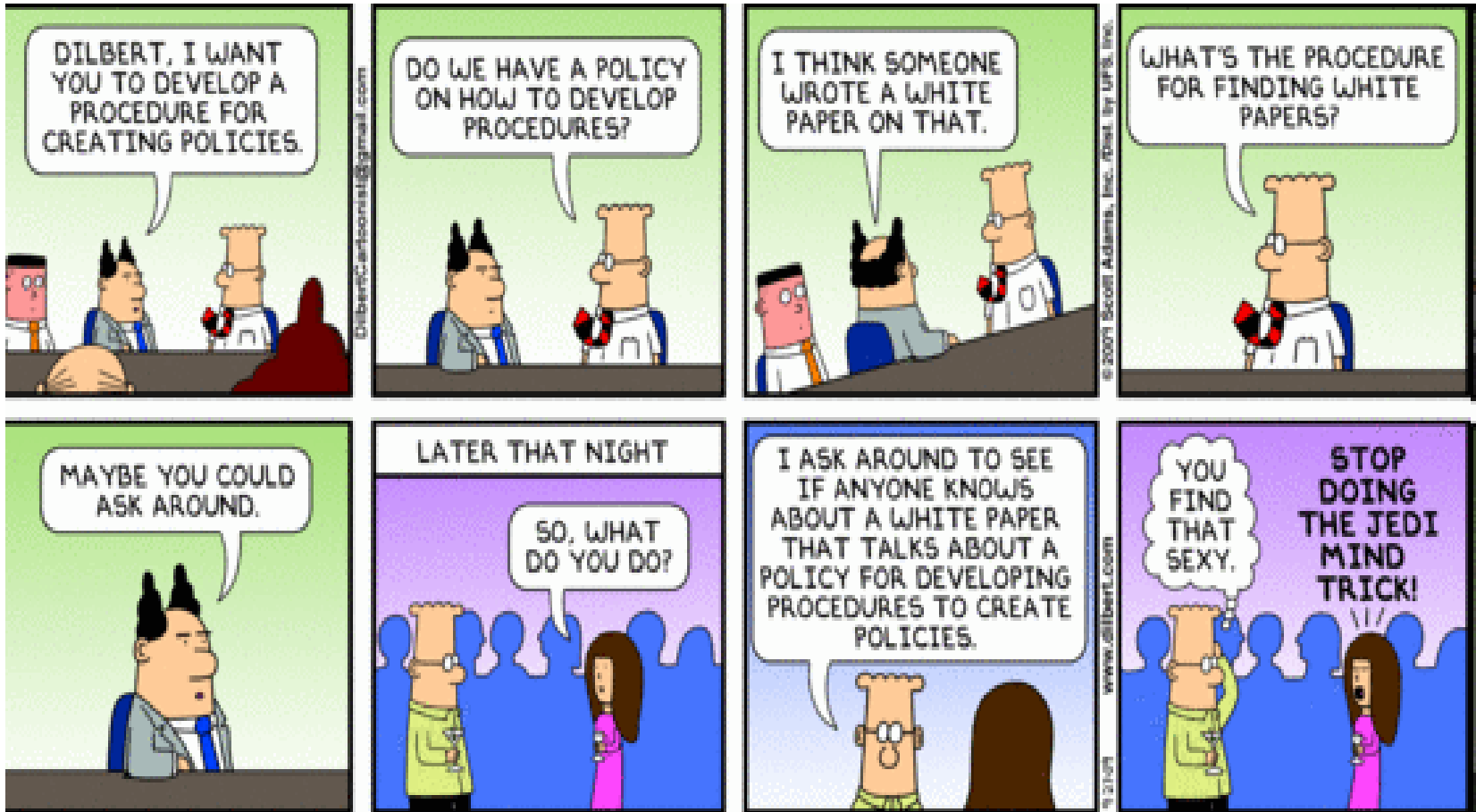
- Executive and Council [Council; Municipal Manager; Public Relations]
- Corporate Services; Property and Records Management; Human Resources; Finances

4. Non-Constitutional Functions[Unfunded Mandates]

- Housing
- Libraries
- Museums
- Vehicle & Driver Licensing

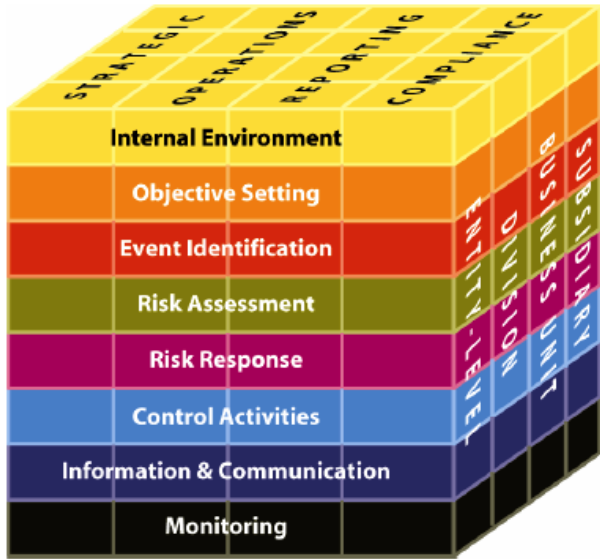


4. How do we make Risk Management accessible to all in our organizations?



5. The COSO ERM Integrated Framework (2004)

2004 COSO ERM Integrated Framework



The COSO ERM framework consists of eight interrelated components derived from the way management runs an enterprise. These components help management achieve key objectives across four categories.

COSO’s Eight Components of ERM

Internal Environment – Encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity’s people.

Objective Setting – Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity’s mission and are consistent with its risk appetite.

Event Identification – Events affecting achievement of an entity’s objectives must be identified, distinguishing between risks and opportunities.

Risk Assessment – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

Risk Response – Management selects risk responses, developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.

Control Activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

Information and Communication – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities.

Monitoring – The entirety of enterprise risk management is monitored and modifications made as necessary.

Source: Committee of Sponsoring Organizations (COSO, 2004)

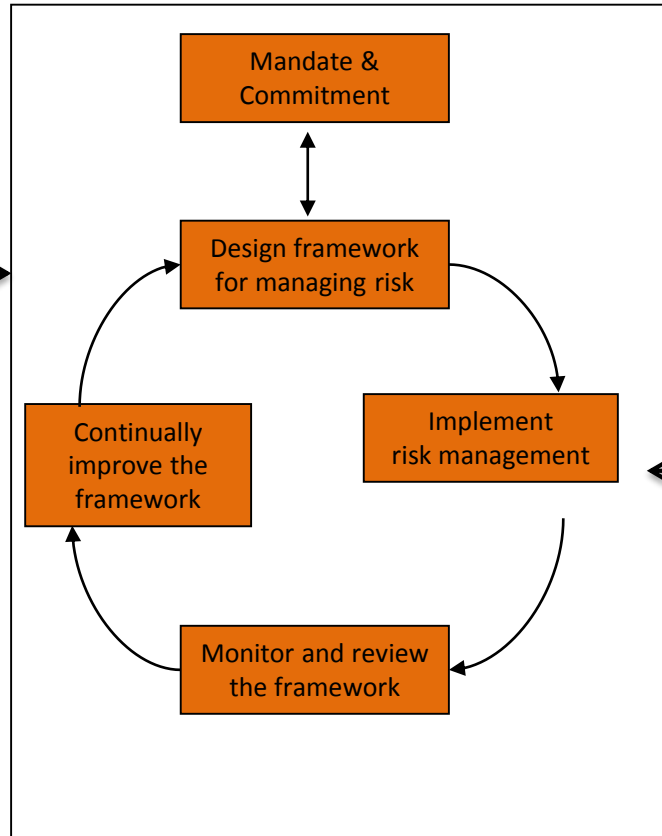


6. The ISO 31000:2009 Risk Management Framework

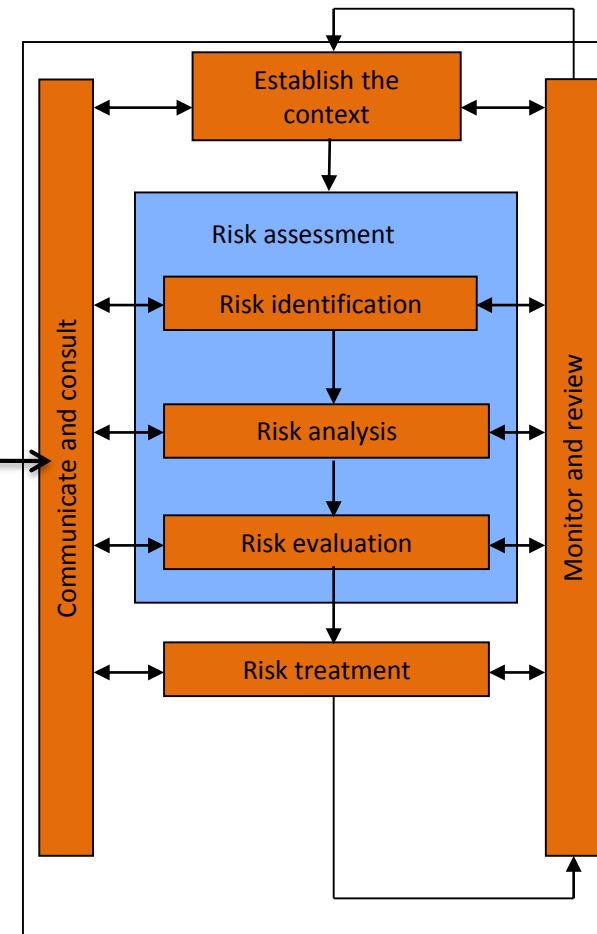
Principles

- Creates value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured & timely
- Based on best available information
- Tailored to organization needs
- Takes human & cultural factors into account
- Transparent & inclusive
- Dynamic, iterative & responsive to change
- Facilitates continual improvement & enhancement of the organization

Framework



RM Process



Source: The International Organizations for Standardization (ISO)



7. Comparing the COSO and ISO 31000 ERM Frameworks

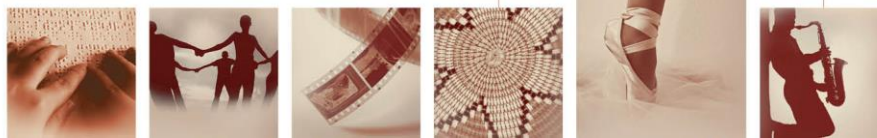
The table below documents a number of key differences between the COSO and ISO 31000 risk management frameworks.

	COSO	ISO 31000
Scope	Most prominent in North America; able to be applied by any industry or sector. COSO is explicitly about ERM.	An international framework; able to be applied by any industry or sector. ISO 31000 is a framework for general risk management; however, its principles can be applied to ERM.
Orientation	COSO is linked to the Sarbanes-Oxley requirements for companies listed in the United States; it therefore has a control and compliance orientation.	ISO 31000 focuses on integrating risk management into the regular management processes of an organization.
Area of Focus	Focuses on the senior levels of the organization	Focuses on all levels of the organization
Definition of Risk Management	Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.	Risk management is a set of coordinated activities to direct and control an organization with regard to risk.
Definition of Risk	The effect of uncertainty upon objectives	The possibility that an event will occur and adversely affect the achievement of objectives

Source: CEB analysis

Question for Discussion

Which framework is most relevant for our corporate culture?



8. Oversight Framework

Executive risk committees are the most common way organizations ensure management oversight of risk management activities.

Implementers

- Accounting Officer
- Management
- Performance Unit
- Internal Audit
- Risk Management

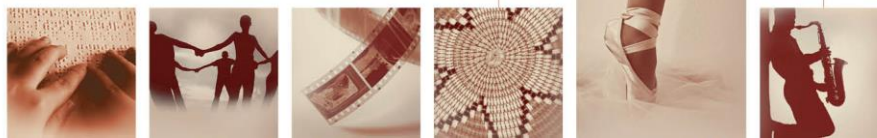
Drivers

- Legal Framework- Sect 62 MFMA 2003[Act no.56 of 2003]
- Corporate Governance Guidelines – King IV
- Service Delivery Imperatives







Oversight Framework

- Executive Authority
- Risk Management Committee
- Audit Committee
- National Treasury
- Provincial Treasury
- Parliamentary Committee



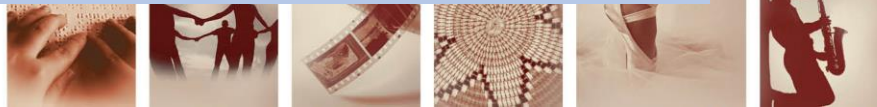
9. Select Assessment Methodologies

It is important to weigh the pros and cons of different methodologies to determine which is most appropriate for your organization. Many organizations often take a hybrid approach, surveying a wide audience while conducting interviews with senior stakeholders.

Assessment Type	Select Benefits	Key Challenges
ERM-Facilitated In-Person Interviews 	<ul style="list-style-type: none"> Allows for free form discussions and can be tailored to individual managers Creates the most insight into risks faced by individual managers 	<ul style="list-style-type: none"> Requires a large time commitment by ERM Requires the aggregation of risk information from qualitative conversations, which may be difficult
Third-Party Facilitated Assessments 	<ul style="list-style-type: none"> Brings a degree of independence and neutrality to the prioritization process Allows the head of ERM to focus on other concerns 	<ul style="list-style-type: none"> Costs the organization more than alternative methodologies Applies a risk assessment that is 'one-size-fits-all' and is not tailored to the culture of the firm
Risk Assessment Surveys 	<ul style="list-style-type: none"> Enables careful consideration of risks and criteria as there is no time constraint Minimizes time and resources required of ERM 	<ul style="list-style-type: none"> Limits 'outside-the-box' or counterintuitive thinking Risks the ERM assessment being viewed as a 'check-the-box' exercise and not taken seriously
Risk Assessment Workshops 	<ul style="list-style-type: none"> Fosters debate within the group Lays bare assumptions and biases of individuals involved in the workshop 	<ul style="list-style-type: none"> Rushes discussions of top risks as too little time may be allocated to workshops Creates opportunity for strong personalities to crowd out others' opinions

Question for Discussion

Which assessment method appeals to you most? Why?



10. Overview of Controls

Four Essential Questions

- How can we design specific measures to prevent risks from occurring?
- How can we design specific measures to decrease the impact of a risk event?
- How do we integrate controls into existing processes?
- How can we determine whether controls are having their intended effect?

Answering these four questions will help risk owners establish effective controls.

Types of Controls

Directive controls: use of objectives and incentives to motivate employees and give them a clear sense of direction.

Preventative controls: use of specific controls, such as segregation of duties or access controls, to prevent abuse.

Detective controls: use of controls designed to pick errors or exceptions, for example reconciliations and variance reporting.

Corrective controls: processes and procedures that ensure diligent management action and follow up in response to problems.

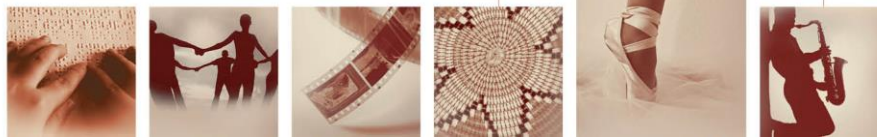
ERM's Role

1. Work with risk owners to identify standard and best practice in establishing controls for risks.
2. Ensure necessary communication and collaboration in setting controls across the organization to avoid gaps, overlap, and unintended consequences.



Question for Discussion

How do you typically identify suitable controls for risks within your purview?



11. ERM's Role in Mitigation

Key Advantages

Head of ERM



- ERM has an understanding of the relationship between risks across different categories (risk interdependencies). This understanding can be applied to assist risk owners in designing effective risk mitigation plans.
- ERM is able to identify organizational best practice.
- ERM has expertise in common risk management techniques.

ERM's Mitigation Responsibilities

- Develop compendium of risk mitigation best practices.
- Review business unit risk mitigation proposals for enterprise-wide alignment and consider their potential impact on other mitigation plans across the organization.
- Advocate for business unit-level risk mitigation funding that will affect enterprise risks.
- Prepare reports for the board and senior leaders on current risk mitigation efforts across the organization.

Risk Owner



- Risk owners have knowledge of the business culture within the organization.
- Risk owners have legitimacy with employees who will implement mitigation.
- Risk owners have specialized knowledge of the function or business process where a risk occurs.

Risk Owner Mitigation Responsibilities

- Coordinate risk mitigation at corporate and business unit levels.
- Establish and execute mitigation plans.
- Report to stakeholders on progress against risks.
- Alert relevant stakeholders about changes to a risk's profile.



Question for Discussion

What is ERM's ideal role in mitigation on a 1-5 scale, 1 being 'does not participate in the risk mitigation process' and 5 being 'leads the risk mitigation process'?

12. Risk Monitoring Overview

Organizations vary considerably in their approach to risk monitoring. More advanced organizations tend to establish relevant metrics and threshold levels to track risks.

Key Benefits of Monitoring Risks



Determine whether risk mitigation or other responses are having their intended effect.



Determine whether internal or external factors are increasing the impact or likelihood of a risk event.

Methods of ERM Monitoring

Less Mature



More Mature

Ad Hoc Monitoring

ERM periodically requests updates from relevant risk owners on changes to a risk's status.

Risk Assessments

Risks are regularly reassessed according to standard risk assessment criteria to determine any changes to its status.

Key Risk Indicators

Key drivers of risks are identified and paired with relevant metrics.

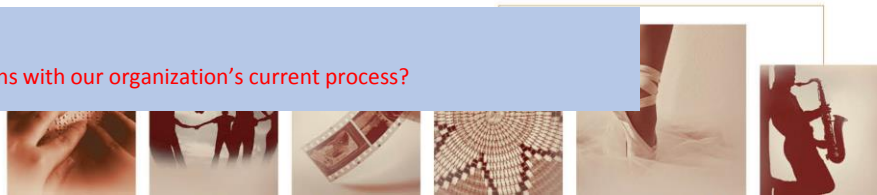
Risk Thresholds

Tolerance levels for metrics are determined, establishing upward and downward boundaries of risk exposures which trigger escalation processes.



Question for Discussion

Which monitoring method most closely aligns with our organization's current process?



13. Outcomes Based Reporting

SPECIFIC



Nature and required level of performance can be clearly identified

MEASURABLE



Nature and required level of performance can be clearly identified

ACHIEVABLE



Realistic given existing capacity

RELEVANT

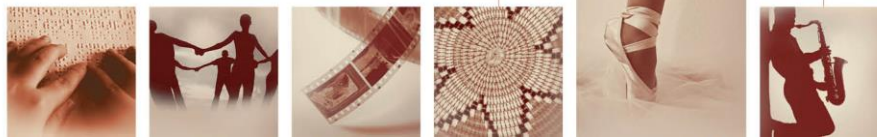


Required performance is linked to achievement of goal

TIME BOUND



Time period/deadline for delivery is specified



14. Types of Risk Reporting

By ensuring risk information is accurate and available, we help employees in our organization make better decisions.

Key Benefits of Reporting

- ✓ **Ensures Executive and Board Oversight**
Senior stakeholders are able to perform effective oversight of the organization's risk management activities and fulfill their fiduciary duties.
- ✓ **Enables Sharing of Risk Information**
Risks that originate in one part of the organization can eventually impact others. By reporting risk information, individuals throughout the organization can be informed and better prepared for possible threats.
- ✓ **Informs Decision Making**
Individuals in the organization are able to better consider risks when making decisions.

Common Types of Risk Reporting



Updates on Top Risks

Reporting on any changes to top risks following regular risk assessments.



Updates on Emerging Risks

Reporting on potential risks that do not currently threaten the organization, but could in the future if those risks continue or intensify.



Updates on Mitigation Efforts

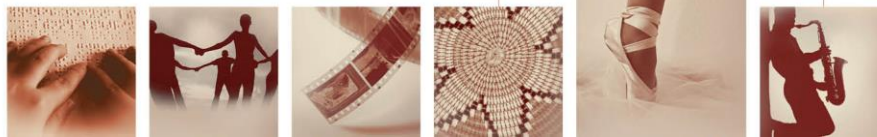
Reporting on status and effectiveness of risk mitigation efforts.



Deep Dive into Specific Risks

Reporting in considerable detail on a given risk, exploring key drivers, the mitigation and continuity efforts that are in place, and other relevant information.

Source: CEB analysis.



15. Three Common Trajectories of ERM Maturity

Level 1 Start & Stagnate

ERM Assessment

Periodic Meetings; no additions of new capabilities

ERM is an event and is viewed as such

Compliance Issue [Regulatory Requirement – Section 62 MFMA General Financial Management function. **‘Accounting Officer ensuring that risk management and internal control processes are effective.’**]

Level 2 Slow Start; React; Atrophy

Led by an event [Fires; housing collapse etc.]

Develop new strategies

No foundations and processes in place.

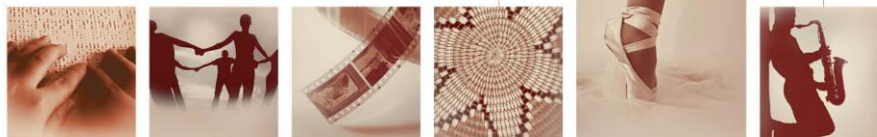
Level 3 Evolve steadily and consistently

Integrate with other programs

Optimise resources

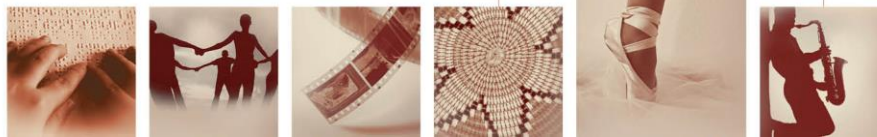
Value proposition is critical

Improve investments in getting risk management and other assurance providers capabilities to function



16. Limitations – The value is reflective in our results

- *Lack of accountability*- RACI over risk mitigation or response plans
- *Limited line of sight*- Risk Owners having limited visibility into how response plans that they own have an impact on risk exposures at an organizational level.
- *Cognitive Biases*- Risk owners opting for the most familiar response option and under-estimating the time it will take to implement their plans.
- *Competing Priorities*- Expectation for revenue growth and cost cutting mean that risk owners focus on financial objectives over the risk objectives.



17. Adapt quickly or be left behind – “A need for Improved Management of the future”

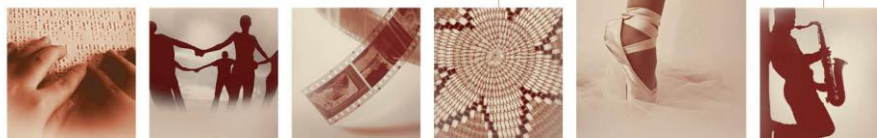
“The future in unpredictable”- Salim Ismail a technology strategist and software engineer sold the concept of ExO. How long can municipalities sustain themselves. [No cost of supply and cost of demand]

What can disrupt the municipal level structure by leveraging the 21st century technology?

- Business landscape has been disrupted [Kodak; Uber; AirBnB etc]
- Speed and efficiency will become the need to survive but not an option
- Politics & patronage
- Paper pushers and tender chasers will be phased out.

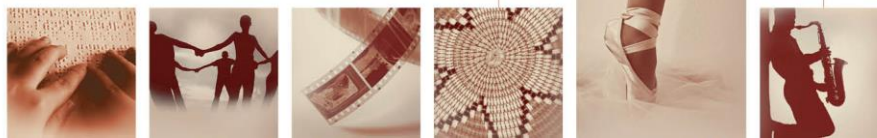
Growth and new direction are taking over:

- Gated communities [Own clinics; schools, refuse removal] . Growth of these will render municipalities, its by-laws irrelevant to those who can afford alternatives.
- The poor if not subsidized will turn to the State
- Staff on demand will replace permanent employment
- Metropolitan will be power and economic engines



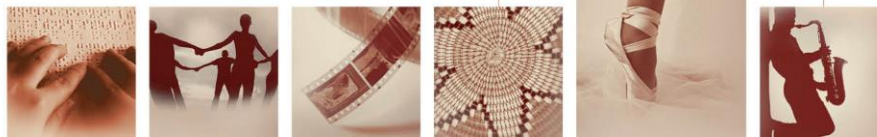
18. How do we get Enterprise Risk Management to evolve in the short-term?

- ERM will only move to newer spaces when the function *uncovers new complexities*.
- *Engage* Executive Management
- Acquire *additional or new skills*
- Review what does not work- enable risk based decision management.
- Respond faster to emerging risks
- Strengthen the collaborations between assurance providers
- Move beyond the annual risk assessment [Move beyond once a year; re-assess and re-rate];
- Apply *deep dives*- use *data analytics* to gauge risk exposure;
- Municipalities have to plan for ways to adapt to mega risks ; namely climate change impacts.



19. Key Take- Aways : Road Map Going Forward

- Conduct a gap analysis of where you are and what you are supposed to have with regards to processes.
- Organizational complexities are getting bigger.
- Poor risk responses become too expensive in the end for the organization.
- Have risk liaisons throughout the organization that will alert you of emerging risks and on-board them early.
- Evolve rapidly with the business cycle of the organization
- Have management to invest in your skills
- ERM Plans should project your three year strategic organizational plan.
- Conduct a functional diagnostic on ERM at an organizational level.
- Present a Quality Improvement Plan
- Assess the potential for Executive Coaching



Thank You

bettys@dac.gov.za

ewrm@dac.gov.za

0726220430

