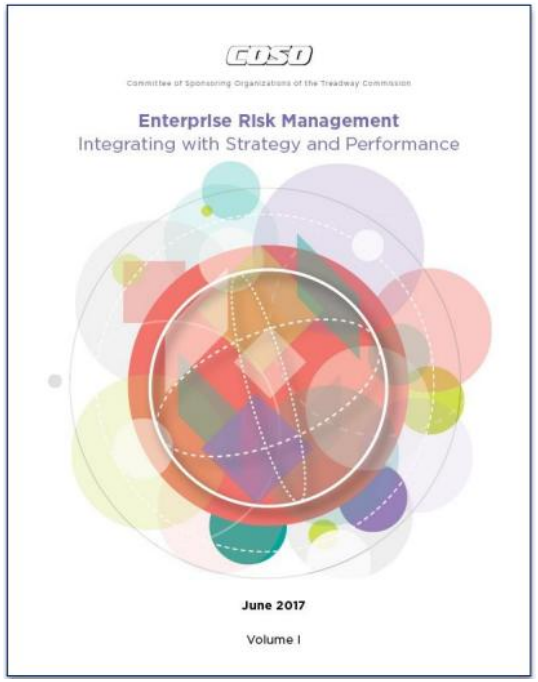
WAG Consulting Pty Ltd
Shaping the future together

nsa
Next Step Academy



Combined assurance and risk management

Deon van der Westhuizen
deon@nsa.edu.za

Need for risk management

- **Risk management creates and protects strategic value to all stakeholders**
- **Risk management is an integral part of all organizational processes**
- **Risk management is part of decision making**
- **Risk management explicitly addresses uncertainty and opportunity**
- **Risk management is systematic, structured and timely**
- **Risk management facilitates continual improvement of the organization**

The RISK Agenda: client issues

Enhance risk strategy

- Improve the overall alignment of risk with corporate goals, major initiatives and emerging market trends
- Clarify the definition of "risk" and determine the management and board's risk appetite and overall tolerance levels
- Communicate overall risk strategy to key stakeholders
- Clarify and strengthen risk oversight at the board and executive management levels
- Deliver greater transparency and accountability at all levels in the organization

Embed risk management

- Define the key "risks to own" that drive growth and create value (day-to-day business, change programs, emerging business)
- Invest differentially in the strategic "risks that matter" to better enable performance
- Link risk management to business planning and performance management
- Align key risk indicators (KRIs) with key performance indicators (KPIs) and key control indicators (KCIs)

Turning risk into results

Improve controls and processes

- Reduce cost of controls spend
- Leverage automated controls vs. manual controls
- Implement more prevent vs. detect controls
- Optimize controls around key business and IT processes
- Monitor critical controls and KPIs continuously to improve decision-making and performance results

Optimize risk management functions

- Improve the effectiveness and efficiency of individual risk management functions
- Reduce redundancies and overlap in risk coverage
- Coordinate risk activities and align skills to better leverage existing infrastructure and resources

Enable risk management

- Harness technology to enhance and more effectively enable risk management, controls and processes

Communicate risk coverage

- Improve transparency and frequency of stakeholder communications
- Provide greater assurance to customers and stakeholders through independent, third-party verifications

Integration= improved decisions = enhanced performance

- It helps organizations to:
  - Anticipate risks earlier or more explicitly, opening up more options for managing the risks
  - Identify and pursue existing and new opportunities
  - Respond to deviations in performance more quickly and consistently
  - Develop and report a more comprehensive and consistent portfolio view of risk
  - Improve collaboration, trust, and information sharing

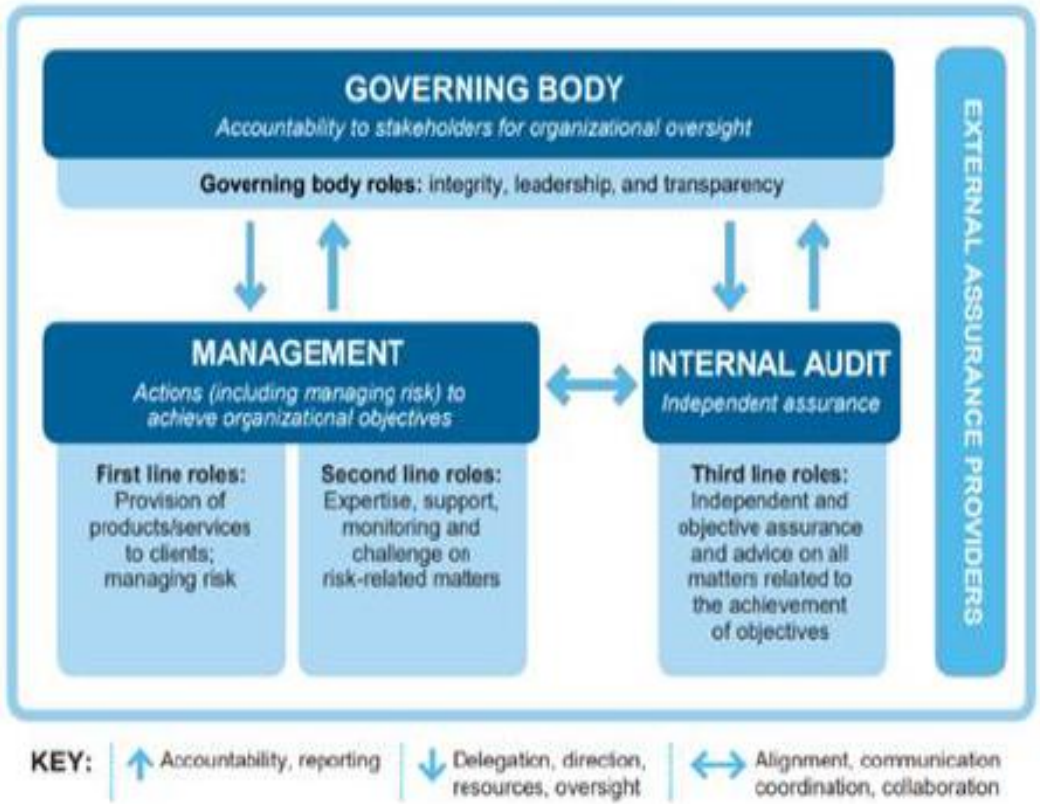
PETROLEUM *Fund*
Looking after your Petroleum Interests

Benefits

MISSION CRITICAL OBJECTIVES

- **Improved knowledge transfer between internal parties.** Everyone benefits from the knowledge, judgement, and approach of other internal parties.
- **More efficient use of resources when eliminating overlapping effort.** Opportunities to share the work improves the efficiency of the work.
- **Focus on higher risk items.** Internal audit is free to focus on the more immediate and significant risk items.
- **One message to executive management and the board.** It is easier for management and stakeholders to synthesize the messages they receive.

The IIA's Three Lines Model



lap and duplication of efforts, which can also
. An effective and fairly easy starting point —
is to create and use an assurance map. An
s in the organization, who provides monitoring
the risk management process, and provides
d and monitored by the appropriate party.

allow or deep as needed to graphically identify
e map identifies the owners of the activities,
vities apply to organizational requirements and
ps in coverage. This exercise of discovery not
stakeholders better execute risk management
ent that can add to management's confidence
ing practices and structures.

Exercising caution is key

While combined assurance is effective for organizational governance in identifying and managing risks, internal audit must take care when relying on the work of others. Relying on the work of others could negatively impact internal audit's independence or objectivity due to:

- Poor quality of work produced by others.
- Differences in view of risk understanding or severity.
- Lack of objectivity of other providers.
- Negative perceptions of internal audit.

A way forward

Risk is complex. Before relying on the work of other parties, a common understanding of risk is needed. The principal challenge with relying on others' work is the setting of boundaries and ensuring a common understanding of definitions. Combined assurance is not to be rushed into. For sound results, take the time to navigate it and achieve an effective way of identifying and verifying the monitoring activities of all providers. Count on the combined assurance approach to help with:

- Coordinating planning and processes.
- Aligning all monitoring activities.
- Alleviating audit fatigue.
- Eliminating duplication of efforts.

Internal audit plays a key role in organizational governance and process improvement. An organization's approach to governance, risk, and control can be strengthen when internal audit works closely with the second line. Embracing this philosophy can be extremely beneficial to the work required, and makes good business sense.

Integrated reporting is a communication framework that explains how a company's strategy, governance, performance, and prospects lead to the creation of value over time, while combined assurance is a model that integrates and optimizes all internal and external assurance processes to provide a holistic view of the organization's risks and controls. Integrated reporting is the **what** (a report), and combined assurance is the **how** (a framework to support the report's integrity).

According to PwC's 24th Annual Global CEO Survey for 2021, CEOs were 'extremely concerned' about the spread of misinformation. At its core, misinformation reflects today's historically low levels of trust. In order to protect stakeholder trust, boards must take a broader and more holistic approach in identifying and managing risk. One such approach to risk management includes the principle of combined assurance as set out in King IV

Key benefits

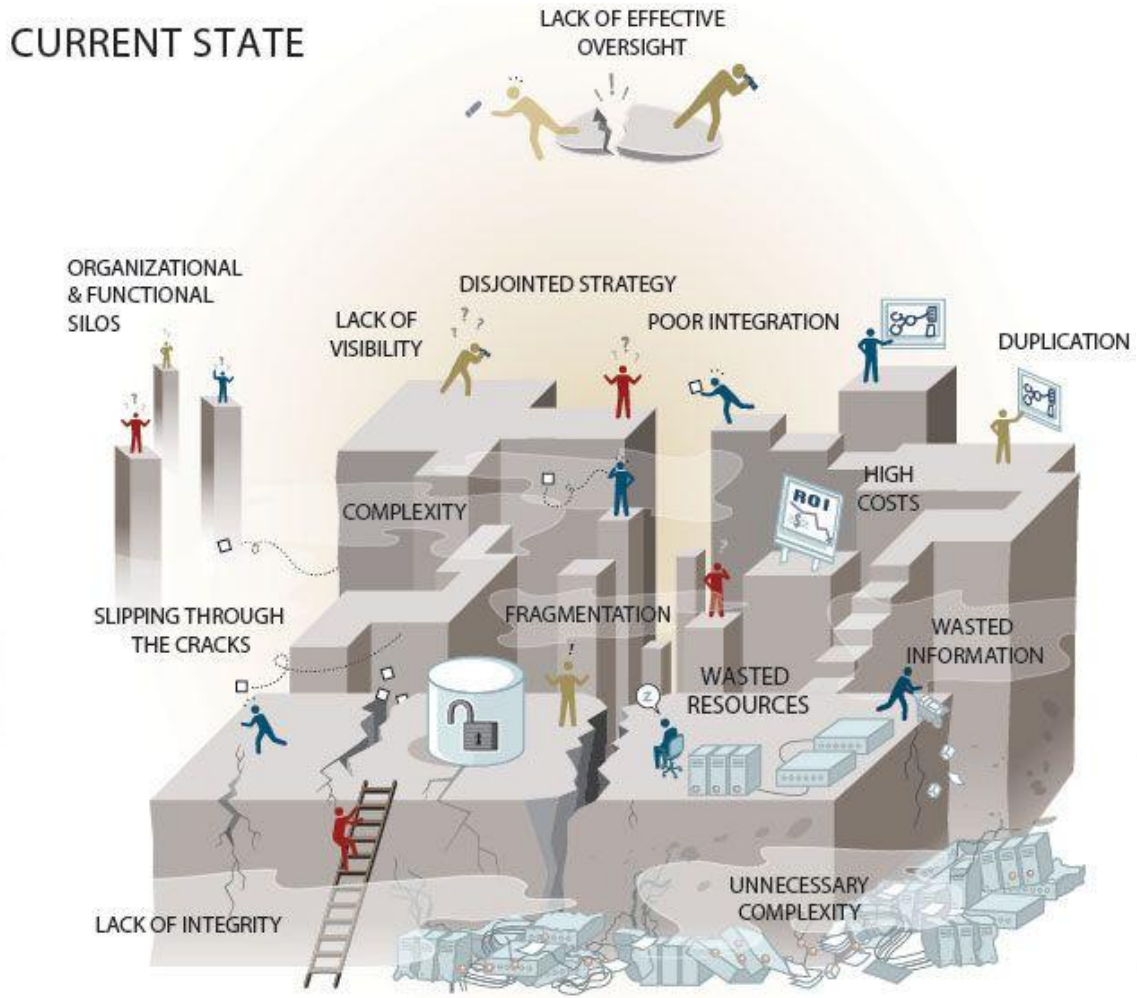
- Coordinated and relevant assurance efforts that are directed to the risks that matter most
- Commitment to enhance controls
- Dashboards that provide an integrated, insightful view for management decision-making
- Assurance activities produce valuable, integrated data based on collaboration and not silos
- Reduction in assurance costs through elimination of duplication and better resource allocation
- A reduction in the repetition of reports by different committees resulting in improved and more efficient reporting
- A comprehensive and prioritised approach in tracking of remedial actions on identified opportunities/weaknesses, and
- The use of combined assurance to support the audit committee and board in making their control statements in the integrated report

New focus of corporate governance

Ethical transparent leadership-improved communication	ESG Factors – competitive advantage
• Integrated reporting	• Environmental responsibility
• Governance practices and ethics	• Social impact
• Disclosure of information	• Risk management
• Stakeholder engagement	• Supplier chain sustainability

Trust **Resilience** **Credibility**

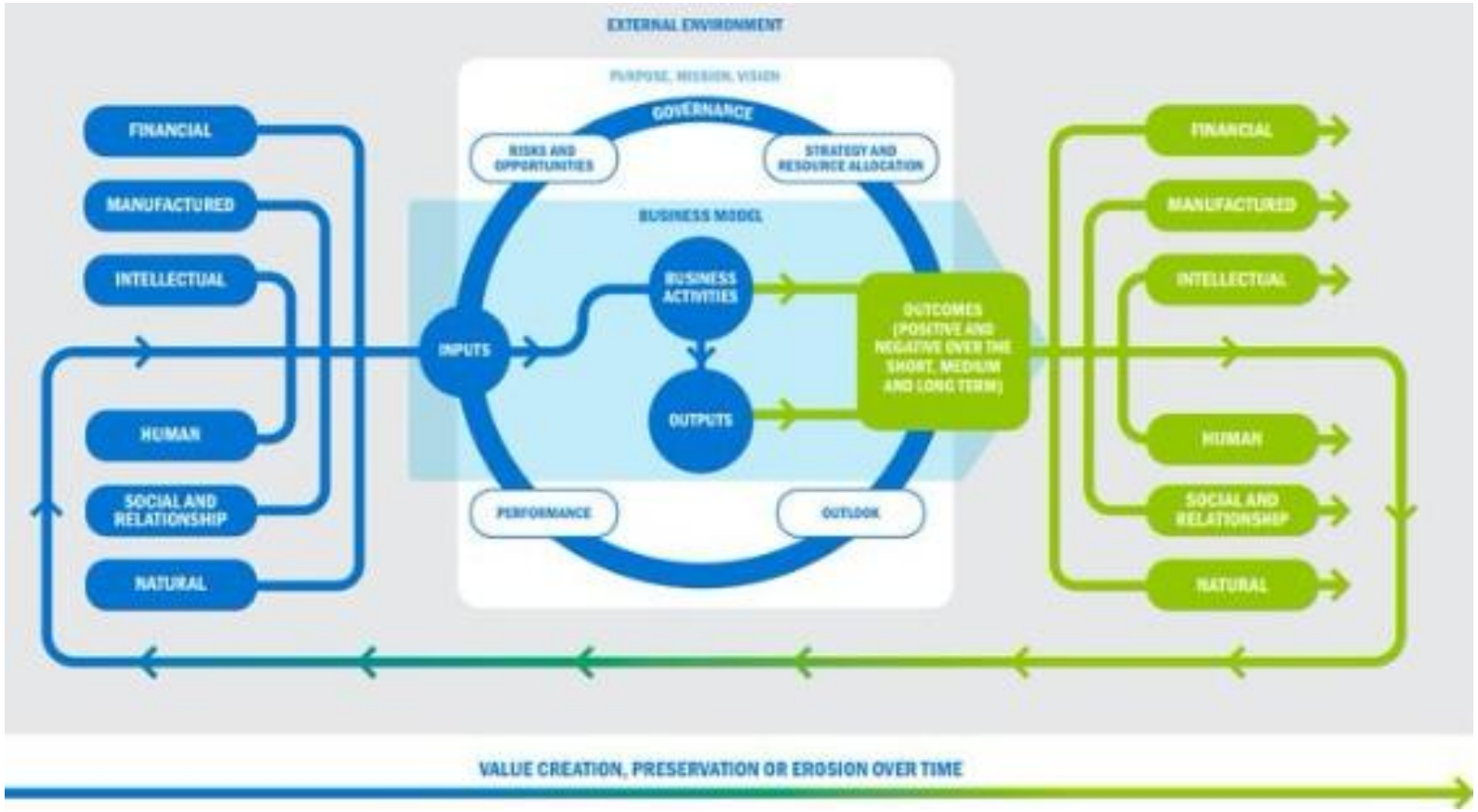
Current State Evaluation – Integrated Governance



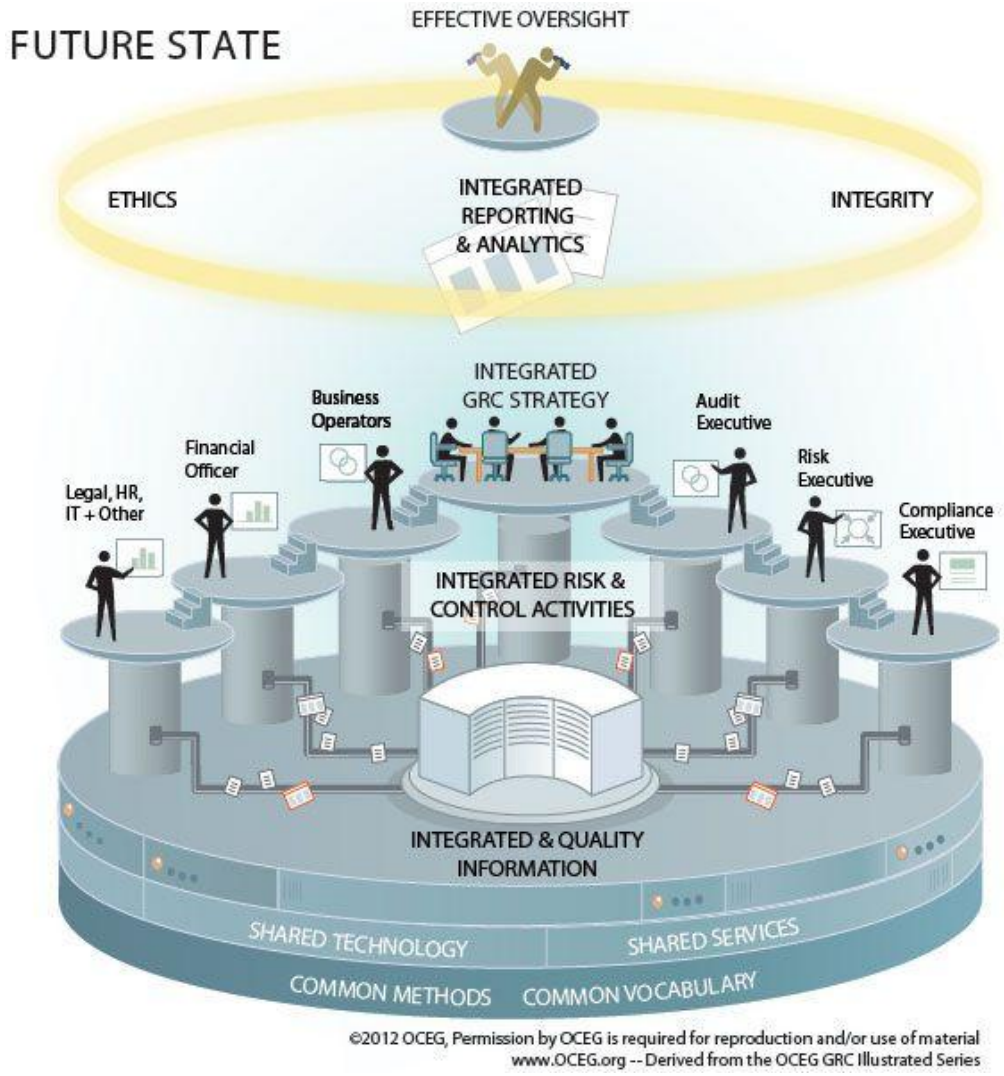
Gut-feel Evaluation

Element	Rating 1	Rating 2	Rating 3	Rating 4	Rating 5
Effective oversight					
Strategic decisions					
Organizational structure | silos					
Visibility – transparency					
Integration of key processes					
Duplication					
Excessive cost					
Fragmentation					
Wasted resources					
Wasted information					
Complexity					
Integrity					

Value creation

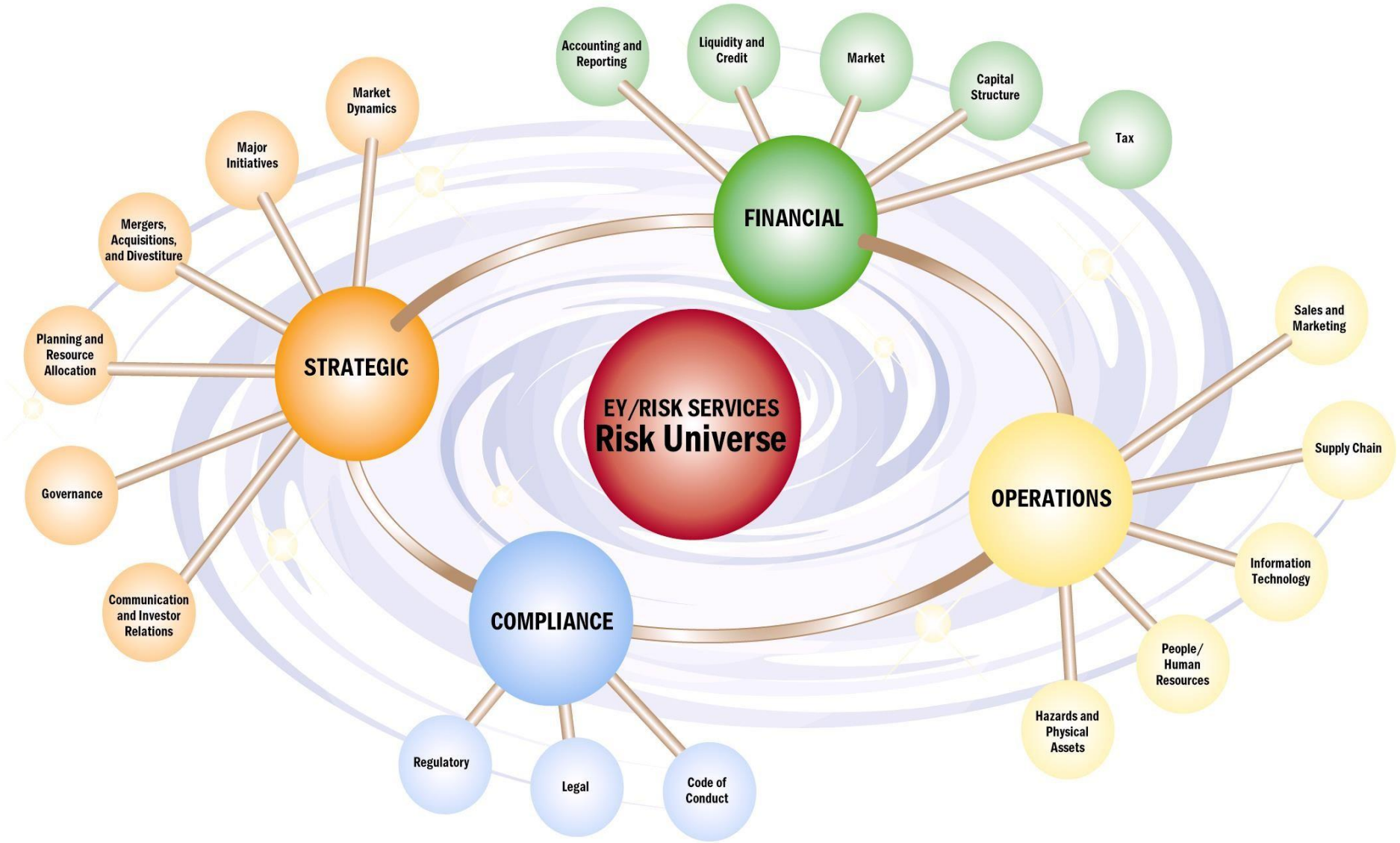


GRC – Implementation Strategy

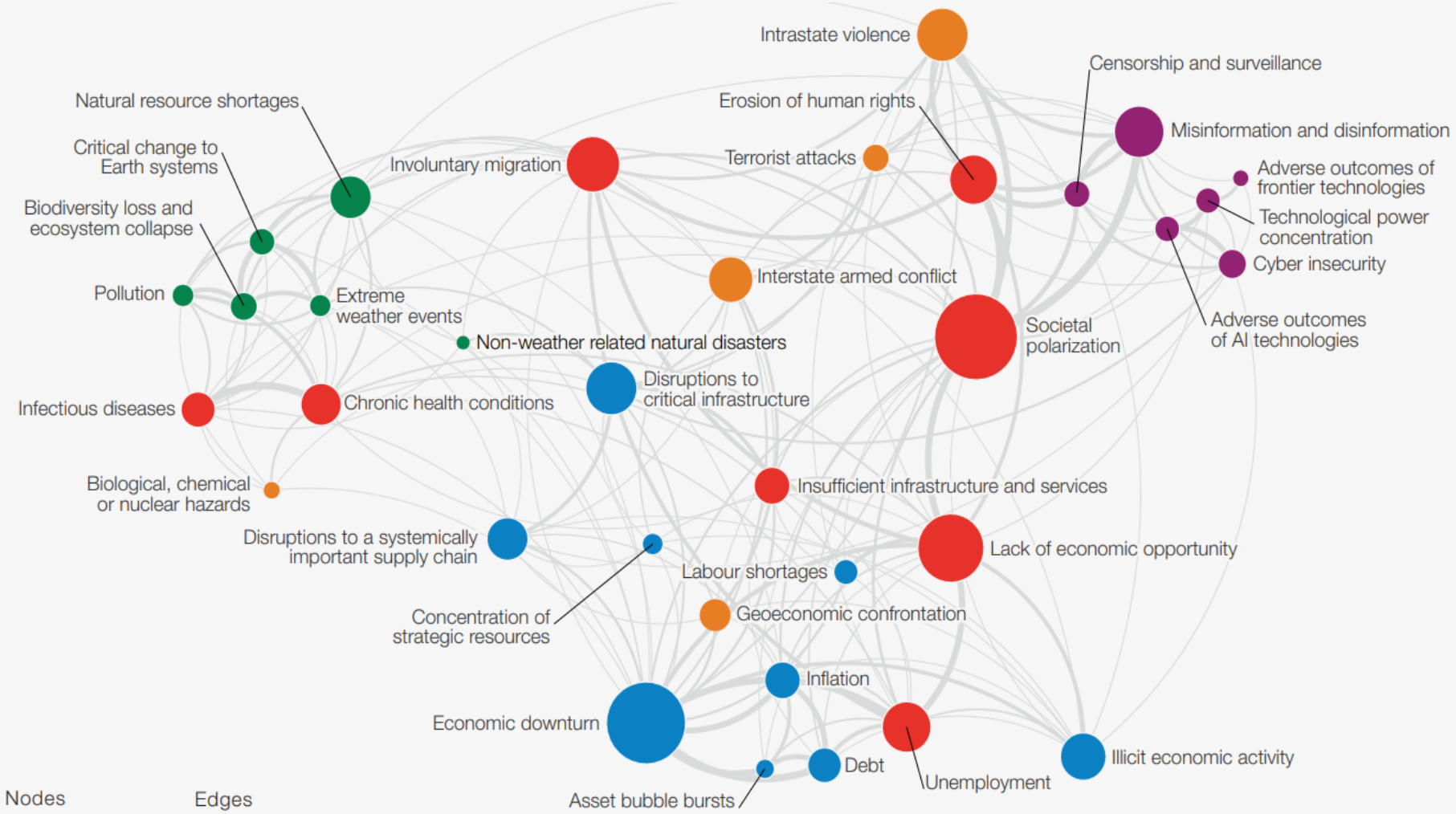



RISK MANAGER
RISK MANAGER
RISK MANAGER
DECISION-MAKER
DECISION-MAKER
DECISION-MAKER

Risk universe



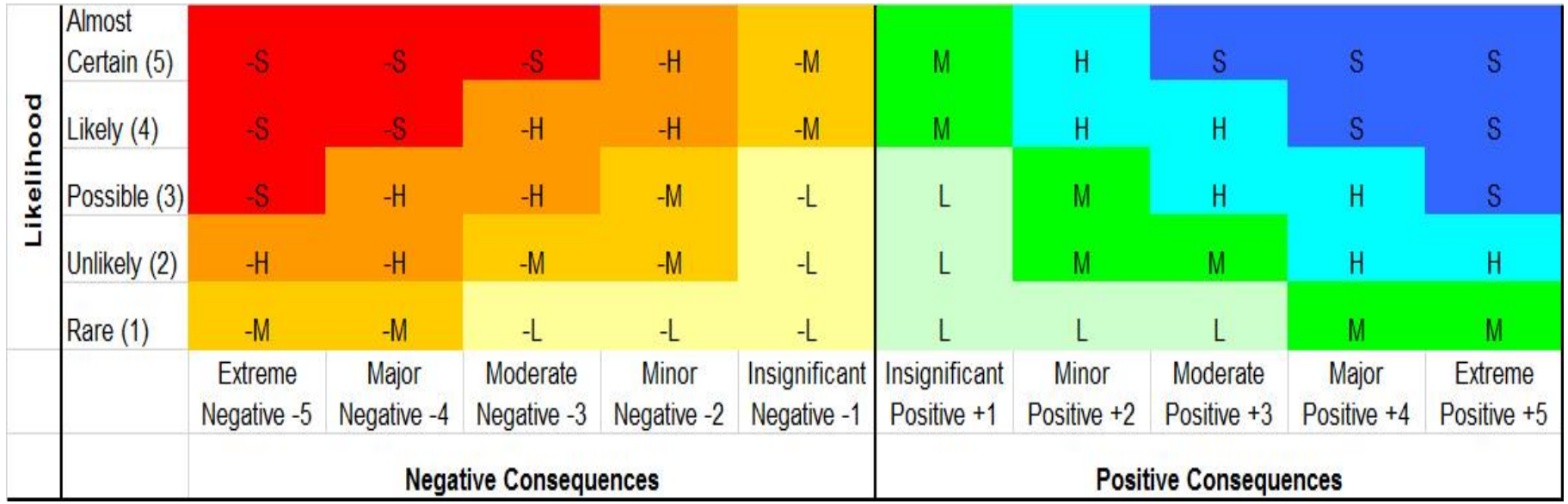
Emerging Risk Radar



Risk Management

- Identifying areas of threat to the business
- Assessing the potential impacts and managing these
- Growth and continued existence of the business

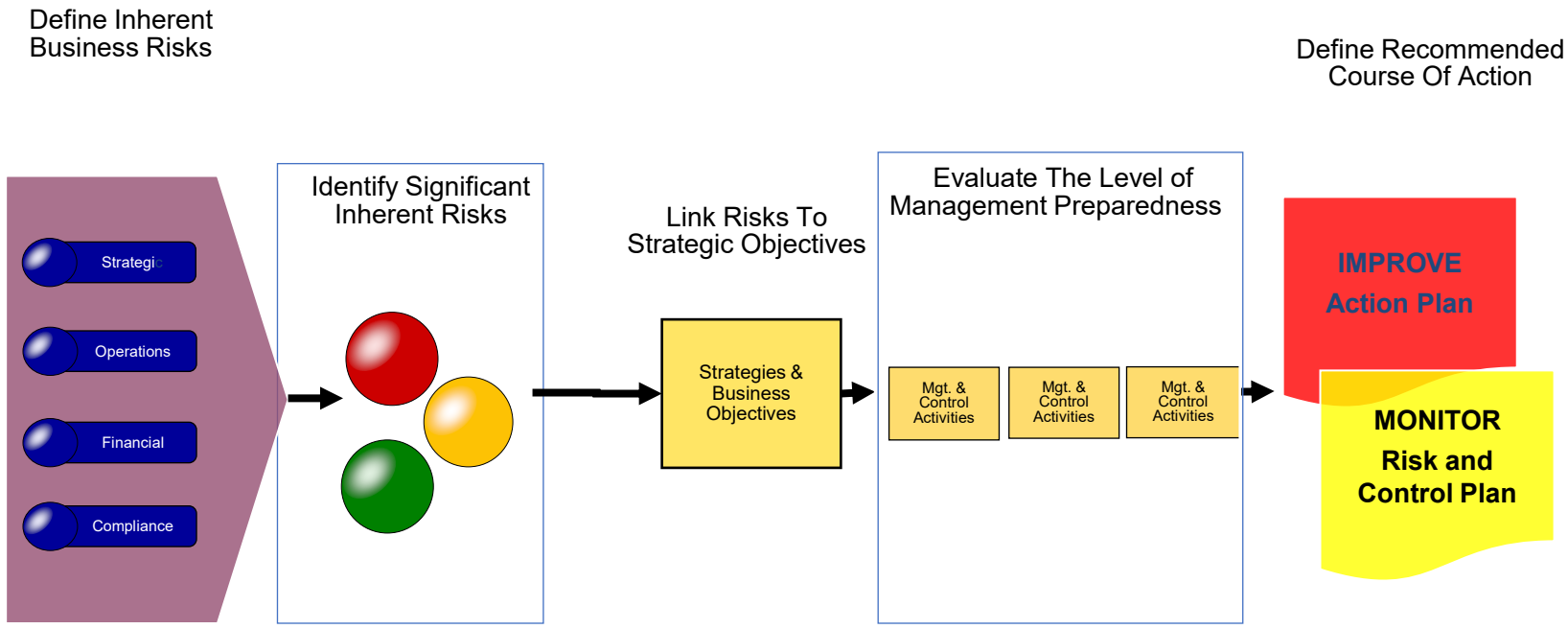
Risk versus opportunity



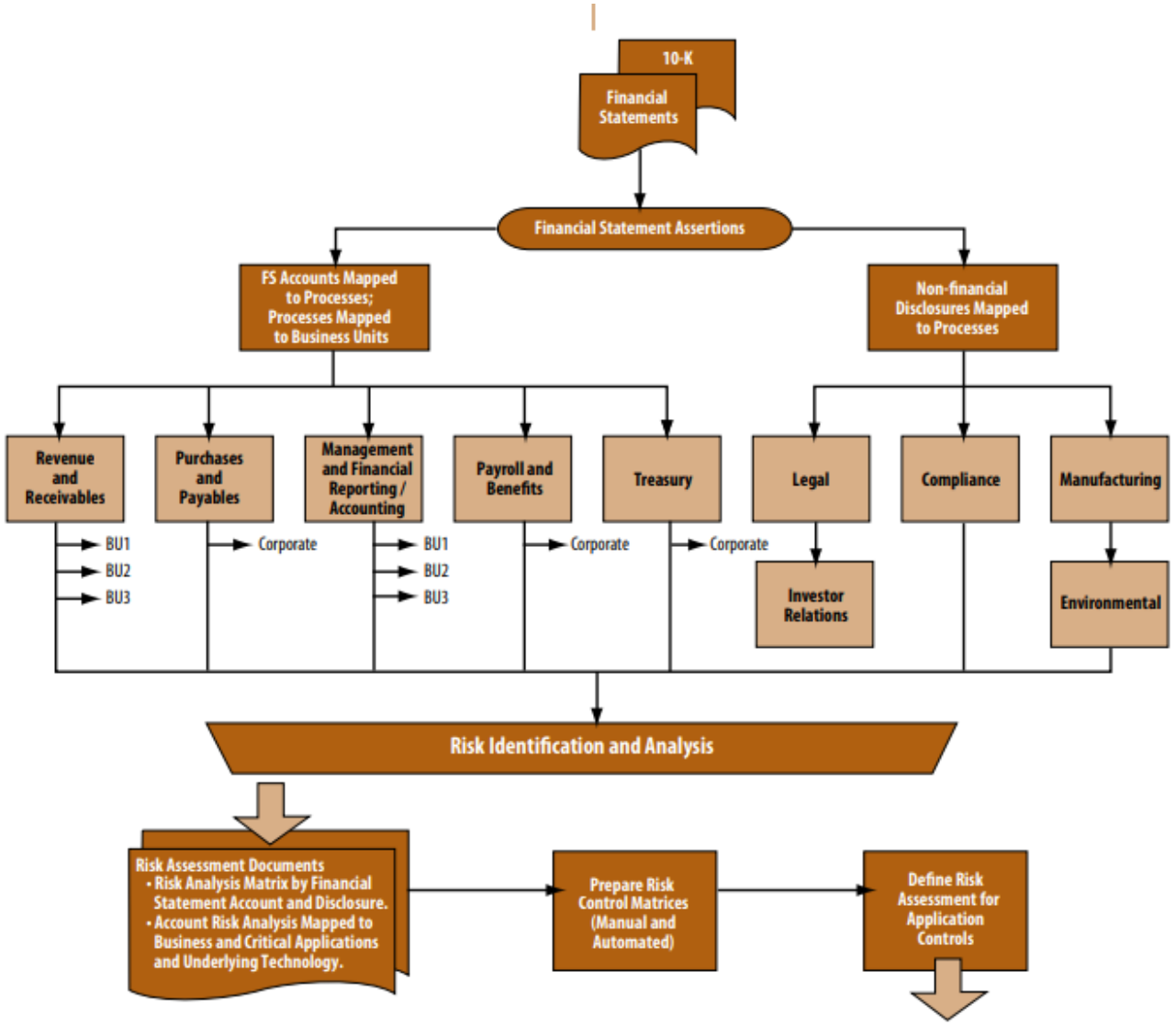
Likelihood											
	Almost Certain (5)	-S	-S	-S	-H	-M	M	H	S	S	S
	Likely (4)	-S	-S	-H	-H	-M	M	H	H	S	S
	Possible (3)	-S	-H	-H	-M	-L	L	M	H	H	S
	Unlikely (2)	-H	-H	-M	-M	-L	L	M	M	H	H
	Rare (1)	-M	-M	-L	-L	-L	L	L	L	M	M
		Extreme Negative -5	Major Negative -4	Moderate Negative -3	Minor Negative -2	Insignificant Negative -1	Insignificant Positive +1	Minor Positive +2	Moderate Positive +3	Major Positive +4	Extreme Positive +5
		Negative Consequences					**Positive Consequences**				

Enterprise Risk Management (ERM) Approach

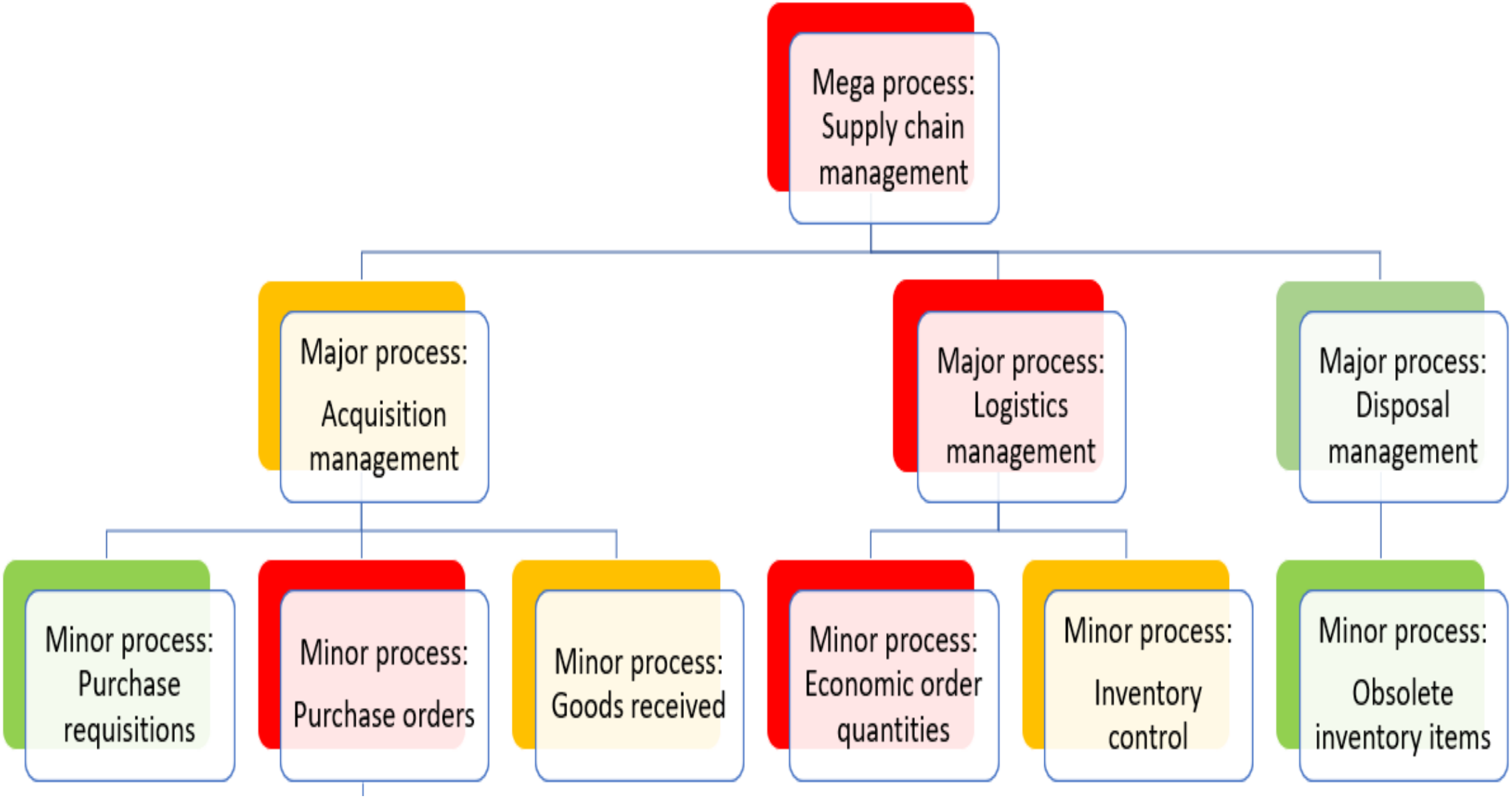
The structured ERM approach defines the key risks to business objectives across the organization and evaluates the level of management preparedness to clearly define opportunities to improve and/or monitor risks.



Process universe



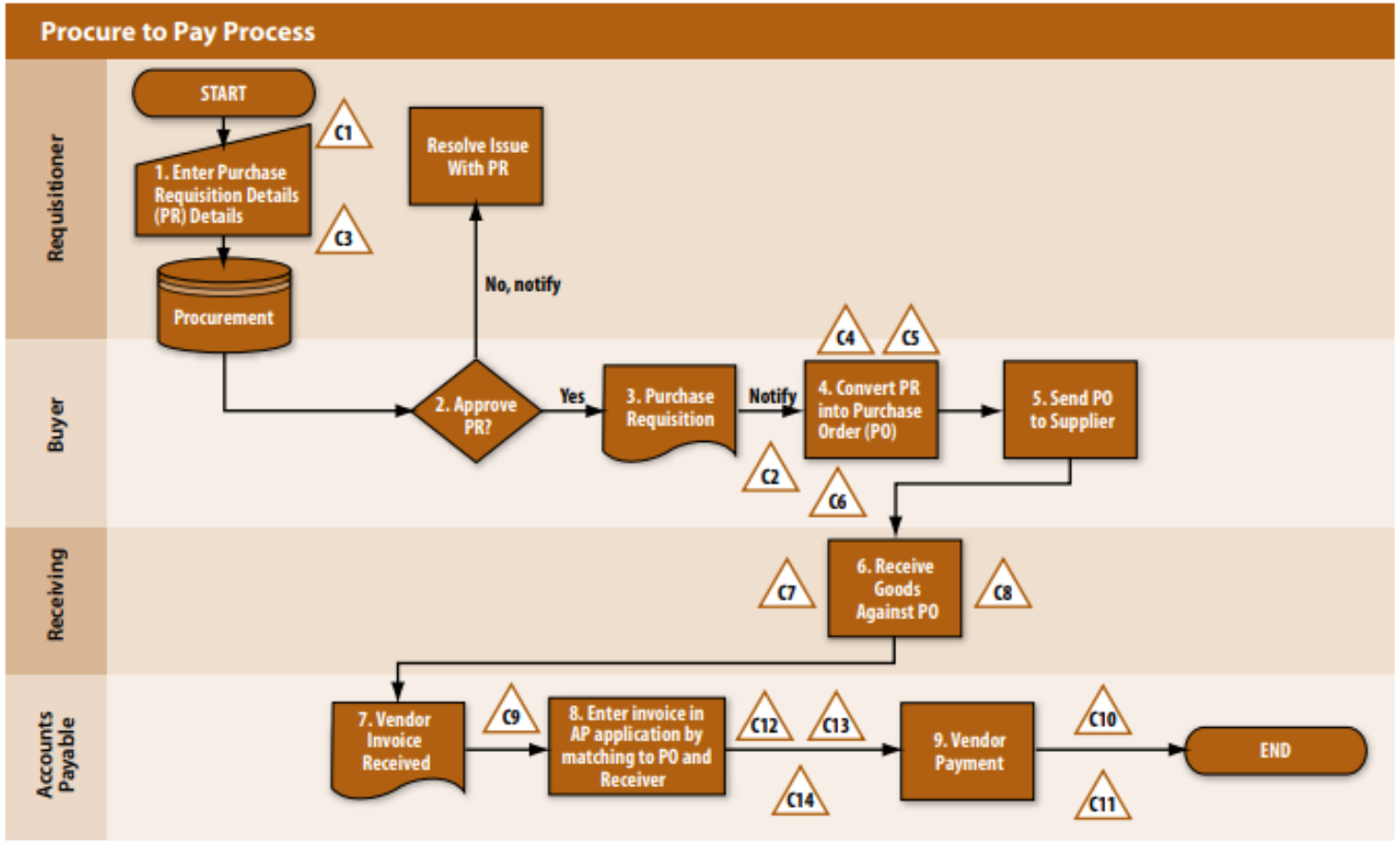
Mega Process (Level 1): Procure-to-Pay		
Major Process (Level 2)	**Subprocess (Level 3)**	**Activity (Level 4)**
Procurement	Requisition processing	Create, change, and delete
	Purchase order processing	Create, change, delete, approval, and release
Receiving	Goods receipt processing	Create, change, and delete
	Goods return processing	Create, change, and delete
Accounts Payable	Vendor management	Create, change, and delete
	Invoice processing	Create, change, and delete
	Credit memo processing	Create, change, and delete
	Process payments	Create, change, and delete
	Void payments	Create, change, and delete


Mega process: Supply chain management
Major process: Acquisition management
Major process: Logistics management
Major process: Disposal management
Minor process: Purchase requisitions
Minor process: Purchase orders
Minor process: Goods received
Minor process: Economic order quantities
Minor process: Inventory control
Minor process: Obsolete inventory items

Control objectives

Safeguarding of assets	Compliance	Reliability and integrity of information	Economic, Effective, Efficient use of resources
• Physical safeguarding • Access controls • Segregation of duties	• Laws and regulations • Policies and procedures • Contractual obligations	• Accuracy • Completeness • Timely • Validity or authorization	• Economic – right CQQT • Efficient – Output versus input • Effective – Outcome versus output

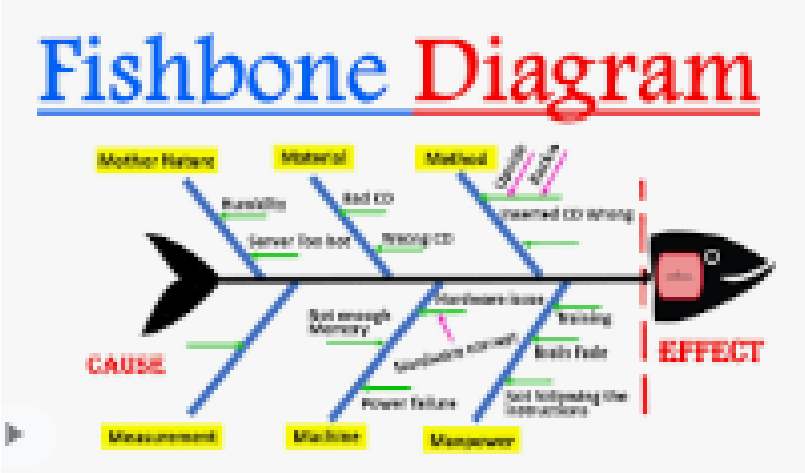
Process overview flowchart



Risk and Control Matrix: Procure-to-Pay

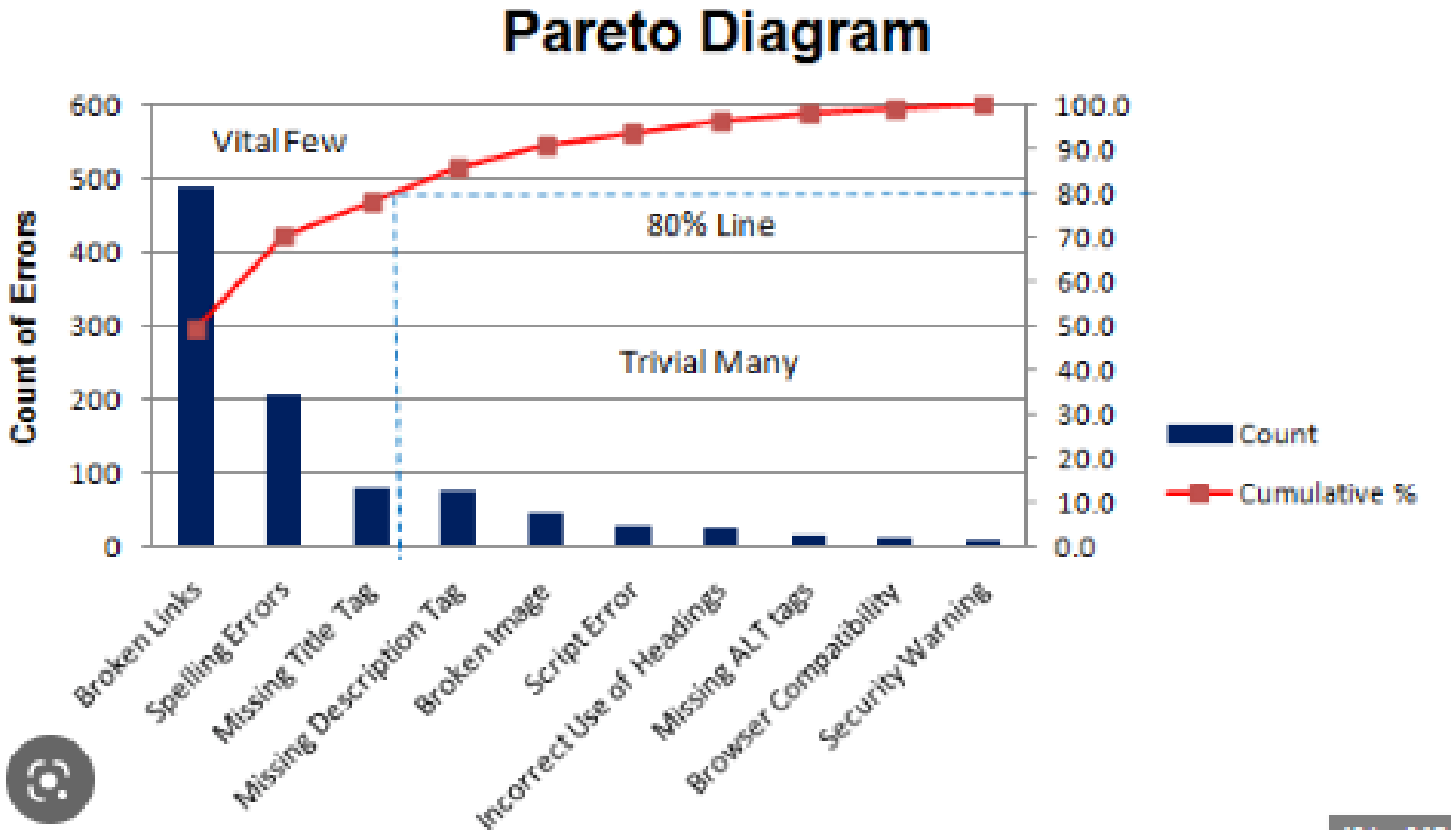
	BUSINESS PROCESS & CONTROL OBJECTIVES	RISKS		CONTROL ACTIVITIES	COSO COMPONENTS					CONTROL ATTRIBUTES				CONTROL CLASSIFICATION						TESTING		
Number	Control Objectives	Risks	Impact/ Likelihood	Control Activities	CE	RA	CA	I/C	M	K (Y/N)	Man/Auto	Pre/Det	Frequency	Real	Recorded	Valued	Timely	Classified	Posted	Test Results	Operational Effectiveness (Y/N)	Notes

Root cause analysis



- Mother nature (Environment)
- Materials (Cash, credit control, Inventory)
- Machines (Assets, maintenance, capital budget)
- Methods (Process design, automation)
- Manpower (Succession planning, vacancy rate, incompetence)
- Measurements (dashboards, monitoring, detection)

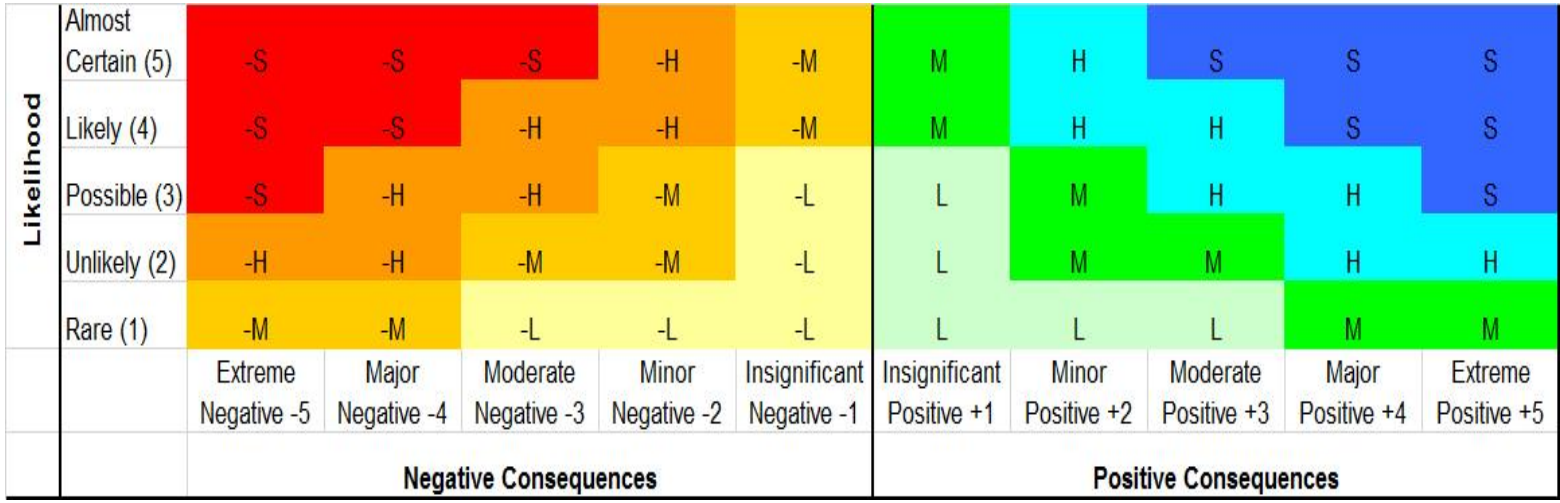
Pareto analysis



Risk management strategy

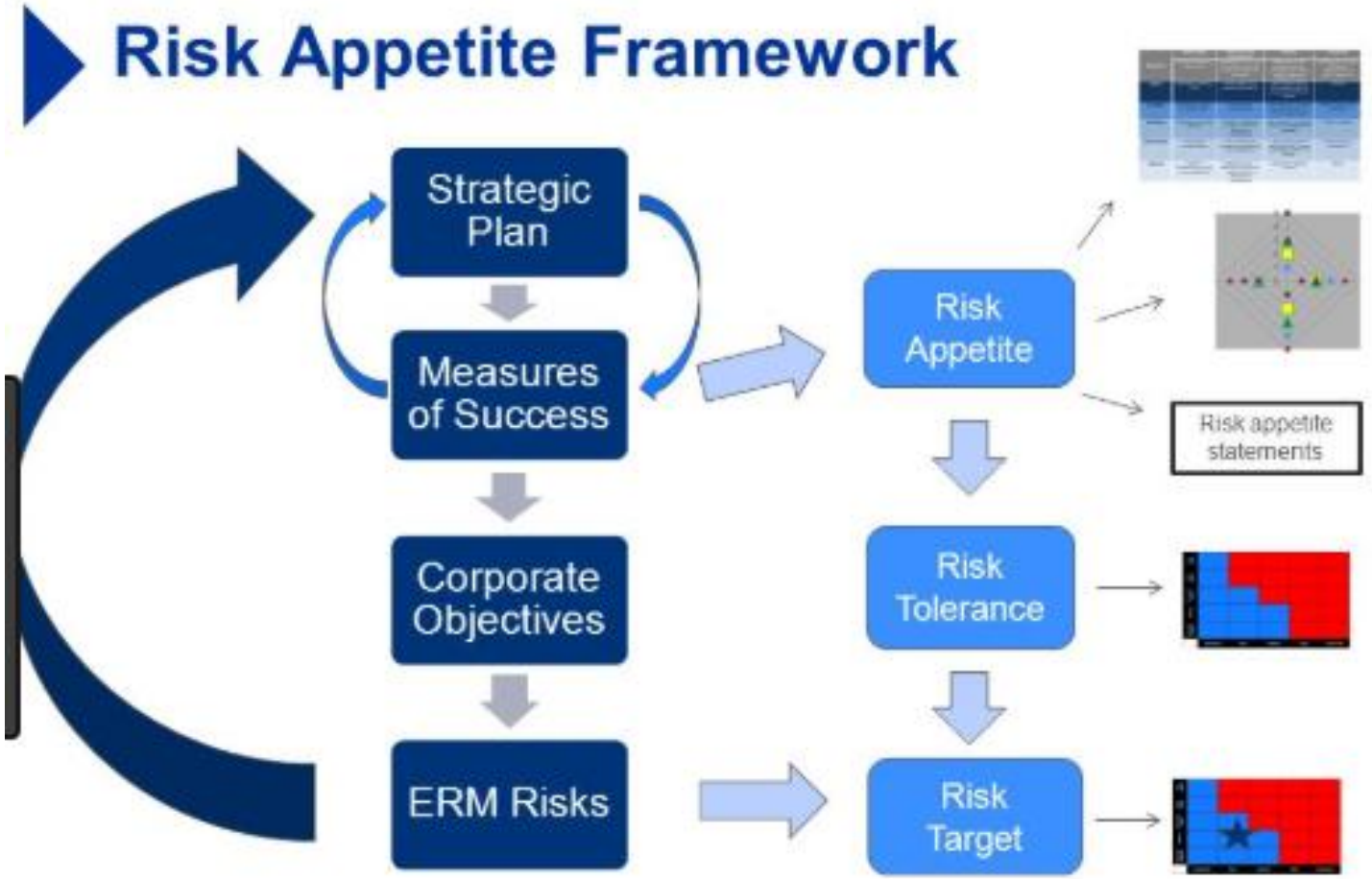
- Avoid
- Accept
- Transfer
- Mitigate

Take risk

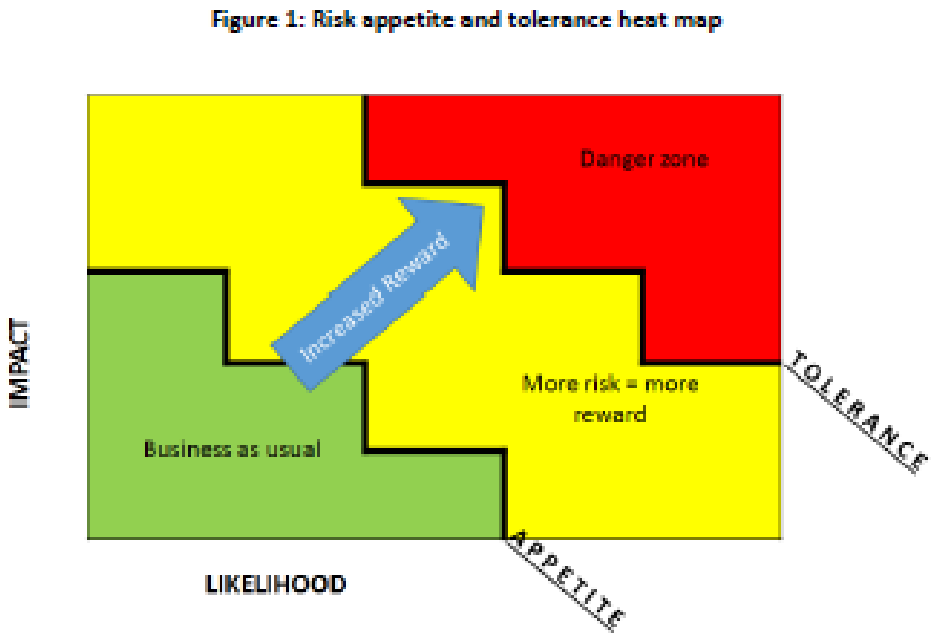


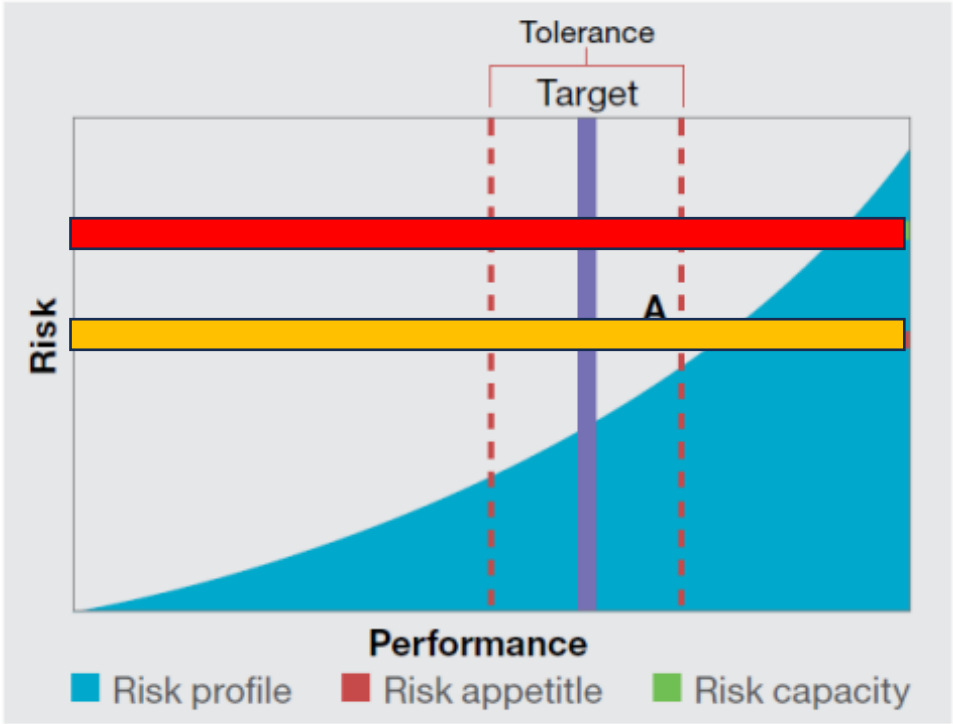
Likelihood											
	Almost Certain (5)	-S	-S	-S	-H	-M	M	H	S	S	S
	Likely (4)	-S	-S	-H	-H	-M	M	H	H	S	S
	Possible (3)	-S	-H	-H	-M	-L	L	M	H	H	S
	Unlikely (2)	-H	-H	-M	-M	-L	L	M	M	H	H
	Rare (1)	-M	-M	-L	-L	-L	L	L	L	M	M
		Extreme Negative -5	Major Negative -4	Moderate Negative -3	Minor Negative -2	Insignificant Negative -1	Insignificant Positive +1	Minor Positive +2	Moderate Positive +3	Major Positive +4	Extreme Positive +5
		Negative Consequences					Positive Consequences				

Residual risk versus risk appetite



Old versus new



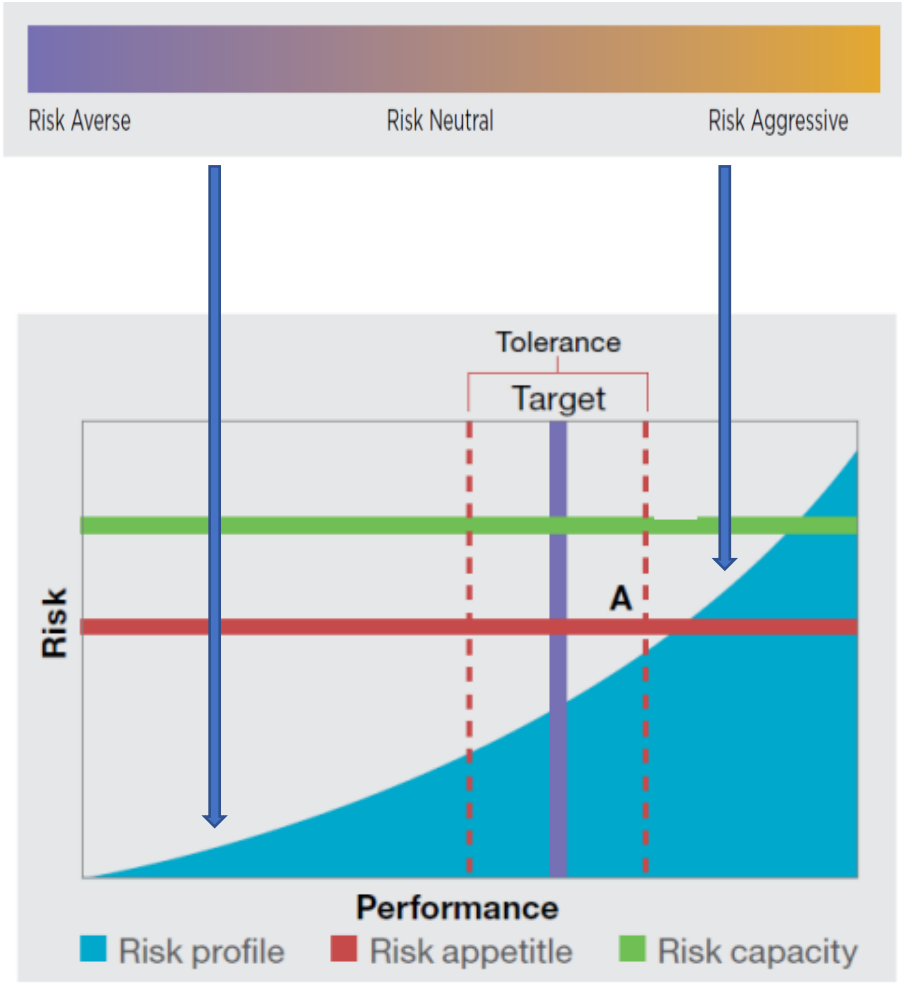


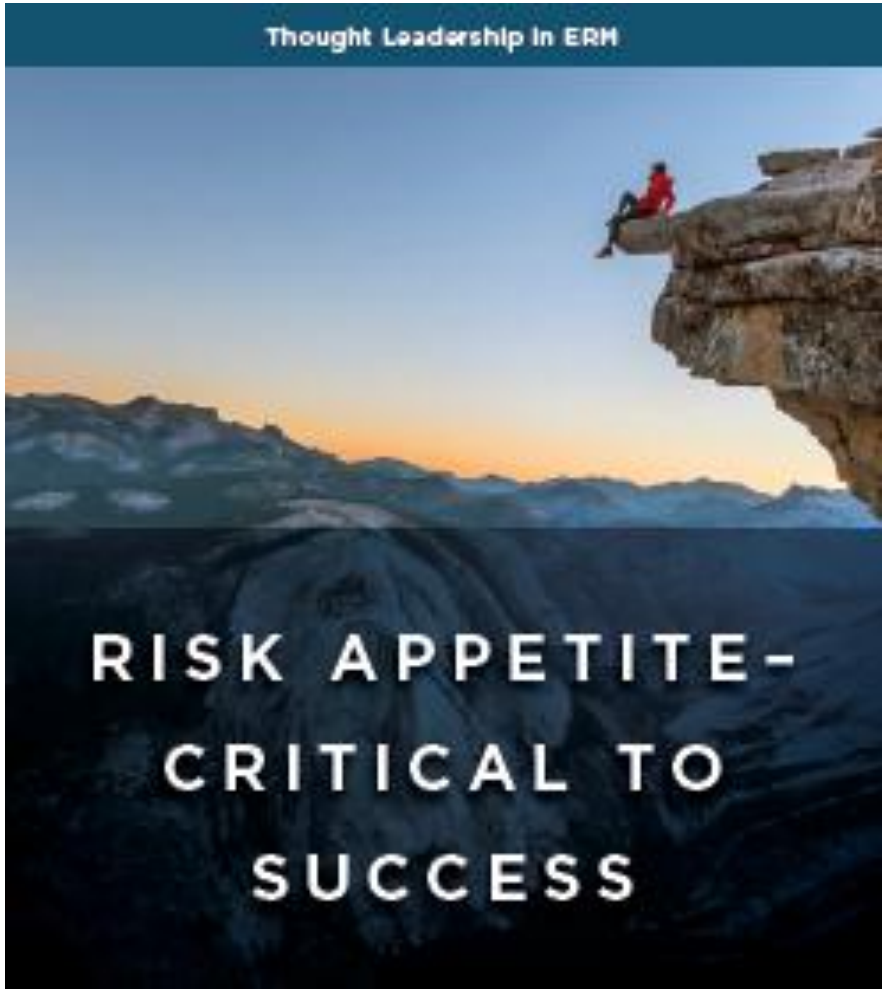
Inputs to risk appetite

Strategic direction

Risk appetite is a fundamental part of setting strategy and objectives, providing context as the organization pursues a given level of performance. For example, setting a goal of growing the customer base by 2% likely has a very different risk profile than growing it by 12%.

The discussion of appetite is not always about taking on too much risk. Sometimes it is about an organization becoming overly risk-averse—that is, being unwilling to accept more risk to drive performance. Revisiting the organization's appetite from time to time can help management and the board understand that the organization may need to take additional risk to thrive, or that it needs to expand, not contract. Moreover, although an organization often can adjust to take on more risk within the set appetite, there may be times where it needs to adjust appetite, or perhaps even strategy, to accommodate a shifting business environment.





Inherent in this definition are several key points. Risk appetite:

- Is intentionally broad to apply across an organization, recognizing that it may differ within various parts of the organization while remaining relevant in changing business conditions.
- Focuses on risk that needs to be taken to pursue strategies that enhance long-term success.
- Recognizes that risk is more than individual decisions.
- Links to value—it is tied to the choices the organization makes on how it creates and preserves value.

This paper is structured into the following sections:

1. **Putting Risk Appetite into Context of the Business**—Focuses on how organizations take on risk to innovate and grow, and shows that appetite must be flexible enough to adapt to changing conditions, helping an organization to remain relevant in an evolving landscape.

2. **Linking Risk Appetite and Strategy**—Emphasizes the importance of understanding strategy and objectives and that taking risks requires a sense of the type and amount of risk acceptable and necessary in pursuing strategies and objectives. It explores a key difference in adopting an objective-focused and a risk-focused approach.

3. **Overview of Inputs to and Application of Risk Appetite**—Provides an overview of how risk appetite is applied in the context of strategy and objectives, developed to support decision-making, and used to enhance performance. Each of these points is developed in the following sections.

4. **Inputs to Risk Appetite**—Considers the inputs that affect how risk appetite is applied. Among the more important are the organization's mission and vision, board and management perspectives on appetite, the current strategy to pursue value, risk profile, and culture.

5. **Developing Risk Appetite to Support Strategy and Objectives**—Considers how an organization develops risk appetite in the context of overall strategy, and how it incorporates risk appetite into objective-setting. This section explores how organizations may use different approaches to build consensus and encourage more consistent decision-making.

6. **Articulating and Communicating Risk Appetite to Support Decision-making**—Considers how an organization can clearly and consistently articulate risk appetite to enhance decision-making, especially when boards and management may not agree. Being able to clearly communicate appetite improves when there is a commonly applied structure, one that considers the choice of language, the intended level of precision, and a focus on strategy and objectives rather than risks.

7. **Using Risk Appetite to Enhance Performance**—Considers how risk appetite is used to develop tolerance, measures, and indicators, and to monitor performance in day-to-day practices.

8. **Supporting the Use of Appetite**—Offers our views on what organizations need to do to sustain risk appetite as part of an effective approach for enterprise risk management.

9. **Final Thoughts**—Wraps up our views that successful organizations take risk to succeed.

Best practice risk management frameworks

20 key principles within each of the five components

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

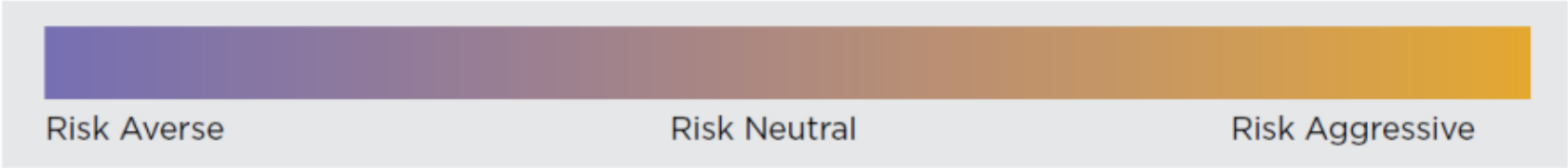
Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Graphic has stronger ties to the business model

Importance of culture

- Addresses the growing focus, attention and Importance of culture within enterprise risk management
- Influences all aspects of enterprise risk management
- Explores culture within the broader context of overall core
- Depicts culture behavior within a risk spectrum



- Explores the possible effects of culture on decision making
- Explores the alignment of culture between individual and entity behavior

- Explores strategy from three different perspectives:
  - The possibility of strategy and business objectives not aligning with mission, vision and values
  - The implications from the strategy chosen
  - Risk to executing the strategy

Integration= improved decisions = enhanced performance

- It helps organizations to:
  - Anticipate risks earlier or more explicitly, opening up more options for managing the risks
  - Identify and pursue existing and new opportunities
  - Respond to deviations in performance more quickly and consistently
  - Develop and report a more comprehensive and consistent portfolio view of risk
  - Improve collaboration, trust, and information sharing

PETROLEUM *Fund*
Looking after your Petroleum Interests

Links to performance

- Enables the achievement of strategy by actively managing risk and performance
- Focuses on how risk is integral to performance by:
  - Exploring how enterprise risk management practices support the identification and assessment of risks that impact performance
  - Discussing tolerance for variations in performance
- Manages risk in the context of achieving strategy and business objectives – not as individual risks

KPI's and KRI's

Key Performance Indicators (KPIs) help a firm see how it is performing in relation to its strategic goals and objectives.

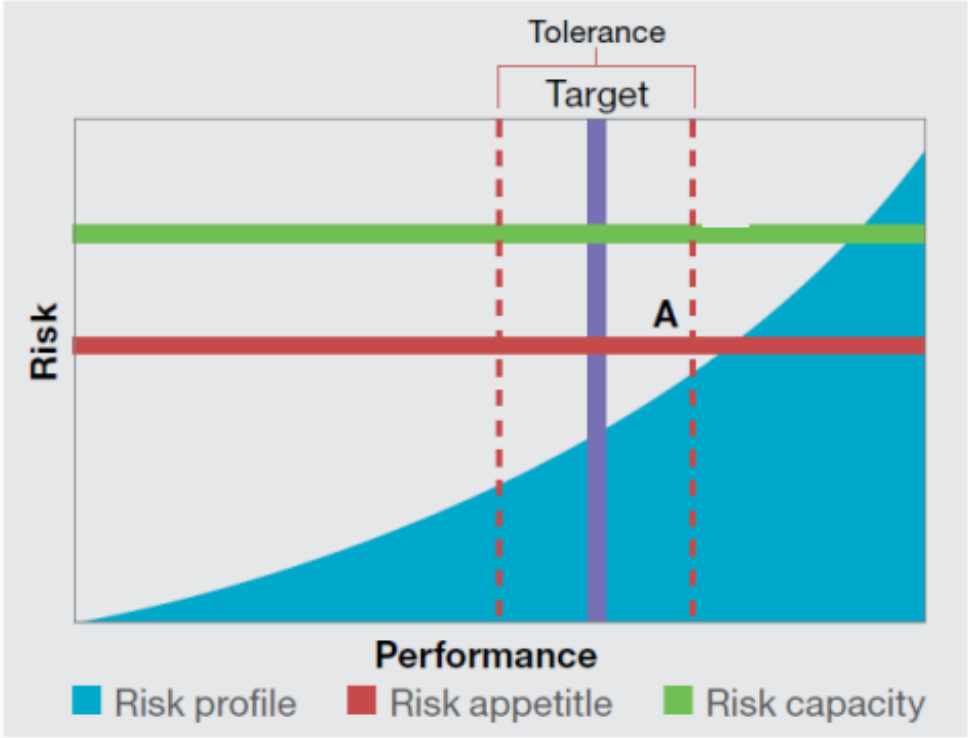
Key Risk Indicators (KRIs) are leading indicators of risk to business performance, giving early warning about potential risk event

Use KRIs to monitor risks are in the areas such as:

- natural catastrophe risks (as % of group shareholder equity)
- asset-liability matching (duration mismatch)
- strategic asset allocation (% allowed in investment category)
- credit risk (weighted average credit rating)
- other risks specific to business or functional areas

Risk versus performance

- Introduces a new depiction referred to as a risk profile
- Incorporates:
  - Risk
  - Performance
  - Risk appetite
  - Risk capacity
- Offers a comprehensive view of risk and enables more risk-aware decision making



- The framework provides a complete depiction of how to build a risk profile in an appendix

Design, build and implementation of Key Risk Indicators

Design

- Establish extent of existing management information and other data flows – indicators in place if applicable
- Identify committees, forums, management meetings etc currently in place that can be used to discuss risk and control issues on an ongoing basis
- Define and document roles and responsibilities of risk and control owners

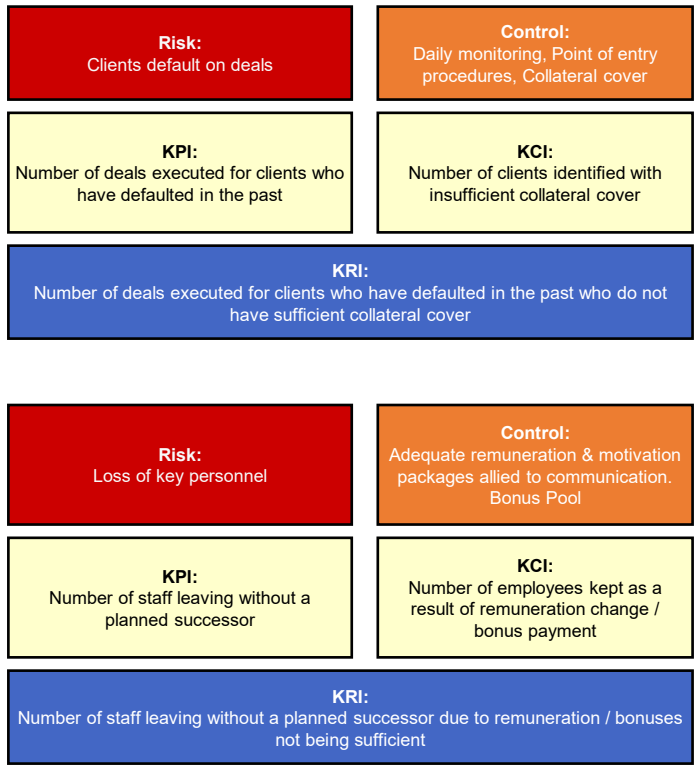
Build Process

- Assign ownership for risks and controls
- Communication with risk and control owners relating to their ongoing responsibilities
- Carry out workshops with all risk and control owners to design indicators to be put in place
- Define how existing information flows and committees etc are to be used to minimise additional workload
- Risk and control owners refine the indicator monitoring process
- Overall analysis of indicators for gaps and dual coverage
- Design reporting protocols

Ongoing Operation of Process

- Design review mechanism (i.e. Corporate Risk department or Internal Audit, etc.)
- Create storage mechanism for information
- Perform ongoing consistency checks of indicators set up across the organisation

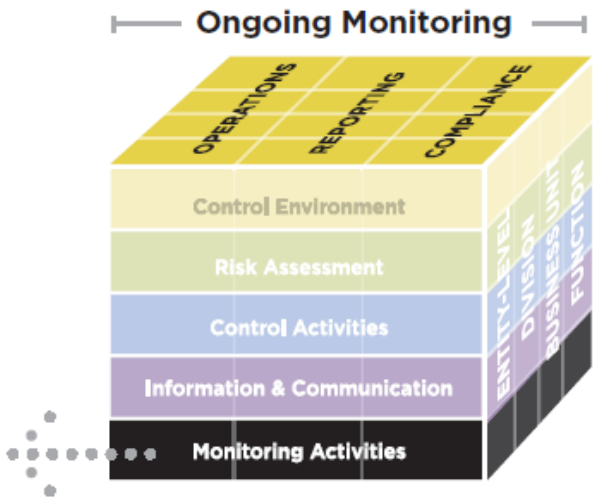
Example KPI, KCI and KRIs



Risk aware decision-making

Second line of defense

Figure 5. COSO and the 2nd Line of Defense

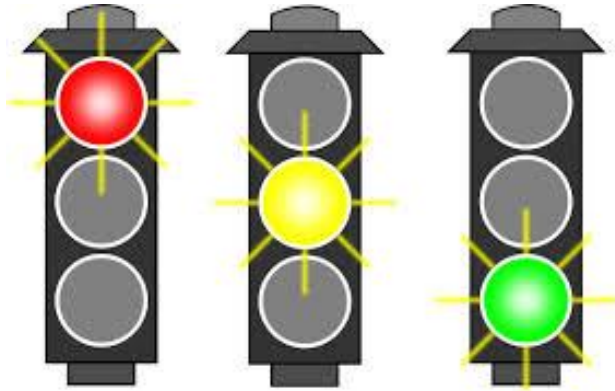


Monitoring Activities

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

2nd Line of Defense

- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

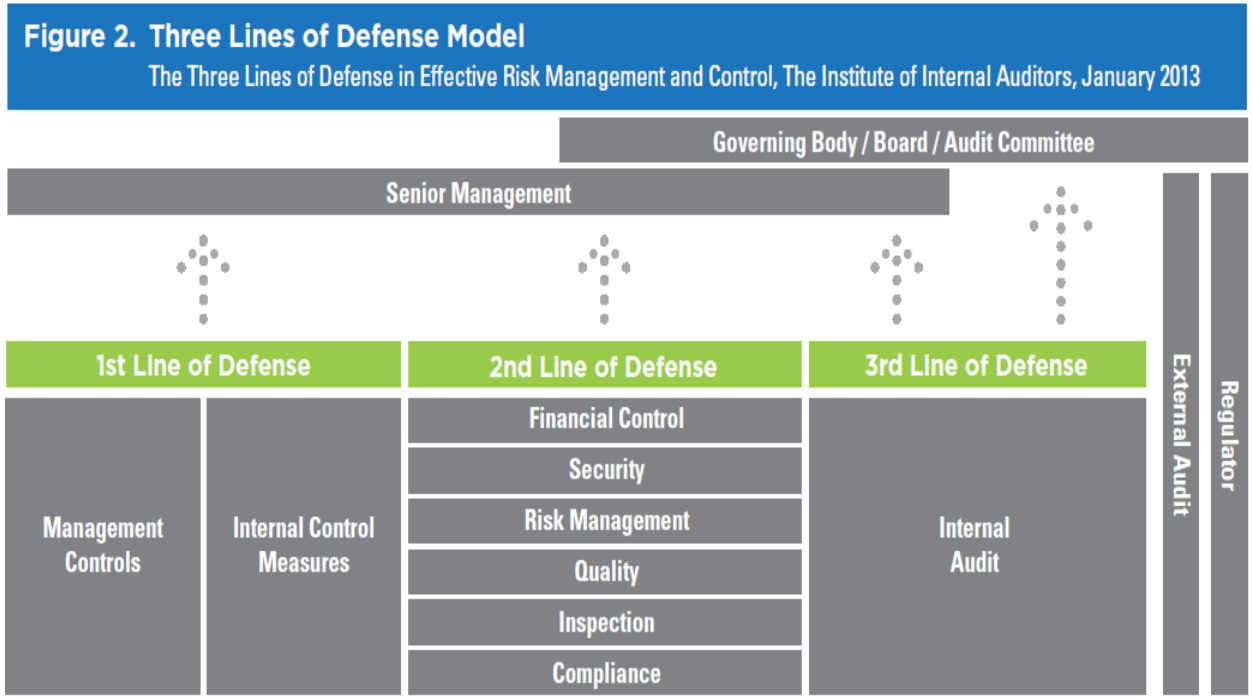


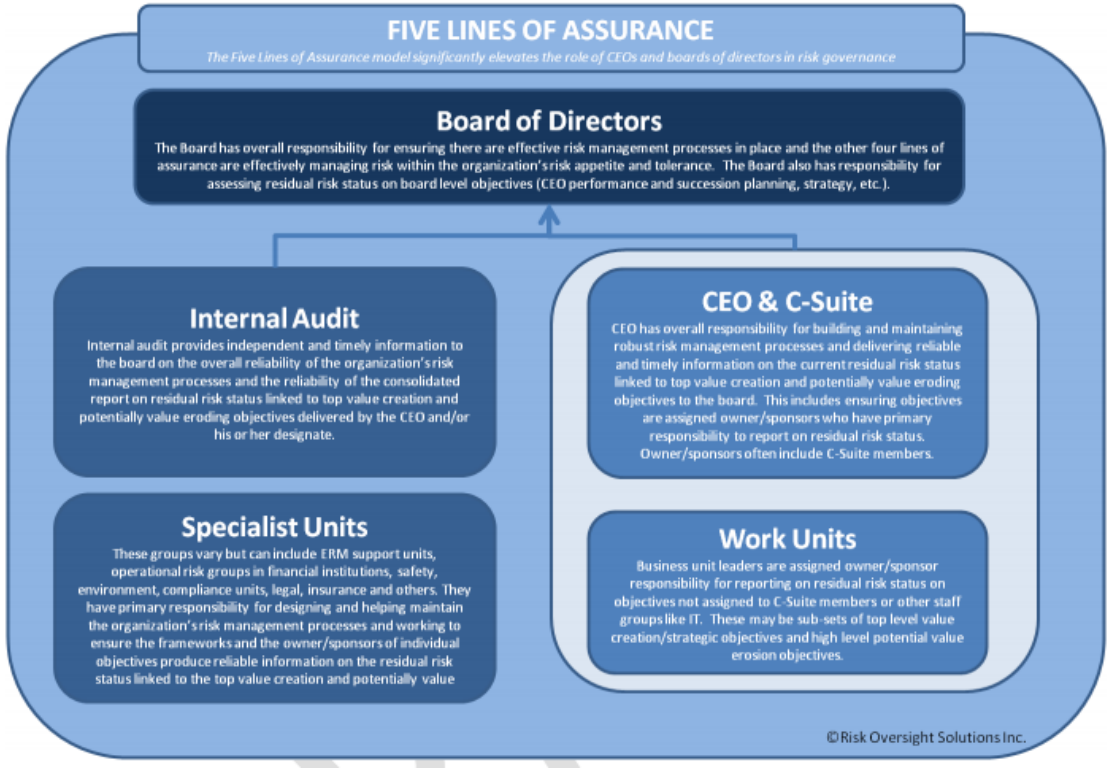
C. EWRM TRAINING – RISK CHAMPIONS (25 PARTICIPANTS)

Duration: 1 Day | **Format:** Hybrid

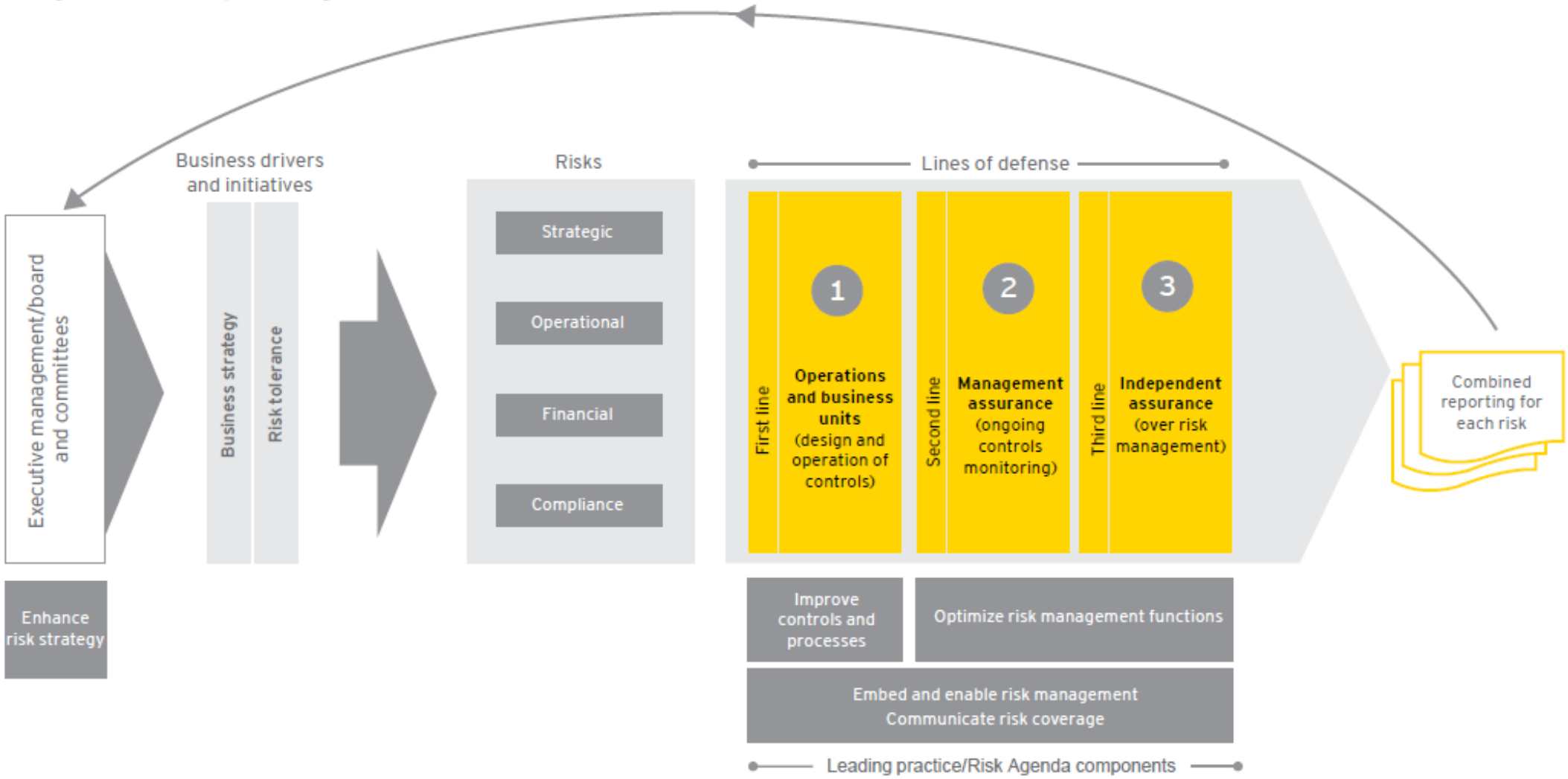
Session	Objective	Key Deliverables	Practical Application
1	Build operational risk awareness within an integrated control environment/ combined assurance structure.	Identify key operational risks. | Link each to control processes. | Map control ownership under the Three Lines Model.	Document 3 operational risk incidents and controls.
2	Develop and maintain risk registers using integrated data systems informing combined assurance and board effectiveness.	Populate risk registers aligned with integrated reporting. | Prioritize key risks using control analytics. | Integrate assurance data sources for accuracy.	Update a sample departmental risk register.
3	Implement control monitoring and risk responses.	Link operational controls to governance requirements. | Evaluate control effectiveness via assurance mapping. | Track remediation actions across departments.	Conduct a control self-assessment exercise.
4	Strengthen risk communication across all the assurance lines.	Develop clear escalation protocols. | Align reporting templates to integrated data and communication principles. | Foster a transparent risk culture.	Simulate a near-miss event escalation.

Combined assurance





Integrated LOD (Lines of Defense) Model

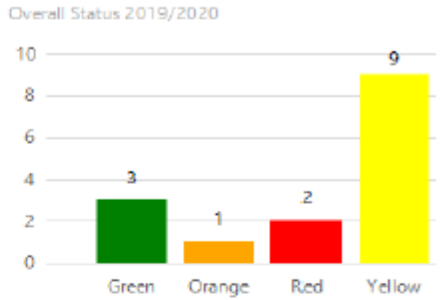


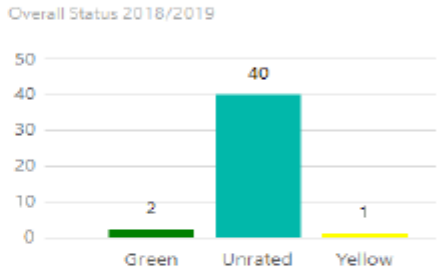
Overall assurance

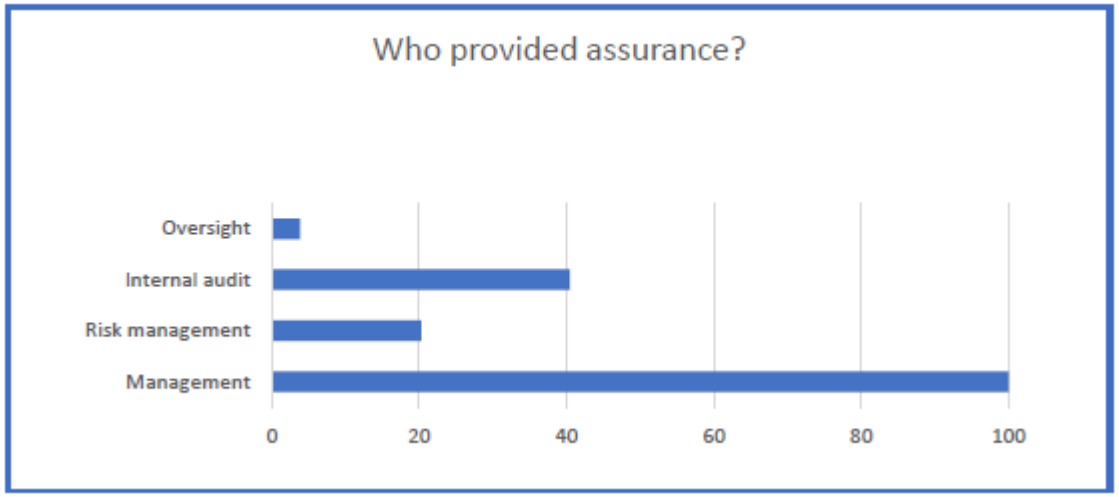
Management expresses their opinion on overall governance in the annual report, and the two status graphs below aligns with their opinion.

Examples of issues to be mentioned here includes:

- Financial sustainability and the ability to operate as a going concern.
- Indigent allowances vs liquidity pressure
- Waste management
- Project management – overspending on capital projects
- High vacancy rate in senior management positions
- Financial leveraging and the refinancing of debt
- Cost of financing over time and the effect of rates and tariffs
- Impairment of indigent debtors
- Debtor collection ratios and impairments
- GRAP issues

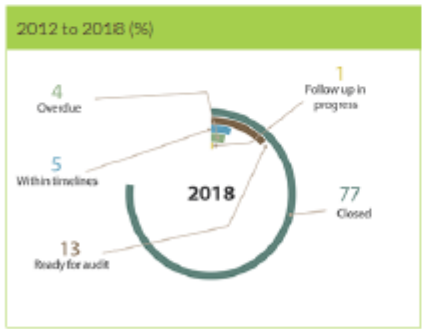






2012 to 2018

Since 2012, 1 981 findings have been raised, broken down below.

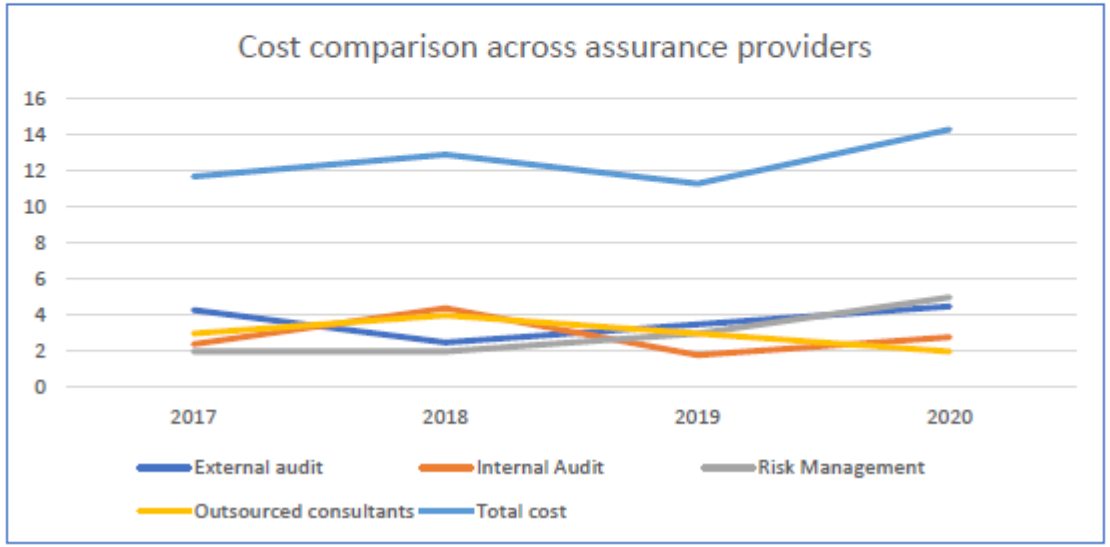


The graphs and tables are an indication of what should be reported.

Functional area	Number findings – Overdue
Good governance	125
Financial sustainability	14
Institutional transformation	111
Physical infrastructure and services	31
Planning and economic development	69
Safety and environmental development	62
Social and community development	41
Total	453

Cost of Assurance

Calculating the cost of insurance will be refined as mSCOA implementation takes effect. The graph below indicated the total cost of assurance (cost to municipality) for the respective years. It needs refinement to allow for proper evaluation of economic and efficient use of resources.



Strategic Risk Register
2019/2020 - Quarter 2 Update

Risk identification		Risk assessment results from workshops				
Ref	Strategic risks	Inherent impact rating	Inherent likelihood rating	Inherent risk rating	Control Effectiveness	Residual risk value
SR1	Financial non-viability	Catastrophic	Almost Certain	Extreme	Good	40
SR2	Inadequate service delivery	Catastrophic	Almost Certain	Extreme	Good	40
SR3	Deficiency in staff skills and capacity	Critical	Likely	High	Satisfactory	32
SR4	Increasing poverty and unemployment	Critical	Likely	High	Weak	39
SR5	Inadequate infrastructure, investment and maintenance	Critical	Likely	High	Satisfactory	32
SR6	Weakness in governance and accountability	Catastrophic	Almost Certain	Extreme	Satisfactory	65
SR7	Unmanaged urbanisation	Critical	Likely	High	Satisfactory	32
SR8	Failure to communicate effectively with stakeholders	Critical	Likely	High	Satisfactory	32
SR9	Inadequate ICT planning, infrastructure and systems	Critical	Likely	High	Satisfactory	32
SR10	National electricity blackout	Catastrophic	Moderate	Extreme	Unsatisfactory	45

Strategic Risk Register
2019/2020 - Quarter 2 Update

Result of assurance provided

Risk identification			Risk owners		Risk management		Independent assurance	
Ref	Strategic risks	Combined assurance	Management controls	Control risk self assessment	Ongoing monitoring	Forensic Auditing	Internal Audit	External Audit
SR1	Financial non-viability							
SR2	Inadequate service delivery							
SR3	Deficiency in staff skills and capacity							
SR4	Increasing poverty and unemployment							
SR5	Inadequate infrastructure, investment and maintenance							
SR6	Weakness in governance and accountability							
SR7	Unmanaged urbanisation							
SR8	Failure to communicate effectively with stakeholders							
SR9	Inadequate ICT planning, infrastructure and systems							
SR10	National electricity blackout							

Status colour coding key
Residual risk high, inadequate or ineffective process
Residual risk medium, risk >risk appetite, not material
Residual risk low, risk < risk appetite
No assurance provided

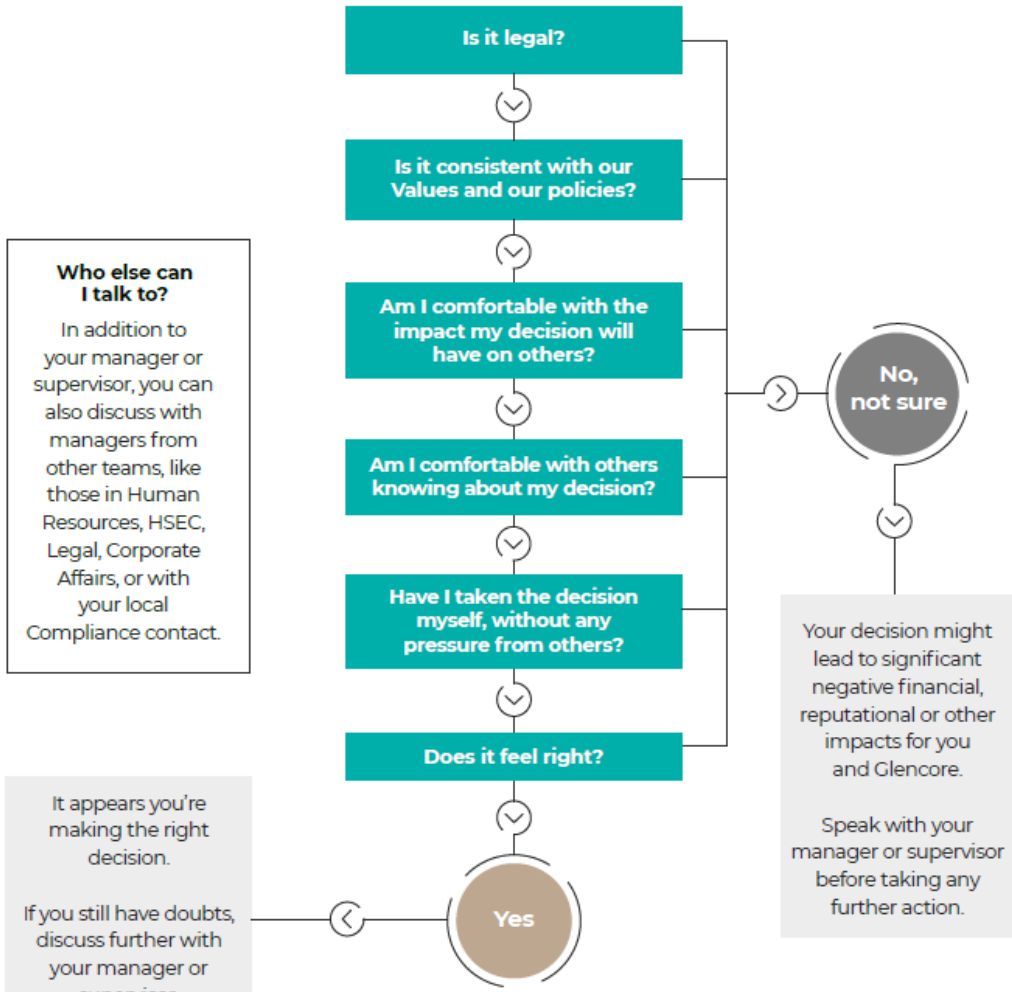
C. EWRM TRAINING – RISK CHAMPIONS (25 PARTICIPANTS)

Duration: 1 Day | **Format:** Hybrid

Session	Objective	Key Deliverables	Practical Application
1	Build operational risk awareness within an integrated control environment/ combined assurance structure.	Identify key operational risks. | Link each to control processes. | Map control ownership under the Three Lines Model.	Document 3 operational risk incidents and controls.
2	Develop and maintain risk registers using integrated data systems informing combined assurance and board effectiveness.	Populate risk registers aligned with integrated reporting. | Prioritize key risks using control analytics. | Integrate assurance data sources for accuracy.	Update a sample departmental risk register.
3	Implement control monitoring and risk responses.	Link operational controls to governance requirements. | Evaluate control effectiveness via assurance mapping. | Track remediation actions across departments.	Conduct a control self-assessment exercise.
4	Strengthen risk communication across all the assurance lines.	Develop clear escalation protocols. | Align reporting templates to integrated data and communication principles. | Foster a transparent risk culture.	Simulate a near-miss event escalation.
5	Embed continuous improvement through integrated governance and effective combined assurance.	Track risk and control KPIs and KRIs. | Conduct lessons-learned reviews. | Enhance operational alignment to governance standards.	Create a “Risk Champion Action Plan.”

A framework for making decisions with integrity

Keeping to the Code helps us make ethical decisions. When facing a tough decision or situation not explicitly covered in the Code, we ask ourselves the following questions:



Value concepts

- Creation
- Preservation
- Destruction

Why are we seeing corporate failures

Reasons for significant value destruction across a number of industries over the past 3 years, globally and in South Africa (for example Steinhoff) highlighted several ***apparent failures*** in terms of:

- Understanding the nature and quantum of risk,
- Appropriate involvement in risk assurance oversight at Board level,
- Strategy and operating models that are able to appropriately respond to declining market conditions,
- Understanding relationships with key stakeholders,
- Regulatory compliance strategies that are able to deal with onerous and ever-changing laws, and
- Risk assurance strategies that provide not only appropriate levels of assurance, but also sufficient personal protection for the Board/Council and Executive management.

Combined Assurance (including Governance)

pwc

What Boards/Councils are saying?

… I need to know that everything is under control".

… I need to know whether what I am being told is correct".

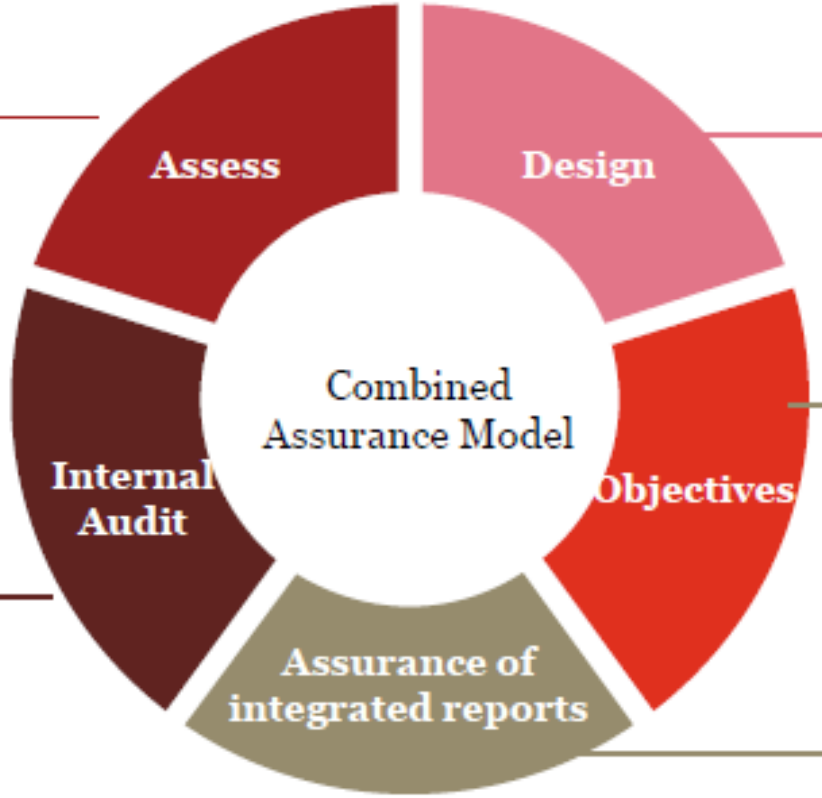
… I need to be confident that I am going to achieve my organisational objectives and goals".

… I need to know if things are going horribly wrong".

… I need to know whether the project is going to finish on time and within budget".

Combined Assurance Model

Governing body should assess the output of combined assurance, & form an opinion on the integrity of information & reports, & if an effective control environment has been achieved



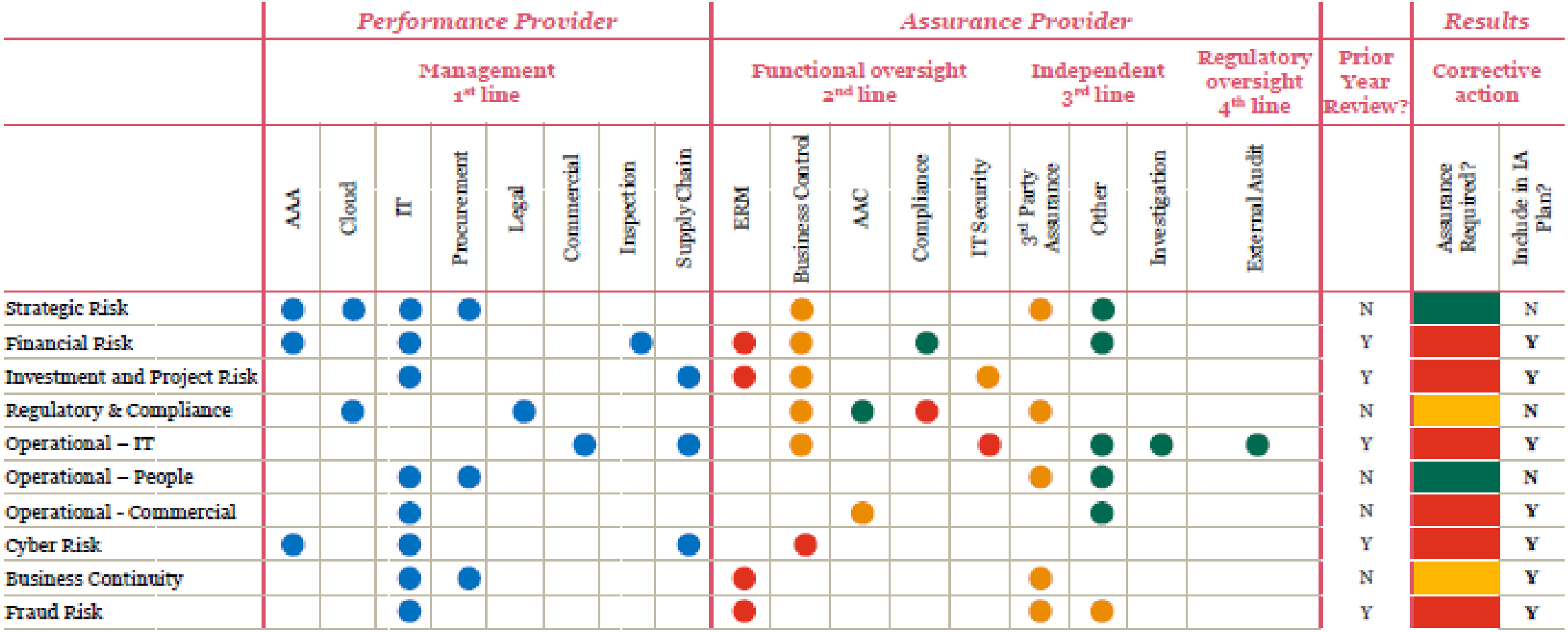
Not prescribed by the Code. Allows for the governing body to use its judgement in this regard

- Responsibility of governing body, may be delegated to audit committee
- Internal audit charter
- Ensure internal audit has the necessary skills & resources to address the complexity & risk faced by the organisation

- Effective internal control environment
- Supporting the integrity of information
- Supporting the integrity of external reports

- Responsibility of the governing body
- Consider legal requirements
- External reports should disclose information about the type of assurance process applied in that report

Its important to understand the integrity of all assurance



Links to performance

- Enables the achievement of strategy by actively managing risk and performance
- Focuses on how risk is integral to performance by:
  - Exploring how enterprise risk management practices support the identification and assessment of risks that impact performance
  - Discussing tolerance for variations in performance
- Manages risk in the context of achieving strategy and business objectives – not as individual risks

KPI's and KRI's

Key Performance Indicators (KPIs) help a firm see how it is performing in relation to its strategic goals and objectives.

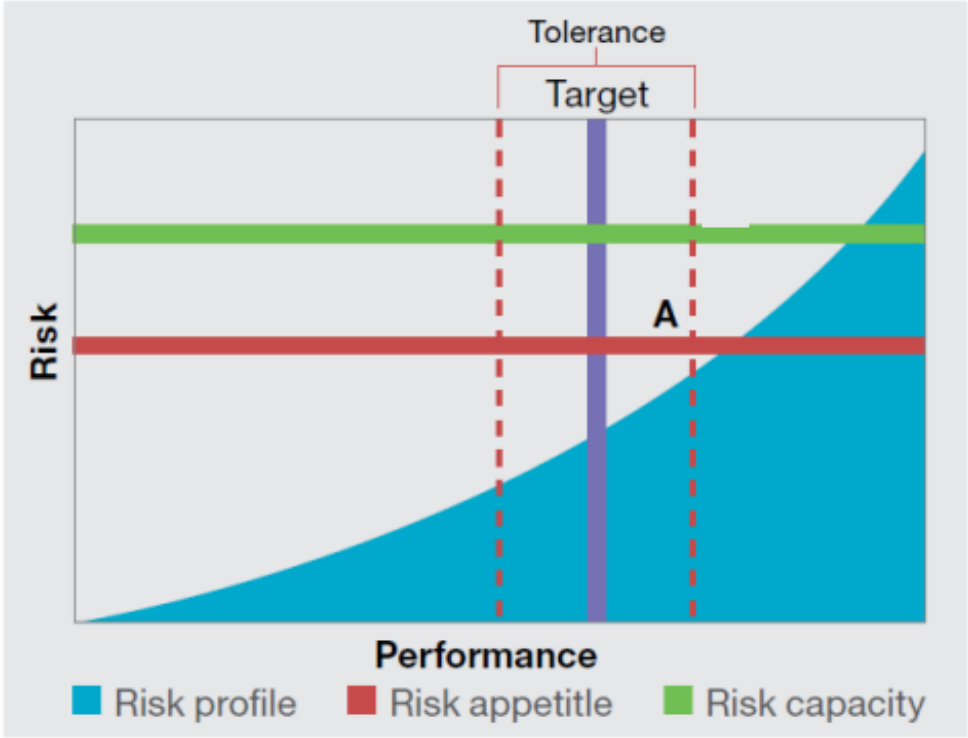
Key Risk Indicators (KRIs) are leading indicators of risk to business performance, giving early warning about potential risk event

Use KRIs to monitor risks are in the areas such as:

- natural catastrophe risks (as % of group shareholder equity)
- asset-liability matching (duration mismatch)
- strategic asset allocation (% allowed in investment category)
- credit risk (weighted average credit rating)
- other risks specific to business or functional areas

Risk versus performance

- Introduces a new depiction referred to as a risk profile
- Incorporates:
  - Risk
  - Performance
  - Risk appetite
  - Risk capacity
- Offers a comprehensive view of risk and enables more risk-aware decision making



- The framework provides a complete depiction of how to build a risk profile in an appendix

Design, build and implementation of Key Risk Indicators

Design

- Establish extent of existing management information and other data flows – indicators in place if applicable
- Identify committees, forums, management meetings etc currently in place that can be used to discuss risk and control issues on an ongoing basis
- Define and document roles and responsibilities of risk and control owners

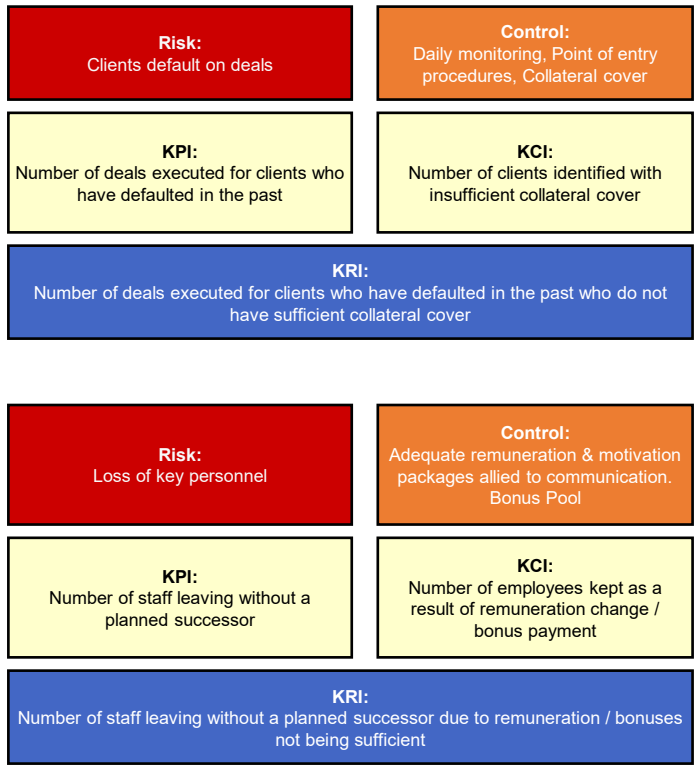
Build Process

- Assign ownership for risks and controls
- Communication with risk and control owners relating to their ongoing responsibilities
- Carry out workshops with all risk and control owners to design indicators to be put in place
- Define how existing information flows and committees etc are to be used to minimise additional workload
- Risk and control owners refine the indicator monitoring process
- Overall analysis of indicators for gaps and dual coverage
- Design reporting protocols

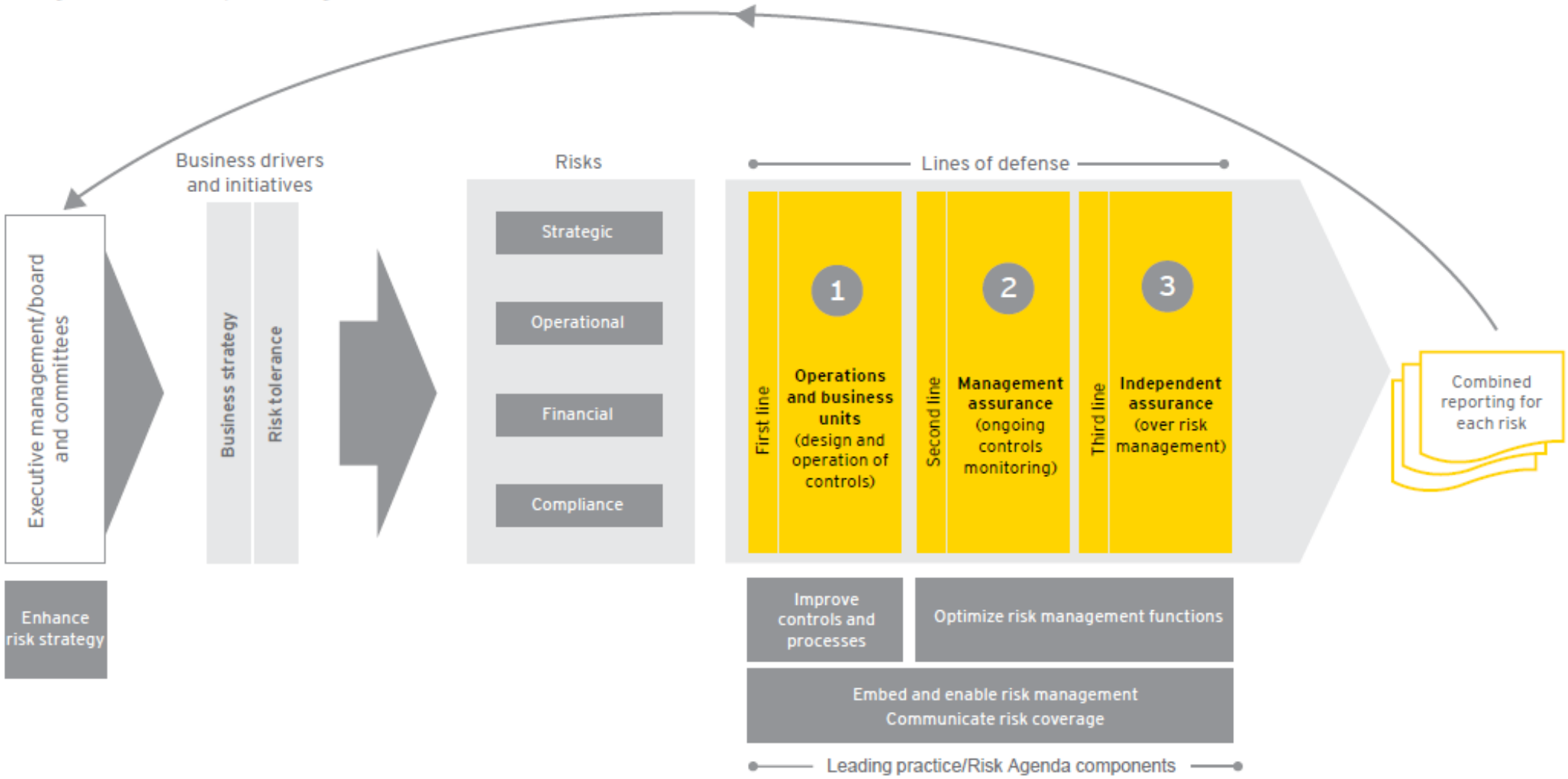
Ongoing Operation of Process

- Design review mechanism (i.e. Corporate Risk department or Internal Audit, etc.)
- Create storage mechanism for information
- Perform ongoing consistency checks of indicators set up across the organisation

Example KPI, KCI and KRIs



Integrated LOD (Lines of Defense) Model



Example: Risk Status Report