arts & culture

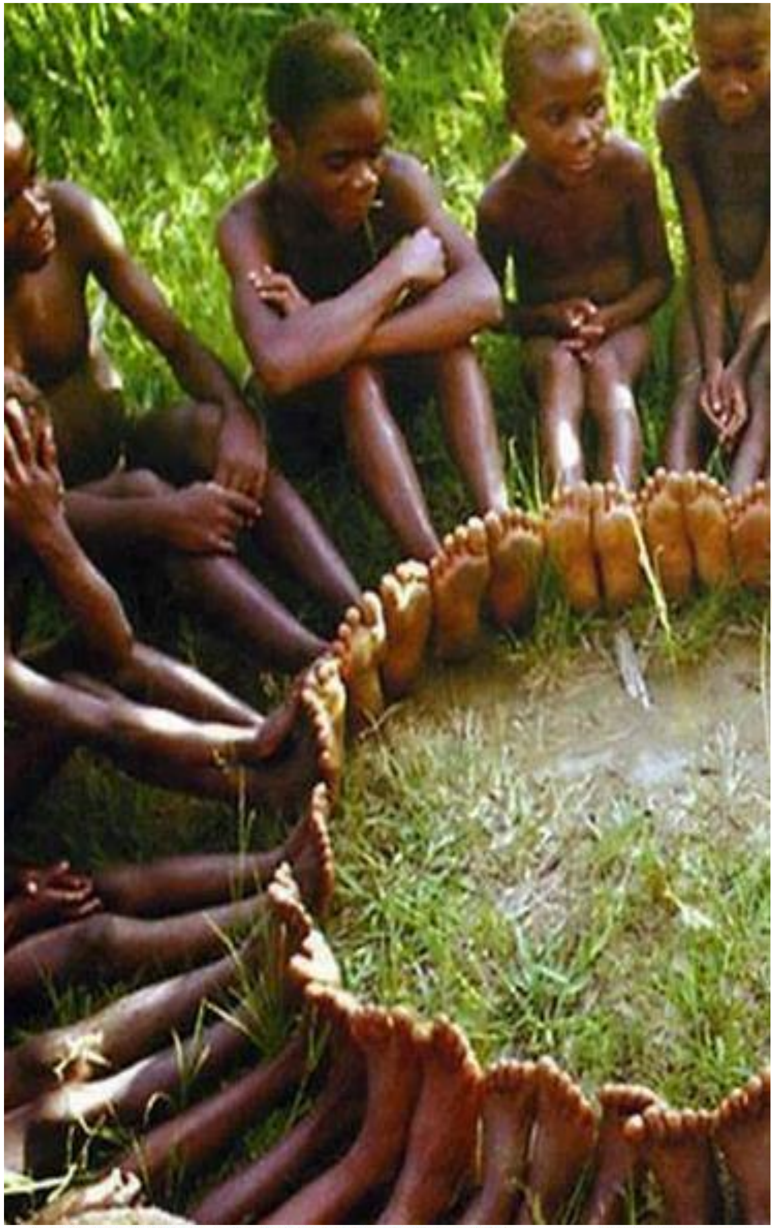
Department:
Arts and Culture
REPUBLIC OF SOUTH AFRICA

Tool-Kits for a Chief Risk Officer in the Public Sector
IRMSA Public Sector Forum

LAYING THE FOUNDATION FOR GREATNESS

1. Overview

- Purpose of the Toolkit
- Understanding the Environment[Structure of government]
- Structural Issues[Basics of Risk Management]
- Risk Governance Roles and Responsibilities
- Three lines of defense
- Oversight Committee [Risk Committee & Audit Committee]
- The path to risk maturity & tools that can assist you as the head of risk or CRO



PURPOSE OF THE TOOLKIT

Do you understand the structures of the Public Sector?

4. Structure of an organization -Public Sector

- Mandate , Vision & Mission
- Values
- Strategy of the Department
- Delivery agreements between Minister & Presidency
- Role & Structure of the political office
- Key delivery outcomes of your organization
- Delivery agents [Public Entities etc]
- Shared mandates / Dual Reporting Responsibilities
- Annual Reports; Shareholders Compacts; Exco Reporting
- Organizational Infrastructure, Personnel ; Processes; and Technology

External Factors [Economic, Social, Political, Social & Technological]

International Treaties impacting the mandates

Custody of country Regulation [Language Act; Heritage Resource Act; National Archives Act]

- Stakeholder Analysis and Terms of Engagement
- National Department
- Provincial Legislature
- Local Authority
- TIC/ MinMec / FOSAD

5. Structural Issues [Development of Frameworks & Policy]

5. 1. Risk Management Basics

5. 2. Risk Management Frameworks

5.3. Risk Management Policy

5.3.1 . Risk Management Language [Taxonomy]

5.4 Fraud Prevention Policy; Strategy; Implementation Plans

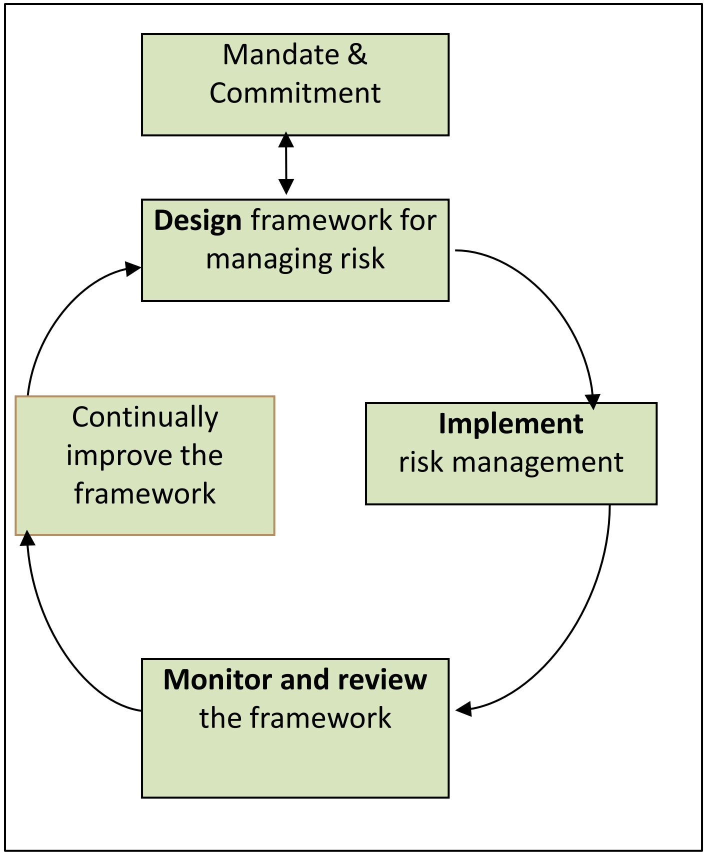
5.5 . Ethics and Integrity Programmes

ERM frameworks represent the agreed upon structure or governing principles an organization uses to manage risks. However, there is no ‘one-size-fits-all’ model and a plurality of organizations develop a framework internally that adapts elements of widely-accepted standards.

Principles

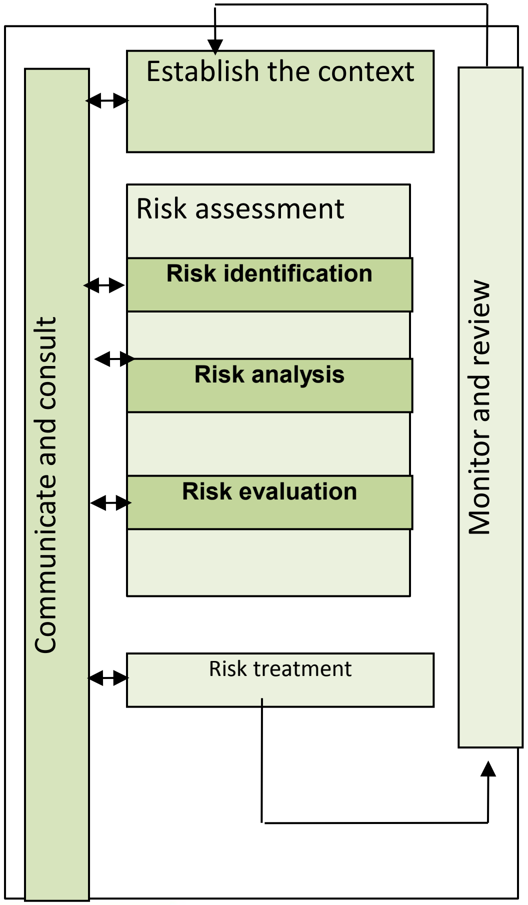
- Creates value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured & timely
- Based on best available information
- Tailored to organization needs
- Takes human & cultural factors into account
- Transparent & inclusive
- Dynamic,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

Framework



Mandate & Commitment
Design framework for managing risk
Implement risk management
Monitor and review the framework
Continually improve the framework

RM Process

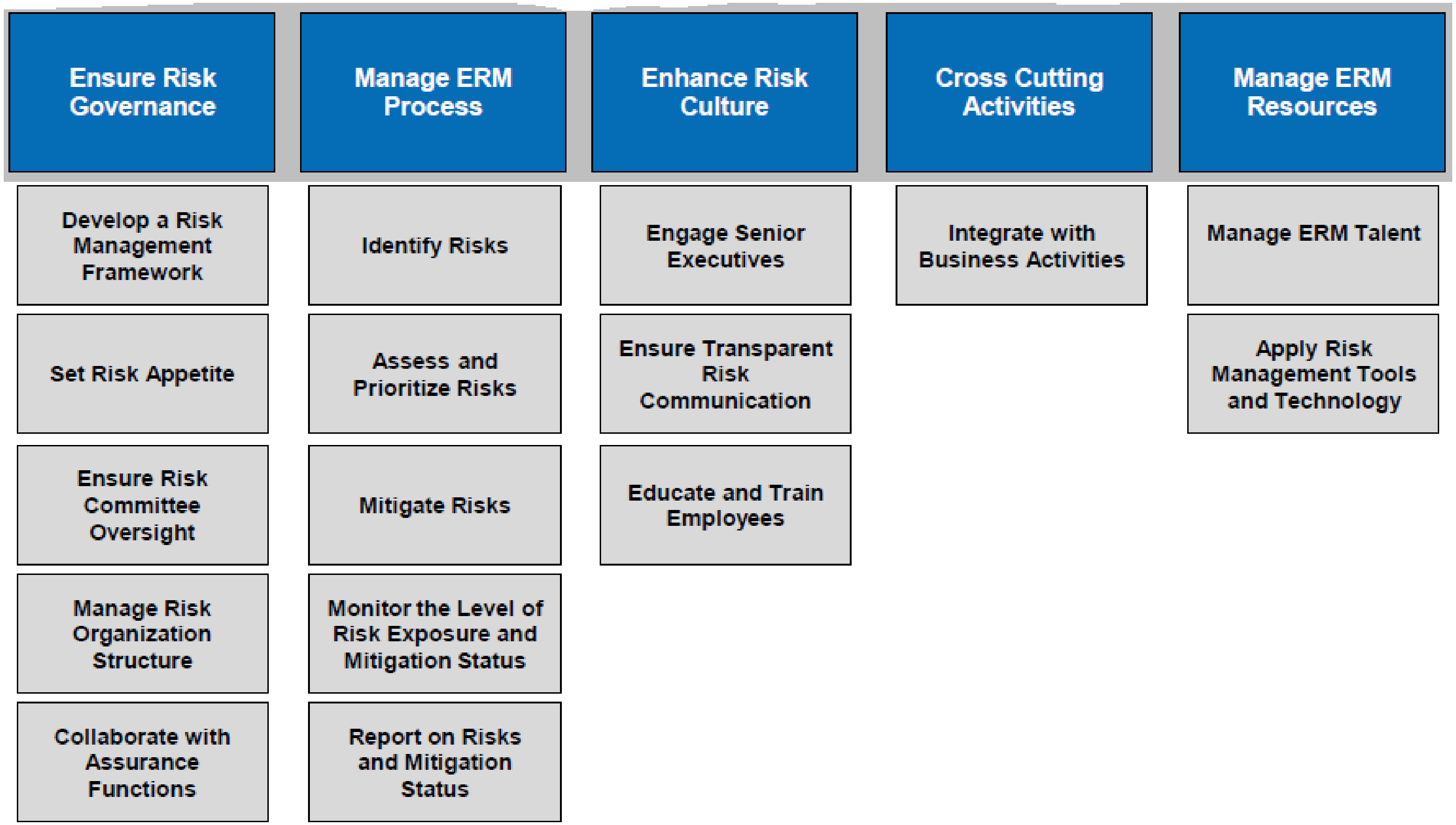


8. Which Framework is suitable for the Public Sector?

	COSO	ISO 31000
Scope	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

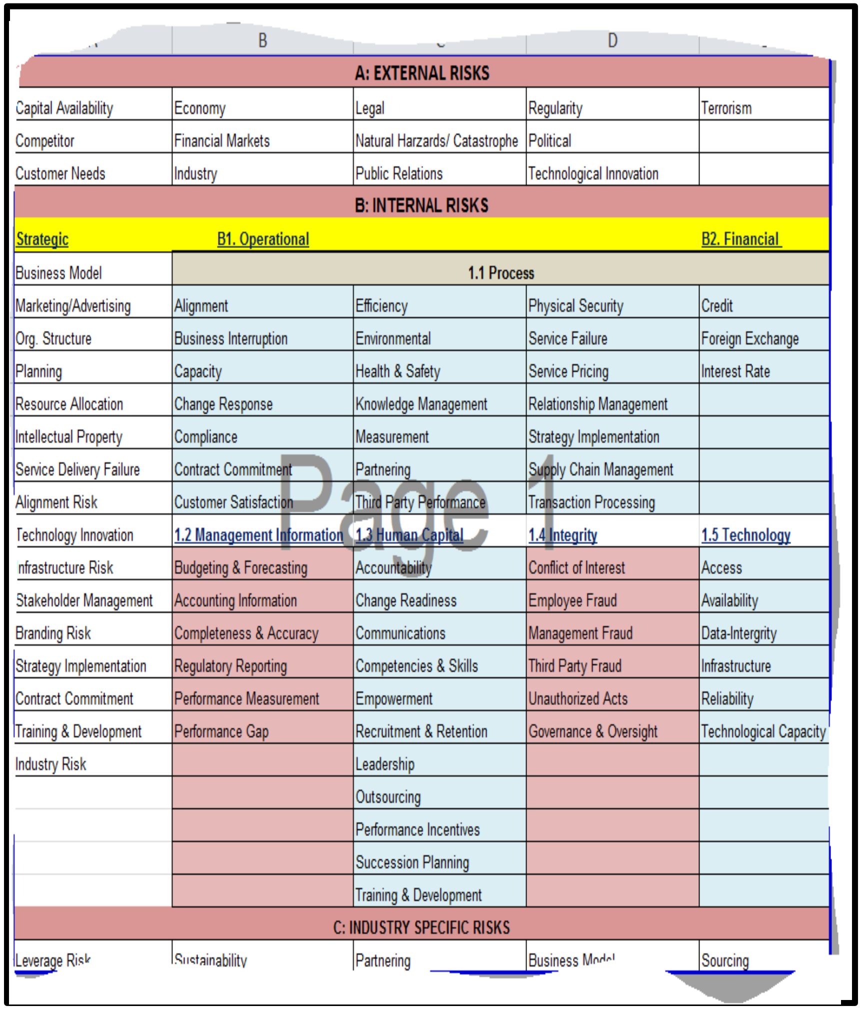
9. Framework for activities in an ERM function

Arts & Culture [CEB Risk Management Functionality Diagnostic –May 2015]

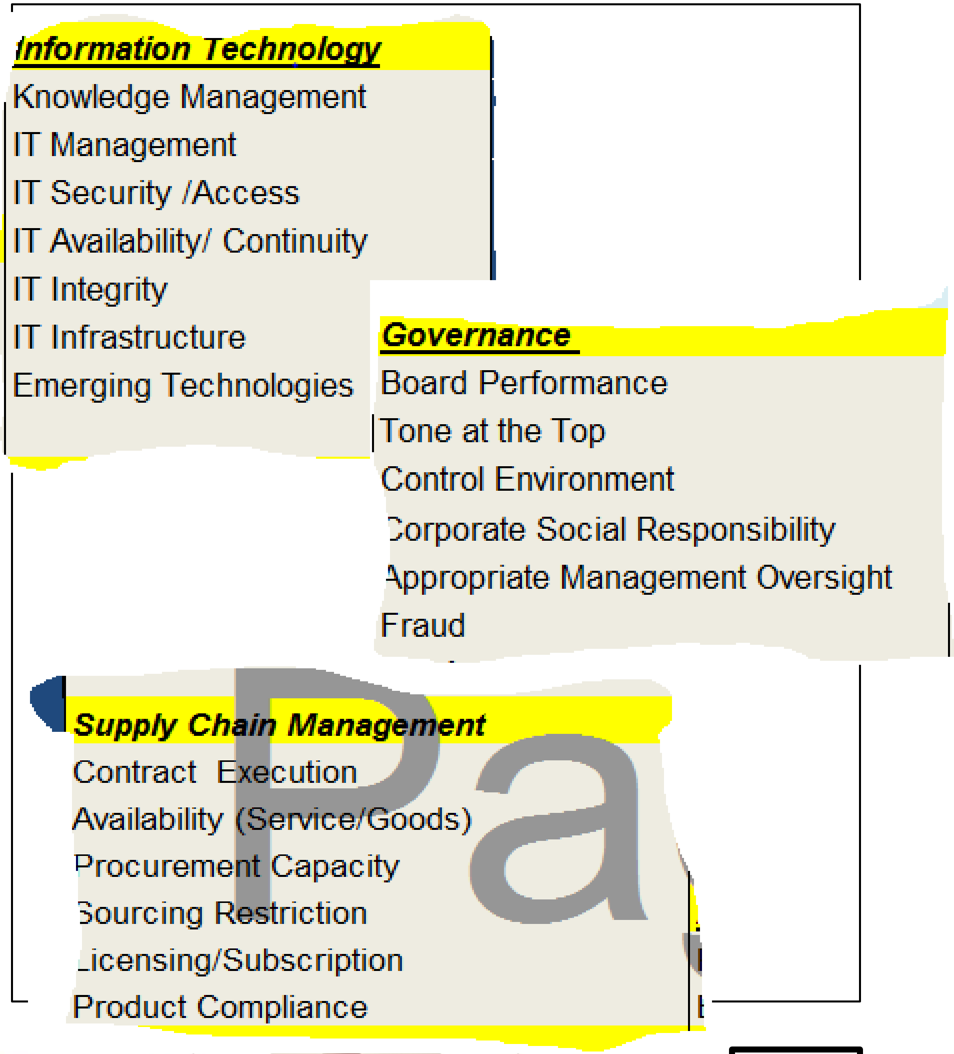


Ensure Risk Governance	Manage ERM Process	Enhance Risk Culture	Cross Cutting Activities	Manage ERM Resources
Develop a Risk Management Framework	Identify Risks	Engage Senior Executives	Integrate with Business Activities	Manage ERM Talent
Set Risk Appetite	Assess and Prioritize Risks	Ensure Transparent Risk Communication		Apply Risk Management Tools and Technology
Ensure Risk Committee Oversight	Mitigate Risks	Educate and Train Employees		
Manage Risk Organization Structure	Monitor the Level of Risk Exposure and Mitigation Status			
Collaborate with Assurance Functions	Report on Risks and Mitigation Status			

10. What is your Risk Language?



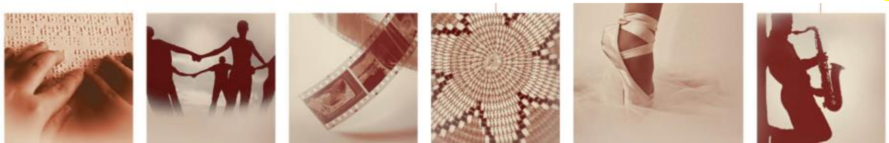
	B		D	
A: EXTERNAL RISKS				
Capital Availability	Economy	Legal	Regularity	Terrorism
Competitor	Financial Markets	Natural Harzards/ Catastrophe	Political	
Customer Needs	Industry	Public Relations	Technological Innovation	
B: INTERNAL RISKS				
Strategic	B1. Operational			B2. Financial
Business Model	1.1 Process			
Marketing/Advertising	Alignment	Efficiency	Physical Security	Credit
Org. Structure	Business Interruption	Environmental	Service Failure	Foreign Exchange
Planning	Capacity	Health & Safety	Service Pricing	Interest Rate
Resource Allocation	Change Response	Knowledge Management	Relationship Management	
Intellectual Property	Compliance	Measurement	Strategy Implementation	
Service Delivery Failure	Contract Commitment	Partnering	Supply Chain Management	
Alignment Risk	Customer Satisfaction	Third Party Performance	Transaction Processing	
Technology Innovation	1.2 Management Information	1.3 Human Capital	1.4 Integrity	1.5 Technology
nfrastructure Risk	Budgeting & Forecasting	Accountability	Conflict of Interest	Access
Stakeholder Management	Accounting Information	Change Readiness	Employee Fraud	Availability
Branding Risk	Completeness & Accuracy	Communications	Management Fraud	Data-Intergrity
Strategy Implementation	Regulatory Reporting	Competencies & Skills	Third Party Fraud	Infrastructure
Contract Commitment	Performance Measurement	Empowerment	Unauthorized Acts	Reliability
Training & Development	Performance Gap	Recruitment & Retention	Governance & Oversight	Technological Capacity
Industry Risk		Leadership		
		Outsourcing		
		Performance Incentives		
		Succession Planning		
		Training & Development		
C: INDUSTRY SPECIFIC RISKS				
Leverage Risk	Sustainability	Partnering	Business Model	Sourcing



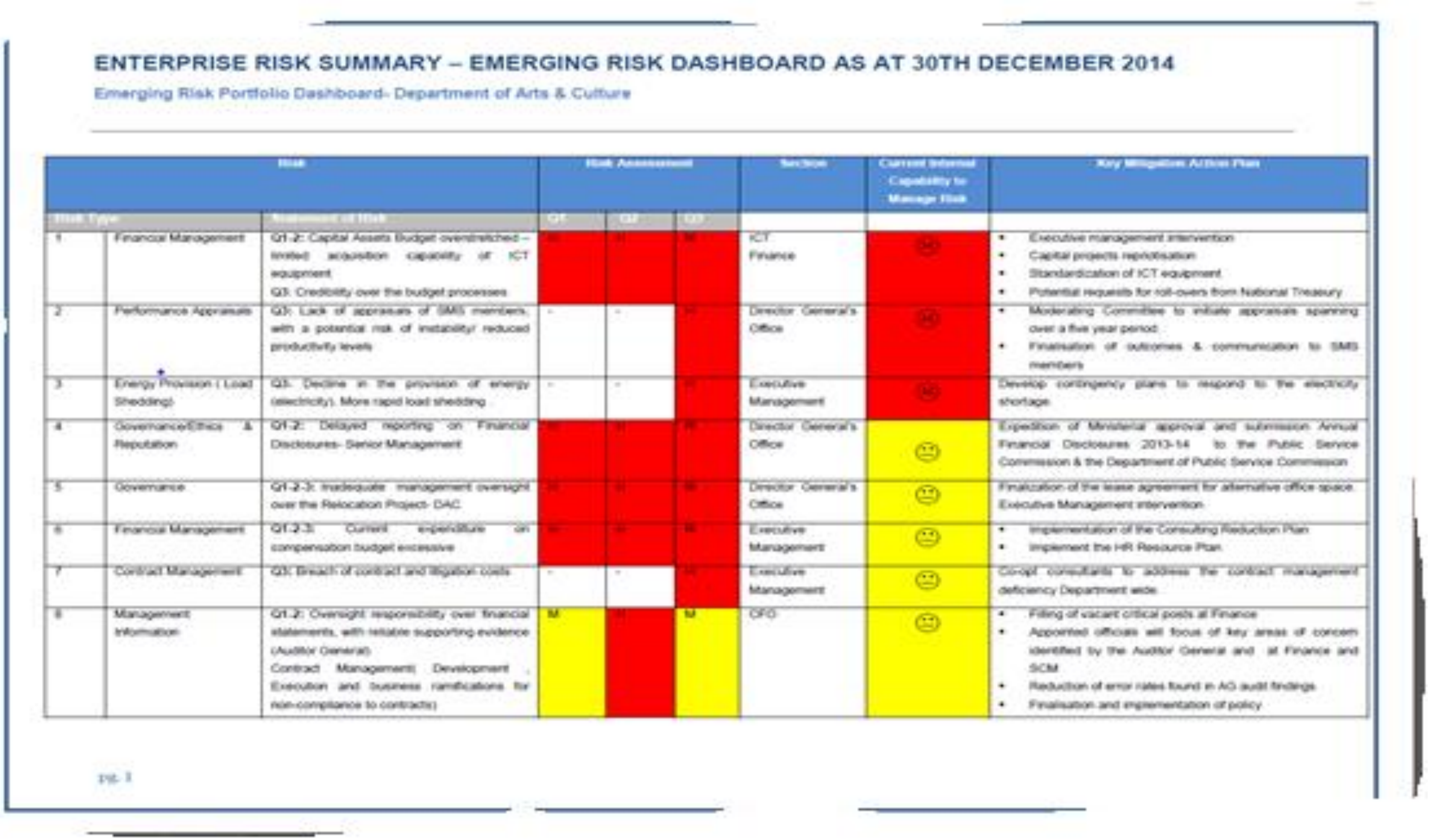
Information Technology
Knowledge Management
IT Management
IT Security /Access
IT Availability/ Continuity
IT Integrity
IT Infrastructure
Emerging Technologies

Governance
Board Performance
Tone at the Top
Control Environment
Corporate Social Responsibility
Appropriate Management Oversight
Fraud

Supply Chain Management
Contract Execution
Availability (Service/Goods)
Procurement Capacity
Sourcing Restriction
Licensing/Subscription
Product Compliance



11. Emerging Risk Reporting



ENTERPRISE RISK SUMMARY – EMERGING RISK DASHBOARD AS AT 30TH DECEMBER 2014

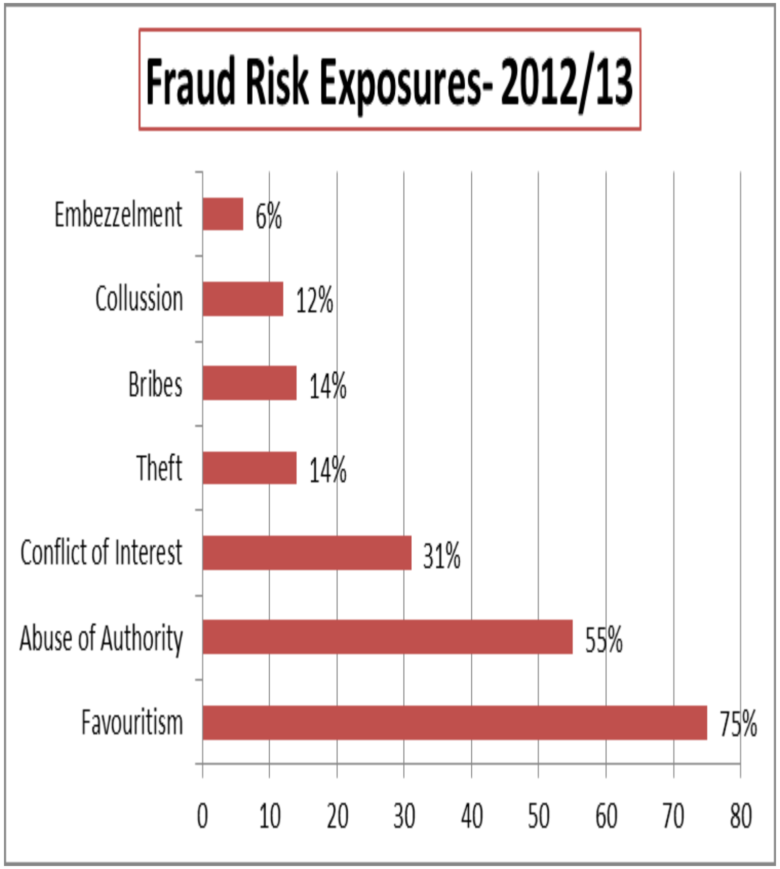
Emerging Risk Portfolio Dashboard- Department of Arts & Culture

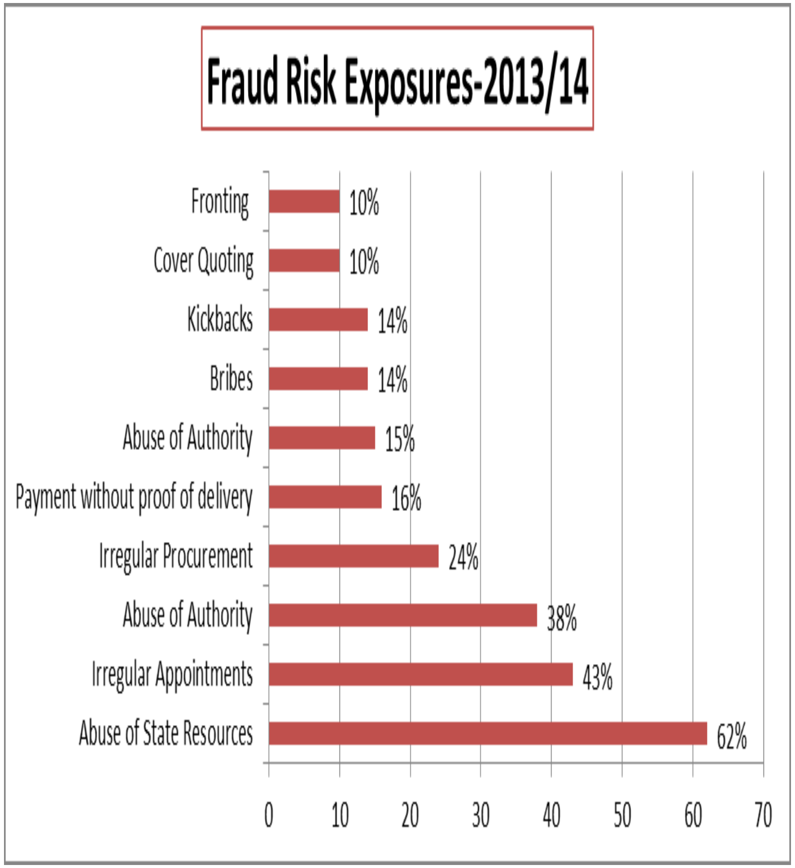
Risk			Risk Assessment			Section	Current Internal Capability to Manage Risk	Key Mitigation Action Plan
Risk Type		Statement of Risk	Q1	Q2	Q3			
1	Financial Management	Q1-2: Capital Assets Budget overstretched – limited acquisition capability of ICT equipment Q3: Credibility over the budget processes	H	H	H	ICT Finance	☹	• Executive management intervention • Capital projects reprioritisation • Standardication of ICT equipment • Potential requests for roll-overs from National Treasury
2	Performance Appraisals	Q3: Lack of appraisals of SMS members, with a potential risk of instability/ reduced productivity levels	-	-	H	Director General's Office	☹	• Moderating Committee to initiate appraisals spanning over a five year period • Finalisation of outcomes & communication to SMS members
3	Energy Provision (Load Shedding)	Q3: Decline in the provision of energy (electricity). More rapid load shedding	-	-	H	Executive Management	☹	Develop contingency plans to respond to the electricity shortage
4	Governance/Ethics & Reputation	Q1-2: Delayed reporting on Financial Disclosures- Senior Management	H	H	H	Director General's Office	😐	Expedition of Ministerial approval and submission Annual Financial Disclosures 2013-14 to the Public Service Commission & the Department of Public Service Commission
5	Governance	Q1-2-3: Inadequate management oversight over the Relocation Project- DAC	H	H	H	Director General's Office	😐	Finalization of the lease agreement for alternative office space. Executive Management intervention
6	Financial Management	Q1-2-3: Current expenditure on compensation budget excessive	H	H	H	Executive Management	😐	• Implementation of the Consulting Reduction Plan • Implement the HR Resource Plan
7	Contract Management	Q3: Breach of contract and litigation costs	-	-	H	Executive Management	😐	Co-opt consultants to address the contact management deficiency Department wide
8	Management Information	Q1-2: Oversight responsibility over financial statements, with reliable supporting evidence (Auditor General) Contract Management(Development , Execution and business ramifications for non-compliance to contracts)	M	H	M	CFO	😐	• Filing of vacant critical posts at Finance • Appointed officials will focus of key areas of concern identified by the Auditor General and at Finance and SCM • Reduction of error rates found in AG audit findings • Finalisation and implementation of policy

12. Fraud Risk Exposure

Source: Department of Arts & Culture Fraud Awareness Campaign Results

The Fraud Policy, Fraud Prevention Strategy, Fraud Prevention Implementation Plan, Whistle Blowers Policy, Fraud Investigation Policy and Awareness Campaigns are the bedrock in creating a fraud aware organization

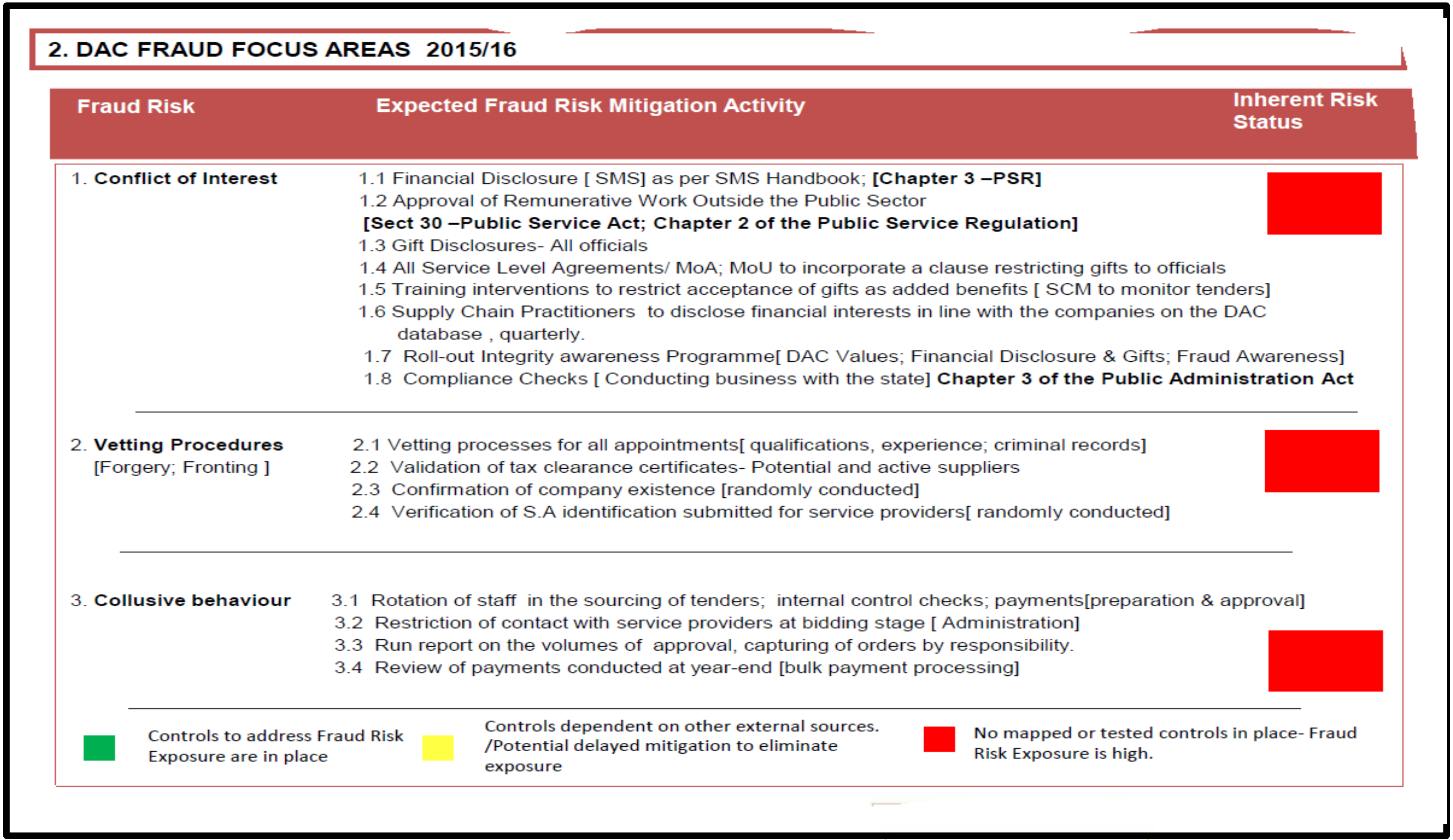




LAYING THE FOUNDATION FOR GREATNESS

13. Fraud Risk Dashboards

Source: Department of Arts & Culture : Fraud Risk Dashboard



2. DAC FRAUD FOCUS AREAS 2015/16

Fraud Risk	Expected Fraud Risk Mitigation Activity	Inherent Risk Status
1. **Conflict of Interest**	1.1 Financial Disclosure [SMS] as per SMS Handbook; **[Chapter 3 –PSR]** 1.2 Approval of Remunerative Work Outside the Public Sector **[Sect 30 –Public Service Act; Chapter 2 of the Public Service Regulation]** 1.3 Gift Disclosures- All officials 1.4 All Service Level Agreements/ MoA; MoU to incorporate a clause restricting gifts to officials 1.5 Training interventions to restrict acceptance of gifts as added benefits [SCM to monitor tenders] 1.6 Supply Chain Practitioners to disclose financial interests in line with the companies on the DAC database , quarterly. 1.7 Roll-out Integrity awareness Programme[DAC Values; Financial Disclosure & Gifts; Fraud Awareness] 1.8 Compliance Checks [Conducting business with the state] **Chapter 3 of the Public Administration Act**	🟥
2. **Vetting Procedures** [Forgery; Fronting]	2.1 Vetting processes for all appointments[qualifications, experience; criminal records] 2.2 Validation of tax clearance certificates- Potential and active suppliers 2.3 Confirmation of company existence [randomly conducted] 2.4 Verification of S.A identification submitted for service providers[randomly conducted]	🟥
3. **Collusive behaviour**	3.1 Rotation of staff in the sourcing of tenders; internal control checks; payments[preparation & approval] 3.2 Restriction of contact with service providers at bidding stage [Administration] 3.3 Run report on the volumes of approval, capturing of orders by responsibility. 3.4 Review of payments conducted at year-end [bulk payment processing]	🟥

🟩 Controls to address Fraud Risk Exposure are in place

🟨 Controls dependent on other external sources. /Potential delayed mitigation to eliminate exposure

🟥 No mapped or tested controls in place- Fraud Risk Exposure is high.

14. Risk governance roles & responsibilities

5. 1. Three lines of defense

5.2. Chief Risk Officer’s Role

5.3 . Role of the Risk Committee

5.4. Role of the Audit Committee

5.5 . Role of the Auditor General

15. Three lines of defense

ERM is a Second Line function, distinguished from Internal Audit, and is meant to provide frameworks, guidelines, and general assistance to management in addressing enterprise risks.

The First Line (Management)

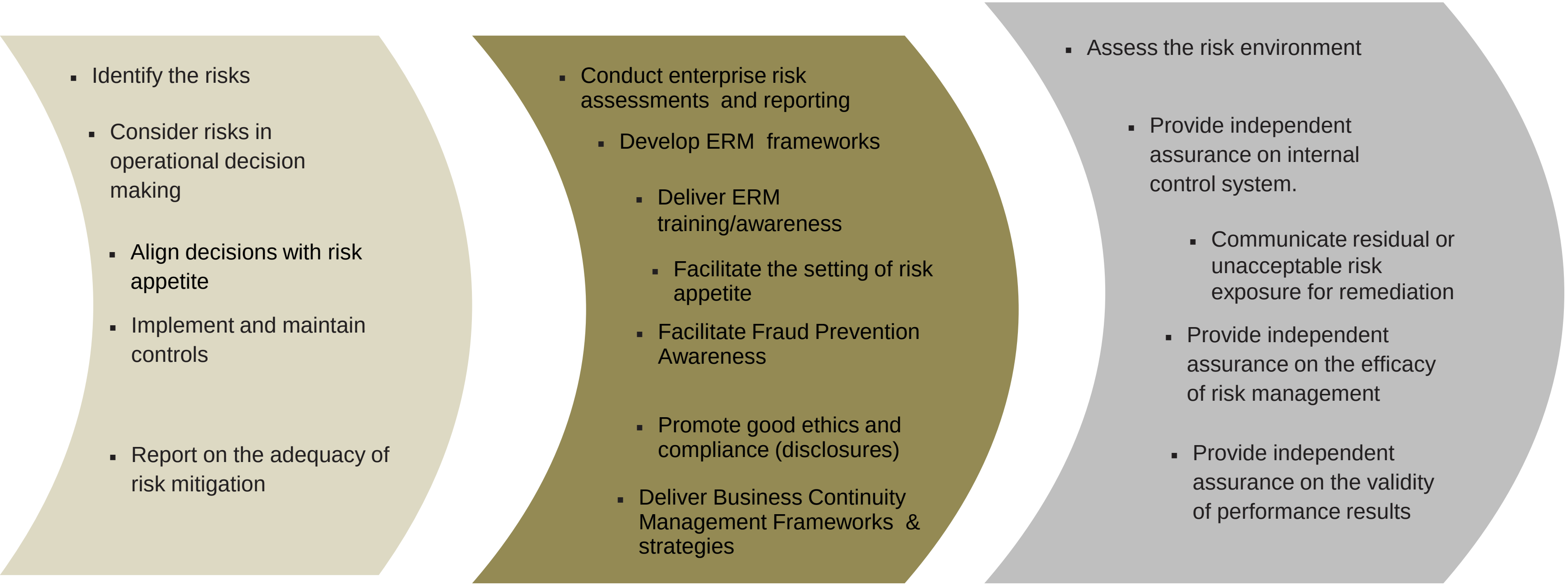
Setting strategy, performance measurement, and establishing and maintaining risk management, control, and governance across the business

The Second Line (ERM Function incl. Legal & Compliance)

Providing a risk framework to improve decision making, planning, and prioritization of business activities

The Third Line Auditor General/ (Internal Audit)/Consulting Services

Providing independent and objective assurance of the overall adequacy and effectiveness of governance, risk management, and control within the organization.

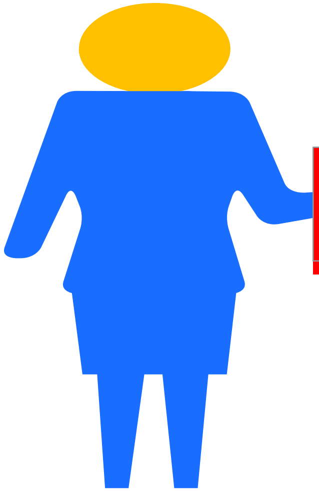


- Identify the risks
- Consider risks in operational decision making
- Align decisions with risk appetite
- Implement and maintain controls
- Report on the adequacy of risk mitigation

- Conduct enterprise risk assessments and reporting
- Develop ERM frameworks
- Deliver ERM training/awareness
- Facilitate the setting of risk appetite
- Facilitate Fraud Prevention Awareness
- Promote good ethics and compliance (disclosures)
- Deliver Business Continuity Management Frameworks & strategies

- Assess the risk environment
- Provide independent assurance on internal control system.
- Communicate residual or unacceptable risk exposure for remediation
- Provide independent assurance on the efficacy of risk management
- Provide independent assurance on the validity of performance results

16. The Role of the Chief Risk Officer



Do you know what is expected from you?

The Role of a Chief Risk Officer

1. Developing and implementing the corporate risk management framework
2. Verifying and validating that operational level risk tolerances and limits have been established consistent with organizational strategy.
3. Ensure that the operational management have processes in place to identify, measure, monitor, mitigate and report on risks and associated mitigation strategies.
4. Managing day to day operations; long-term plans of risk management within your organization
5. Engaging employees in the management of risk and ensuring they are aware of their accountabilities with regards to risk management.
6. Monitoring mitigation strategies to verify their appropriateness and effectiveness.

17. Risk Committees

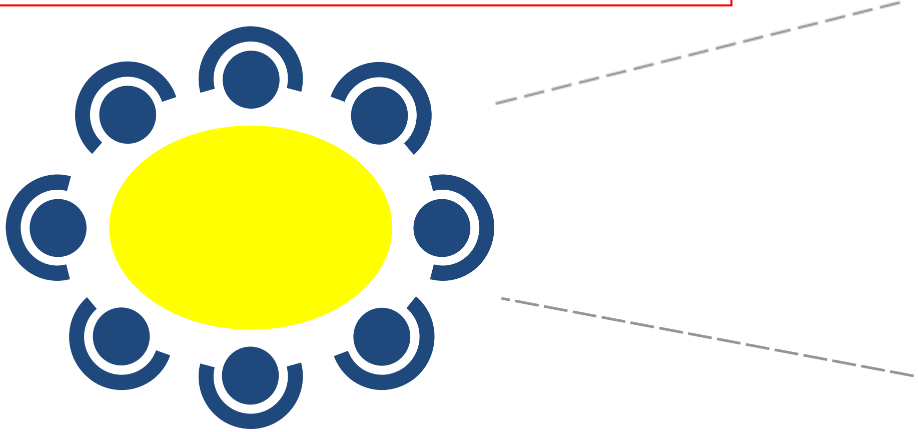
Responsibilities of the Risk Committee

Core Committee responsibilities

- Coordinates decision making on risk management
- Monitors ERM program performance
- Aligns risk responses to overall organization strategies and objectives
- Reviews the suitability of the risk management processes and the organization's risk response
- Prioritizes risk conversations for senior leadership and the board

Frequency of Meetings

- The committee will have a standing meeting every quarter. In certain circumstances, a special meeting may be called to address pressing issues.
- Preparatory Meetings with the Risk Committee Chairperson are key.



Composition of Committee

Members:
Independent Chairperson
Director General
Deputy Director General
C-Suite [CFO;COO;CIO]
Executive Legal Advisor
Chief Audit Executive
Chief Directors/Business Unit
Executives/Senior Management

18. Tool-kit towards risk maturity for the CRO ?

HOW mature is risk management in your organization?

19. DAC Maturity Road-Map

- Checklist; Compliance requirement
- Consultants asking officials to rate predetermined risk
- Shrink-wrap reports that were not understood or usable
- Risk aware organization that takes risk ownership
- Risk Management should assist to attain organizational objectives
- Projects being managed based on risk informed decisions
- Integrated risk management carrying through to risk based internal audits

20.What our stakeholders think.. *Jonathan Crisp- MD [IDI Developments]*

- Mainstream discipline, no longer tick box, annual event
- Buy-in from executive management
- Still areas where it a **“has to do**” and not a **“want to do”**
- Risk has to reflect real value
- Identify realistic objectives ;
- rate risks scientifically and consistently

- Refine and use risk model [Finance, OSH, reputational, social and environmental issues]
- Monitor your controls
- Identify Key Risk Indicators[use them as sanity checks]
- Link inter-related risks together

- Promote accountability, action plans with due dates.
- Link performance information to risk management
- Provide business intelligence information for early warnings, and to conduct root cause analysis.
- All this can be done through a properly designed risk system

21.What our stakeholders think.. *Ian Beale- Executive Corporate Executive Board[Risk Leadership Council]*

- Good business management practice
- Identify top key risk[**Never lose sight BIG RISKS= G+BIG IMPACT**]
- Risk governance culture[Risk Committee; Risk Champions]
- Be creative, effective to leverage risk management
- Communication & risk training
- Clear accountability
- Build capability

- Chief Risk Officer’s have changed change[collate vs mitigation]
- Drive down risk appetite to an operational level

- Be consistent within the development of risk statement, policy and guidelines
- Demonstrate value creation and light of touch
- Risk can be a drag, don’t be the drag..

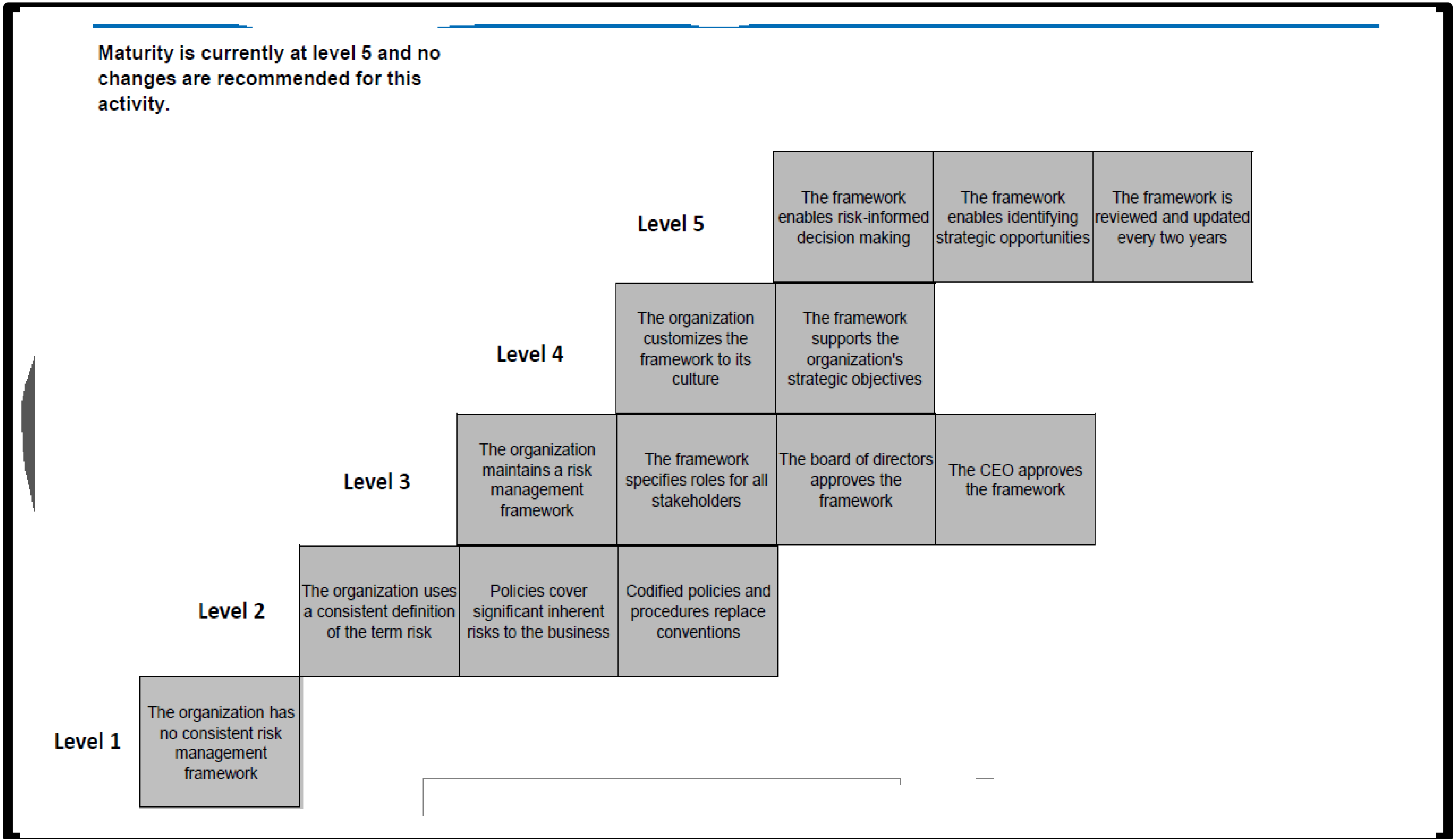
22.What our stakeholders think.. *[Michael Ferendinos-* Group Chief Risk Officer AECI]

- **Industry is continually looking for ways to add more value to organisations.**
- **Senior management teams questioned the actual value of the function**
- **Gradually becoming integrated with organisational strategy**
- **Unlike other roles there is very little chance of a risk manager being fired for poor performance because the actual purpose of the role is not well understood.**

- **Next step for greater risk maturity requires it to be a filter behind all organisational decision making**
- **the future of risk management should support informed and proactive decision making**
- **Management base their decisions on the information that we have at our disposal[additional layer of information and our decisions change]**
- Communicate risks to management through an efficient medium
- **Real time nature of the disseminated information is crucial [Context setting ISO 31000]**
- **Communication…at all levels and in all directions.**
- Integrated reporting

23. Develop a Risk Management Framework

Source: DAC [CEB Risk Management Maturity & Functionality Diagnostic May 2015]



Maturity is currently at level 5 and no changes are recommended for this activity.

Level 5	The framework enables risk-informed decision making	The framework enables identifying strategic opportunities	The framework is reviewed and updated every two years	
Level 4	The organization customizes the framework to its culture	The framework supports the organization's strategic objectives		
Level 3	The organization maintains a risk management framework	The framework specifies roles for all stakeholders	The board of directors approves the framework	The CEO approves the framework
Level 2	The organization uses a consistent definition of the term risk	Policies cover significant inherent risks to the business	Codified policies and procedures replace conventions	
Level 1	The organization has no consistent risk management framework			

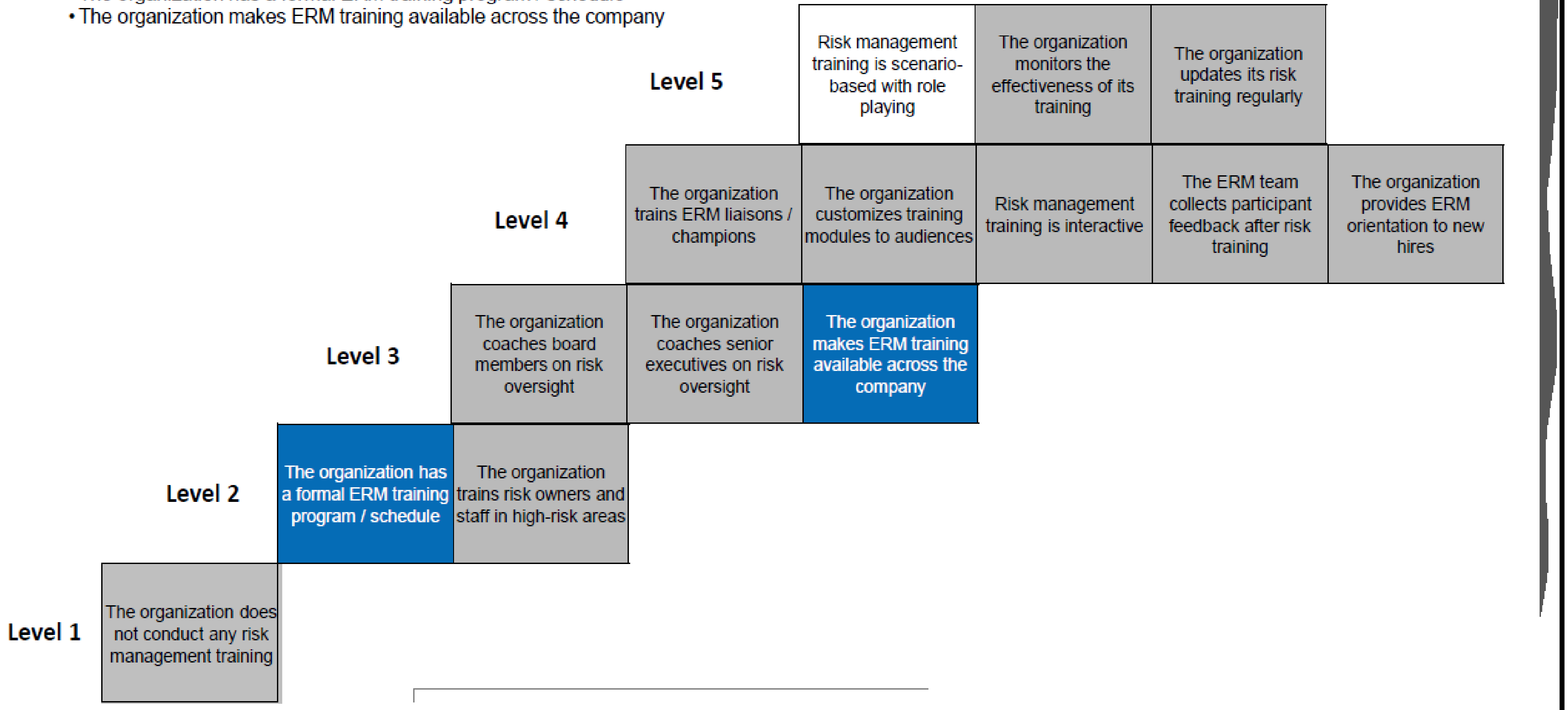
24. Education & Training of employees on ERM

Source: DAC [CEB Risk Management Maturity & Functionality Diagnostic May 2015]

Consider these steps to reach the next level of maturity:

Start doing the following:

- The organization has a formal ERM training program / schedule
- The organization makes ERM training available across the company



Level 5

- Risk management training is scenario-based with role playing
- The organization monitors the effectiveness of its training
- The organization updates its risk training regularly

Level 4

- The organization trains ERM liaisons / champions
- The organization customizes training modules to audiences
- Risk management training is interactive
- The ERM team collects participant feedback after risk training
- The organization provides ERM orientation to new hires

Level 3

- The organization coaches board members on risk oversight
- The organization coaches senior executives on risk oversight
- The organization makes ERM training available across the company

Level 2

- The organization has a formal ERM training program / schedule
- The organization trains risk owners and staff in high-risk areas

Level 1

- The organization does not conduct any risk management training

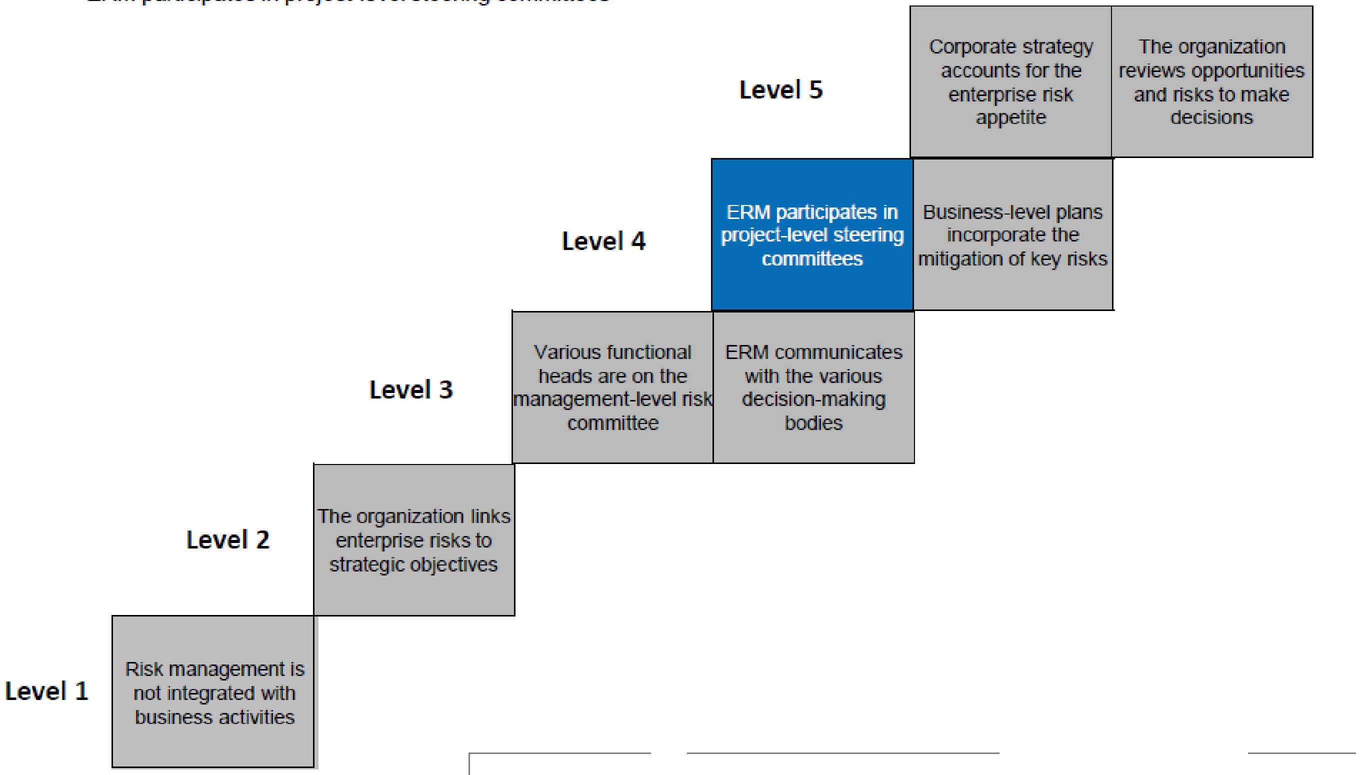
25. Integrated ERM with business activities?

Source: DAC [CEB Risk Management Maturity & Functionality Diagnostic May 2015]

Consider these steps to reach the next level of maturity:

Start doing the following:

- ERM participates in project-level steering committees



Level 5

Corporate strategy accounts for the enterprise risk appetite

The organization reviews opportunities and risks to make decisions

Level 4

ERM participates in project-level steering committees

Business-level plans incorporate the mitigation of key risks

Level 3

Various functional heads are on the management-level risk committee

ERM communicates with the various decision-making bodies

Level 2

The organization links enterprise risks to strategic objectives

Level 1

Risk management is not integrated with business activities

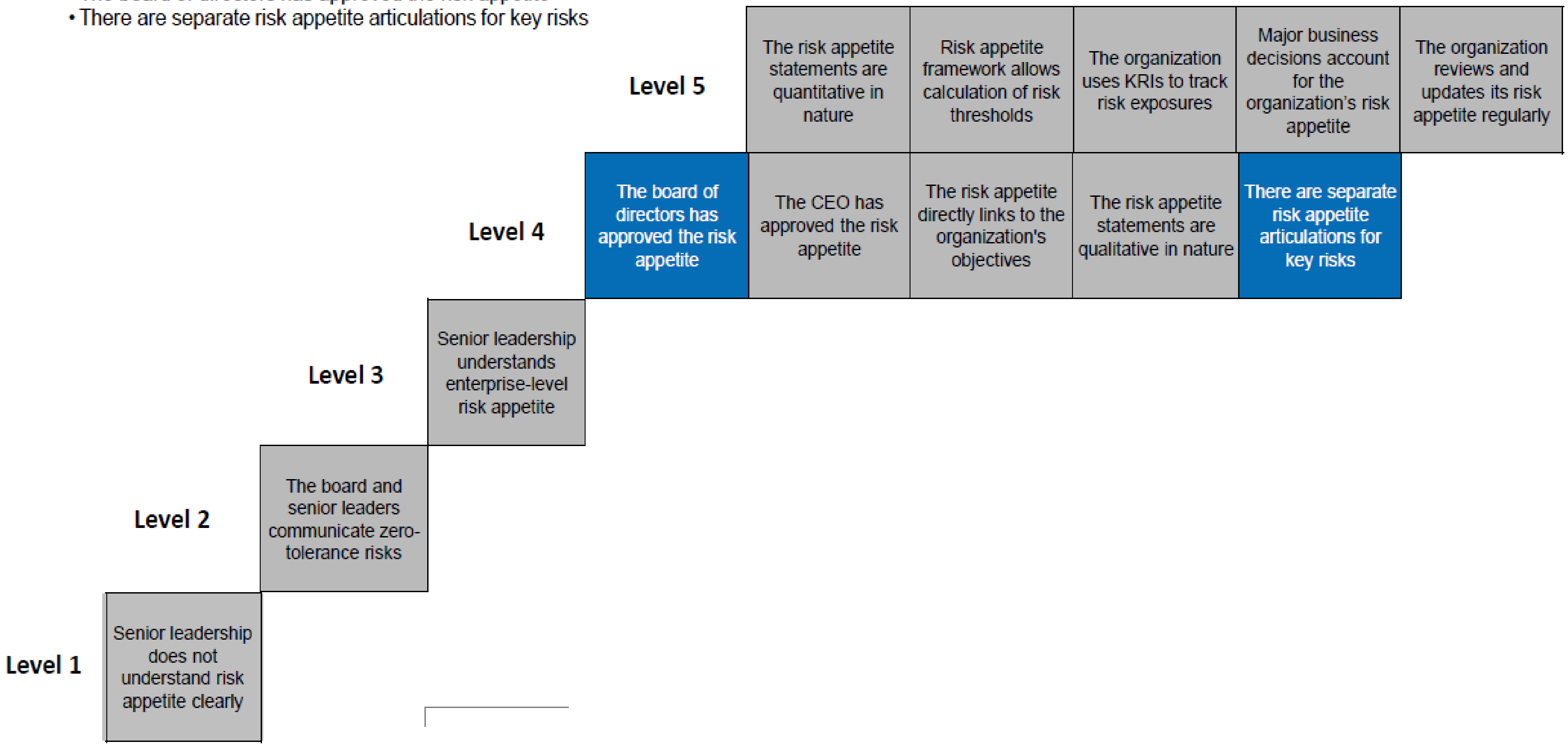
26. Set a Risk Appetite

Source: DAC [CEB Risk Management Maturity & Functionality Diagnostic May 2015]

Consider these steps to reach the next level of maturity:

Start doing the following:

- The board of directors has approved the risk appetite
- There are separate risk appetite articulations for key risks



Level 5

- The risk appetite statements are quantitative in nature
- Risk appetite framework allows calculation of risk thresholds
- The organization uses KRIs to track risk exposures
- Major business decisions account for the organization's risk appetite
- The organization reviews and updates its risk appetite regularly

Level 4

- The board of directors has approved the risk appetite
- The CEO has approved the risk appetite
- The risk appetite directly links to the organization's objectives
- The risk appetite statements are qualitative in nature
- There are separate risk appetite articulations for key risks

Level 3

- Senior leadership understands enterprise-level risk appetite

Level 2

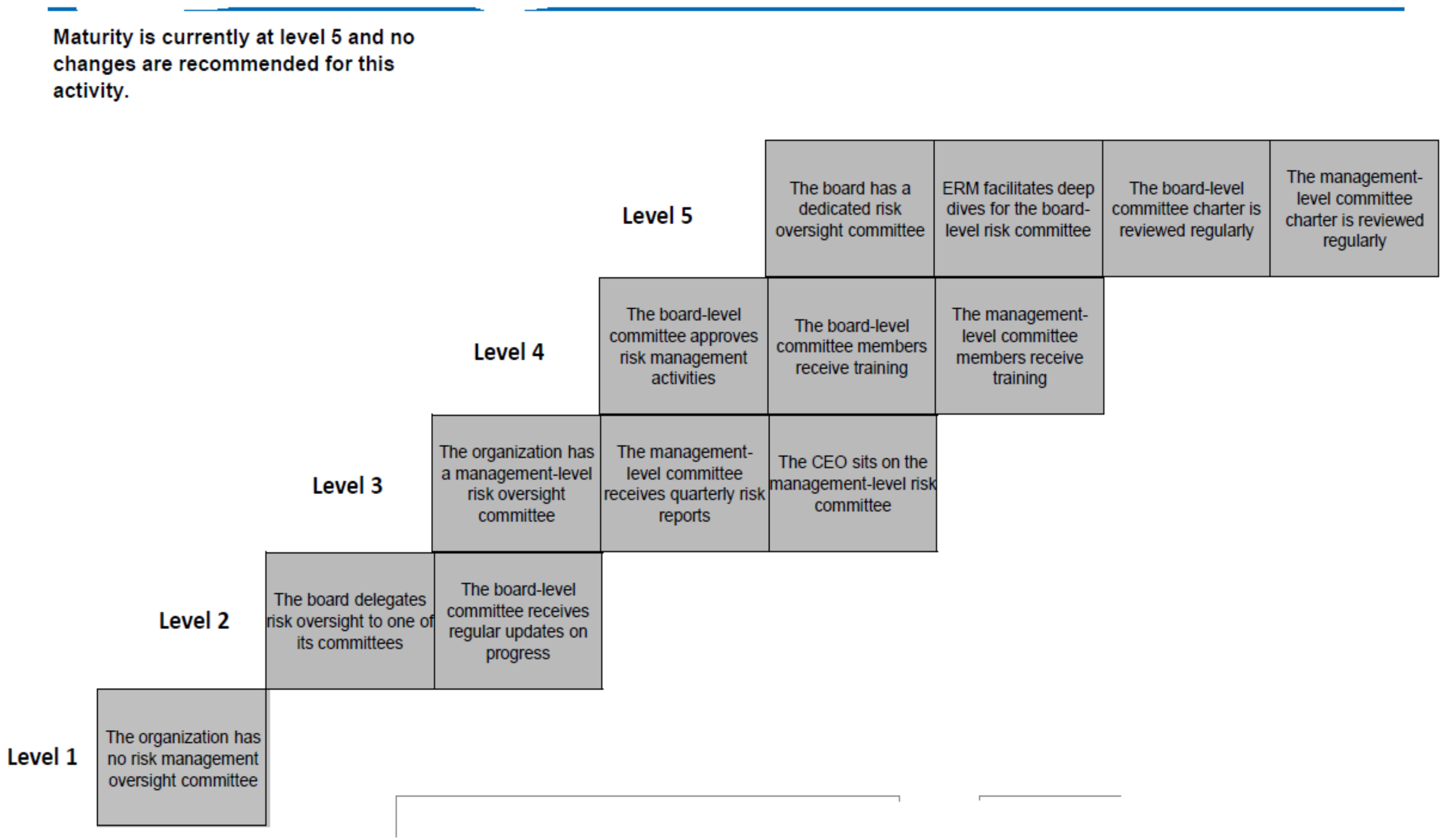
- The board and senior leaders communicate zero-tolerance risks

Level 1

- Senior leadership does not understand risk appetite clearly

27. Ensure Risk Committee Oversight

Source: DAC [CEB Risk Management Maturity & Functionality Diagnostic May 2015]



Maturity is currently at level 5 and no changes are recommended for this activity.

Level 5
- The board has a dedicated risk oversight committee
- ERM facilitates deep dives for the board-level risk committee
- The board-level committee charter is reviewed regularly
- The management-level committee charter is reviewed regularly

Level 4
- The board-level committee approves risk management activities
- The board-level committee members receive training
- The management-level committee members receive training

Level 3
- The organization has a management-level risk oversight committee
- The management-level committee receives quarterly risk reports
- The CEO sits on the management-level risk committee

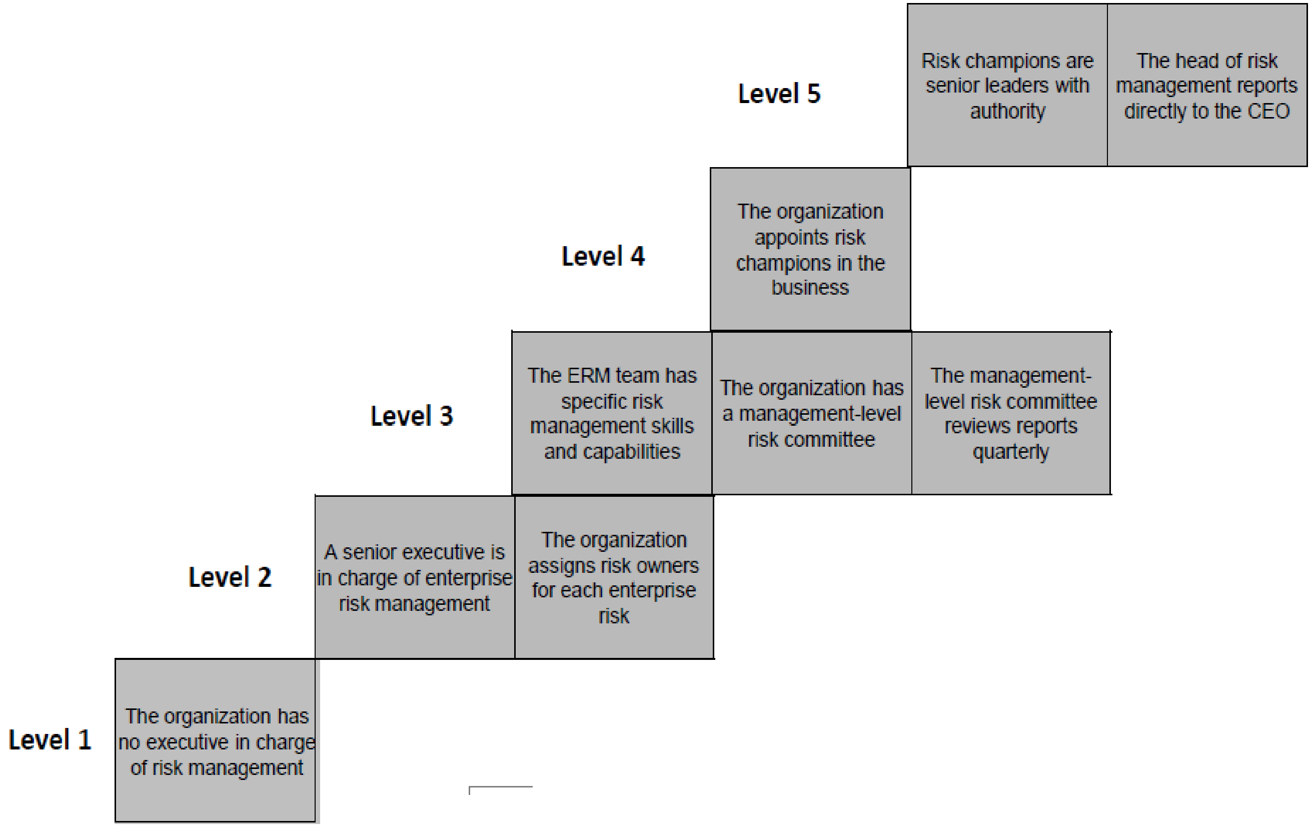
Level 2
- The board delegates risk oversight to one of its committees
- The board-level committee receives regular updates on progress

Level 1
- The organization has no risk management oversight committee

28. Manage Risk Organization Structure

Source: DAC [CEB Risk Management Maturity & Functionality Diagnostic May 2015]

Maturity is currently at level 5 and no changes are recommended for this activity.



Level 5

Risk champions are senior leaders with authority

The head of risk management reports directly to the CEO

Level 4

The organization appoints risk champions in the business

Level 3

The ERM team has specific risk management skills and capabilities

The organization has a management-level risk committee

The management-level risk committee reviews reports quarterly

Level 2

A senior executive is in charge of enterprise risk management

The organization assigns risk owners for each enterprise risk

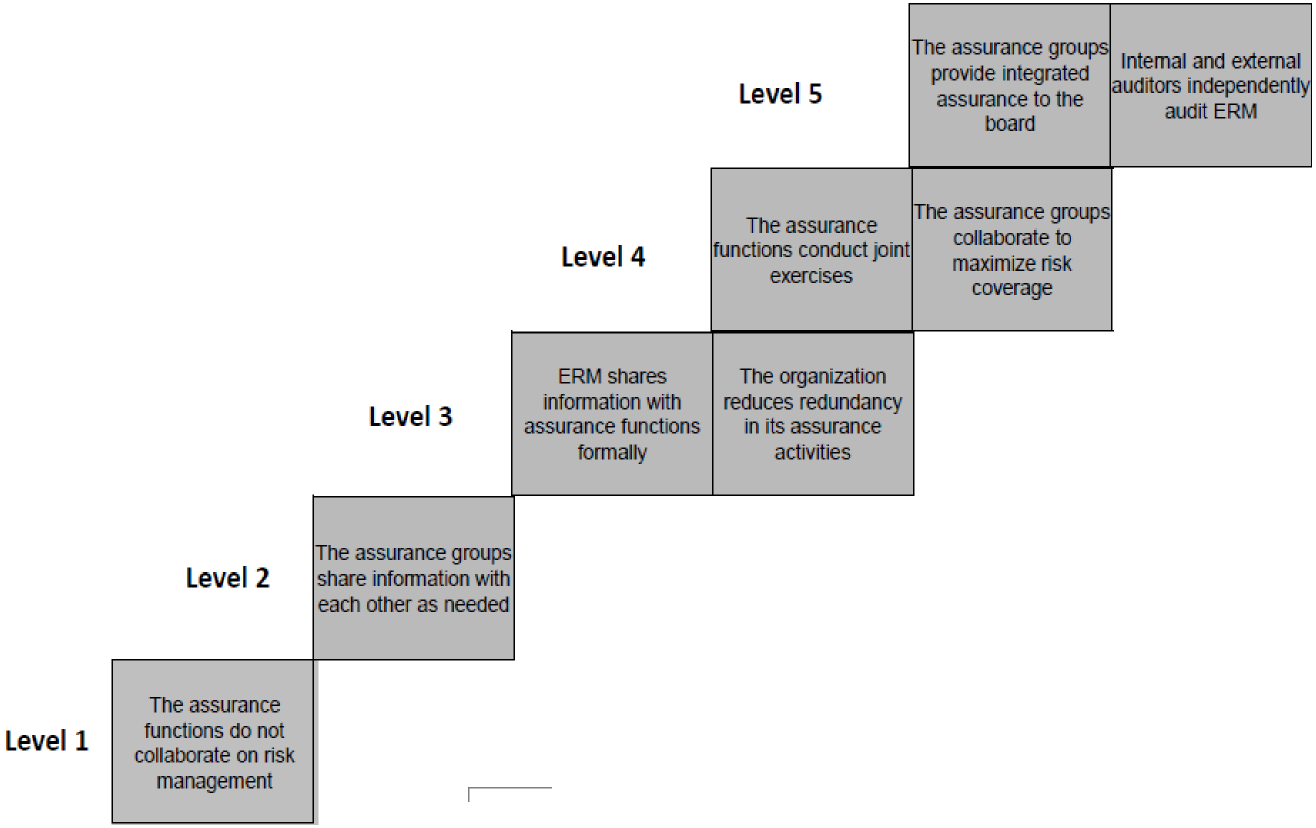
Level 1

The organization has no executive in charge of risk management

29. Collaborate with other assurance functions

Source: DAC [CEB Risk Management Maturity & Functionality Diagnostic May 2015]

Maturity is currently at level 5 and no changes are recommended for this activity.



Level 1

The assurance functions do not collaborate on risk management

Level 2

The assurance groups share information with each other as needed

Level 3

ERM shares information with assurance functions formally

The organization reduces redundancy in its assurance activities

Level 4

The assurance functions conduct joint exercises

The assurance groups collaborate to maximize risk coverage

Level 5

The assurance groups provide integrated assurance to the board

Internal and external auditors independently audit ERM

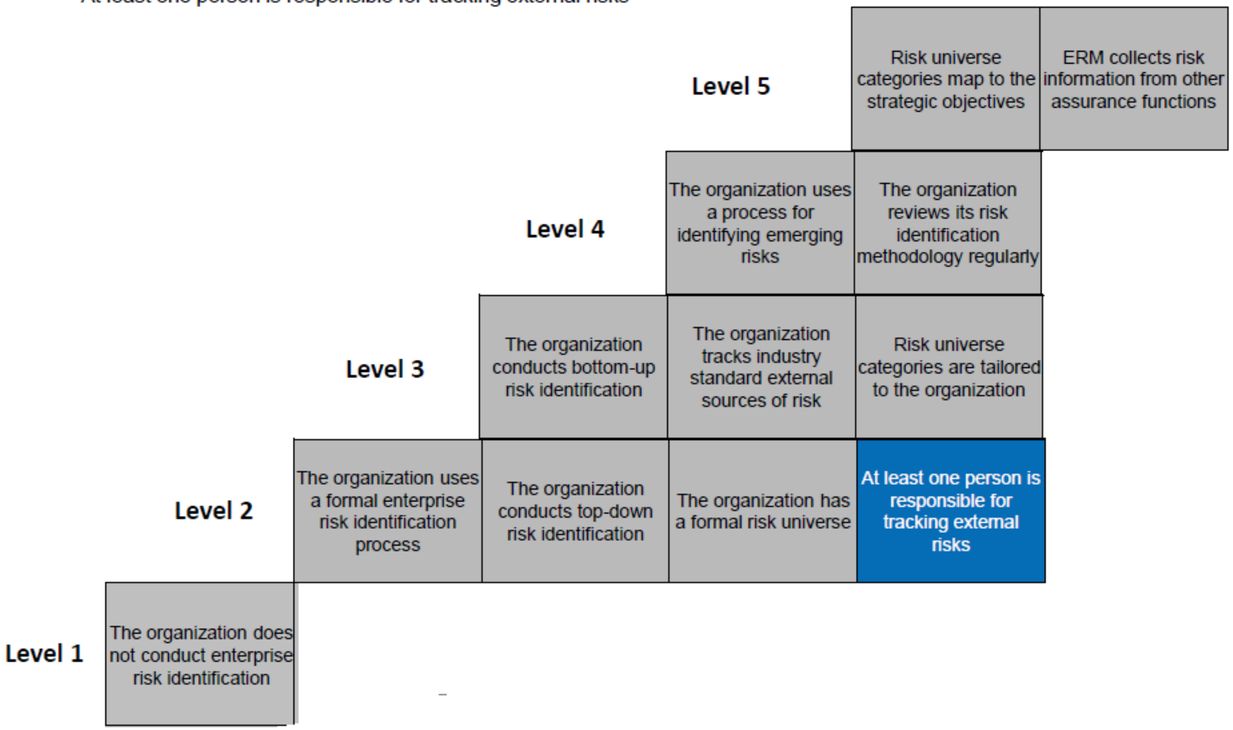
30. Risk Identification

Source: DAC [CEB Risk Management Maturity & Functionality Diagnostic May 2015]

Consider these steps to reach the next level of maturity:

Start doing the following:

- At least one person is responsible for tracking external risks



Level 5

Risk universe categories map to the strategic objectives

ERM collects risk information from other assurance functions

Level 4

The organization uses a process for identifying emerging risks

The organization reviews its risk identification methodology regularly

Level 3

The organization conducts bottom-up risk identification

The organization tracks industry standard external sources of risk

Risk universe categories are tailored to the organization

Level 2

The organization uses a formal enterprise risk identification process

The organization conducts top-down risk identification

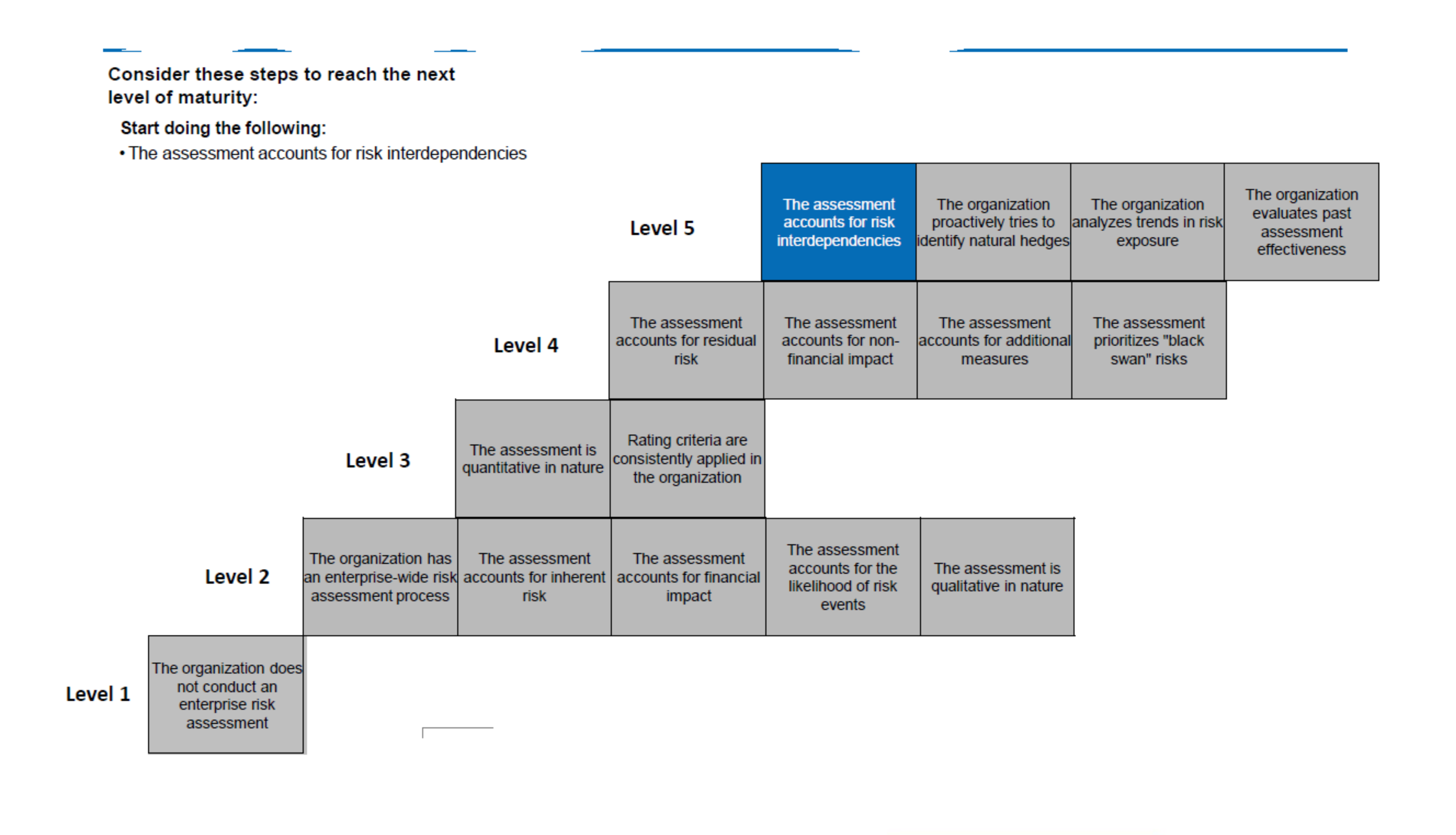
The organization has a formal risk universe

At least one person is responsible for tracking external risks

Level 1

The organization does not conduct enterprise risk identification

31. Assess & Prioritize Risks



Consider these steps to reach the next level of maturity:

Start doing the following:

- The assessment accounts for risk interdependencies

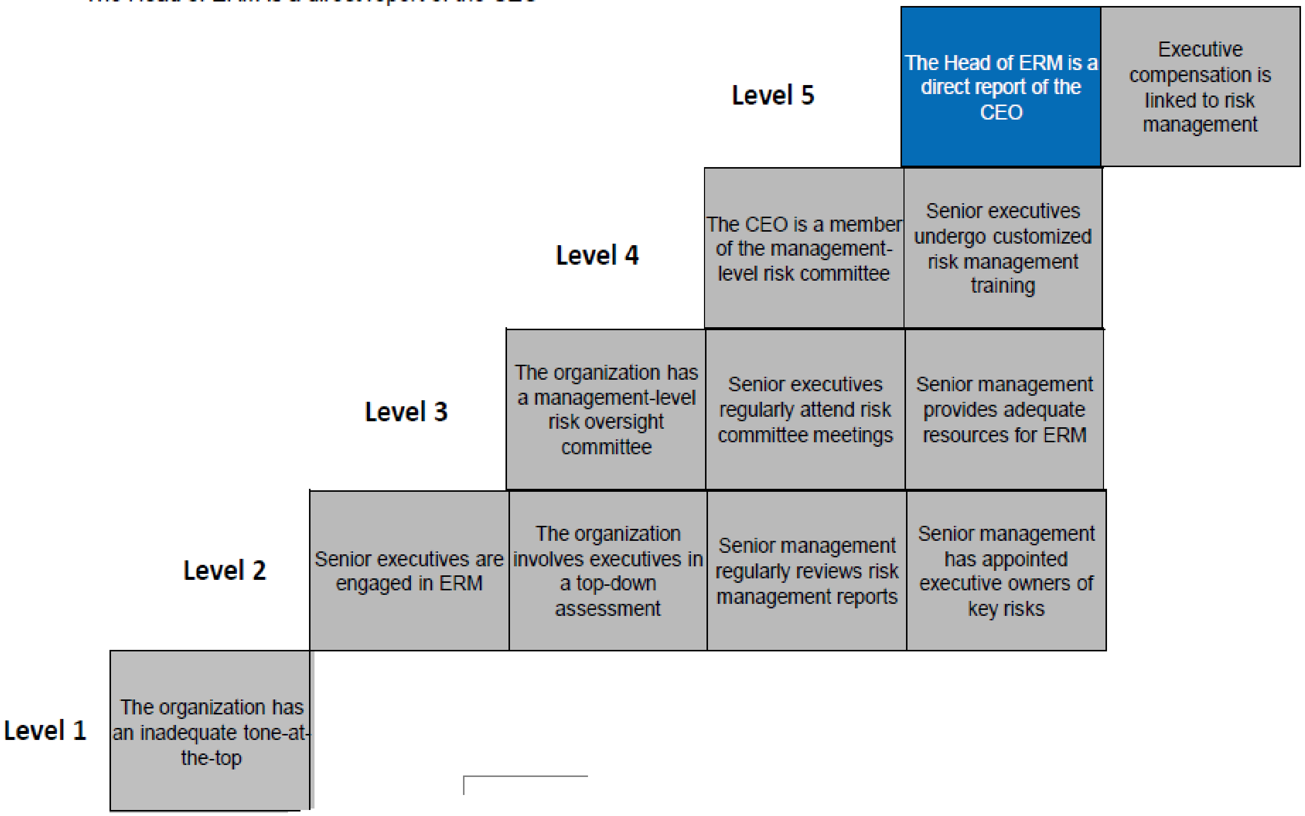
Level 5	The assessment accounts for risk interdependencies	The organization proactively tries to identify natural hedges	The organization analyzes trends in risk exposure	The organization evaluates past assessment effectiveness	
Level 4	The assessment accounts for residual risk	The assessment accounts for non-financial impact	The assessment accounts for additional measures	The assessment prioritizes "black swan" risks	
Level 3	The assessment is quantitative in nature	Rating criteria are consistently applied in the organization			
Level 2	The organization has an enterprise-wide risk assessment process	The assessment accounts for inherent risk	The assessment accounts for financial impact	The assessment accounts for the likelihood of risk events	The assessment is qualitative in nature
Level 1	The organization does not conduct an enterprise risk assessment				

32. Engage Senior Executives

Consider these steps to reach the next level of maturity:

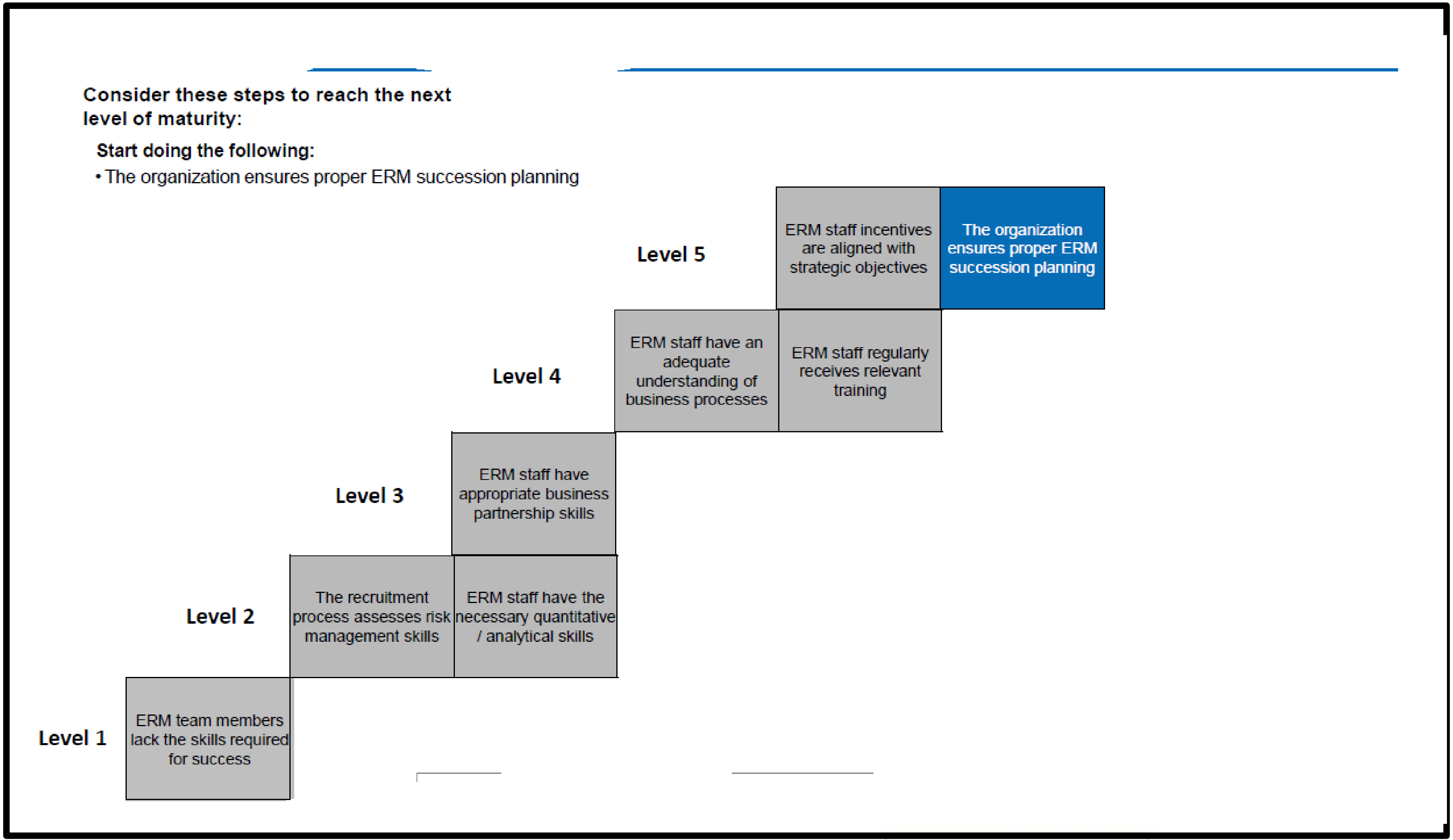
Start doing the following:

- The Head of ERM is a direct report of the CEO



Level 5					The Head of ERM is a direct report of the CEO	Executive compensation is linked to risk management
Level 4				The CEO is a member of the management-level risk committee	Senior executives undergo customized risk management training	
Level 3			The organization has a management-level risk oversight committee	Senior executives regularly attend risk committee meetings	Senior management provides adequate resources for ERM	
Level 2		Senior executives are engaged in ERM	The organization involves executives in a top-down assessment	Senior management regularly reviews risk management reports	Senior management has appointed executive owners of key risks	
Level 1	The organization has an inadequate tone-at-the-top					

33. Manage ERM talent



Consider these steps to reach the next level of maturity:

Start doing the following:

- The organization ensures proper ERM succession planning

Level 5

ERM staff incentives are aligned with strategic objectives

The organization ensures proper ERM succession planning

Level 4

ERM staff have an adequate understanding of business processes

ERM staff regularly receives relevant training

Level 3

ERM staff have appropriate business partnership skills

Level 2

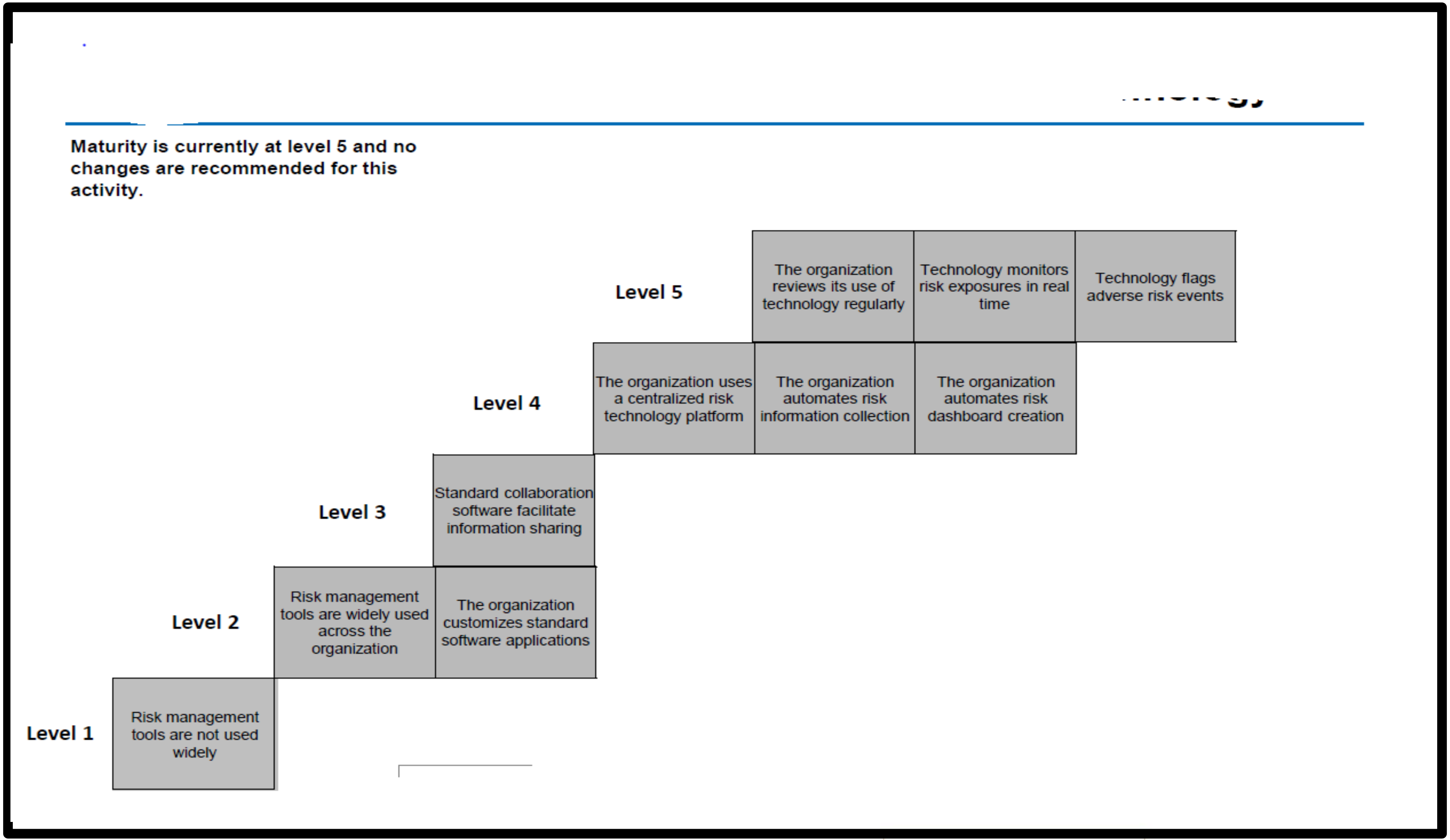
The recruitment process assesses risk management skills

ERM staff have the necessary quantitative / analytical skills

Level 1

ERM team members lack the skills required for success

34. Apply Risk Management Tools & Technology



Maturity is currently at level 5 and no changes are recommended for this activity.

Level 5
The organization reviews its use of technology regularly
Technology monitors risk exposures in real time
Technology flags adverse risk events

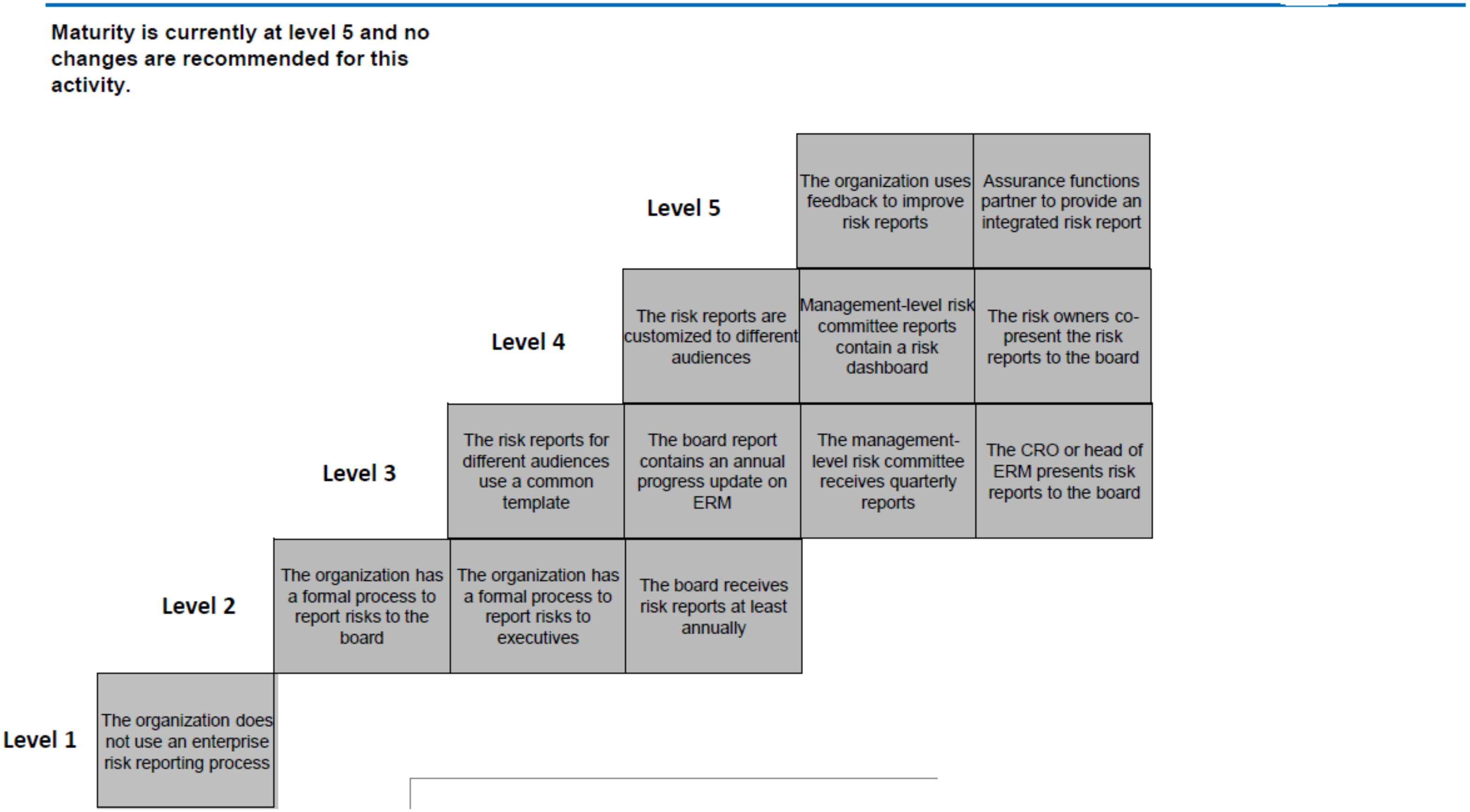
Level 4
The organization uses a centralized risk technology platform
The organization automates risk information collection
The organization automates risk dashboard creation

Level 3
Standard collaboration software facilitate information sharing

Level 2
Risk management tools are widely used across the organization
The organization customizes standard software applications

Level 1
Risk management tools are not used widely

35. Report on Risk Mitigation Status



Maturity is currently at level 5 and no changes are recommended for this activity.

Level 5

- The organization uses feedback to improve risk reports
- Assurance functions partner to provide an integrated risk report

Level 4

- The risk reports are customized to different audiences
- Management-level risk committee reports contain a risk dashboard
- The risk owners co-present the risk reports to the board

Level 3

- The risk reports for different audiences use a common template
- The board report contains an annual progress update on ERM
- The management-level risk committee receives quarterly reports
- The CRO or head of ERM presents risk reports to the board

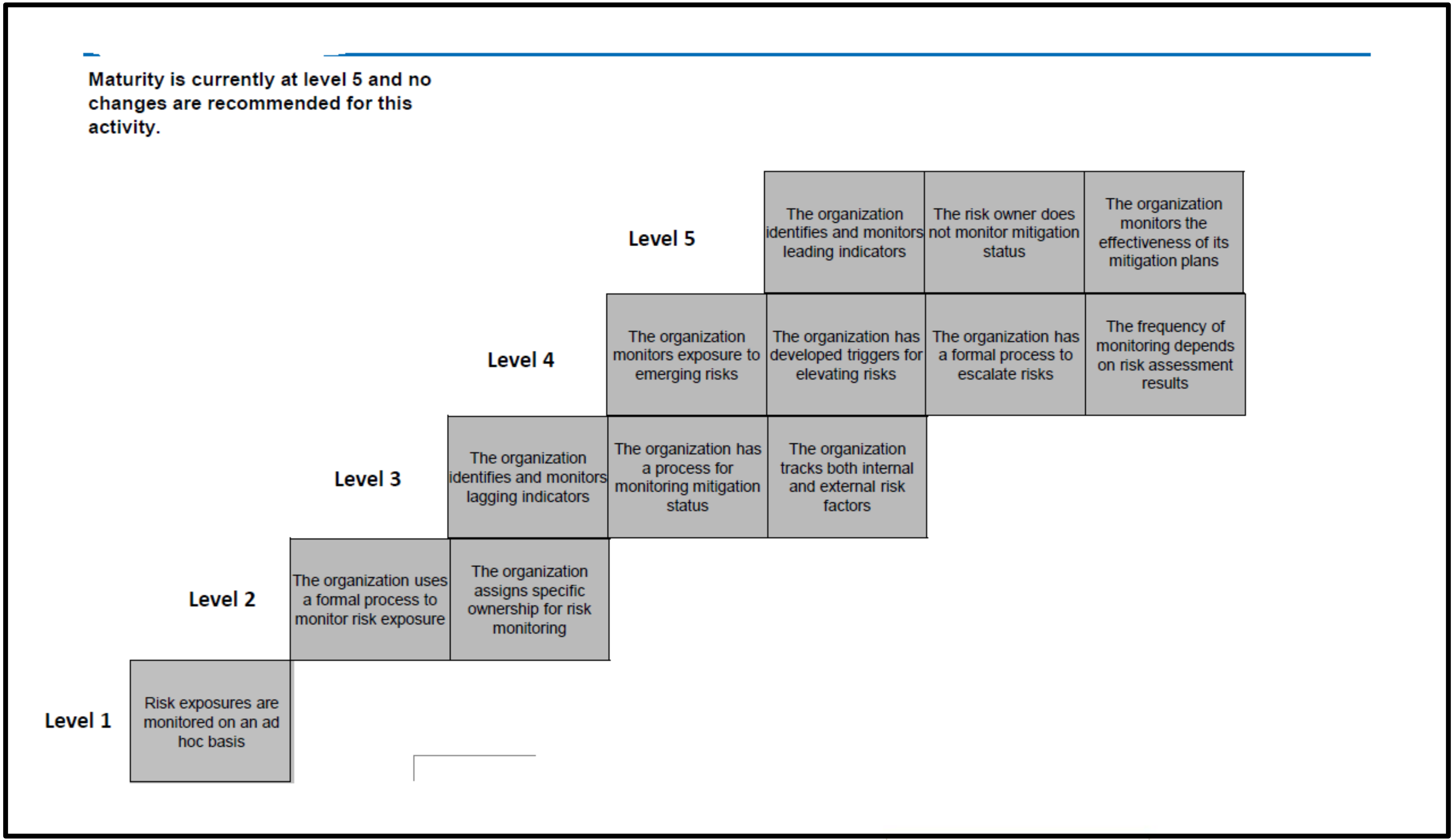
Level 2

- The organization has a formal process to report risks to the board
- The organization has a formal process to report risks to executives
- The board receives risk reports at least annually

Level 1

- The organization does not use an enterprise risk reporting process

36. Monitor level of risk exposure & Mitigation Status

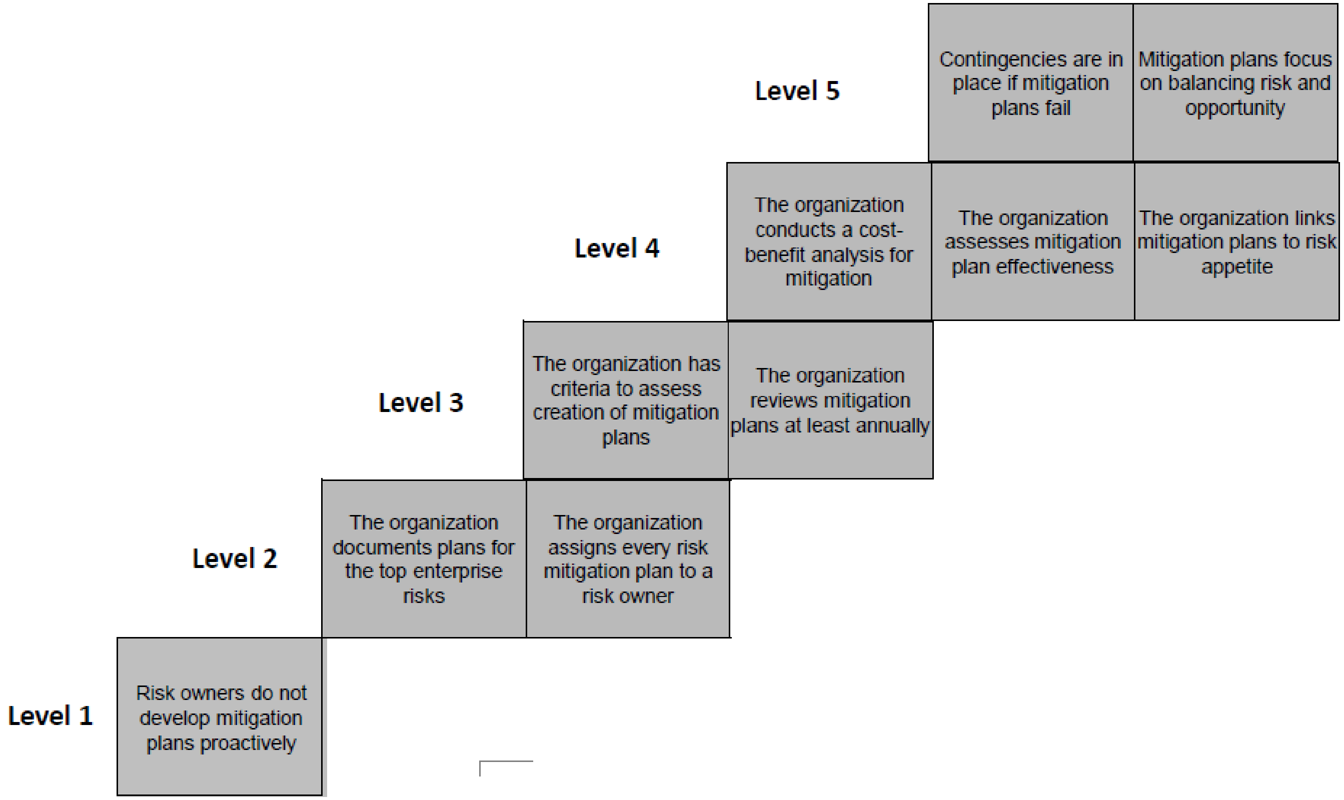


Maturity is currently at level 5 and no changes are recommended for this activity.

Level 5	The organization identifies and monitors leading indicators	The risk owner does not monitor mitigation status	The organization monitors the effectiveness of its mitigation plans	
Level 4	The organization monitors exposure to emerging risks	The organization has developed triggers for elevating risks	The organization has a formal process to escalate risks	The frequency of monitoring depends on risk assessment results
Level 3	The organization identifies and monitors lagging indicators	The organization has a process for monitoring mitigation status	The organization tracks both internal and external risk factors	
Level 2	The organization uses a formal process to monitor risk exposure	The organization assigns specific ownership for risk monitoring		
Level 1	Risk exposures are monitored on an ad hoc basis			

37. Mitigate Risks

Maturity is currently at level 5 and no changes are recommended for this activity.



Level 5

- Contingencies are in place if mitigation plans fail
- Mitigation plans focus on balancing risk and opportunity

Level 4

- The organization conducts a cost-benefit analysis for mitigation
- The organization assesses mitigation plan effectiveness
- The organization links mitigation plans to risk appetite

Level 3

- The organization has criteria to assess creation of mitigation plans
- The organization reviews mitigation plans at least annually

Level 2

- The organization documents plans for the top enterprise risks
- The organization assigns every risk mitigation plan to a risk owner

Level 1

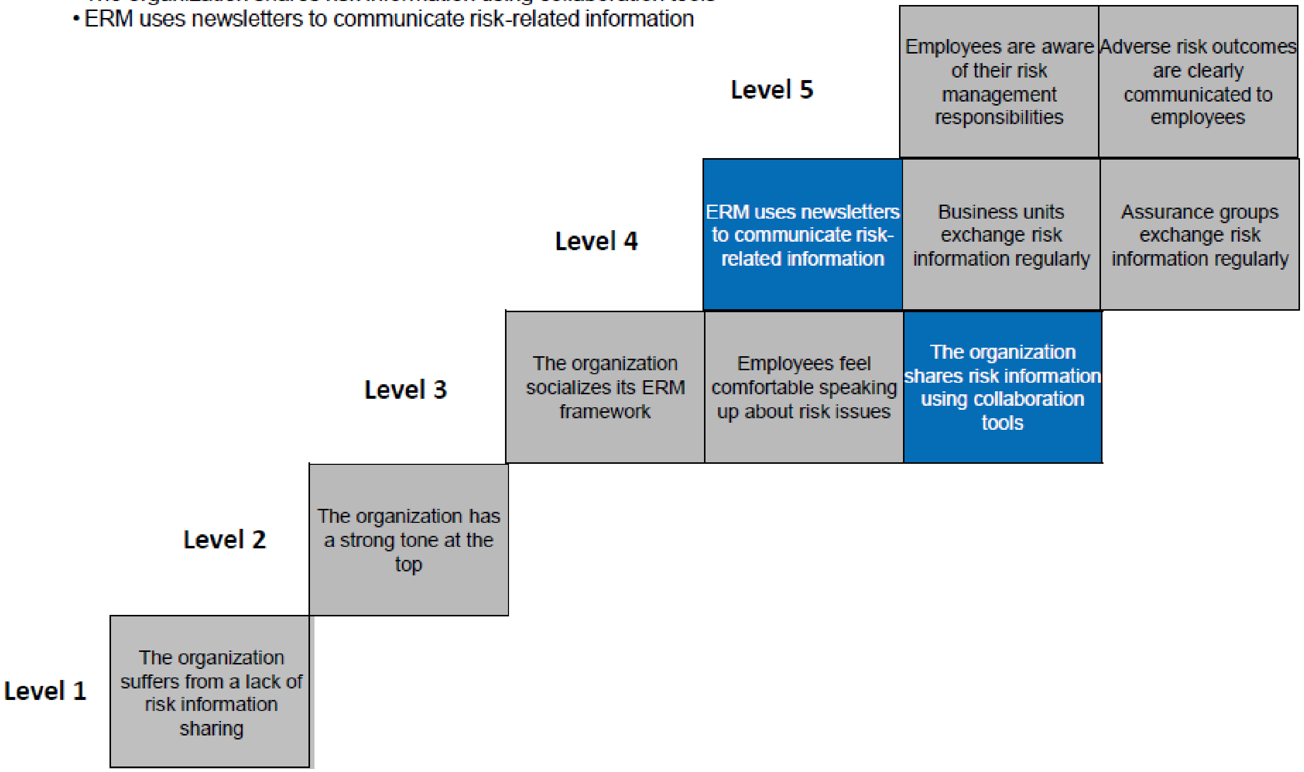
- Risk owners do not develop mitigation plans proactively

39. Is there transparent Risk Communication?

Consider these steps to reach the next level of maturity:

Start doing the following:

- The organization shares risk information using collaboration tools
- ERM uses newsletters to communicate risk-related information



Level 5

Employees are aware of their risk management responsibilities

Adverse risk outcomes are clearly communicated to employees

Level 4

ERM uses newsletters to communicate risk-related information

Business units exchange risk information regularly

Assurance groups exchange risk information regularly

Level 3

The organization socializes its ERM framework

Employees feel comfortable speaking up about risk issues

The organization shares risk information using collaboration tools

Level 2

The organization has a strong tone at the top

Level 1

The organization suffers from a lack of risk information sharing