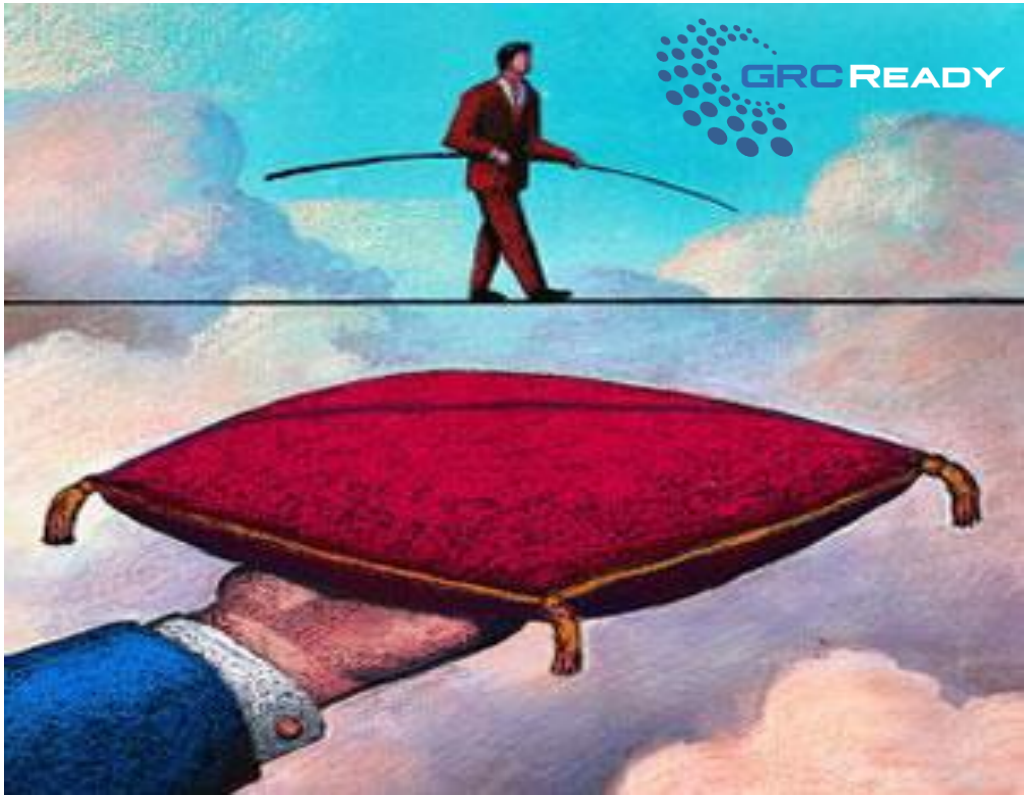
Risk Based Audit



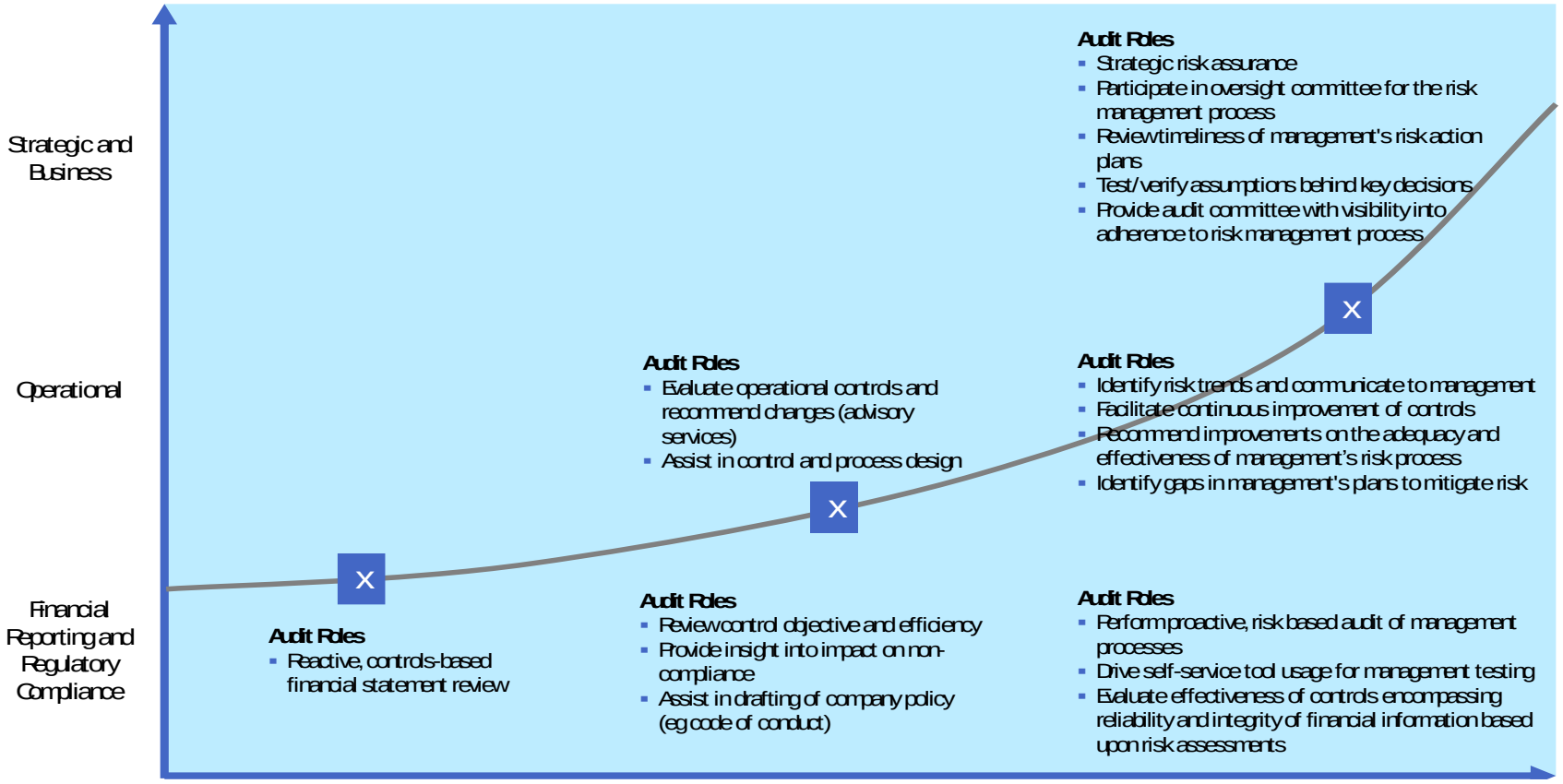
Click here for the session recording.

“Together we make a difference”
25 April 2024

Risk Based Audit - Agenda for today

- **Evolution of the profession**
- **Customer survey & BARC requirements**
- **Internal Audit role and position of risk auditing**
- **Risk based audit – How do we know that we are doing the:**
  - **right audits? (Focus of this session)**
  - **audits right? (Next session)**
- **Do the Right Audits unpacked / steps**
  1. **Strategic & business model alignment**
  2. **Risk profile mapping**
  3. **Emerging risk mapping**
  4. **Legal & compliance**
  5. **Reoccurring and systemic issues**
  6. **BARC and Management requests**
- **Summary and questions**

Evolution of the Internal Audit Function



Source: Audit Director Round Table Research

Feedback from Stakeholders received from over 60 visits to clients

BARC Requirement

Rio Tinto Director
Lord John Olav **Kerr**, Baron **Kerr of Kinlochard** GCMG

“Steve 2 questions please:

1. How do we know that you are doing the right audits? and
2. How do we know that every audit is executed properly?”

Overview of internal audit

The Institute of Internal Auditors :

Internal auditing:	Is designed to:	Achieve:
• is an independent, objective assurance and consulting activity	• add value; • improve operations; and • help an organisation accomplish its objectives	improvements to: • risk management; • internal control; and • governance process

Internal audit activity evaluates risk exposures relating to the organisation's governance, operations and information systems in relation to:

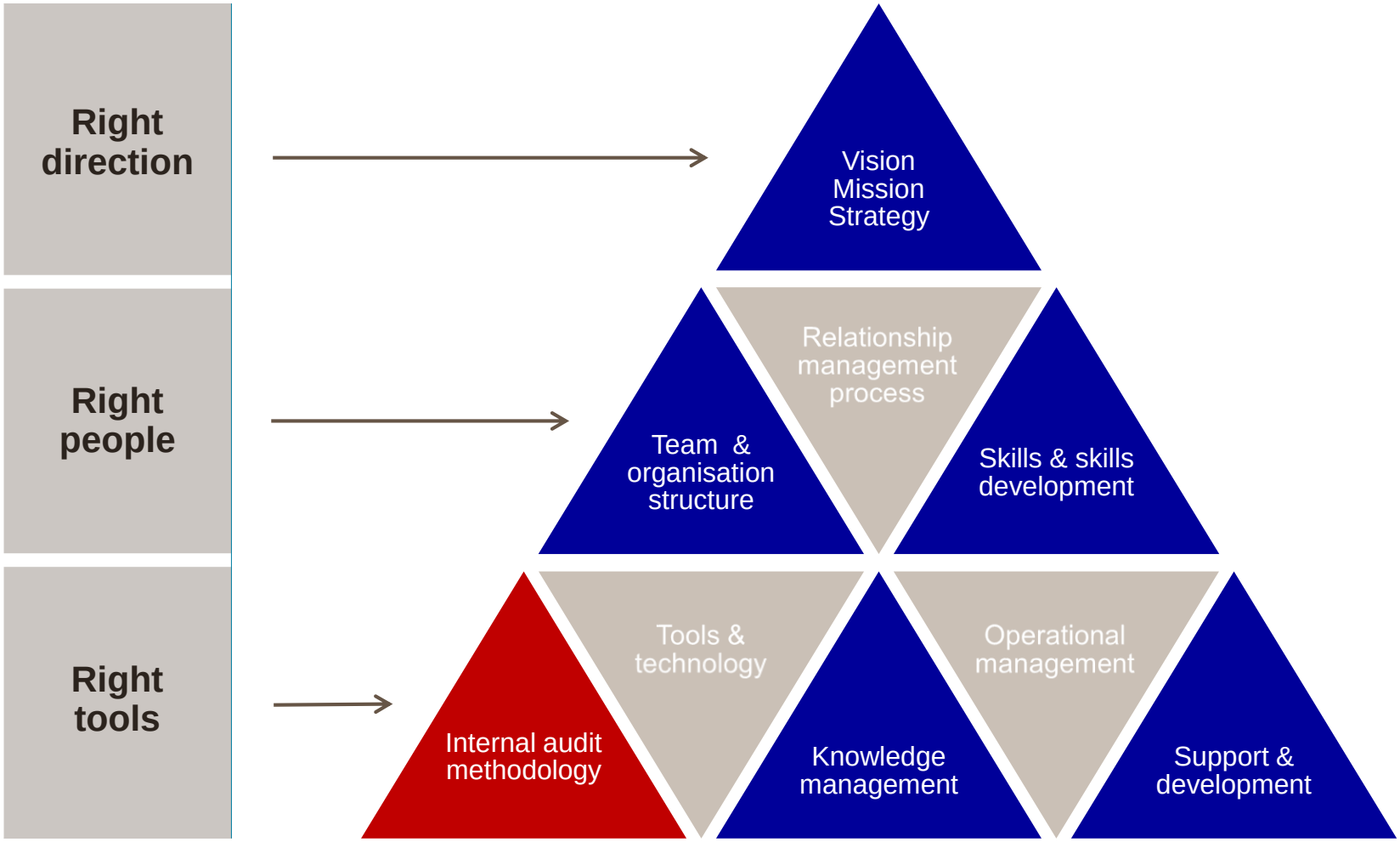
1. Design, effectiveness and efficiency of operations
2. Reliability and integrity of financial and operational information
3. Safeguarding of assets
4. Compliance with laws, regulations and contracts

In order to facilitate a good governance process, Internal Auditors:

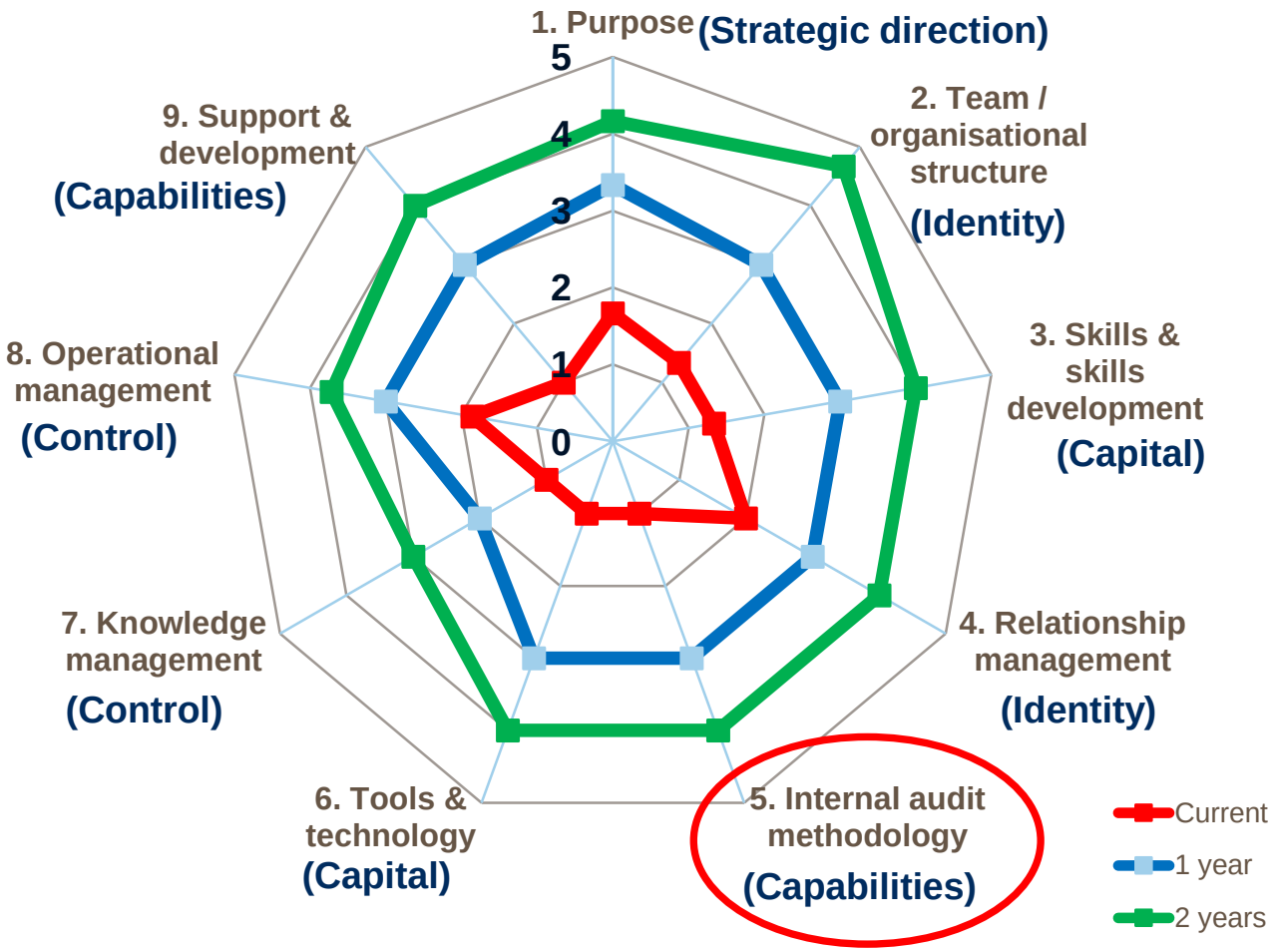
Assess adequacy & effectiveness of risk identification processes and management	Assess the ethics and values of the organisation	Assess performance management	Communicate risk & control information

Nine attributes for internal audit excellence

To achieve our mission & vision, we focus on developing the nine attributes which provides the basis for **leading-practice internal audit capability**.



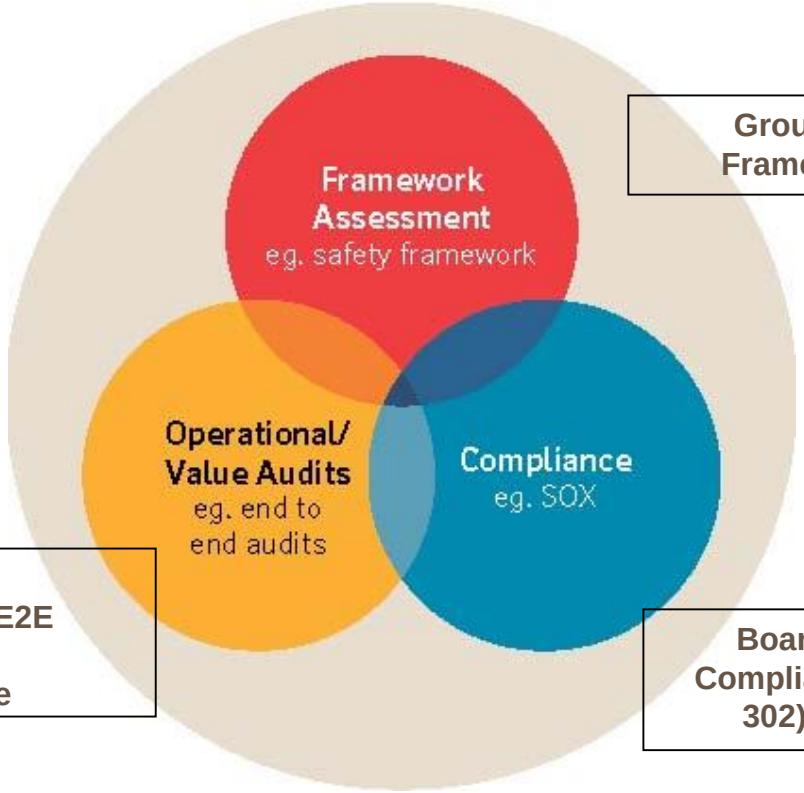
The IA function's maturity example below



Maturity level

1	Ad-hoc
2	Base
3	Satisfactory
4	Good
5	Best practice

Do the right audits – unpacked – overview of BARC and Management needs



Group Functions: Framework (COSO)

Operations: Commercial (E2E reviews) Value Leakage

Board/CEO/CFO Compliance (SOX404, 302), ASX P4&7

Do the risk audits - Approach and Methodology

A structured, logical and coordinated approach has been taken to ensure we do the right audits

Step 1 – Strategic Plan and business model mapping

Historical and planned audit need to be mapped to the Organisation's strategic objectives reflected in the business model

Core Activities

1 Exploration 74 days	2 Appraisal*	3 Development 400 days	4 Production 240 days	5 Maintenance 75 days	6 Distribution 40 days	7 Sales & Marketing (#) 257 days	8 Mine Closure*
• Exploration strategy • Plan for exploration • Explore & evaluate potential prospects • Acquire permit / license	• Market appraisal • Geological appraisal • Commercial appraisal • Beneficiation appraisal	• Development strategy • Define scope • Design and engineer • Seek approvals • Consent • Commission	• Production strategy and planning • Production Agreement Management • Extract • Beneficiate • Product Quality • Manage Inventory • Manage Cost	• Asset Maintenance strategy • Critical inventory management • Maintenance Management Planning • Decommission/ assess disposal	• Distribution strategy • Logistic Planning and coordination • Distribute product	• Planning & Forecasting • Sales negotiations • Manage customers • Sales & Shipping • Credit Management • Billing & Receivables	• Closure strategy • Closure operational management • Closure community management • Post closure management

Support Activities

(#) ABS Contract to Cash included in Sales and Marketing

- 7 **Sales & Marketing (#) 257 days**
- 9 **Strategy & Executive - 249 days**
- 10 **Plan & Manage – Financial management, Treasury, Taxation, Costing, etc 1535 days**
- 11 **Information Systems and Technology 882 days**
- 12 **Technology & Innovation 25 days**
- 13 **Manage People 415 days**
- 14 **Procure to Pay 665 days**
- 15 **Manage Physical Assets 258 days**
- 16 **Health, Safety & Environment***
- 17 **Risk (Insurance) 25 days**
- 18 **Legal/ Compliance/Security 391 days**
- 19 **Communication and External Relations 50 days**
- 20 **Company Secretarial 20 days**
- 21 **Manage Joint Ventures 115 days**
- 22 **Sustainable Development***
- 23 **Land Management 50 days**

Step 1– Process Description

Define the key processes within the organisation that link to those activities

1) **Manage People** (Forecast / review resource requirements, recruit and mobilise, train, retain, retire)
2) **Planning, Budgeting & Financial Management** (Development of business plans and supporting financial budgets, monitoring and forecasting, preparation of financial reports)
3) **Information & Knowledge Management** (effectively and securely capture, analyse and disseminate organisational information and knowledge for decision making)
4) **IS&T** (Development, implementation and maintenance of Information System and Technology solutions to support business strategy)
5) **Sales & Marketing** (Formulate and implement marketing strategy, negotiate and agree contract terms, manage contract performance, process sales transactions)
6) **Strategy & Execution Process** (Develop vision, strategic plans and corporate policies to provide overall direction for the company. Implement and monitor plans to achieve strategy)
7) **Capital Projects** (Capital investment decision, project management lifecycle & post implementation review)
8) **Manage Mine Production** (Establish mine plan, execute and monitor mining operations, manage assets, logistics)
9) **Distribution** (Negotiate contracts with shipping companies, arrange shipment and delivery of product to customers)
10) **Health, Safety & Environment** (Operate mine sites and facilities to comply with health, safety and environmental standards, regulations & goals.
11) **External Relationship Management** (Effectively manage external stakeholder information requirements and expectations through appropriate communication content, mechanism and timing.)
12) **Treasury** (Manage cash, portfolio of investments and ability to obtain long term financing)
13) **Tax Management** (Tax planning, strategy, implementation and compliance.)
14) **Property & Real Estate** (planning for property requirements, securing and fit out property to meet business requirements, effective utilisation of property)
15) **Exploration** (Identification and appraisal of viable resource bodies. Negotiation and securing of mineral rights and licence to operate)
16) **Innovation** (Identification, assessment and trial implementation of new technologies to achieve process improvement and competitive advantage)
17) **Mine Closure** (Planning, review and execution of key activities to return the land to a desirable state following the decommissioning of the mine site)
18) **Manage Physical Assets** (Strategies, processes and activities that are in place to ensure the optimal and continued utilisation of critical assets)
19) **Governance, Risk, Compliance & Legal** (Maintain integrity of the Group's governance structure, provision of risk management standards, tools and reporting, provision of group policies and procedures to comply with laws and regulations, legal advice and compliance)

Step 1 – define the high-level risks and potential scope – example Manage People

Process Overview

Key Risks

- Inadequate demand planning to achieve right people at right time
- Inability to attract key talent / increase candidate pipeline leakage
- Increased lead time or reduced return on investment
- Insufficient or inadequate resources to meet business requirements impacting business performance

Scope and Approach

Select 2 / 3 business units and review

- Resource forecasting and planning processes including consideration of current resource gaps
- Sourcing and recruitment processes including consideration of pipeline leakage and post hire performance / tenure
- Development, execution and assessment of training and development programmes
- Retention strategies (compensation / packages, upskilling, engagement) and current turnover
- Exit process management including liability management and gathering of process improvement feedback

Value to Business

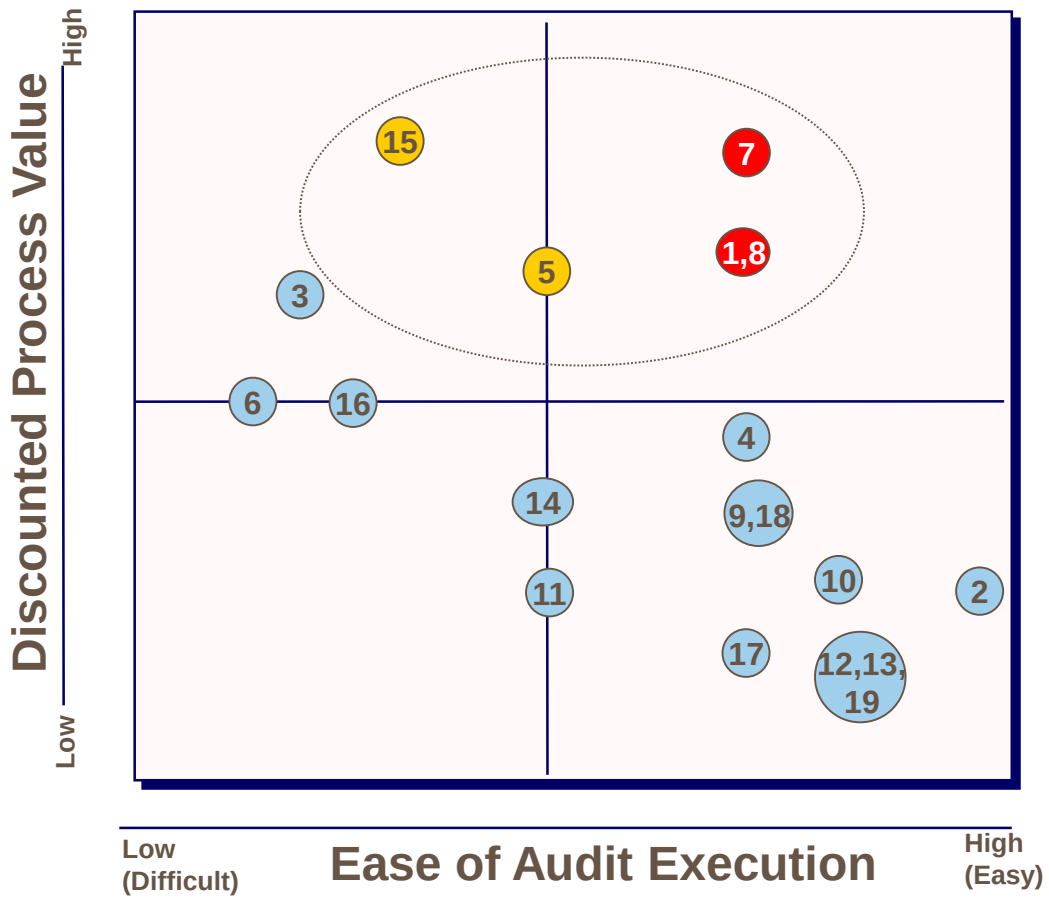
Assurance to the Audit Committee and Management over

- Robustness and effectiveness of workforce planning processes
- Recruitment and retention practices are in line with Group objective and best practice;
- Training and development practices are in line with Group objectives and best practice

Potential identification of systematic issues leading to resource gaps, talent leakage and reduced ROI impacting achievement of business objectives. Recommendations for group improvement.

Step 1 – Prioritisation Matrix

Evaluate and prioritise the key processes based on process value (discounted for existing assurance) and the ease of executing an end-to-end review



Key

1 – Manage People

2 – Budgeting, Forecasting & Financial Management

3 – Information & Knowledge Management

4 – IS&T

5 – Sales & Marketing

6 – Strategy & Executive

7 – Capital Projects

8 – Manage Mining Production

9 – Distribution

10 – Sustainable Development

11 – External Affairs

12 – Treasury Management

13 – Tax Management

14 – Property & Real Estate

15 – Exploration

16 – Innovation

17 – Mine Closure

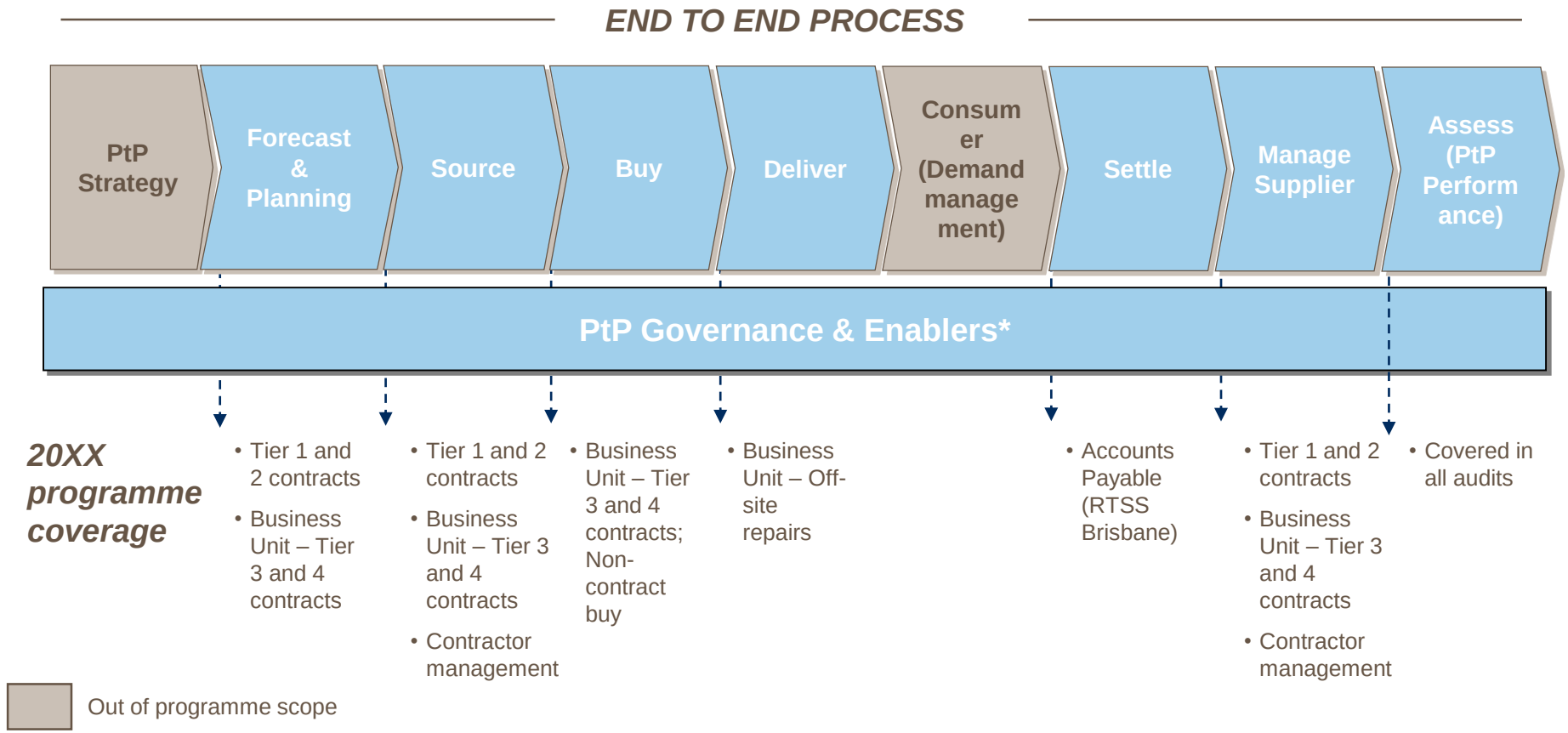
18 – Manage Physical Assets

19 – Governance, Risk, Compliance & Legal

Scope and Approach example

The key objectives of the PtP program audit is to assess controls design adequacy, effectiveness and efficiency across the full PtP process Chain

At the commencement of the planning phase for this programme, BU representatives and Corporate Assurance agreed the following components of the Procure-to-Pay end to end process

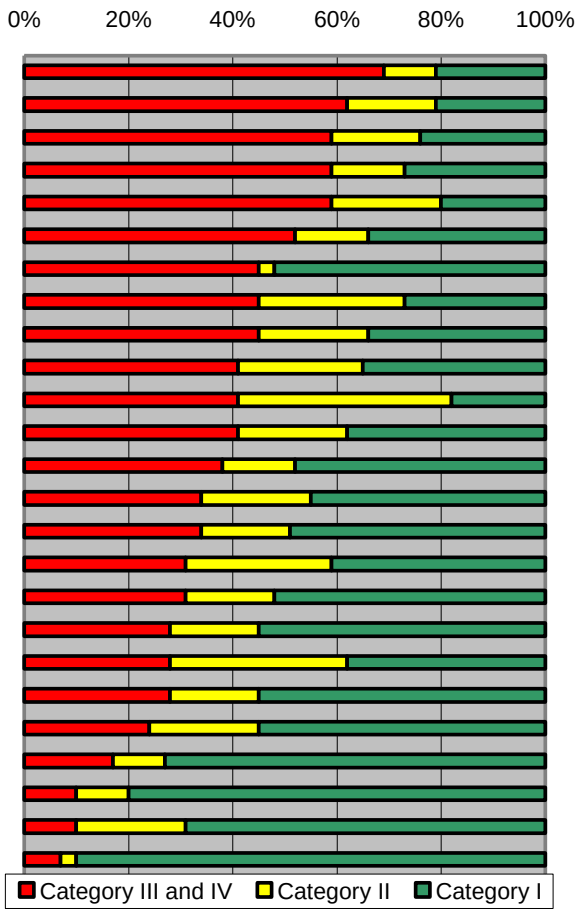


Step 2 – Risk Profile mapping

Extract from BARC paper

"This graph consolidates business unit ratings for each risk category and shows the percentage of risks classified as Class III or IV, Class II and Class I risk as well as the audit days allocated against each category."

Risk Category	2020	2021
1. Economic Risks (2)		12
2. Health and Safety Risks (3)		
3. Business Continuity Risks (4)	147	59
4. Operational Risks (1)	1148	1418
5. Information Technology risks (5)	879	691
6. Development Risks (8)	155	261
7. Commodity Trading Risks (13)		80
8. Environmental Risks (7)		
9. Business Integrity Risk (16)	65	120
10. Community Relations Risks (10)	10	50
11. Financial risks (including SOX) (15)	1694	2217
12. Human Resources Risks (6)	79	33
13. Financing and Currency Risks (9)		115
14. Technology Risks (19)	31	30
15. Land Use, Min. Rights & Ore Res. Risks (11)	93	20
16. Investment Risks (12)	70	75
17. Country Risks (18)		54
18. Taxation Risks (21)	30	73
19. Legal Risks (17)		
20. Closure Risks (14)		197
21. Joint Venture Risks (20)		
22. Exploration Risks (22)	35	209
23. Pension/ Foundation Risks (24)	10	25
24. Business Disclosure Risks (25)		20
25. Closed Operation Risks (23)		



Step 3 – Consider Emerging Risks

Hot Spot	Description	CA Response
1. INTERNATIONAL OPERATIONS	Reviews of risks associated with common business practices in emerging market operations that would constitute fraud or ethical violations for an organization	
2. COMPLIANCE	An evaluation of the transition and implementation of IFRS and continued focus on FCPA compliance, especially for companies operating in emerging markets.	
3. FRAUD	Increased attention and emphasis on fraud prevention as poor economic conditions increase the likelihood of fraud and financial misstatement.	
4.THIRD PARTY RELATIONSHIPS	Ensuring basic quality standards for goods and services received; also a focus on the control environment and financial viability of external partners.	
5. LIQUIDITY RISK	Reviews of company exposure to liquidity risk and the processes by which to identify, measure, monitor, and control this risk; also includes evaluations of management's understanding of liquidity risk and the transparency and reporting of this risk to company management and the Board.	
6. CORPORATE REPUTATION	A look at the impact to corporate brand from corporate social responsibility and sustainable development initiatives, as well as the impact of compliance failures	
7 HUMAN RESOURCES	Reviews of staff training and retention processes, as well as knowledge management strategies used to replicate and enable easy adoption of business activities.	
8. IMPACT OF COST REDUCTION PROGRAMMES	An evaluation of the potential negative impact of company cost cutting initiatives on the control environment and business outcomes.	
9. STRATEGIC RISK ASSURANCE	An examination of the identification and communication to the Board of strategic risks, as well as reviews of project management of large scale changes to corporate objectives.	
10. PRODUCT MANAGMENT	A focus on project management of new product implementations and reviews of existing product lines.	

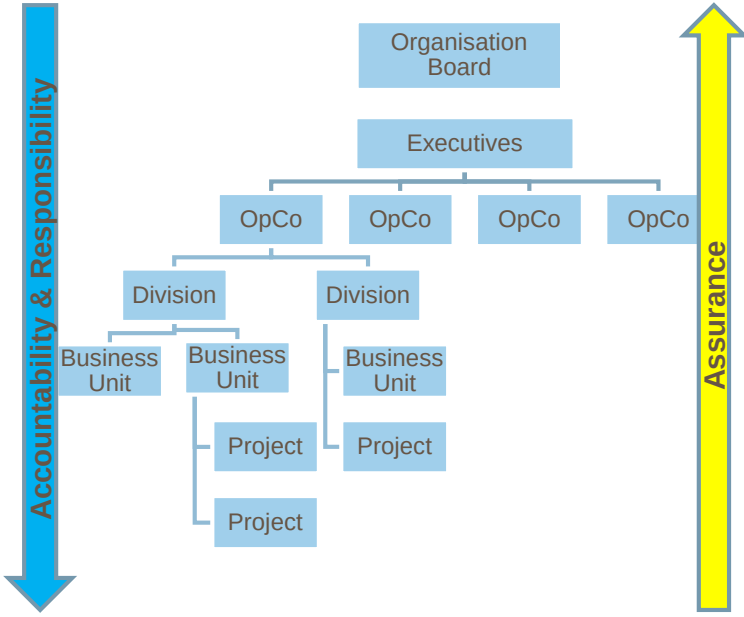
Step 4 – Legal Obligation and Compliance requirements

Obligations Based Compliance Framework

The obligations and governance framework will ensure material obligations for the Group are defined and all governance and compliance processes are aligned at a Group level and cascaded into all parts of the organisation. The model will act as the basis for your risk management system and Combined Assurance process.

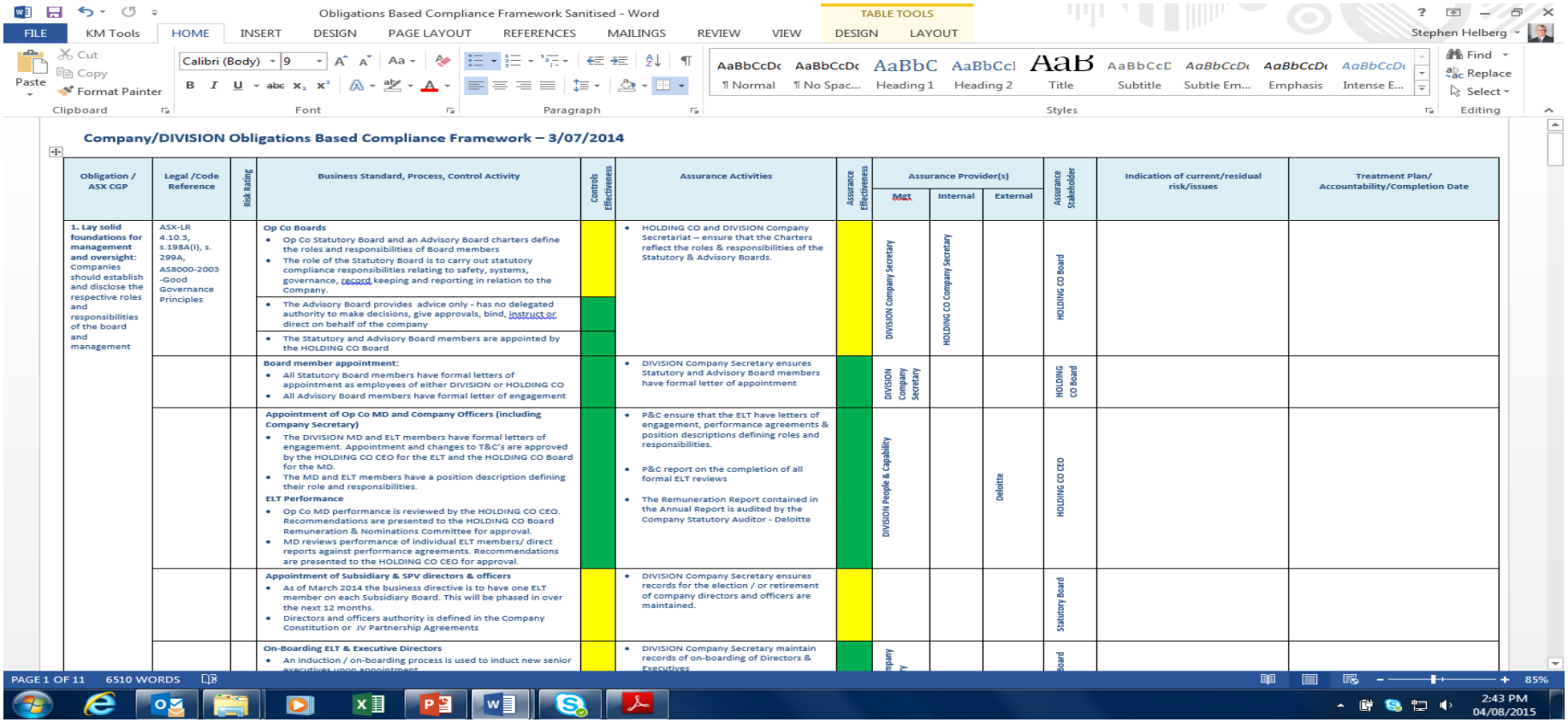
The framework will provide the Organisation and various levels of management with adequate comfort that:

- the main board obligations have been identified;
- the appropriate enterprise processes have been designed and are in place to effect or deliver these;
- Governance, policies and compliance processes throughout the Group are aligned and designed to meet the Group's obligations; and
- there are adequate measurement, monitoring and reporting systems in place to provide assurance these obligations are delivered.



Step 4 – Legal Obligation and Compliance requirements

Obligations Based Compliance Framework



Obligations Based Compliance Framework Sanitised - Word

Company/DIVISION Obligations Based Compliance Framework – 3/07/2014

Obligation / ASX CGP	Legal /Code Reference	Risk Rating	Business Standard, Process, Control Activity	Controls Effectiveness	Assurance Activities	Assurance Effectiveness	Assurance Provider(s) – Met	Assurance Provider(s) – Internal	Assurance Provider(s) – External	Assurance Stakeholder	Indication of current/residual risk/issues	Treatment Plan/ Accountability/Completion Date
1. Lay solid foundations for management and oversight: Companies should establish and disclose the respective roles and responsibilities of the board and management	ASX-LR 4.10.3, s.198A(I), s. 299A, AS8000-2003 -Good Governance Principles		**Op Co Boards** • Op Co Statutory Board and an Advisory Board charters define the roles and responsibilities of Board members • The role of the Statutory Board is to carry out statutory compliance responsibilities relating to safety, systems, governance, record keeping and reporting in relation to the Company. • The Advisory Board provides advice only - has no delegated authority to make decisions, give approvals, bind, instruct or direct on behalf of the company • The Statutory and Advisory Board members are appointed by the HOLDING CO Board		• HOLDING CO and DIVISION Company Secretariat – ensure that the Charters reflect the roles & responsibilities of the Statutory & Advisory Boards.		DIVISION Company Secretary	HOLDING CO Company Secretary		HOLDING CO Board		
			Board member appointment: • All Statutory Board members have formal letters of appointment as employees of either DIVISION or HOLDING CO • All Advisory Board members have formal letter of engagement		• DIVISION Company Secretary ensures Statutory and Advisory Board members have formal letter of appointment		DIVISION Company Secretary			HOLDING CO Board		
			Appointment of Op Co MD and Company Officers (including Company Secretary) • The DIVISION MD and ELT members have formal letters of engagement. Appointment and changes to T&C's are approved by the HOLDING CO CEO for the ELT and the HOLDING CO Board for the MD. • The MD and ELT members have a position description defining their role and responsibilities. **ELT Performance** • Op Co MD performance is reviewed by the HOLDING CO CEO. Recommendations are presented to the HOLDING CO Board Remuneration & Nominations Committee for approval. • MD reviews performance of individual ELT members/ direct reports against performance agreements. Recommendations are presented to the HOLDING CO CEO for approval.		• P&C ensure that the ELT have letters of engagement, performance agreements & position descriptions defining roles and responsibilities. • P&C report on the completion of all formal ELT reviews • The Remuneration Report contained in the Annual Report is audited by the Company Statutory Auditor - Deloitte		DIVISION People & Capability		Deloitte	HOLDING CO CEO		
			Appointment of Subsidiary & SPV directors & officers • As of March 2014 the business directive is to have one ELT member on each Subsidiary Board. This will be phased in over the next 12 months. • Directors and officers authority is defined in the Company Constitution or JV Partnership Agreements		• DIVISION Company Secretary ensures records for the election / or retirement of company directors and officers are maintained.					Statutory Board		
			On-Boarding ELT & Executive Directors • An induction / on-boarding process is used to induct new senior executives upon appointment		• DIVISION Company Secretary maintain records of on-boarding of Directors & Executives		Company			Board		

Step 5 - Reoccurring & systemic issues & follow up audit actions

All prior period issues are mapped and re-occurring & systemic issues identified are considered in future audits

Issues		Business Unit / Function																								
		Business A	Business B	Business C	Business D	Business E	Business F	Business G	Business H	Business I	Business J	Business K	Business L	Business M	Business N	Business O	Business P	Business Q	Business R	Business S	Business T	Business U	Business V	Business W	Business X	Business Y
Report Rating		M	M	M	M	M	M	S	M	S	S	S	S	M	M	S	S	S	S	M	S	M	M	-	-	S
1	Invoices are not always reconciled to timesheets or checked against scheduled rates, and expenses are not always verified	M	L	M	L	M			M		L			M	M	L	M			H		H	M		H	
2	The completion of agreed actions in accordance with agreed timeframes is not always monitored		L	L	L	L	L																			
3	Purchase Requisitions completed with an inappropriate GL Account or Cost Centre																					M				

Report Rating: G = Good S = Satisfactory M = Marginal W = Weak

Risk Rating

High | Medium | Low | Issues identified but not rated

Do the risk audits - Approach and Methodology

A structured, logical and coordinated approach has been taken to ensure we do the right audits

Summary

Guy Elliott Group CFO/FD…

"I am very happy with the PtP end product. I am going to take Tom [Albanese] through the report and I found this approach very valuable to Rio Tinto. I fully support that we do one of these types of reviews a year. Please convey my appreciation to every person who worked on this project." Guy Elliott

Question time…..