

FINANCIAL REPORTING & MANAGEMENT CONFERENCE FOR COUNTY GOVERNMENTS



CPAK

Credibility . Professionalism . AccountAbility

Governance – *The Nexus b/t Risk Management & Performance*



Risks

are part of business, but
business doesn't need
to be risky.

Speaker Background



MBA (Strategic Mgt), Bsc (Applied Acc.), CPA, FCCA, Dip (Risk Mgt)



13years – Banking, DPFB (Meriedien Biao, Pan African Bank, EuroBank, Trust Bank, Delphis Bank, Bank Supervision, Internal Audit, Finance and National Debt Registry



2 years – Credit Risk & Enterprise-wide Risk Management



6.5 years – Enterprise-wide Risk Management, specialization on Non-financial Risks



Todate – HELB – Board Leadership

Who we are



The Institute of
Risk Management - Kenya

Transforming the Risk Management Practice





*The Institute of Risk Management Kenya (IRM-K) is a **non - profit** professional, education and research Institution established and registered in Kenya to answer the growing need for risk management education in Kenya and wider Sub-Saharan (SSE) region.*



*The Institute of
Risk Management - Kenya*

Our Proposition

- **We passionately believe in the importance and relevance of risk management**
- **Advocate for enterprise wide risk approach**
- **Understands that risk management is as much about the people as it is about processes**
- **Risk Management efforts must be linked to the needs of the business communities.**
- ➔ **Our mission is to raise latent risk management, entrepreneurial and managerial competency of Kenyan and regional businesses, communities and organizations to become increasingly competitive and to seamlessly integrate into regional and international arena.**

Our vision –

"To be a leading and professional firm in business and management training and consulting in Africa and Developing world".

Happy Clients



**“The Institute's Vision Is
To Lead And Inspire
Sustainable Value
Adding Enterprise Risk
Management.”**



Vision Statement, IRM (K)

**“Promote Organizational
Effectiveness, Professional Growth,
And Economic Development Through
Integrated Enterprise Risk
Management.”**



Mission Statement, IRM (K)

Collaborations

Aptivaa

150+
implementations

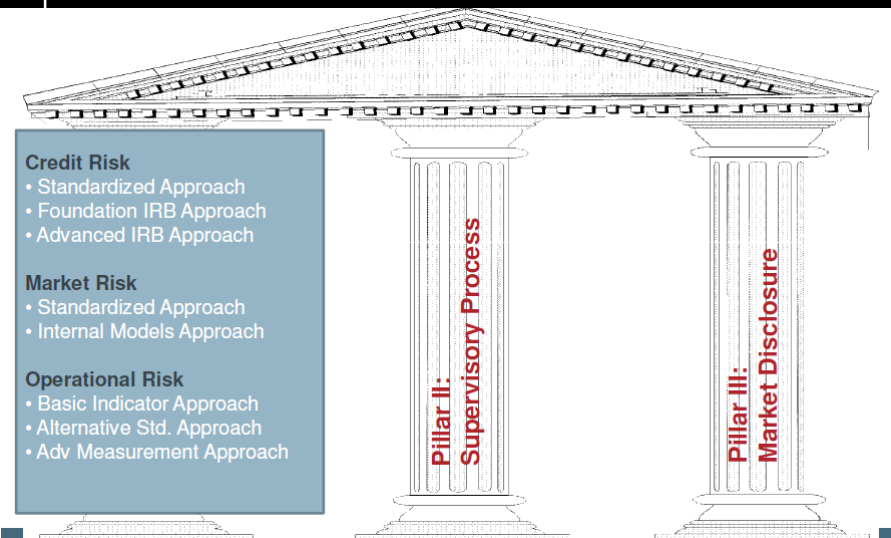


AA2SH
the ideal approach

CHASE COOPER
A Dion Global Solutions Company



Why Elaborate collaborations



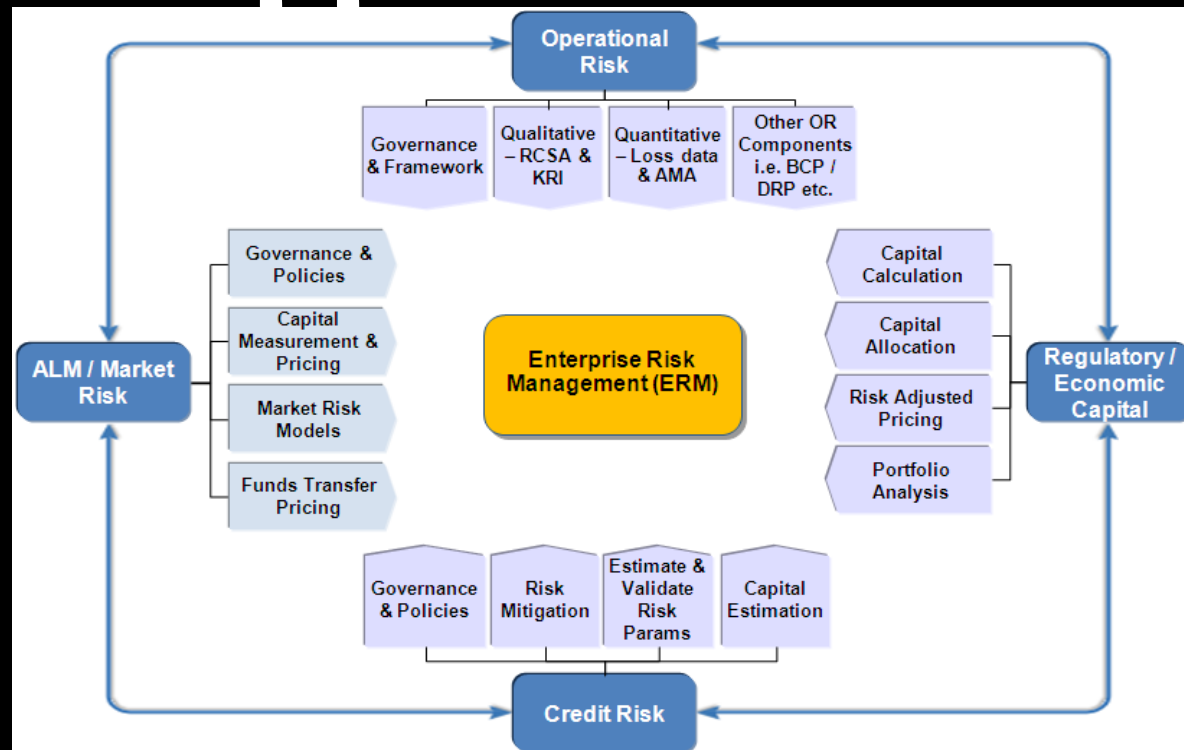
Global Association
of Risk Professionals



Energy Risk Professionals (ERP®)



Our Approach



Consulting

The Consulting and advisory services provides clients with solutions to the issues faced at every stage of the risk management process. We look to provide value based services by using our cutting edge skill sets to put clients on par with globally suited best practices.

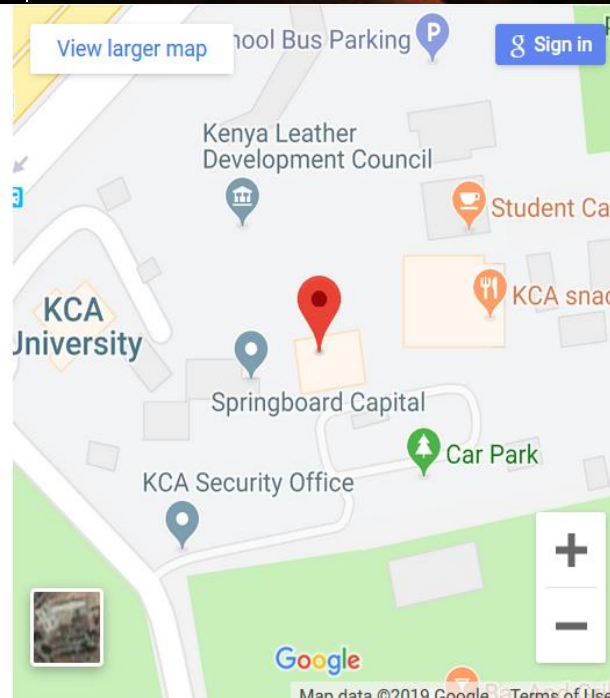
Solutions

Solutions provides the backbone of implementation of the risk management goals ensuring that activities are process dependant rather than on a person

Analytics

Analytics forms the risk / business interpretation of the risk management vision leveraging the technological platform and is result oriented

Contact



Location & Contacts

 CPA CENTER, BLOCK A
THIKA ROAD
P.O Box 79084 00400 Nairobi,
Kenya

 +254-20-2632180

 info@irmke.org



Outline

1

2

3

4

5

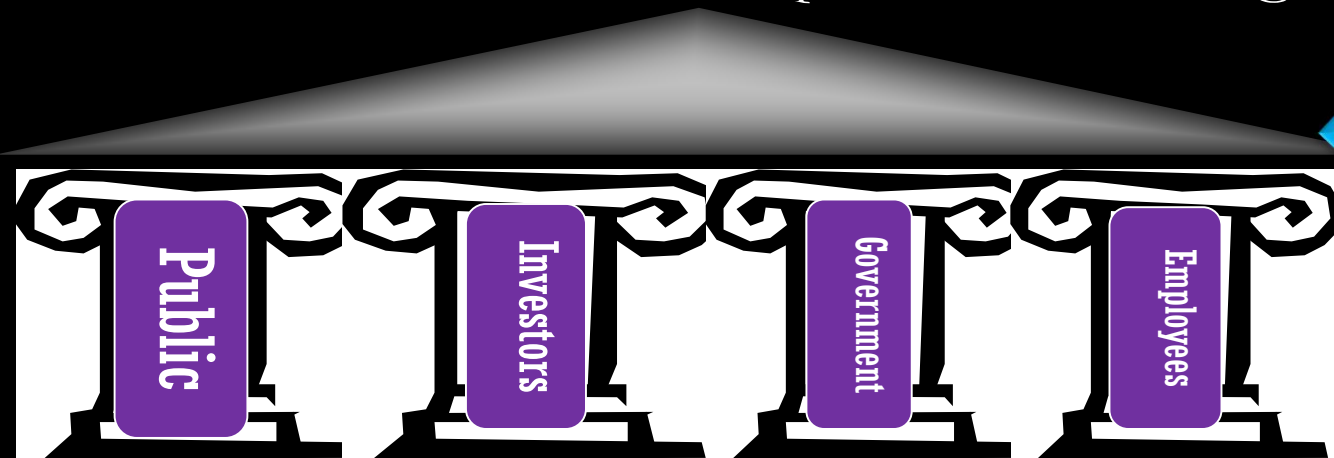


**Risk = Anything that impedes
from achieving corporate objectives**

ERM DEFINED

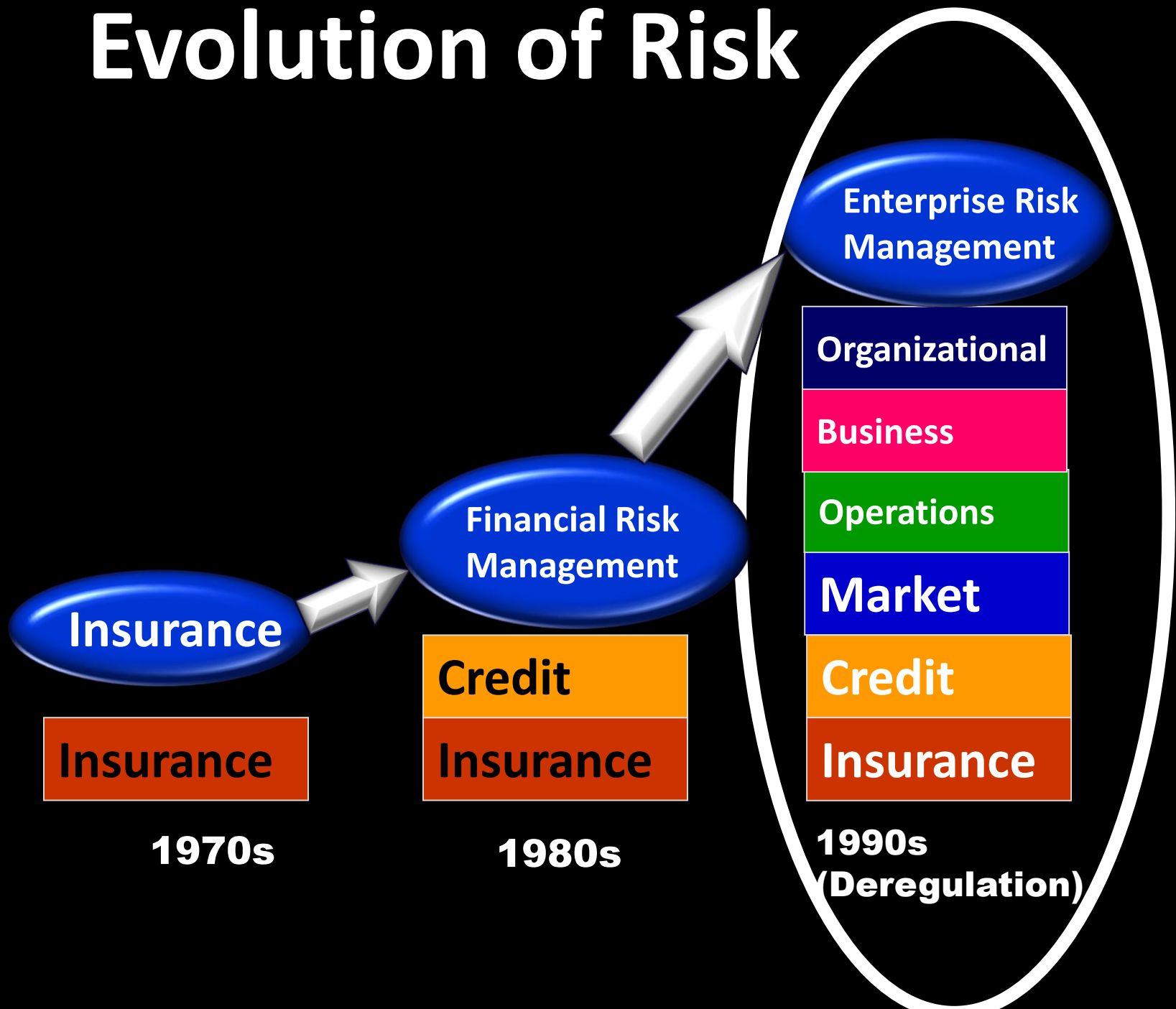
“... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

Source: COSO Enterprise Risk Management

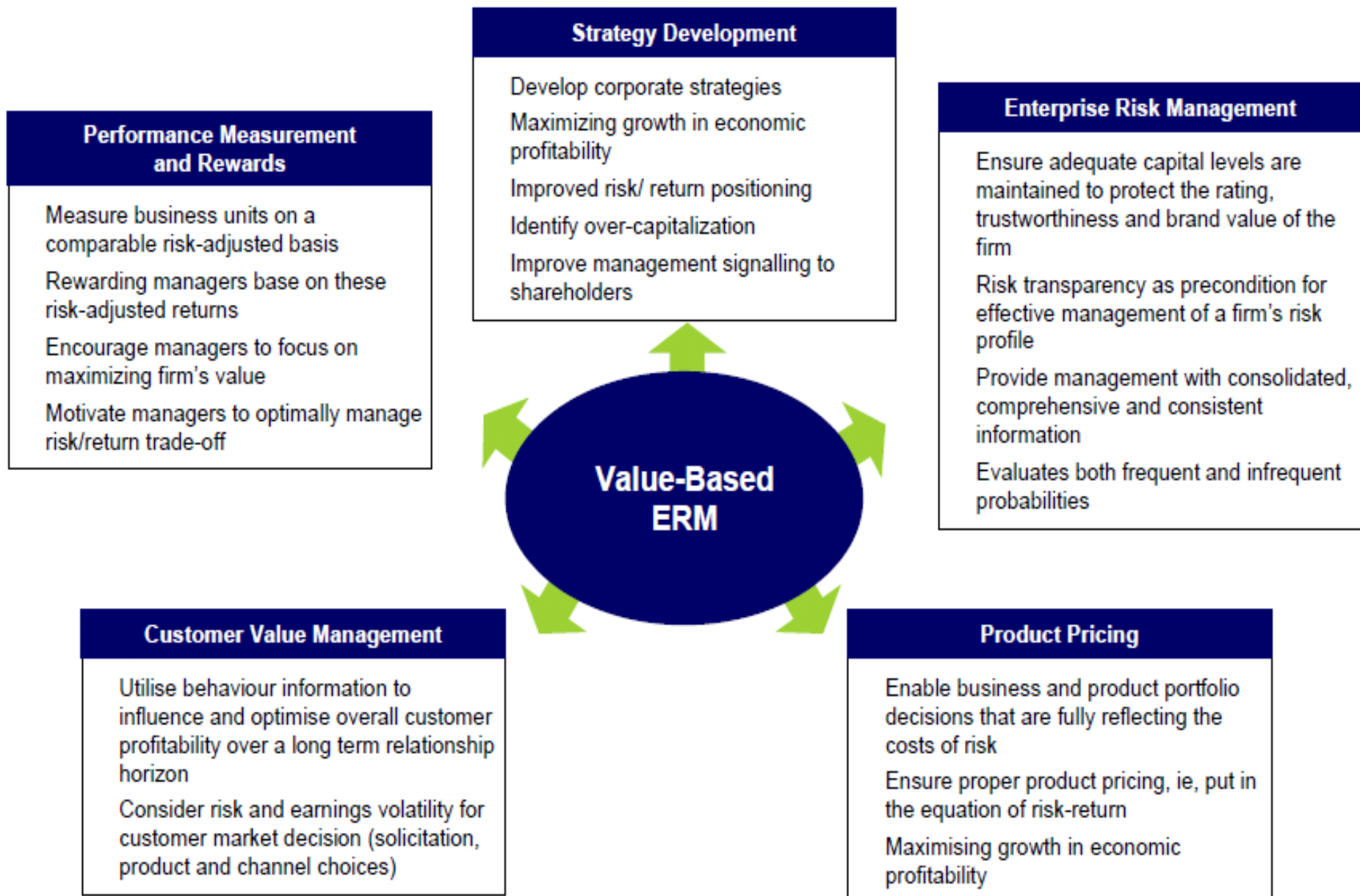


What are your
pillars

Evolution of Risk



Linking strategy to ERM



ERM and Strategy are intertwined

Best Practice Model aims at creating a comprehensive view of the alignment of ERM and business risks @ strategy formulation and execution



E.g.



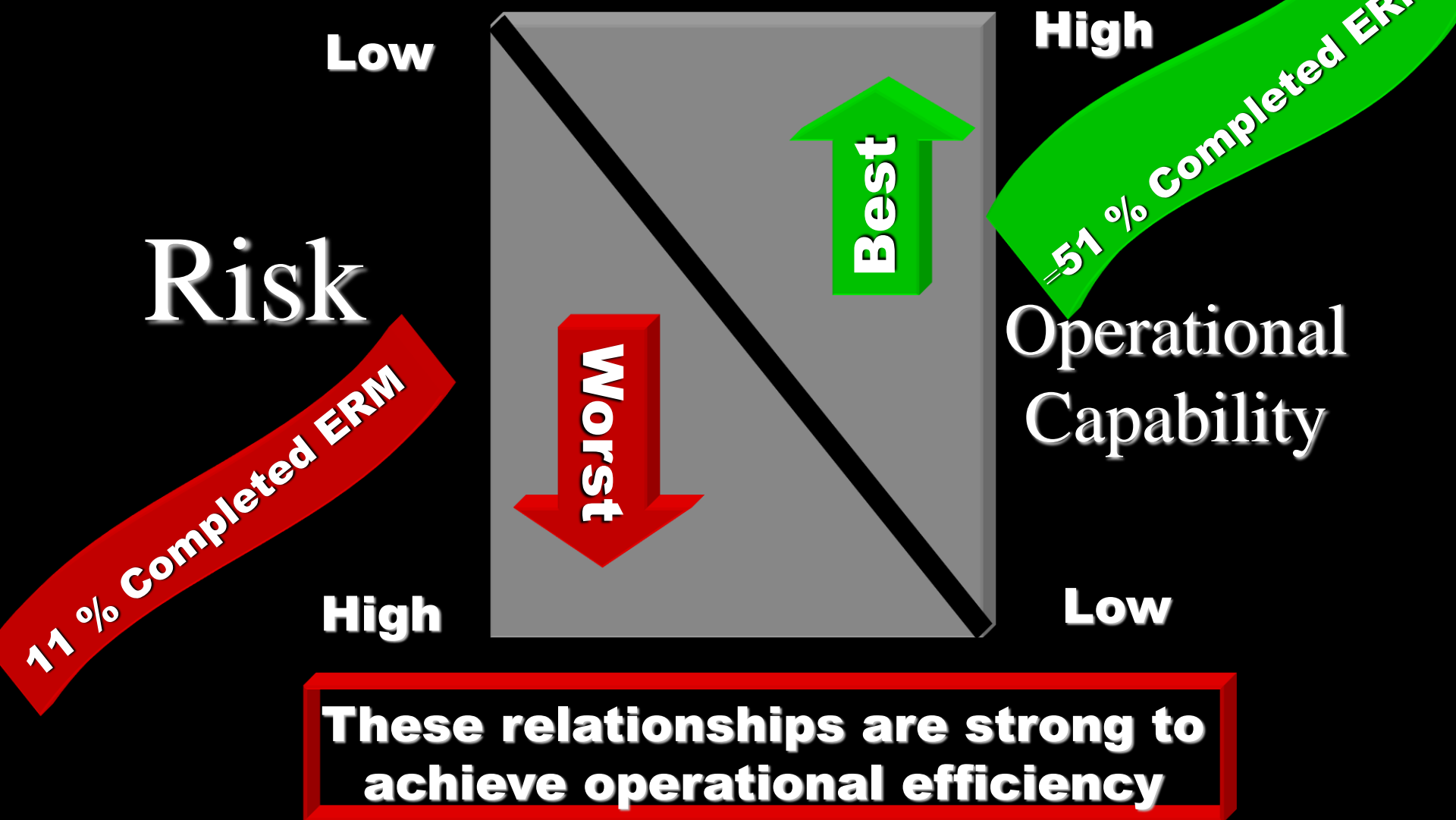
SUSTAINABLE
DEVELOPMENT
GOALS



KENYA
VISION 2030

BIG 4
AGENDA

Risk & Capability: a core relationship







Global Financial crisis



Performance Shortcomings of *immense proportion*

The Great meltdown 2008 Financial crisis



Lessons from the Global Financial Crisis

Who will save the world against the global financial system?

Wake up Mr. Regulator

“Too Big to fail”



APRA



HONG KONG MONETARY AUTHORITY
香港金融管理局



Basel III

“... The general consensus is that the failure to understand the true nature of enterprise-wide risk exposures was one of the core reasons behind collective downfall of organizations.

**Regulations
Regulations
Regulations**

**Change
of Investor
Behavior –
RISK**

**Reduction
In margin
Of error**

**Managing
Risk profile
Now a must
4
survival**

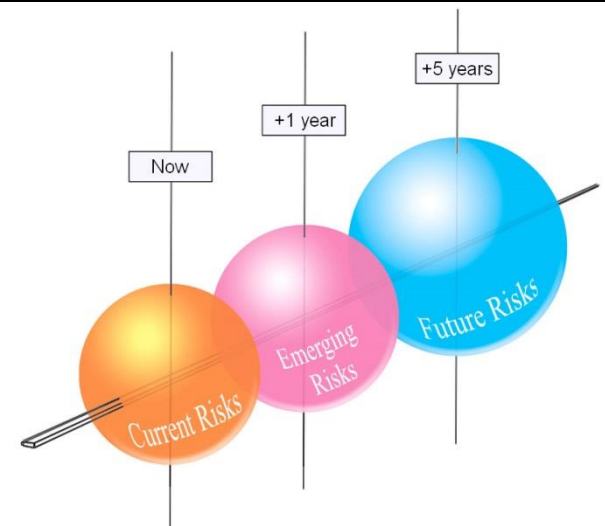
**Decision
Making now
Purely based
On associated
risk**



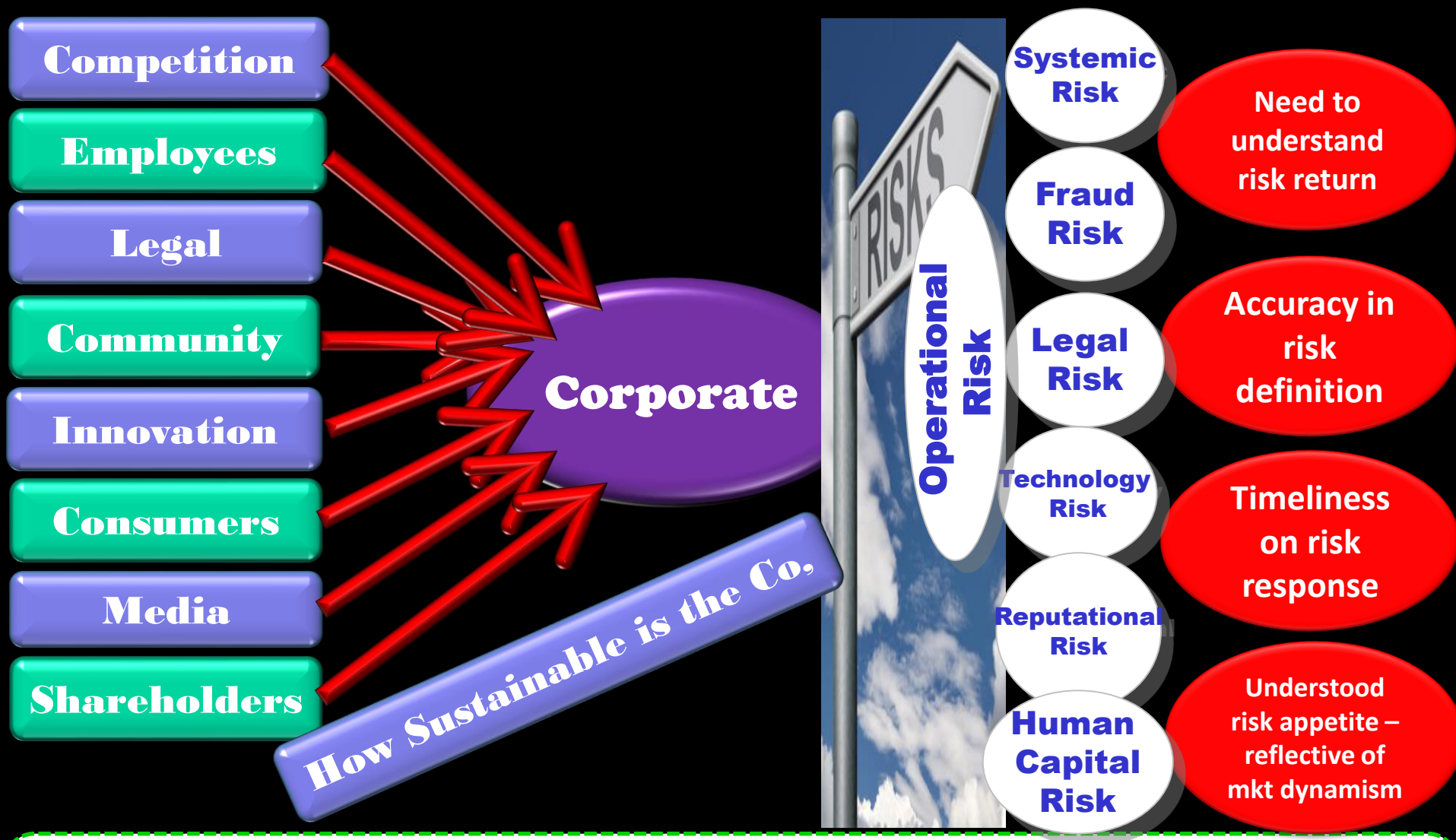
Balancing Risk and Rewards



“... BOD = midpoint of Shareholders & Management. This critical role requires BOD to understand risk appetite & Corporate actions around risk appetite. Being an independent entity, the board has the perspective to spot emerging risks and areas of concern that may be missed by risk managers immersed in the daily functioning of the organization.”



Risk nightmares



"We remain prepared to lose \$6 billion in a single event, if we have been paid appropriately for assuming that risk. We are not willing, though, to take on even very small exposures at prices that don't reflect our evaluation of loss probabilities.....Warren Buffer

Common Tendency for most Boards is to avoid

Risks

**are part of business, but
business doesn't need
to be risky.**

*Visionary Boards
however know “there
can be no rewards
without risk”*

*These Boards are able to distinguish, successfully,
between risks that need to be mitigated and
risks that can be capitalized on or
optimized. They know which RISKS to focus on
for maximum and effect. What gives them this
advantage is, to a large extent, the quality of
risk intelligence/information that
they receive.*



Enterprise Risk Intelligence

Evolution

8 step process to best practice ERI

Reaction

Prevention

1

Notify of events

2

Investigate events

3

Corrective actions to prevent further events from occurring

4

Compliance process to audit/test control frameworks/corrective actions

5

Introduction of risk - risks identified from investigations & auditing of control framework

6

Top Risks – manage significant risks, I,A,C,M = ISO 31000

7

Integration of all risk categories - permeation of the compliance process across all obligations (internal/external)

8

ERI full collaboration & analysis of event, risk & compliance management processes

↑ VALUE ADD FOR ORGANISATIONS

TIME →

- Essential to Institutions

RMSS Copyright © 2011

- Risk Appetite is now prominent in the Board

- Institutions must now consistently speak of their largest risks, & present facts that facilitate dialogue on risk.



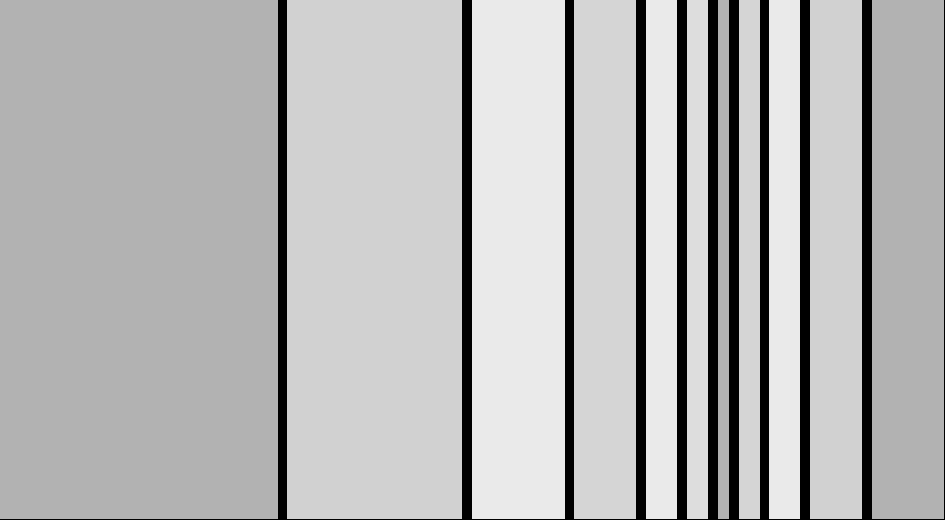
- Boards must now understand deeply their organization risk profiles – this improves decision making and maintains firm competitive edge.



THE ROLE OF THE BOARD IN ERM



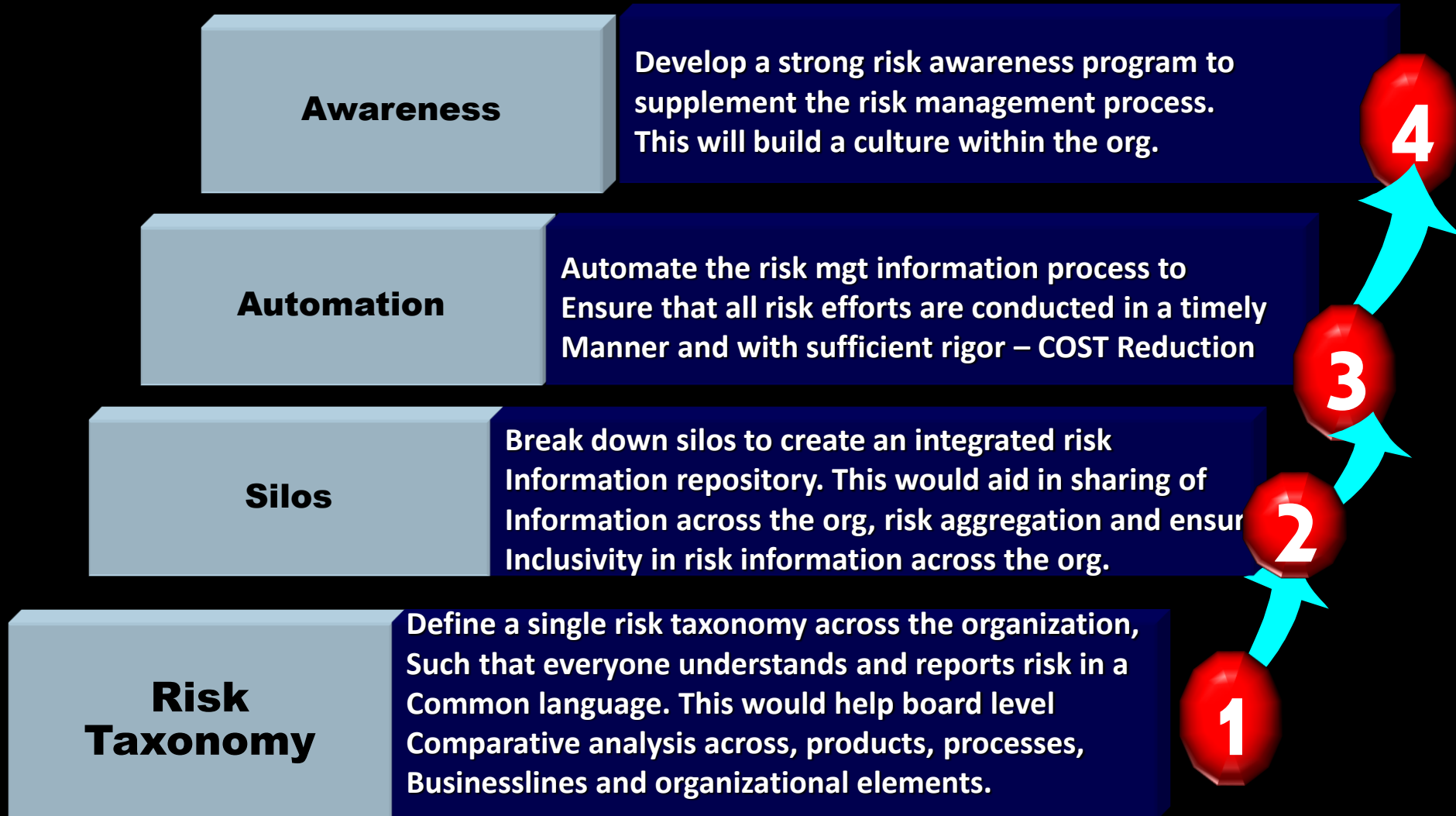
Role of the
Board



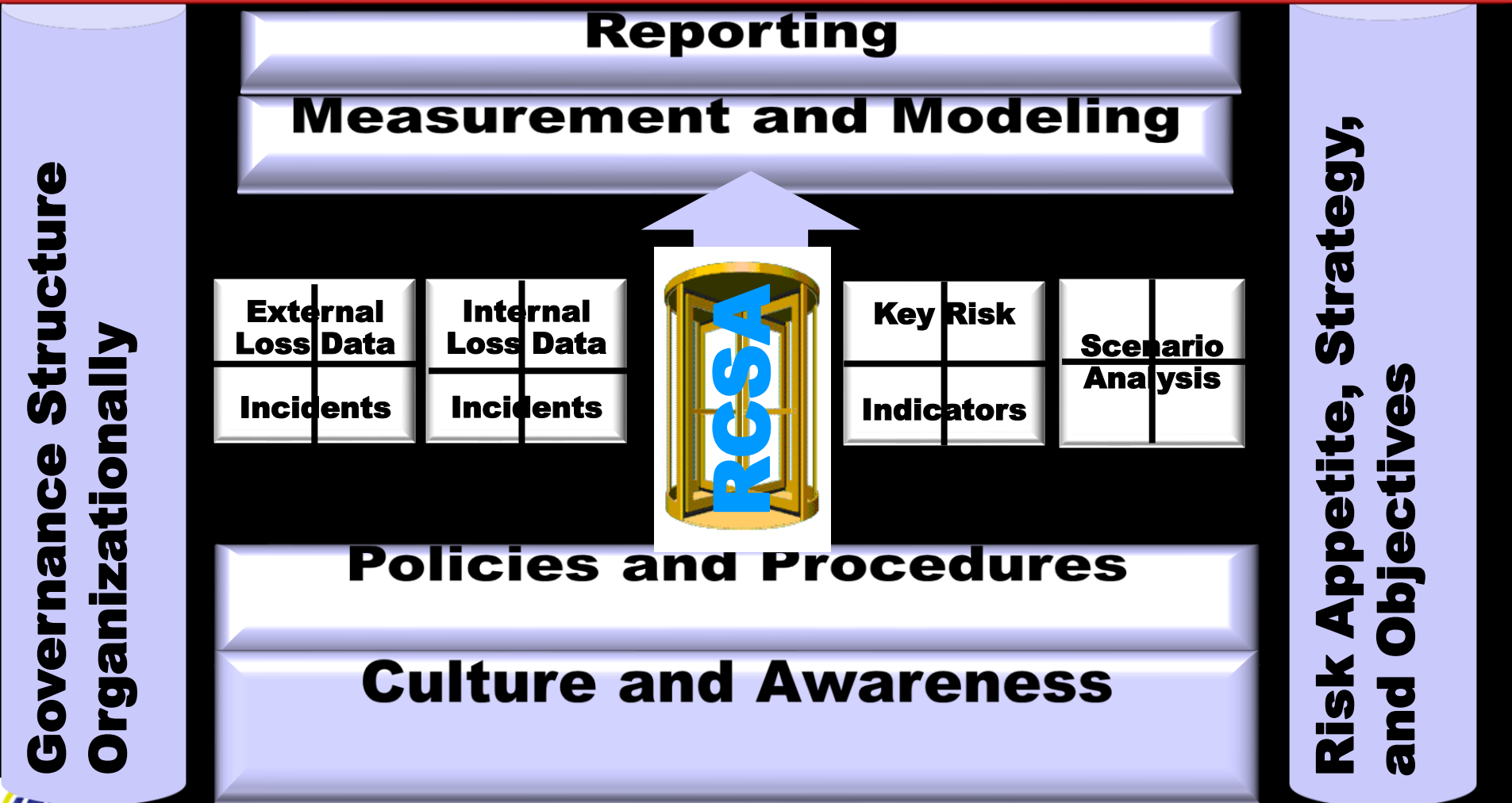
Building a Risk Intelligence Programme

“... Even though the need for risk intelligence in strategic decision making is critical, the actual practice of providing relevant, timely and forward looking risk information requires meticulous planning and seamless execution of an integrated enterprise-wide risk management program”

To develop a risk program that is efficient and effective in providing information to the board – consider the following steps



Framework Structure





- **Go short of nothing but *International best practice* -**

BS 31100:2008



31000

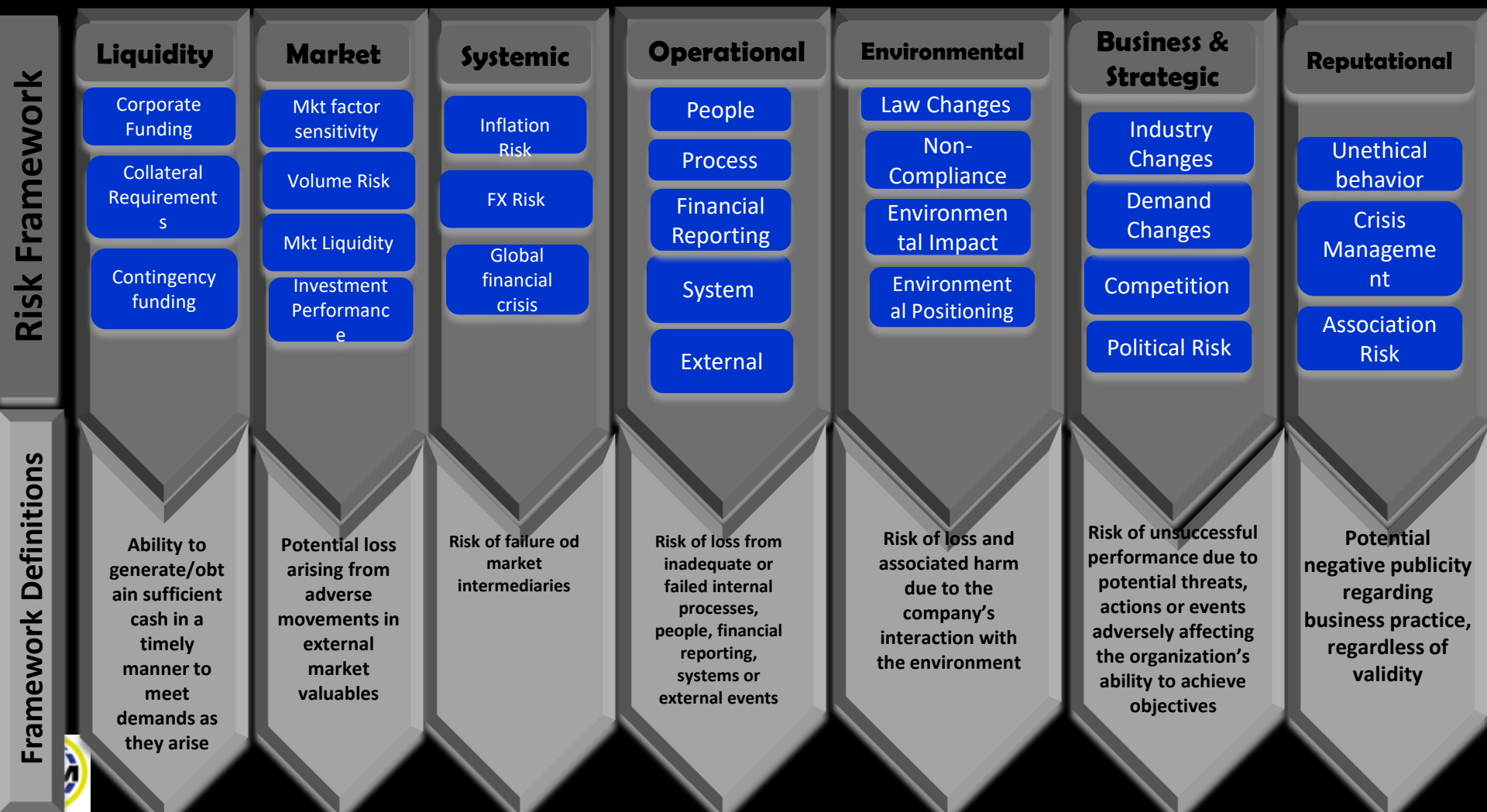
International
Organization for
Standardization

- **It must be a consultative document**
- **Win the mind and souls of people**
- **Senior Mgt must approve it and adopt the implementation road map**
- **Internal Audit must give concurrence about resiliency of the framework**
- **BOD must approve**

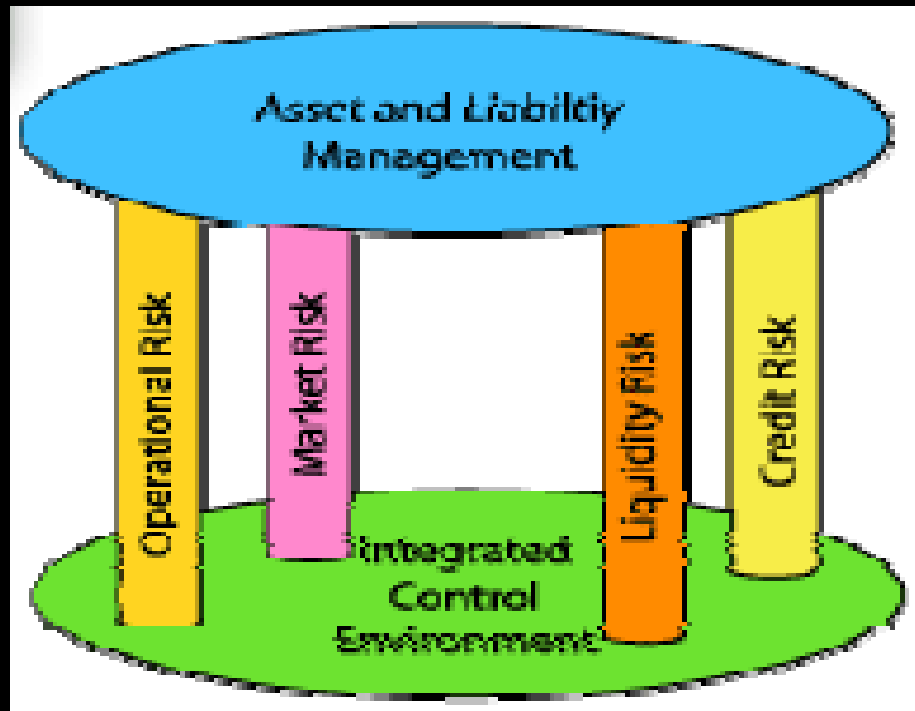
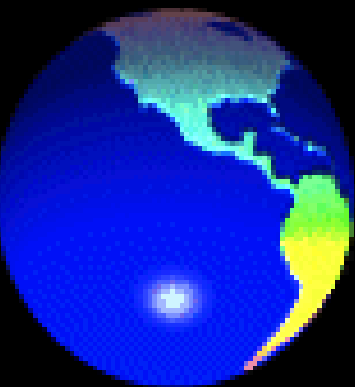


Your Risk Universe

A company focused on ERM constantly assesses risk factors to ensure they reflect business realities – both quantifiable or non-quantifiable risks or Financial & Non-financial risks



Why Risk Universe Description is Key



Risk Taxonomy

Clarity

Consistency

Focus

Relevancy

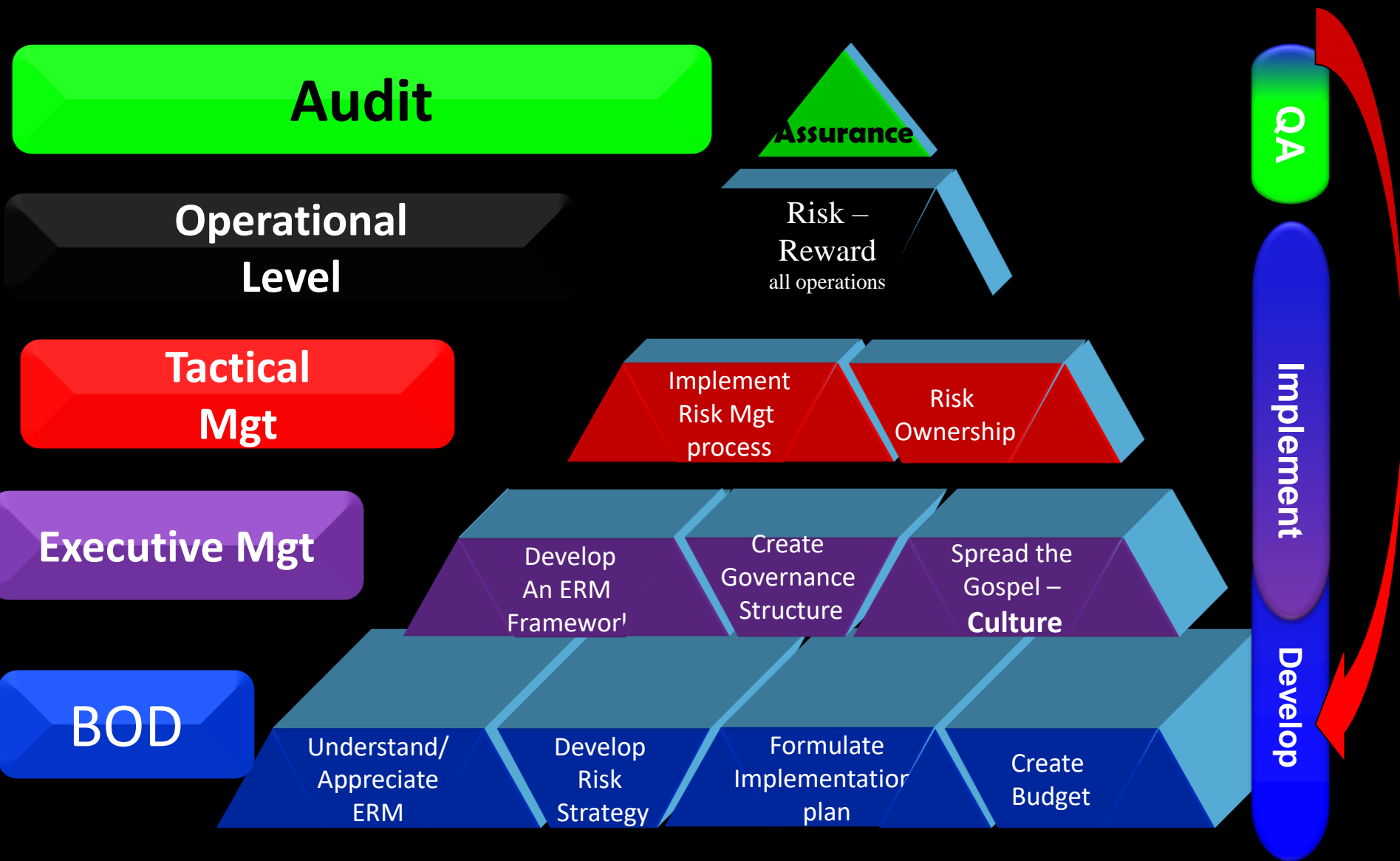
**Resonates with
Corporate strategy**

Training

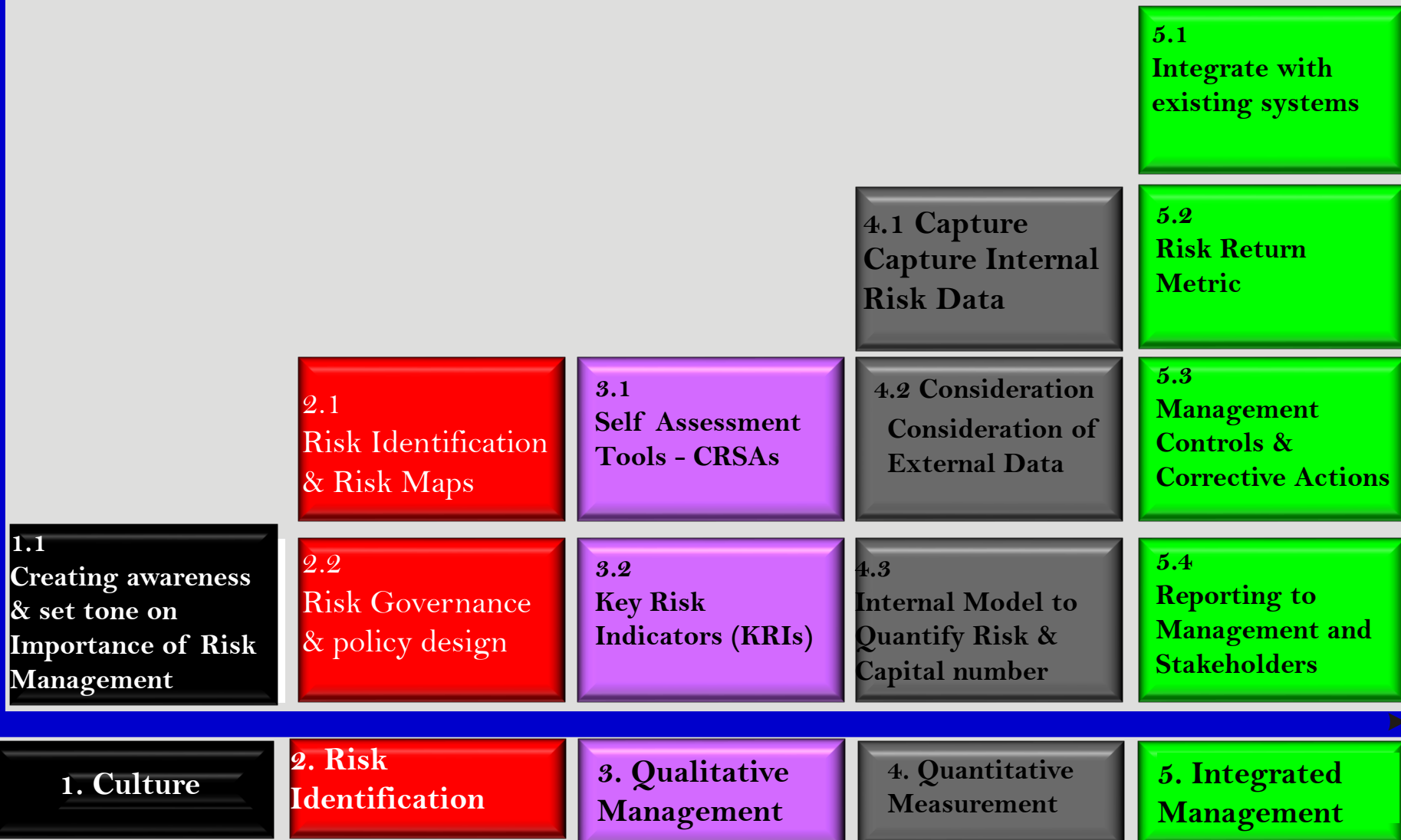
Culture

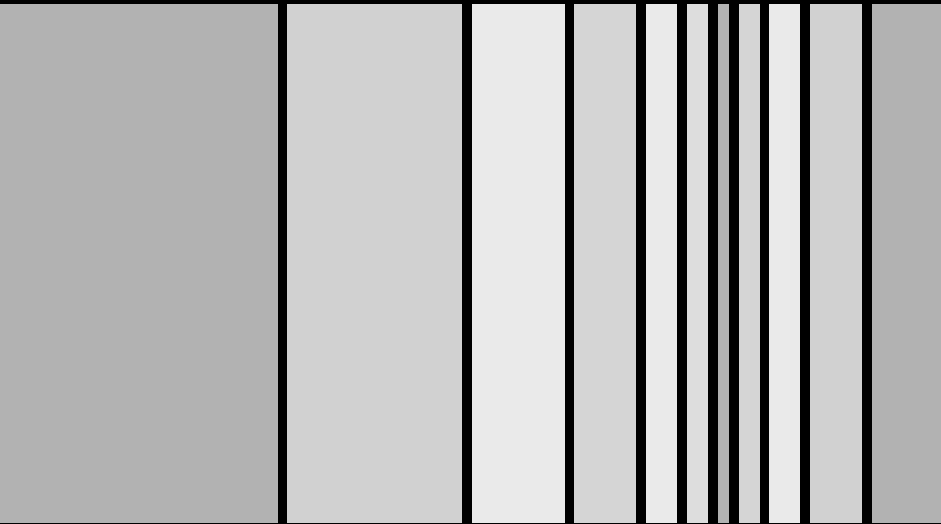
Automation

Implementation Building Blocks

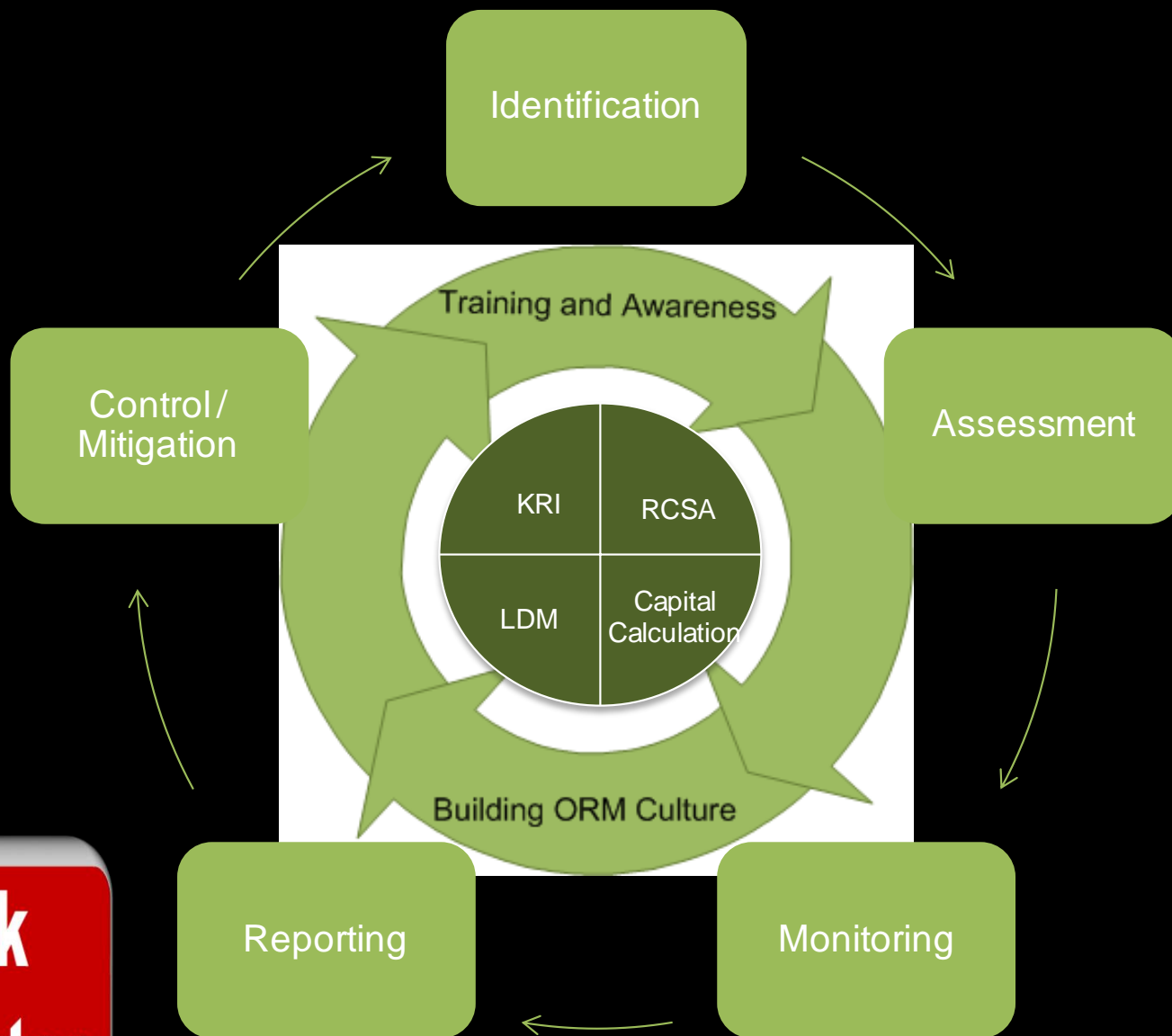


Are we succeeding? – Measuring success



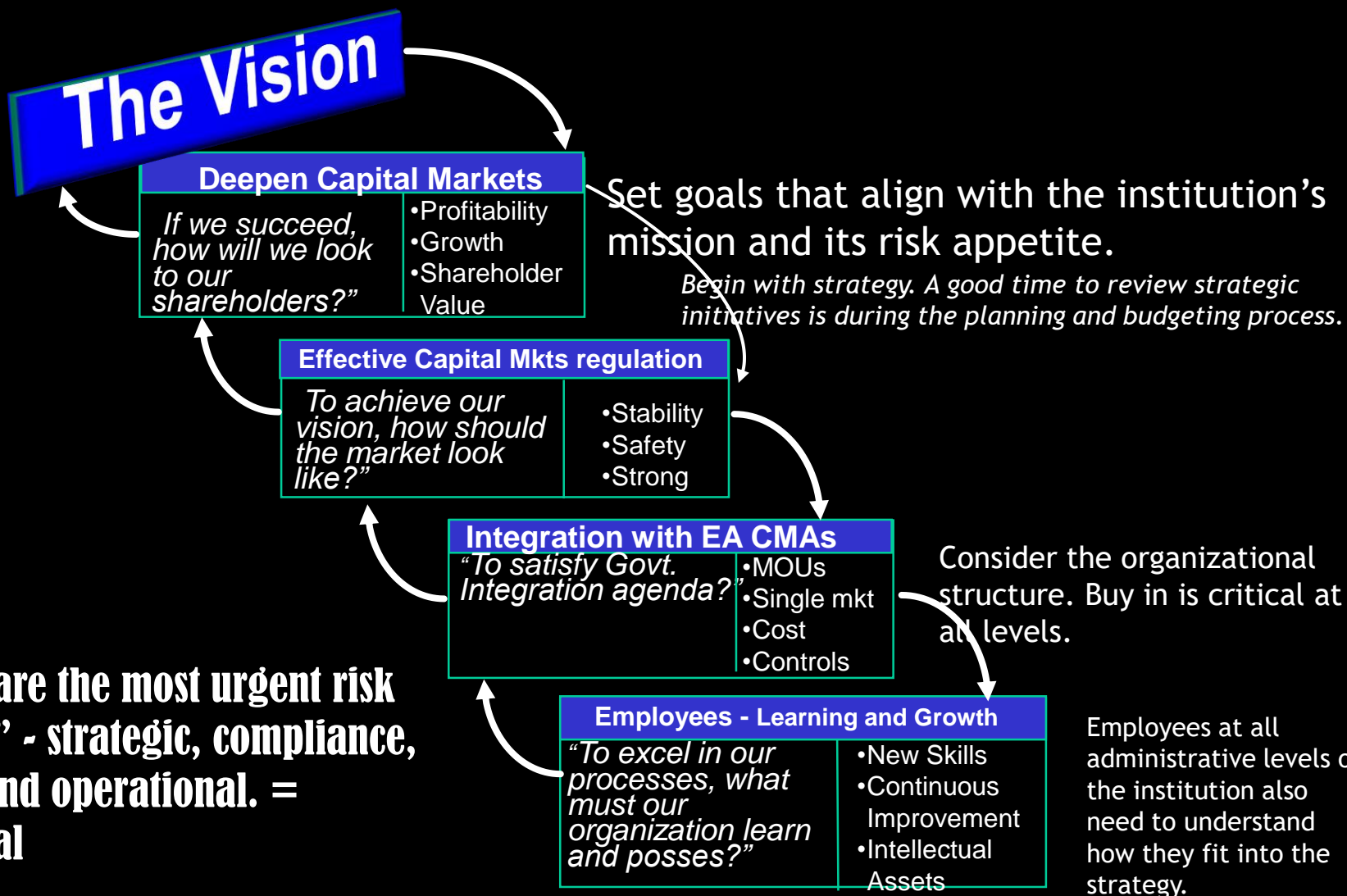


Formal risk management processes



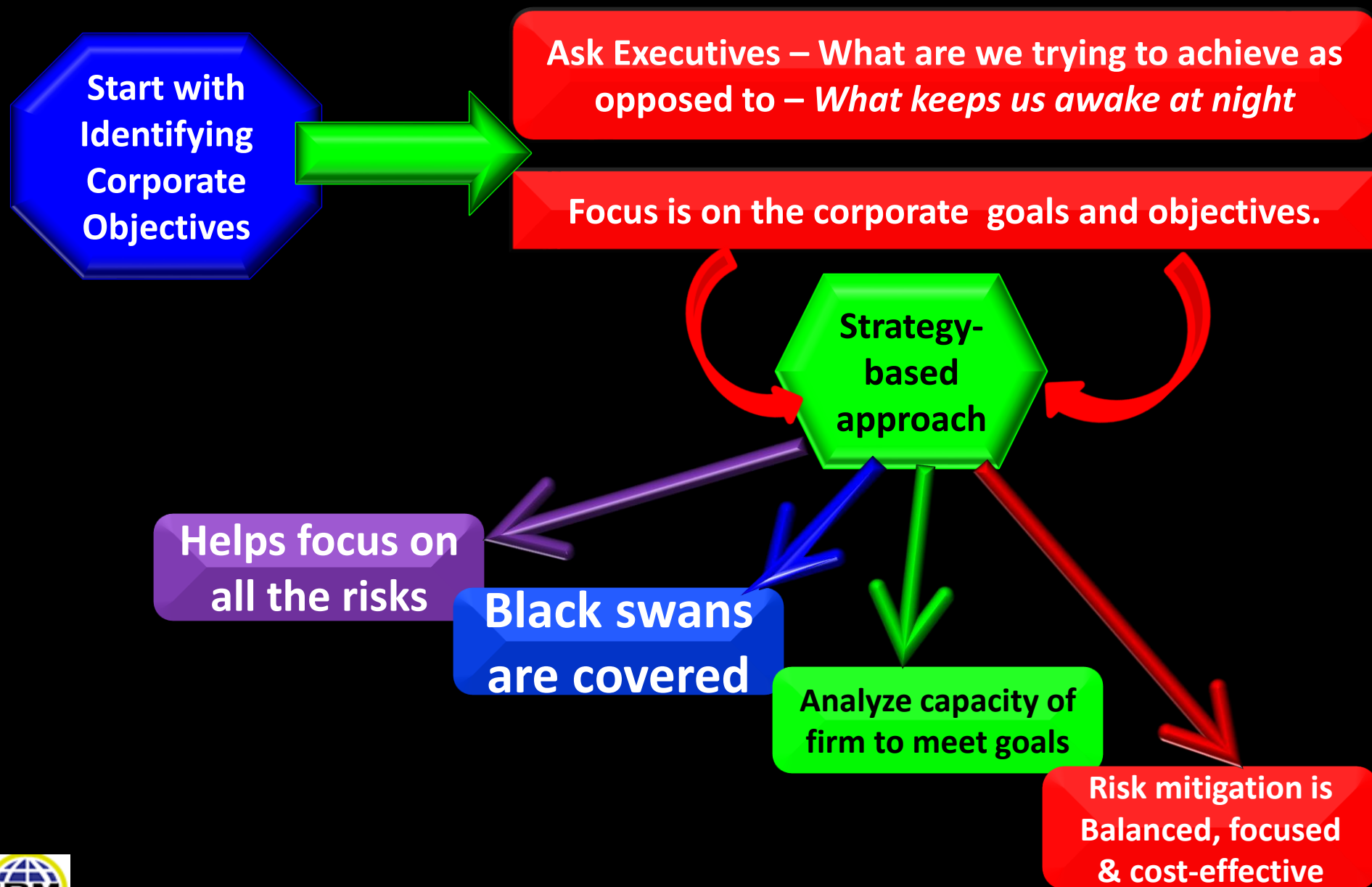
Risk Event Description	Inherent Impact	Inherent Likelihood	Description of Standard Controls	Control Rating	Residual Impact	Residual Likelihood	Action plan	Responsible Person	Due Date
------------------------	-----------------	---------------------	----------------------------------	----------------	-----------------	---------------------	-------------	--------------------	----------

Objective Setting



"Ask What are the most urgent risk objectives?" - strategic, compliance, financial, and operational. = Reputational

Risks Identification Process - Risk *in* Strategy



Risk Identification



Egypt/Tunisia/Bahrain/Libya



Workshops

• Business & Risk expert

• Collaborative

• Produce a list of risks – focus on key

• Non-victimization

• All responses are correct

Events Losses & Incidents

• Understand business “as is”

• performance shocks

• Look at Audit report

• Media publicity, shareholder/investor expectation to stimulate a “fact-based discussion

SWOT Analysis

Internal Strengths Weaknesses

External Opportunities Threats

Use analytical tool PESTEL

“Managers invent and then consider, in depth, several varied stories of equally plausible futures. The stories are carefully researched, full of relevant detail, oriented toward real-life decisions, and designed (one hopes) to bring forward surprises and unexpected leaps of understanding.”

Risk Assessment

Risk Assessments

Inherent risk would be identified on the basis of the likelihood and impact of risk event – No Controls considered

The control effectiveness would be assessed in terms of **design effectiveness** and operating effectiveness

Residual risk would be identified on the basis of the likelihood and impact of risk event after considering overall control effectiveness

Scale

Inherent Risks Assessment

5 Critical - Inability to achieve business objectives

4 High - Constrained ability to achieve business objectives

3 Moderate - Moderate impact on achievement of business objectives

2 Low - Limited impact on achievement of business objectives

1 Minor - Relatively insignificant impact on the achievement of business objectives

SCALE	Description	IMPACT (KES)
5	Critical	<ul style="list-style-type: none"> Inability to achieve business objectives, e.g.: <ul style="list-style-type: none"> Loss of significant business Massive reduction in company reputation with stakeholders Excessive costs dramatically impacting long term profitability and viability Inability to attract new business Significant IT disruptions leading to significant delays in business operations Estimate total cost is over KES 20 Mn
4	High	<ul style="list-style-type: none"> Constrained ability to achieve business objectives, e.g.: <ul style="list-style-type: none"> Significant but recoverable reduction in company credibility and/or reputation Significant reduction in service and business capability incurring excessive costs that impact current earnings and profitability Loss or misappropriation of significant assets Loss of significant number of key personnel Estimate total cost is > KES 5 Mn and < KES 20 Mn
3	Moderate	<ul style="list-style-type: none"> Moderate impact on achievement of business objectives, e.g.: <ul style="list-style-type: none"> Loss of high value customers or alliances Temporary loss of service or business capability Temporary, but recoverable reduction in credibility/reputation Short term increase in costs or loss of revenue Estimate total cost is > KES 1 Mn and < KES 5 Mn
2	Low	<ul style="list-style-type: none"> Limited impact on achievement of business objectives e.g.: <ul style="list-style-type: none"> Temporary delay in reaching objectives Short term or limited reputation damage Limited impact on customer retention Limited increase in costs Minimal impact to revenue or earnings Estimate total cost is > KES 500,000 and < KES 1 Mn
1	Minor	<ul style="list-style-type: none"> Relatively insignificant impact on the achievement of business objectives. Estimated total cost < KES 500,000

SCALE	RATING	PROBABILITY
5	Expected	Above 60%
4	Highly Likely	40 to 60 %
3	Likely	20 to 40 %
2	Not Likely	10 to 20 %
1	Remote	0 to 10 %

Residual risks
These consider risk net of controls on both likelihood and impact axis

Controls Evaluation

Risk Event Description	Inherent Impact	Inherent Likelihood	Description of Standard Controls	Control Rating	Residual Impact	Residual Likelihood
			<div> <div>Checker</div> <div>Maker</div> </div>	<div> <div>Rating</div> <div>Efficient</div> <div>Acceptable</div> <div>To Improve</div> <div>Defective</div> </div>		

Controls Effectiveness Scoring Criteria

- Efficient
- Acceptable
- To Improve
- Defective

Each Control or a set of controls effectiveness is /are rated on a four point scale of

Efficient - The internal control system is efficient and adequate

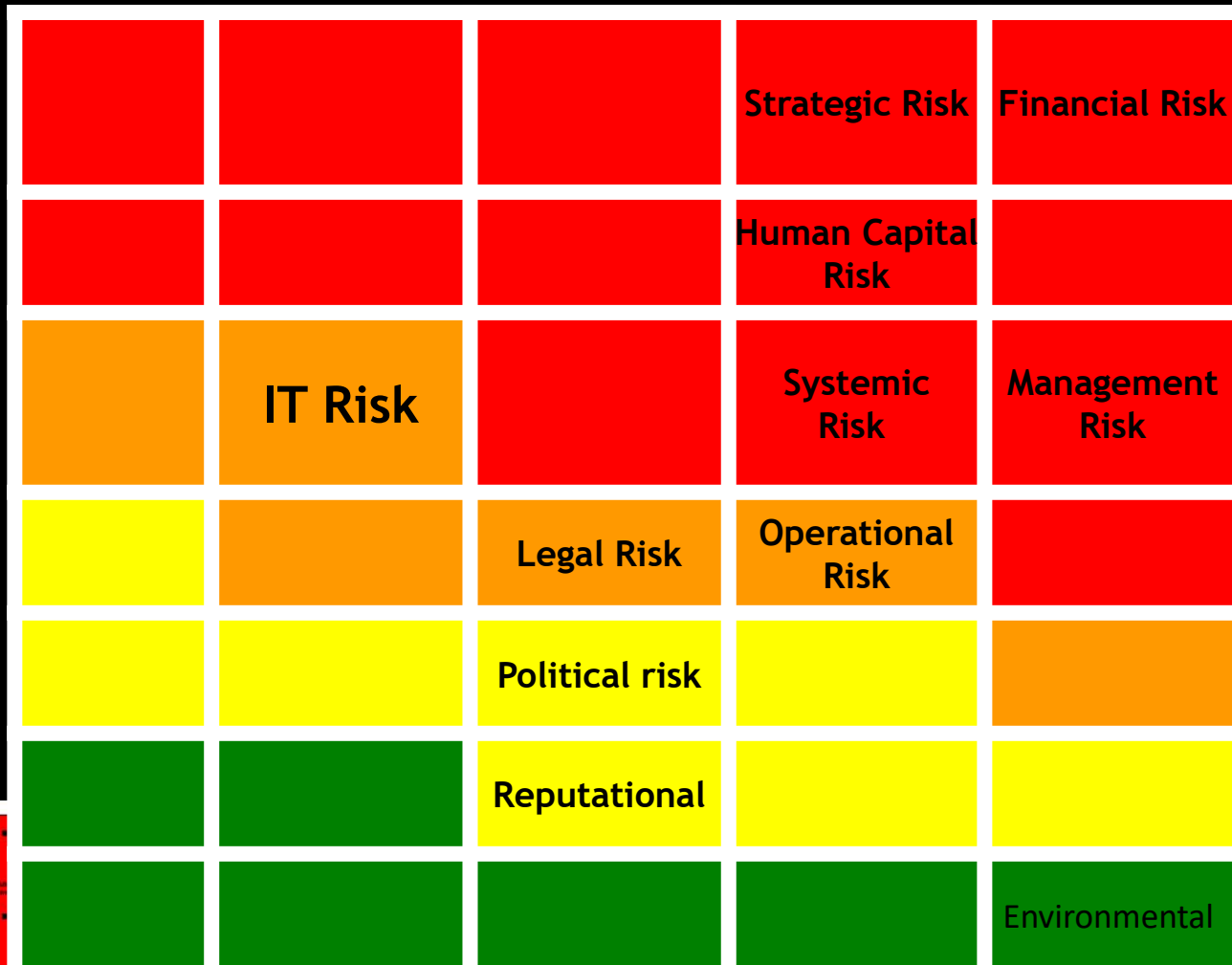
Acceptable - A few corrections should make the internal control system satisfactory

To Improve - The internal control system has to be enhanced and the process monitored more closely

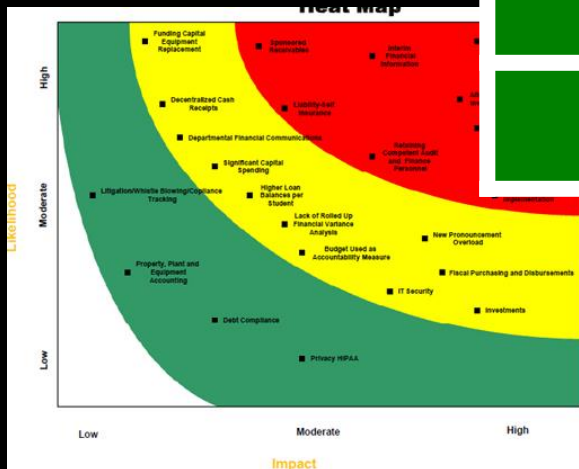
Poor - The internal control system of the process has to be reorganized

Organizational Risk Heatmap - Profile

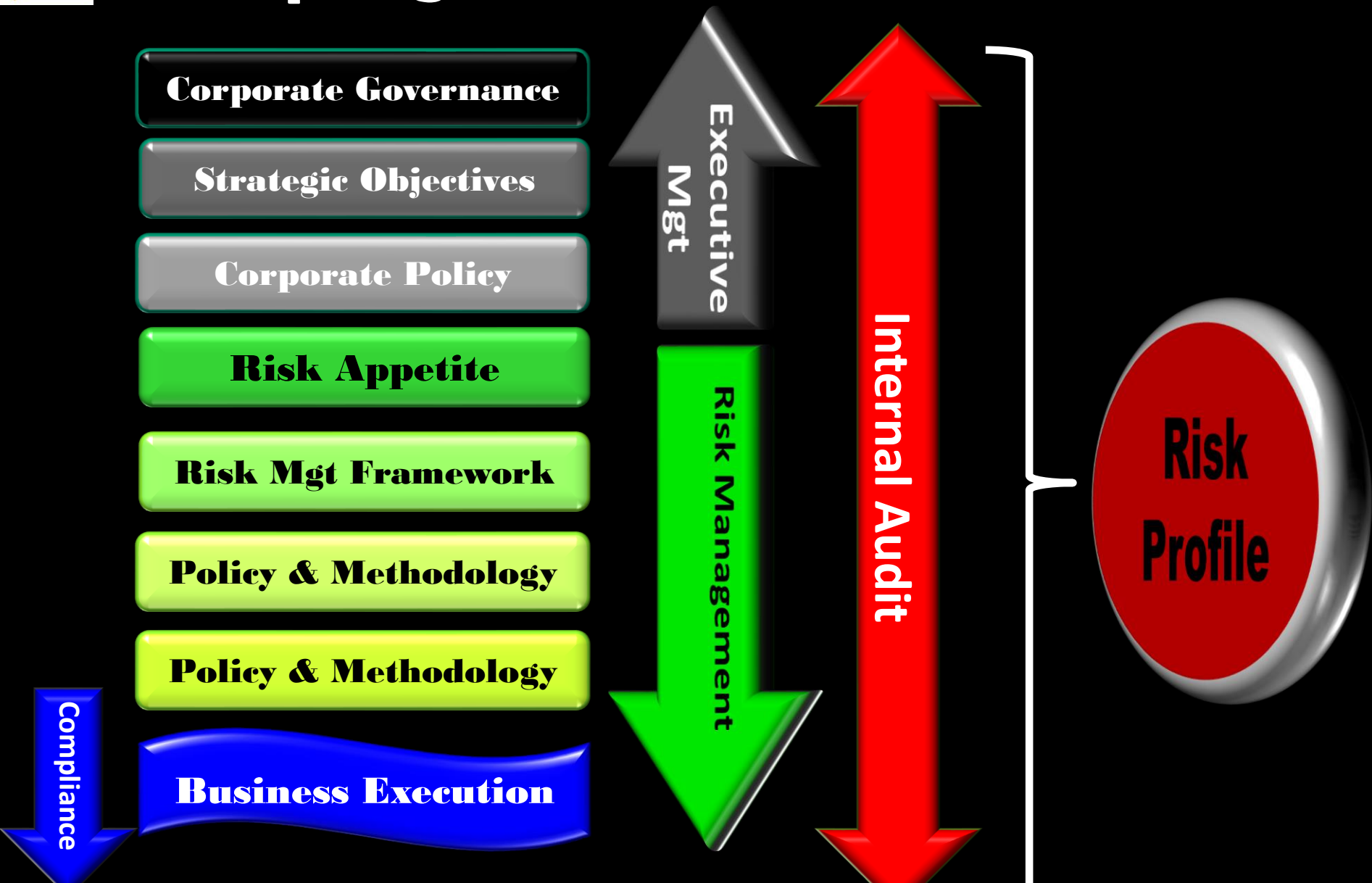
Impact



Probability



Adopting the various blocks

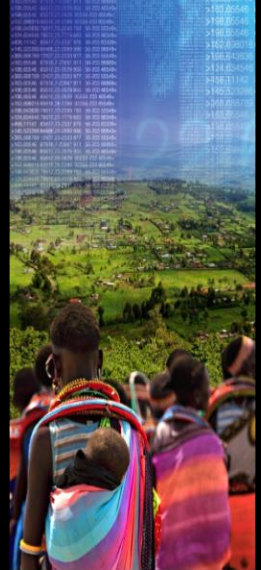


Your Corporate Governance structure sets the scene for all risk activities resulting into the organizational risk profile



**Desired
Risk
Profile**

**Actual
Risk
Profile**



**Perceived
Risk
Profile**



Spend time to think what the Risk profile means

Impact of Risk profile

Risk Universe



Liquidity

Credit

Market

Operational

Environmental

Business & Strategic

Reputational

PROFIT/LOSS STATEMENT

INCOME	EXPENSE
MARKET RISK	OPERATIONAL RISK
CREDIT RISK	
LIQUIDITY RISK	

Which Risk
impact more on
my P&L

What are the
priorities

Profit

Do I have the
right
infrastructure

BALANCE SHEET

ASSET	LIABILITIES
STRATEGIC RISK	LIQUIDITY RISK
ASSET/LIABILITY MANAGEMENT	

Risk Response

Action plan

Responsible
Person

Due
Date



RISK/BREAKDOWN/BREACH RANKING

<div style="display: flex; align-items: center;"> <div style="width: 10px; height: 10px; border: 1px solid black; margin-right: 5px;"></div> <div style="writing-mode: vertical-rl; transform: rotate(180deg);">Impact</div> </div>	Very High	H	VH	VH	VH
	High	H	VH	VH	VH
	Moderate	M	H	VH	VH
	Low	L	M	H	H
	Insignificant	L	L	M	M
		Unlikely	Possible	Likely	Material ized
		<div style="display: flex; align-items: center;"> <div style="width: 10px; height: 10px; border: 1px solid black; margin-right: 5px;"></div> <div style="writing-mode: vertical-rl; transform: rotate(180deg);">Likelihood</div> </div>			

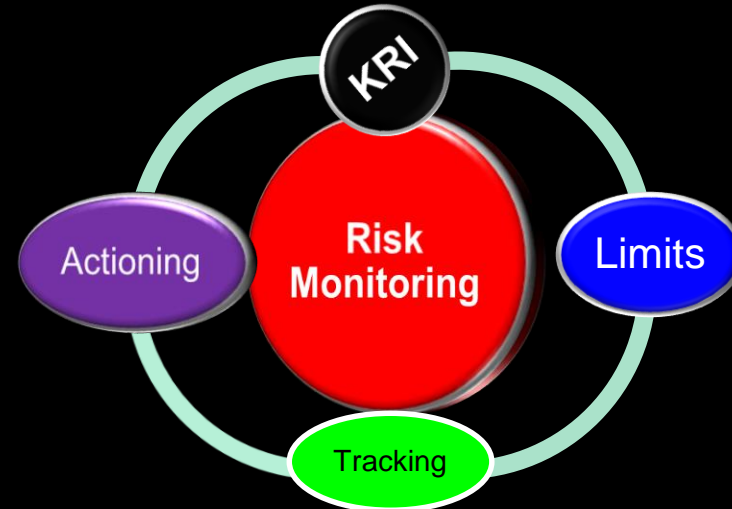
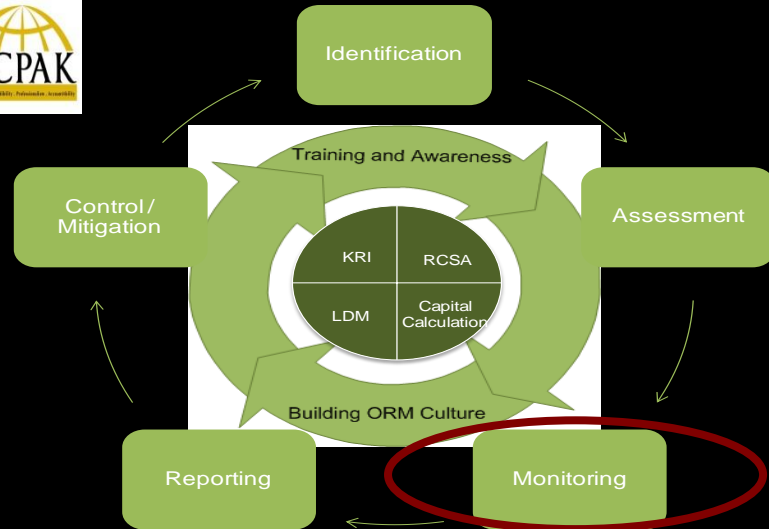
Tolerate

Treat

Transfer

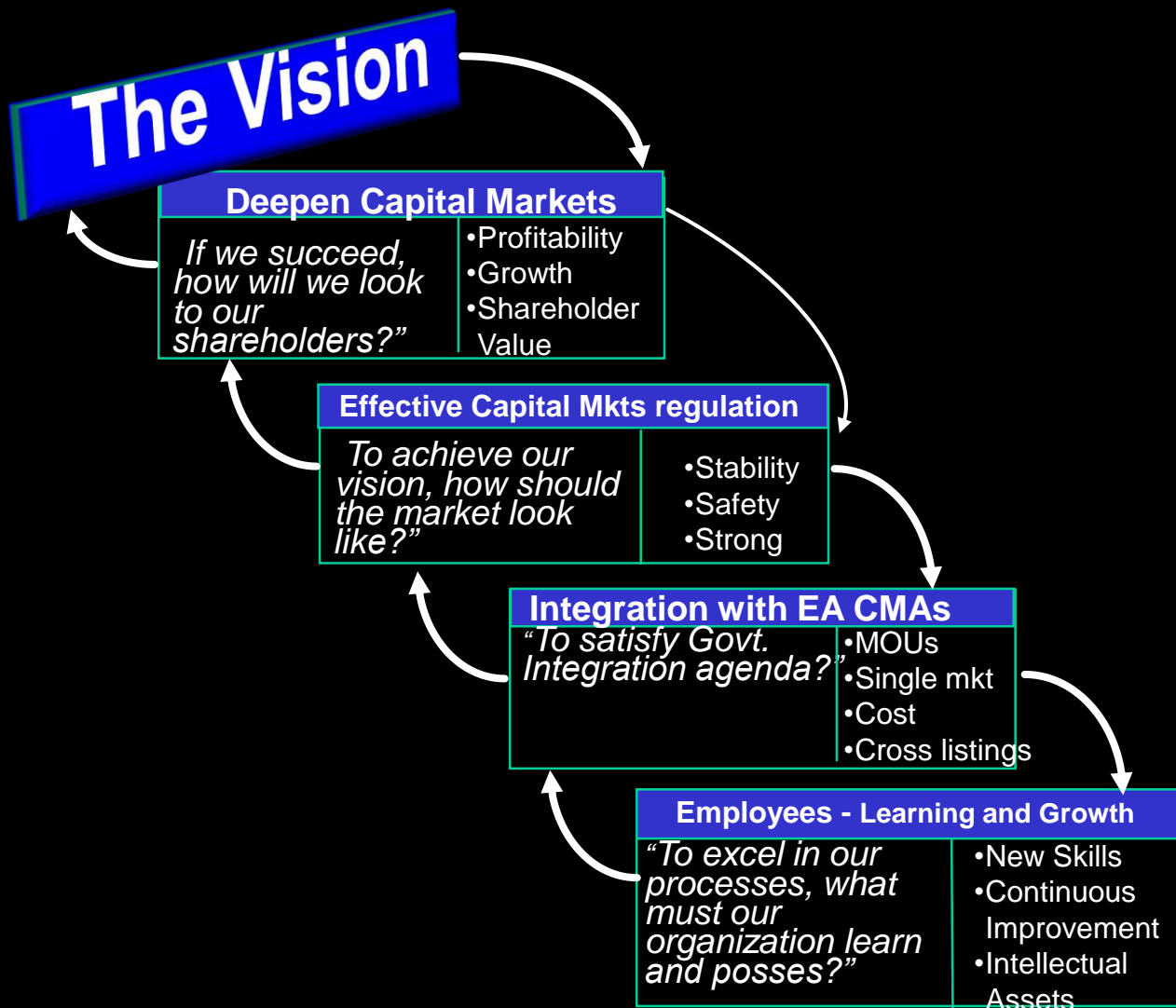
Terminate

**The 4 T Response
plan**



Risk Monitoring

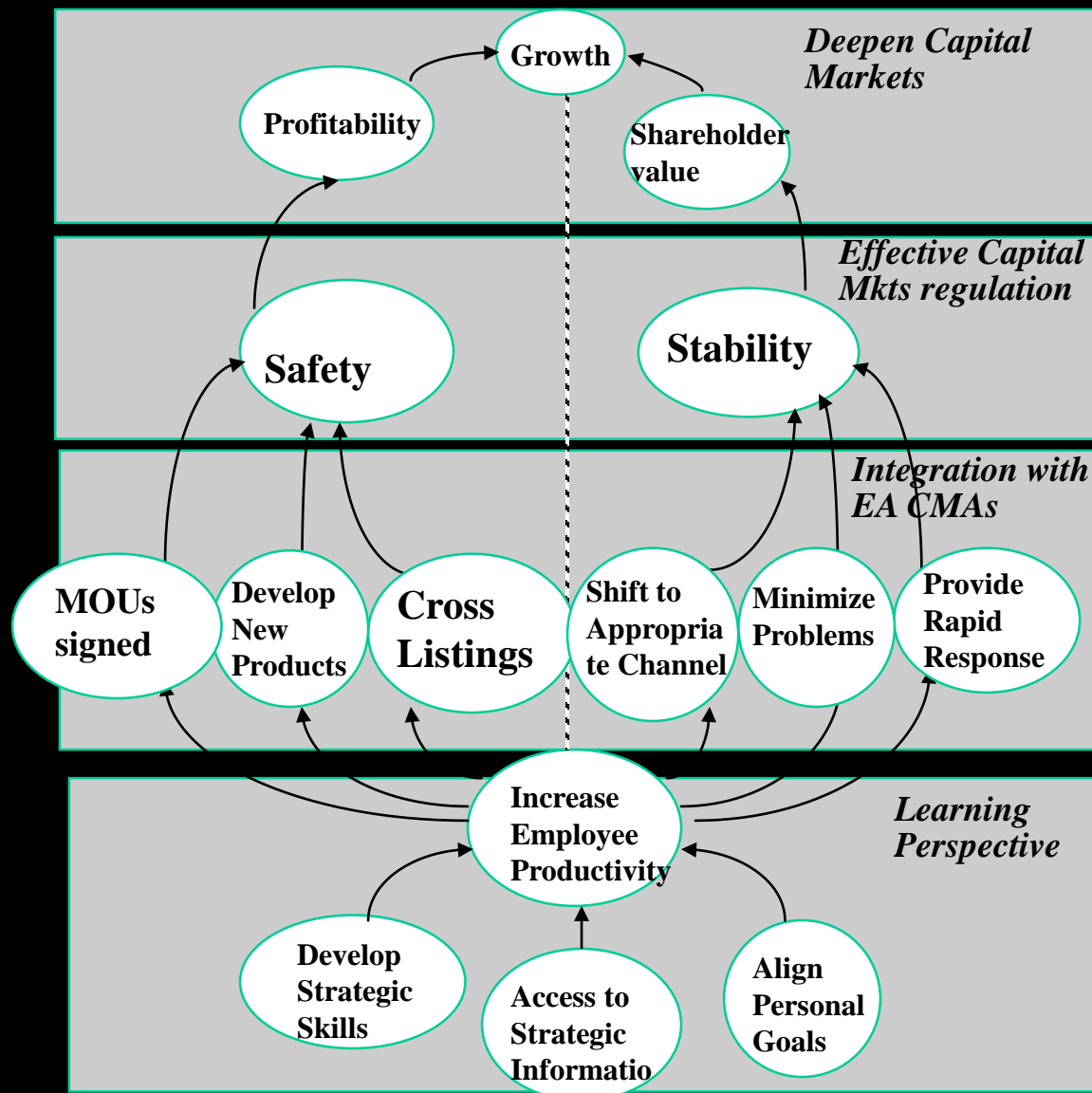
Objective Setting



Market Stability

The Productivity Strategy

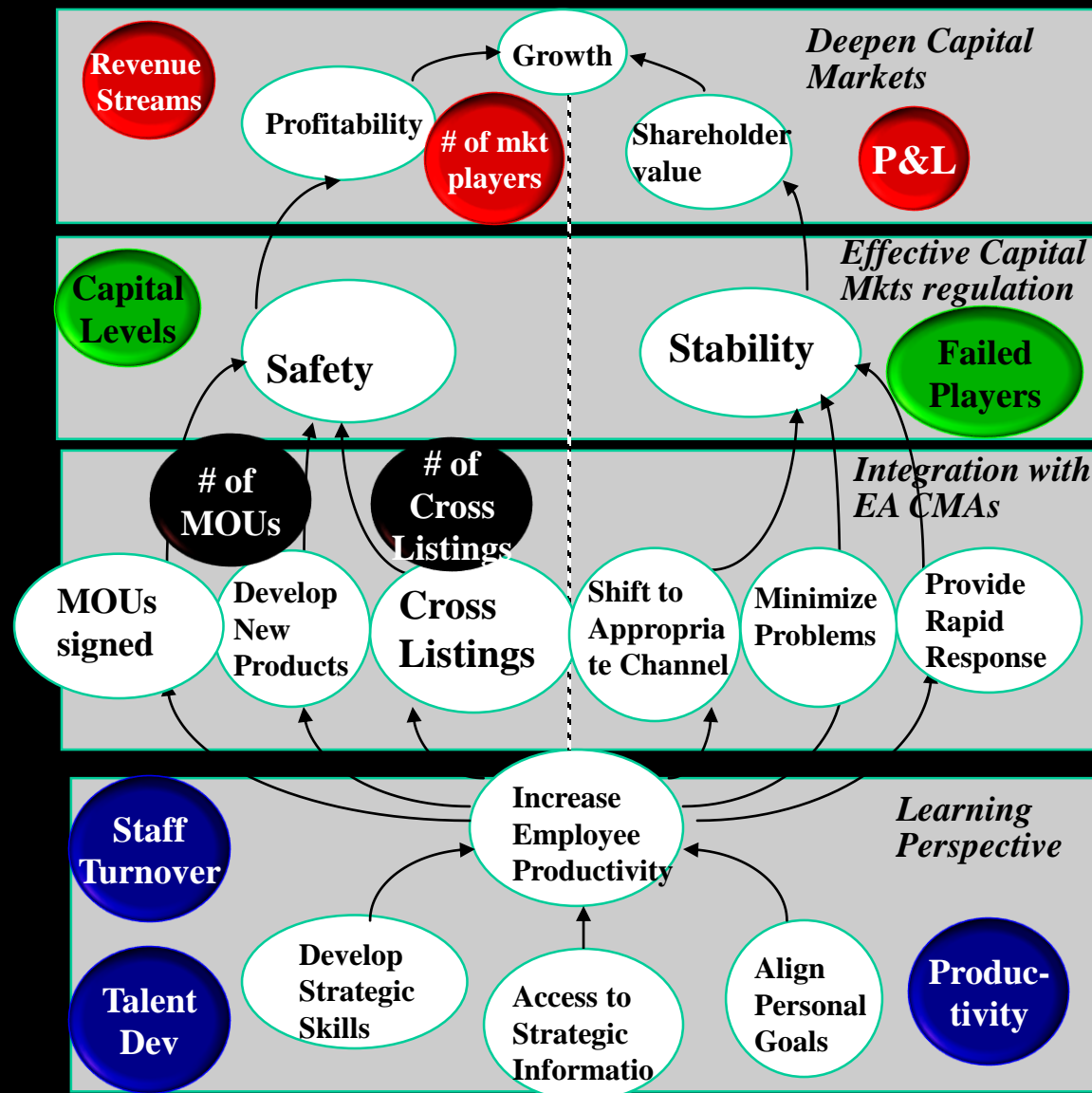
“Improve operating performance”



*Deepening
Financial
Markets”*

Market Stability

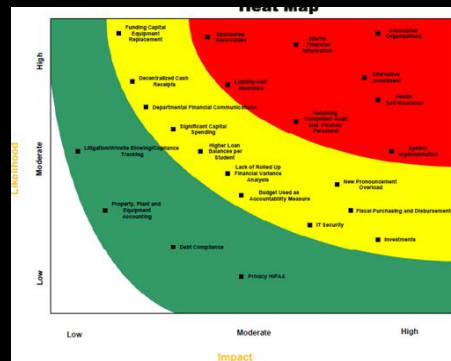
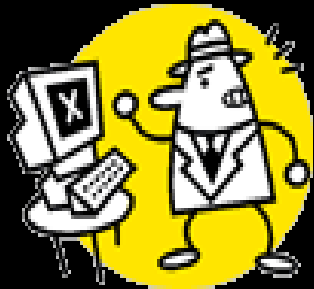
The Productivity Strategy



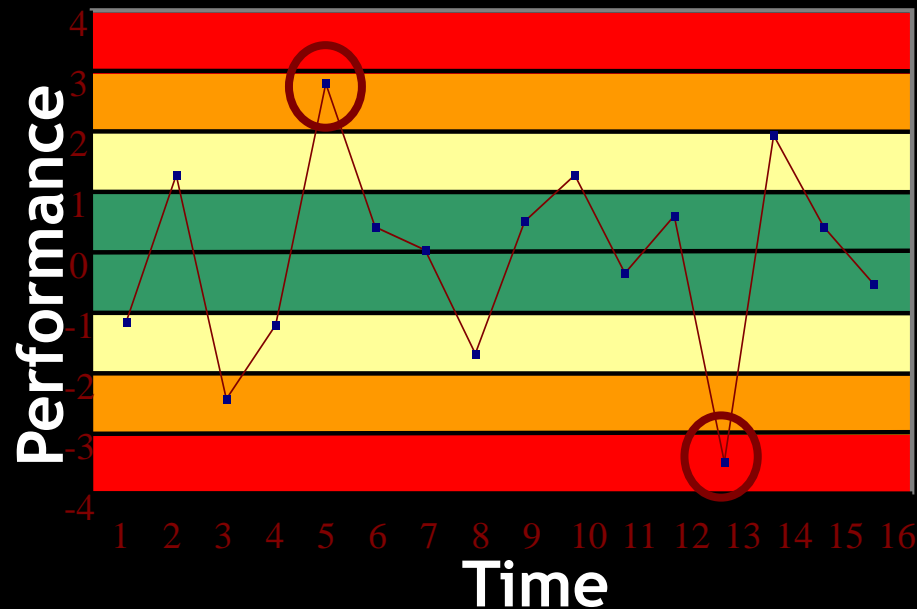
*“Improve
operating
efficiency”*

KRI – Risk Monitoring

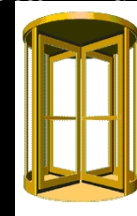
Computer Breakdowns



Internal Limit Violations



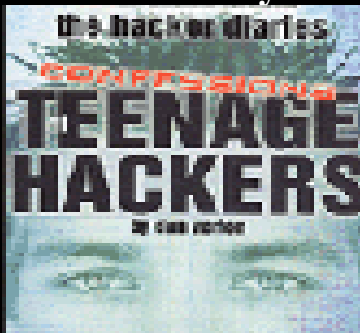
Staff Turnover



Customer Complaints

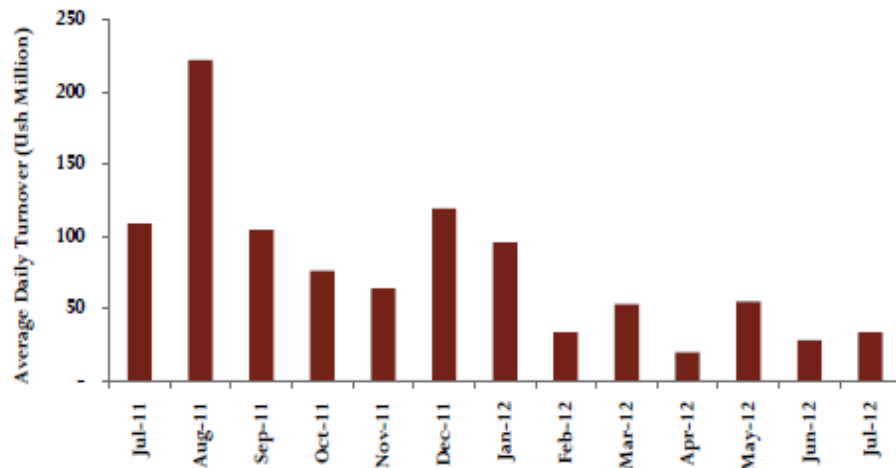


Electronic Security Breaches



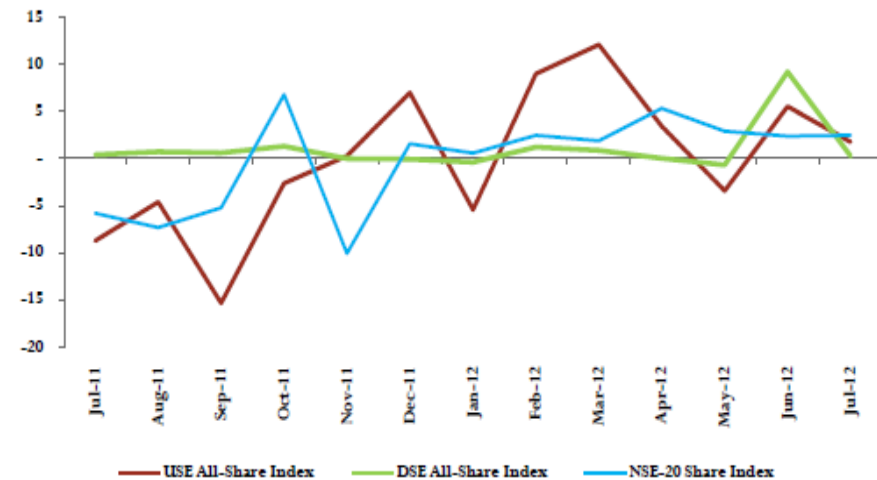
Sample selected KRI

Figure 3: Trends in Average Daily Turnover at the USE (July 2011-July 2012)



Source: USE Market Reports.

Figure 4: Percentage Change in the USE All-share, DSE All-share and NSE-20 Share Indices⁴



Source: USE Market Reports, NSE Monthly Bulletins, DSE Market Reports.

Figure 1: Trends in Market Capitalization for the DSE, NSE, RSE and USE¹

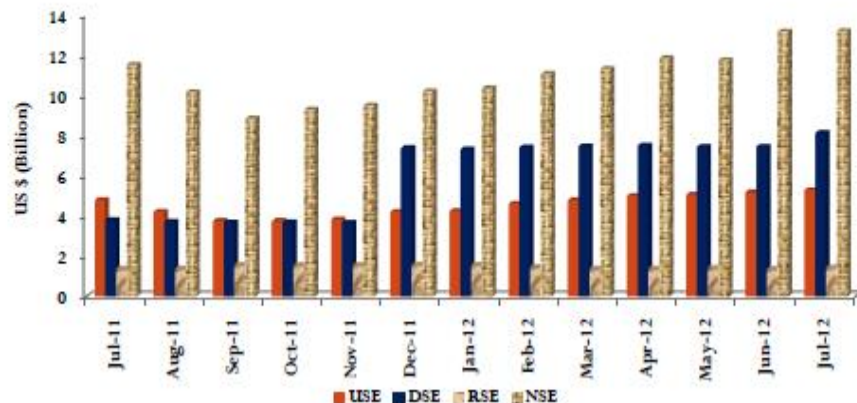
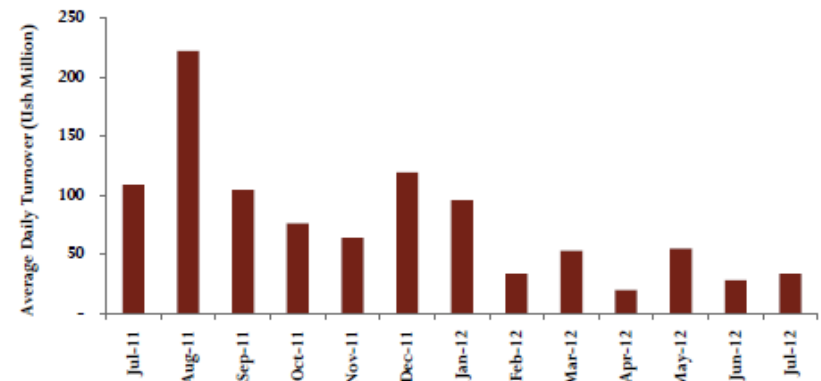
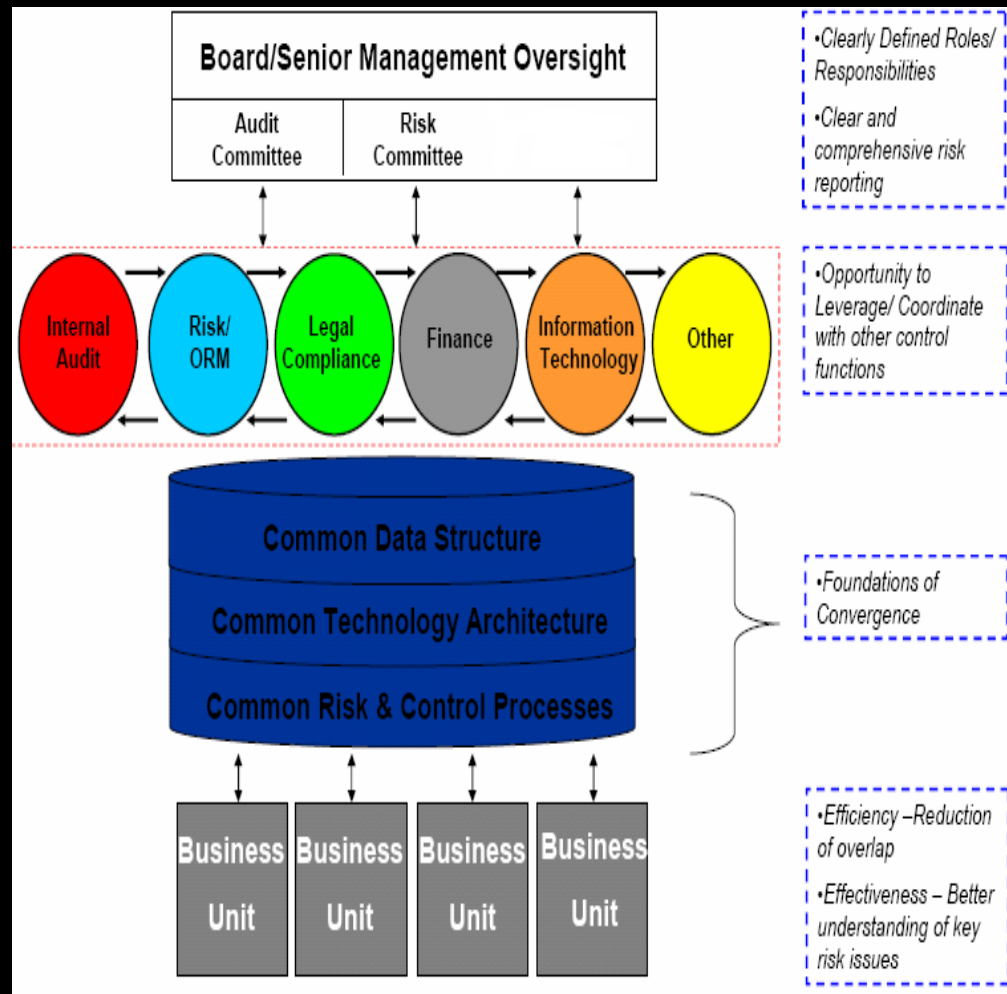
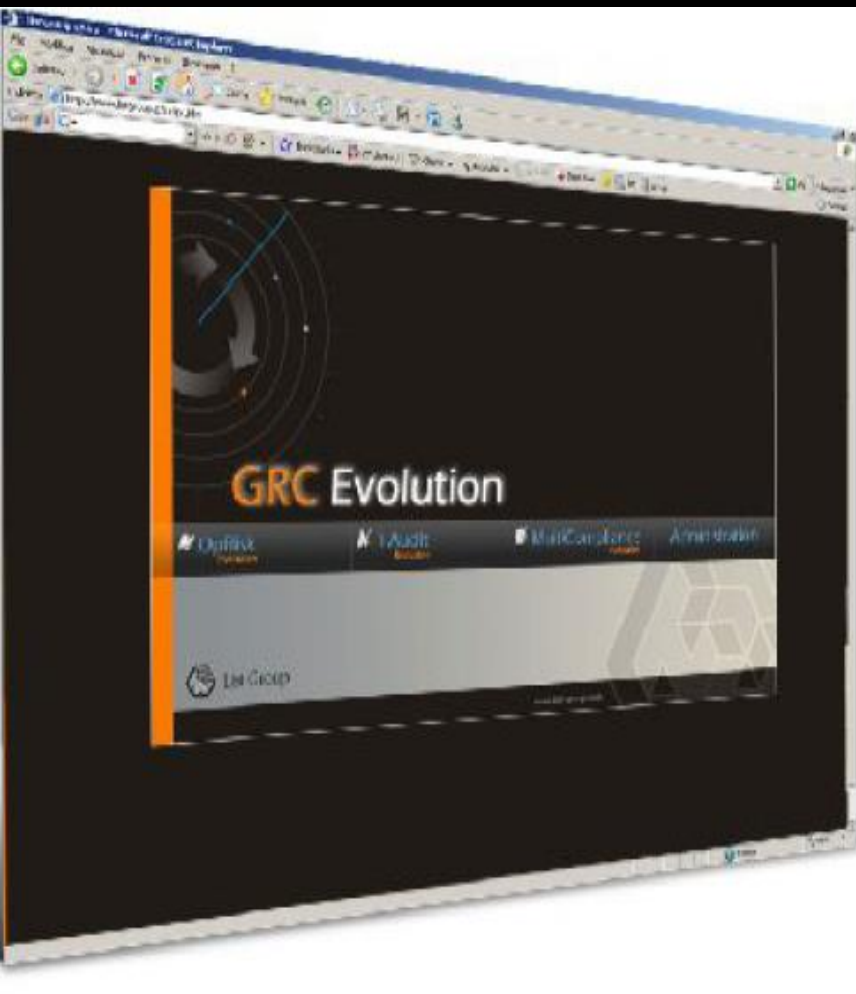


Figure 3: Trends in Average Daily Turnover at the USE (July 2011-July 2012)



Source: USE Market Reports.

Risk Reporting





Q-RADAR - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address http://belgium/roots/index.htm Go Links

Search Web Get IE7 now! Mail My Yahoo! Answers Games Music Personals

Q-RADAR
Your Quantum Leap to Excellence

System Admin | Change Password | Log Off

User Name : Senior Manager, Operational Risk
Screen ID : DSBFRM003

Dashboard Home Help

Risk Dashboard

Scorecard Name : All Search

Gross Rating

Nett Rating

Target Rating

My Risks

No.	Risk Factor	Gross	Nett	Target
1	Business Continuity Management	Red	Red	Yellow
2	SERVE project	Red	Red	Red
3	Manpower planning	Red	Red	Orange

My Exception

Category : Audit Risks Review Pass Due Date

No.	Risk Factor	Description
-----	-------------	-------------

Page : [1] | Total Record : [0]

NAVIGATING CORPORATE POLITICS



CAUTION:
MINES
AHEAD

TOM SPEARS

Corporate Acceptance

- Prioritizing Risk...budgets!
- Relevance to biz.
- Talk business language
- Risk as part of strategic planning

CMA EX DIARY-20/9/2012

CEOs to do list:

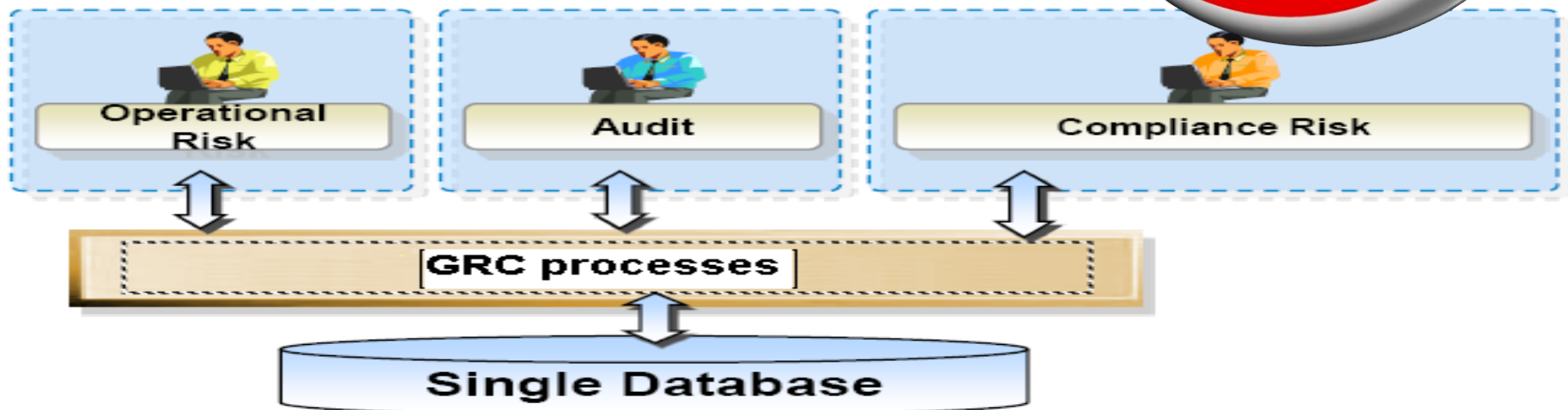
- ① Review Risk mgt Report for August
- ② Enquire action plan progress from Hqs
- ③ Review top 10 Risk Report with Head of Risk
- ④ Give progress action to Chair Risk Comm.



Linking - Risk, internal controls & enterprise value

**Three communities:
Different roles / Different
disciplines / Different risks**

Confusion



A Strategic GRC Framework



Communication Barriers



- Turf battles;
- Developing a risk communications process and taxonomy;
- Making risk management relevant and meaningful for the business



Integration -Risk Language & Culture

How quickly can this management and cultural change take place?

You can't change it overnight. When you get to be a CRO, the likelihood is that you have a pretty sizable organization. Many traders understand risk, and with all the traders unemployed right now, you might say there are plenty who can do risk management. That's probably true at some level. But the other piece of the job is managing the people, having a strategic framework for thinking about the kind of technology support those people need to do their jobs well. You also have a massive data collection problem, and once the data is collected, it has to be distilled into something that is usable. And you have to use influencing skills to reach the conclusions that allow the institution to take enough risk to deliver a return to shareholders, but not so much that it becomes dangerous or too concentrated. It's a blend of past experience, some quantitative skills, the ability to ask tough questions and to challenge and to manage people. You also have to be something of a diplomat – and a dictator if all else fails after you've done your best to facilitate an outcome. On rare occasions you may end up having to go head-to-head.

Develop a Common Risk and Control Language:

- Take an inventory of all current risk practices and taxonomies.
- Determine which ones best meet our business needs.
- Align remaining practices and taxonomies with the ones we determined are best.

Train

Train

Train

Train

Roles & Responsibilities



Who does what?



The Holy Trinity



The 3 Lines of Defence

“Fit for purpose”

1st Line of Defence

2nd Line of Defence

3rd Line of Defence

WHO?

Business function

Senior Risk Committee (s)

Internal Audit

Does What?

Manages & owns risks
Executes Risk methodologies

Drives consistent
Deployment of EMRF
Group wide

Asks whether the risks
identified are the right
risks; & are the right
controls chosen

And Why?

Effective Assurance

Ensures right governance
Check self assurance is
working as designed

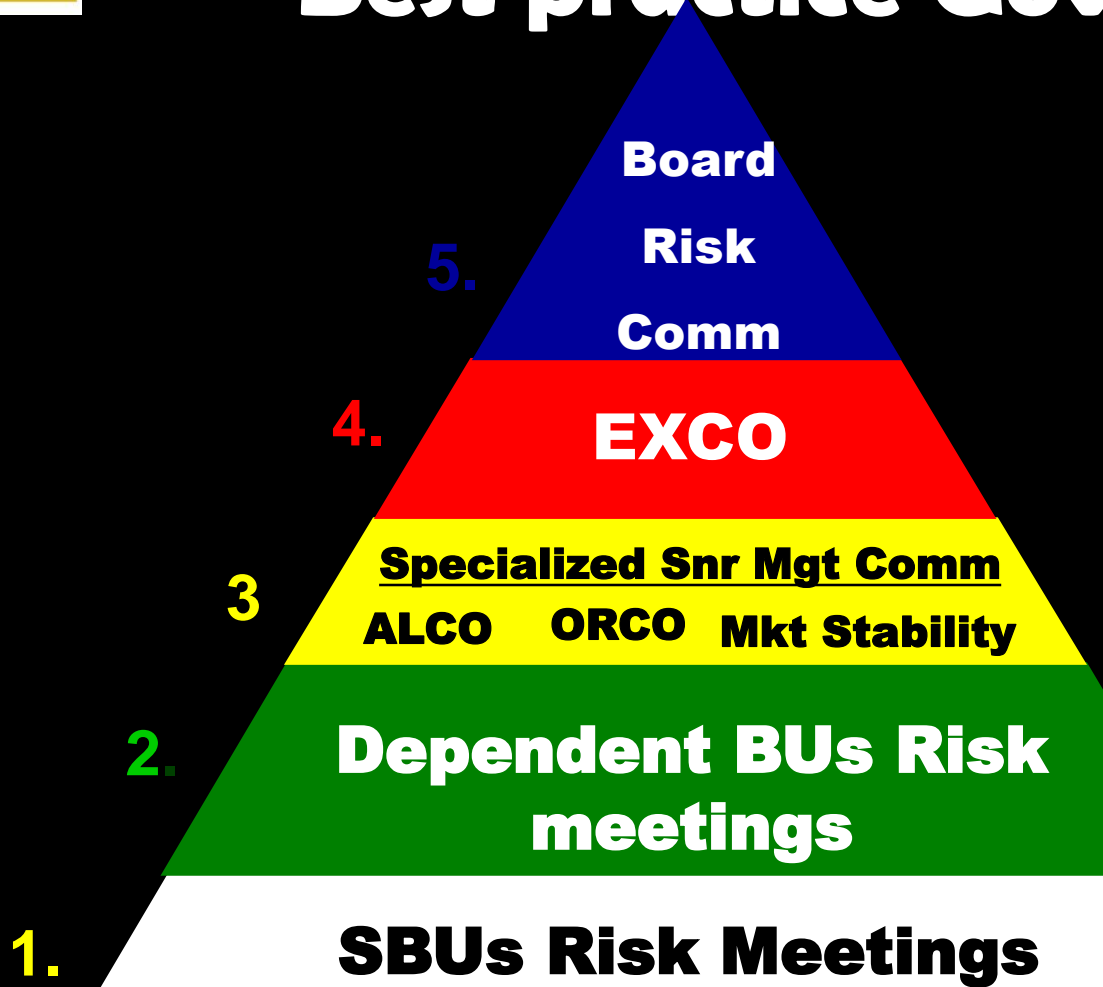
Reviews overall
control
appropriateness and
effectiveness



Risk bulletin

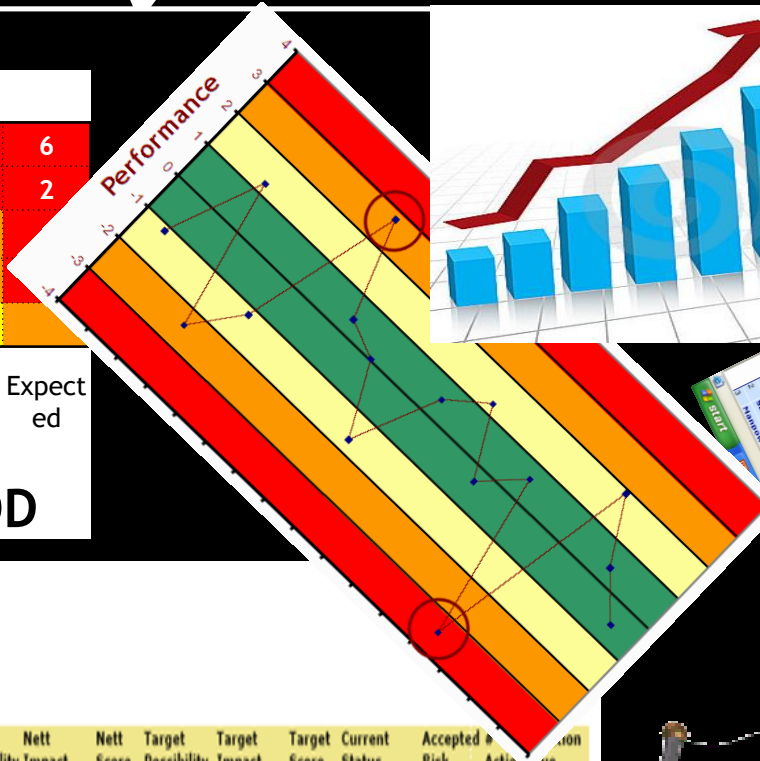
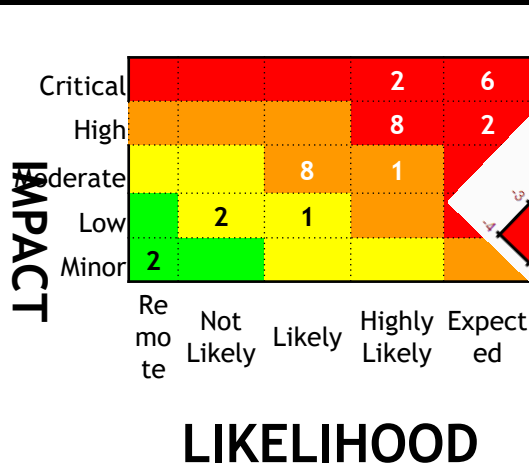


Best practice Governance Arch



	Jan	Feb	Mar	Apr	May	Jun	Jul
Mrs XXX	√	X	A	√	√	A	√
Mr YYY	√	L	√	X	A	√	√
M/s WWW	√	√	√	A	A	X	√

What do you discuss at the Risk Meetings



CORPORATE RISK SCORECARD REPORT Top 20 Risks (Nett)

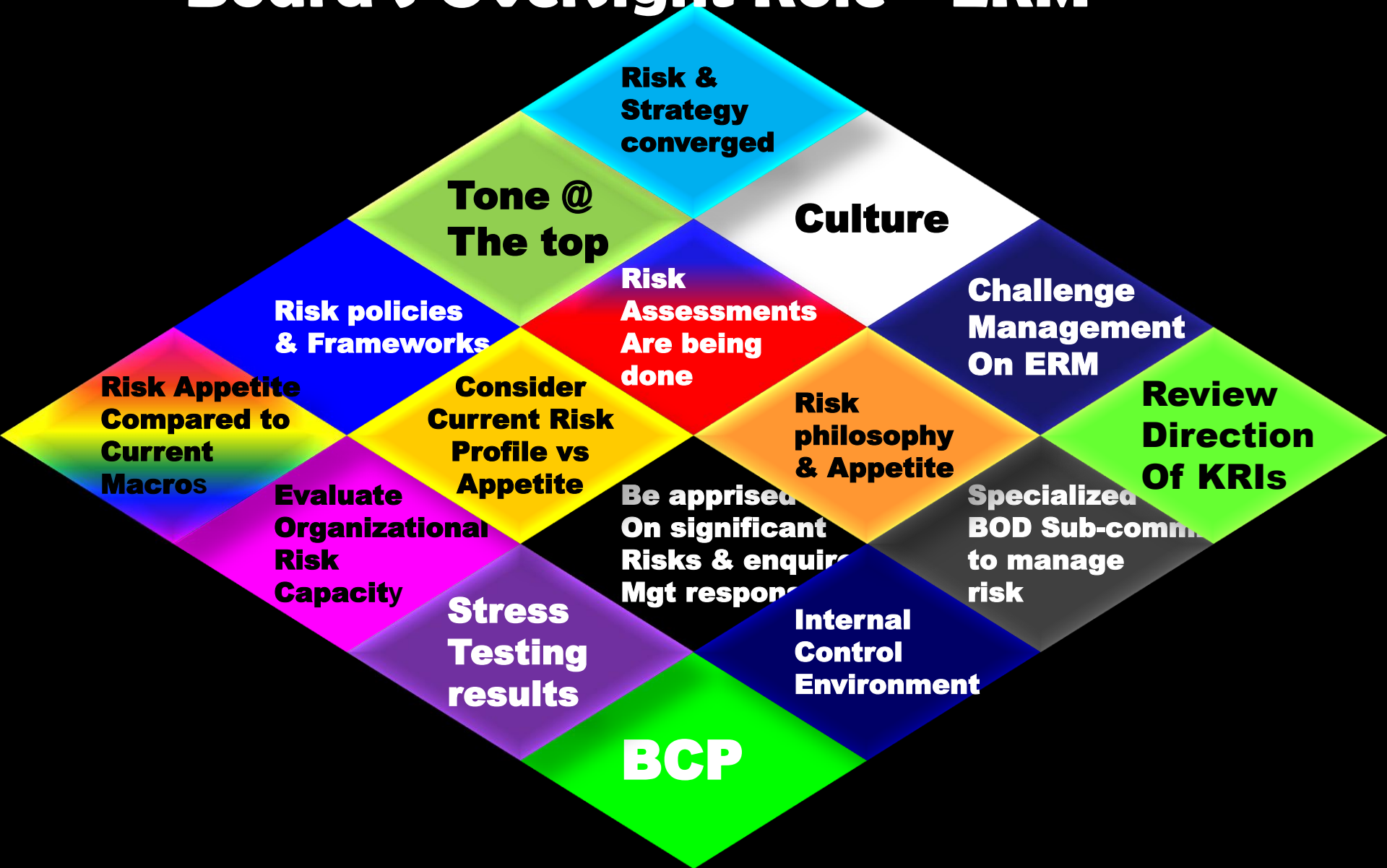
Scorecard Name : Finance Department
Scorecard Owner : General Manager, Finance
Report Date : 08-Nov-2006

No	Risk Factor	Ref	Possibility	Impact	Gross Score	Nett Possibility	Nett Impact	Nett Score	Target Possibility	Target Impact	Target Score	Current Status	Accepted Risk	Action	Due
1.	Government policies	E11101	Very High	Very Significant	QA	Very High	Major	QA	Medium	Major	QA	May Need Improvement	N	1	0
2.	Clearance of Contributions With Incomplete Information (CTML)	Oc1108	Very High	Very Significant	QA	Very High	Major	QA	High	Major	QA	May Need Improvement	N	2	0
3.	Management Information System	Oc1110	Very High	Very Significant	QA	Very High	Major	QA	Unlikely	Major	QB	May Need Improvement	N	1	0
4.	Manpower planning	Hc1105	High	Major	QA	Medium	Major	QA	Medium	Major	QA	Within Expectation	N	0	0



Risks
are part of business, but
business doesn't need
to be risky.

Board's Oversight Role - ERM





Automation



In a competitive, fast-moving business or industry, the organizations that make the best use of Operational Intelligence will be the market leaders. a competitive, fast-moving business or industry, the organizations that make the best use of Operational Intelligence will be the market leaders.

Not News





*Dynamic, real time
Operational Intelligence
about a
company's
exposure to
risk is an
essential tool
for leaders of
large
organizations*

New Concept in Risk Management



GRC is the umbrella term covering an organization's integrated approach to governance, risk and compliance.

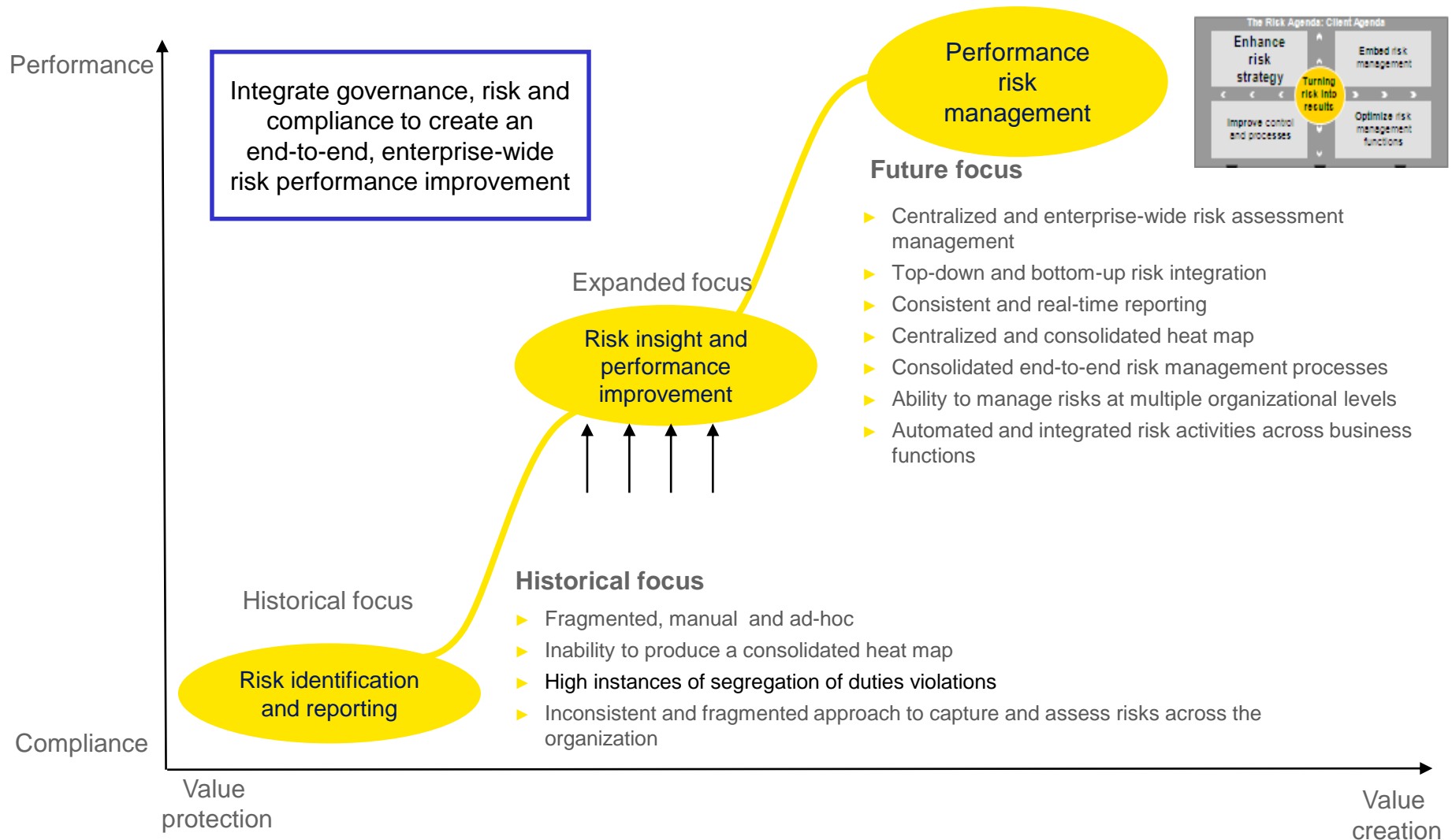
GRC typically encompasses activities such as governance, enterprise risk management (ERM), internal controls, regulatory compliance and internal audit.

GRC technology helps improve financial performance by embedding cost-effective consistent and sustainable risk management practices into daily business activities, while improving management's ability to make decisions.

GRC activities are increasingly being integrated and embedded into organizational structures, processes, systems and data structures in order to avoid redundancies, as well as identifying and closing gaps

GRC acts as “assurance as a whole” for the entire organization.

Technology-enabled GRC transformation

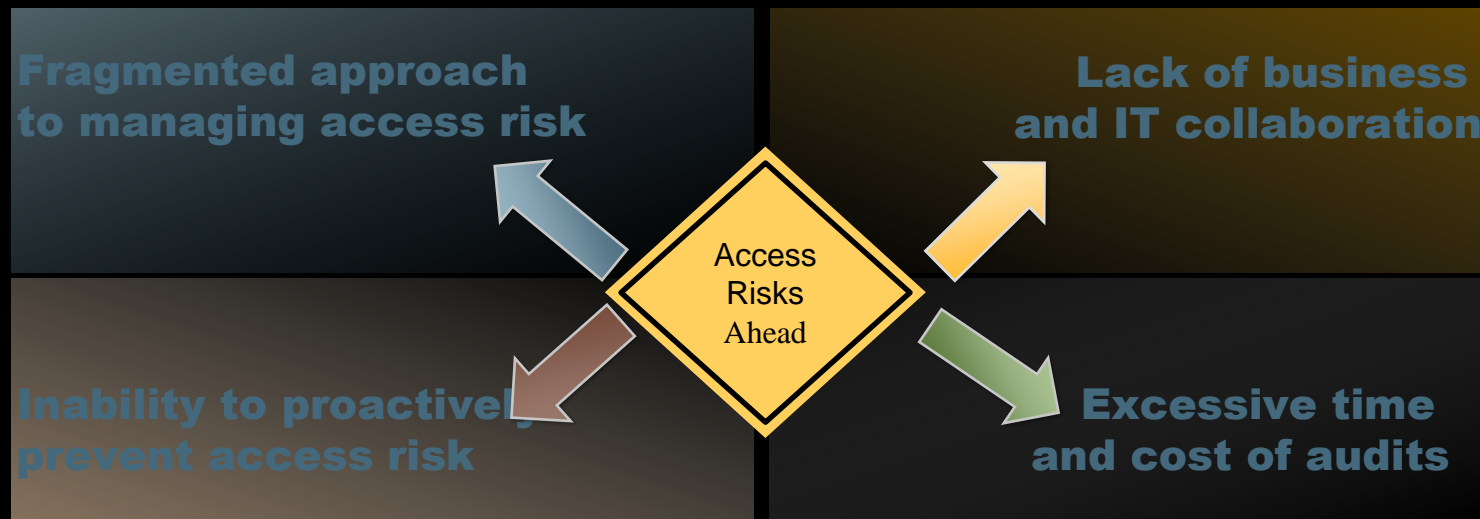


What's happening in the Marketplace?

Segregation of Duties continues to be a top contributor in fraud activities

“A lack of internal controls, such as segregation of duties, was cited as the biggest deficiency”

Control Weaknesses That Contributed to Fraud -
Report to the Nations on Occupational Fraud and Abuse, 2010, ACFE



Risk Appetite Matrices (RAMs)



Risk Window

Accelerate Analyser - Operational Risk Assessment

File Goals Controls Actions Assessments Linked Risks Linked KIs Log Windows Help

Entity: ENT00046 FinanceCorp Retail Banking

Operational Models: Division: All; Mega/Major Process: All; Minor Process: All; Micro Process: All; Location: All; Legal Entity: All;

CR Description: (CRR00005) Inability to retain, recruit and retain key staff

Description: Failure to attract, recruit and retain key staff

Risk Category: EMP Employment practices and workplace safety

Causal Category: Not Set

Risk Ref: RSK00052

Linked Risk: None

Residual Severity: **Minor**

Residual Ann Exp: 250,000 USD

Risk Actions: 4 (3 Open)

Amend **Attest**

Ref	Date	Attested	I	R	T
ASM00247 *	28/02/2010				
ASM00244	28/02/2010				
ASM00241	28/02/2010				
ASM00238	28/02/2010				
ASM00235	30/09/2009	✓			
ASM00232	31/03/2009	✓			
ASM00154	31/01/2009	✓			

Assessment:

Date: 28/02/2010 NOT ATTESTED Due on: 25/02/2010

Assessed by: DBA Database Administrator

Commentary:

RAM: Retail Banking RAM

Head Office Currency: USD Rate Date: 25/02/2010 Rate: 1

	INHERENT	RESIDUAL	TARGET
Likelihood:	Medium High <i>2.00 times a year</i>	Medium Low <i>0.50 times a year</i>	Low <i>0.20 times a year</i>
Impacts (loss per event):			
Financial	Medium High 2,500,000	Medium Low 500,000	Low 50,000
Financial (Extreme)	N/A 0	N/A 0	N/A 0
Reputation	N/A	N/A	N/A
Total Exp (USD):	2,500,000	500,000	50,000
Annual Exp (USD):	5,000,000	250,000	10,000
Severity:	Major	Minor	Negligible

Save Assessment Cancel Edits

Close Window

View Risk Controls

Accelerate Analyser - Operational Risk Assessment

FileGoalsControlsActionsAssessmentsLinked RisksLinked KIsLogWindowsHelp

Entity: ENT00046 Retail Banking

Operational Models: **Division:** Corporate Banking; **Mega/Major Process:** N/A; **Minor Process:** N/A; **Micro Process:** N/A; **Location:** UK; **Legal**

CR Description: (CRR00005) Inability to retain, recruit and retain key staff

Description: Failure to attract, recruit and retain key staff

Risk Category: EMP Employment practices and workplace safety

Causal Category: Not Set

Risk Ref: RSK00052
Linked Risk: None
Residual Severity: Moderate
Residual Ann Exp: 1,851,852 USD
Risk Actions: None

Add Control

Amend Control

Delete Control

General

Goals

Controls

Actions

Assessments

Risk Focus

Linked Items

Log

Ref	Description	Key Ctrl	Last Assess. Date	Last Assess. Design	Last Assess. Pfmnce	Last Assess. Creator	Last Assess. status
CTR00019	Salary surveys		03/03/2009	Average	Average	DBA Database Adminis	NOT ATTESTED
CTR00020	Training and mentoring schemes		03/03/2009	Good	Average	DBA Database Adminis	NOT ATTESTED
CTR00021	Retention packages for key staff		03/03/2009	Good	Good	DBA Database Adminis	NOT ATTESTED

Details

History (1)

Actions

KIs

Documents

Test Plans

Test Results

Control Library Ref: CTL00020

Compensation / Remuneration

Control Category : Preventative

Description: Retention packages for key staff

Personnel:

Owner: Kazi D

Nominee: Kazi D

Reviewer: DBA Database Administrator

Review Date:

Notes:

Retention packages for key staff

☐ Key Control

☒ Control Is Active

Operation:

Frequency: Annually

Last Operate:

Sign Off

Next Operate: 03/03/2009

Assessment:

Frequency: Semi Annually

Next Assess: 31/05/2009

Sign Off / Add Next

Save Control

Cancel Edits

Control History

Accelerate Analyser - Operational Risk Assessment

File Goals Controls Actions Assessments Linked Risks Linked KIs Log Windows Help

Entity: ENT00046 FinanceCorp Retail Banking

Operational Models: **Division:** All; **Mega/Major Process:** All; **Minor Process:** All; **Micro Process:** All; **Location:** All; **Legal Entity:** All;

CR Description: (CRR00005) Inability to retain, recruit and retain key staff

Description: Failure to attract, recruit and retain key staff

Risk Category: EMP Employment practices and workplace safety

Causal Category: Not Set

Risk Ref: RSK000052

Linked Risk: None

Residual Severity: **Minor**

Residual Ann Exp: 250,000 USD

Risk Actions: 4 (3 Open)

Add Control

Amend Control

Delete Control

Amend Assess

Attest Assess

General

Goals

Controls

Actions

Assessments

Risk Focus

Linked Items

Log

Ref	Description	Key Ctrl	Last Assess. Date	Last Assess. Design	Last Assess. Pfmnce	Last Assess. Creator	Last Assess. status
CTR00020	Training and mentoring schemes		03/03/2009	Good	Good	DBA Database Adminis	NOT ATTESTED
CTR00021	Retention packages for key staff		25/02/2010	Average	Good	DBA Database Adminis	NOT ATTESTED
CTR00087	Salary Surveys		29/01/2010	Good	Good	DBA Database Adminis	NOT ATTESTED

Details

History (2)

Actions

KIs

Documents

Test Plans

Test Results

Control Focus

Date	Notes	Design	Pfmnce
25/02/2010		Average	Good
03/03/2009	Retention packages for key staff	Good	Good

Performance: Good Efficiency: 0 - Not Assessed

Design for Risk: Average Cost: USD

Assessed on: 25/02/2010 Due on:

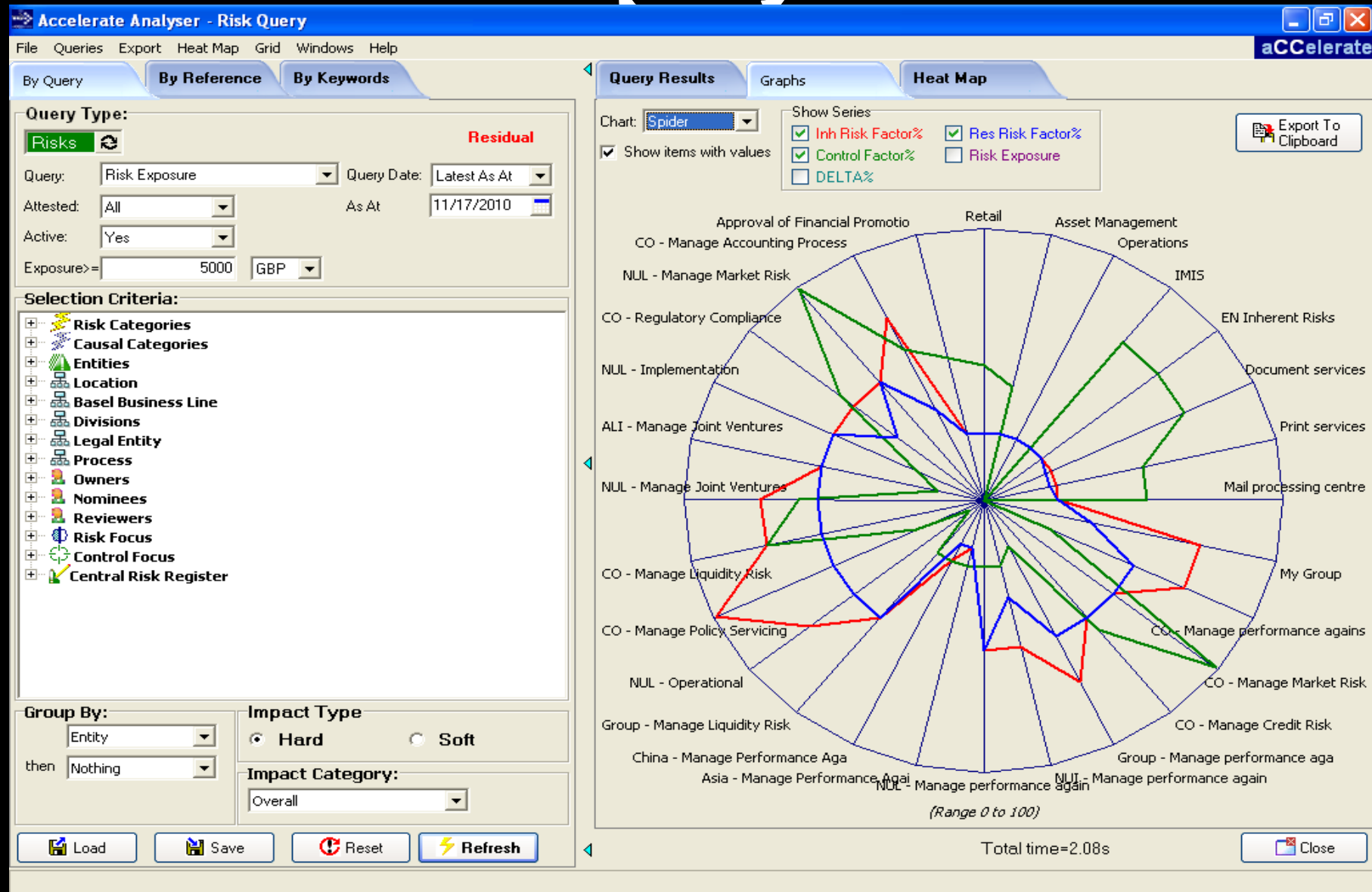
Assessed by: DBA Database Administrator

Notes:

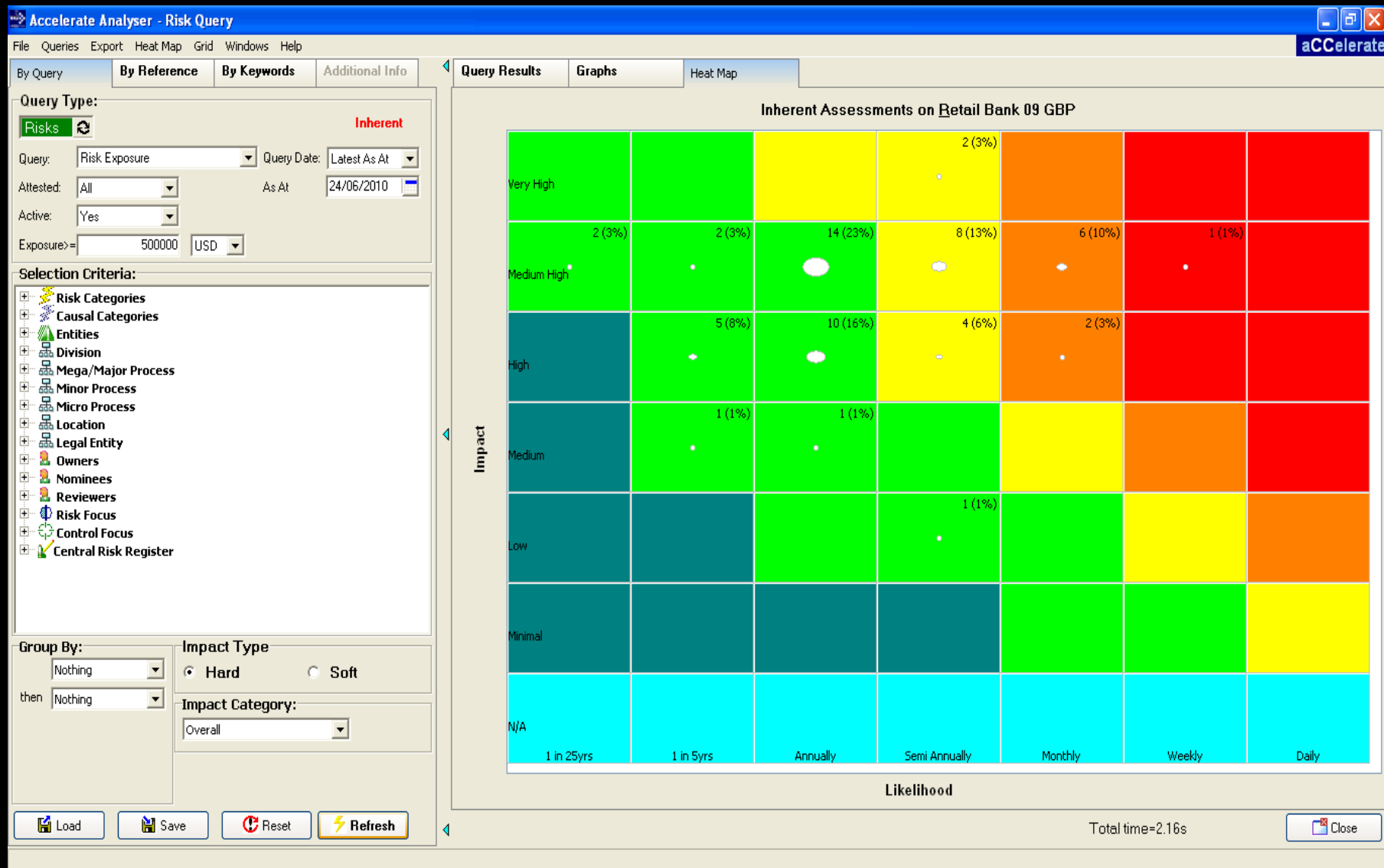
Save Assess Cancel Assess

Close Window

Risk Query Tool



Risk Query Tool Heat Map



Applying Mitigating Actions

Accelerate Analyser - Operational Risk Assessment

File Goals Controls Actions Assessments Linked Risks Linked KIs Log Windows Help

Entity:

ENT00046 Retail Banking

Operational Models:

Division: Corporate Banking; Mega/Major Process: N/A; Minor Process: N/A; Micro Process: N/A; Location: UK; Legal Entity: Retail Bank Plc;

CR Description:

(CRR00005) Inability to retain, recruit and retain key staff

Description:

Failure to attract, recruit and retain key staff

Risk Category:

EMP Employment practices and workplace safety

Causal Category:

Not Set

Risk Ref: RSK00052

Linked Risk: None

Residual Severity: Moderate

Residual Ann Exp: 1,500,000 USD

Risk Actions: 4 (3 Open)

Add Action

Amend Action

Close

Void

General

Goals

Controls

Actions

Assessments

Risk Focus

Linked Items

Log

4 Actions shown: (3 Open including 1 Imminent)

Action Ref	Description		
ACT00021	Implement a process for Succession Planning for key staff	26/02/2010 0%	Risk Management 1: High
ACT00022	HR to be internally audited this quarter	31/03/2010 30%	Internal Audit 3: Low
ACT00023	Review HR recruitment procedures against FSA regulations re: legal dept	02/02/2010 80%	Compliance 1: High
ACT00024	HR recruitment policies to be updated as per new Employment Legislation Q	31/03/2009 0%	Legal

Action Ref: ACT00024

Originating Event Ref: None

Action State: Voided

Source: Legal

Priority:

Reference:

Commentary

Progress

Log

Completion %:

Date:

Personnel:

Owner: DBA Database Administrator

Nominee: DBA Database Administrator

Reviewer:

Review Date: 03/01/2010

Target Date: 31/03/2009

Cost: 50,000 GBP

Documents

Save Action

Cancel Action

Close Window

Accelerate Analyser - Operational Risk Assessment

Recipient(s): jane.usher@xyz.com

Subject: Operational Risk RSK00013 Action ACT00011 (target date 20/05/2005)

Message: Review standby communications facilities to see if more resilience can be built-in.

Attachment:

Send

Cancel

Risk Events (Basic Flow)

Accelerate Analyser - Risk Event

File Windows Help

Event Ref: EVT00001

Current State: APPROVED

Current Locks:

Description: Failing to act in its customer's best interests

Total Losses: 459,488.31 USD

External Ref: 5

Amend

Delete Event

Unlock Origin

Close Event

Print Single Event Report

Failing to act in its customer's best interests

Actions

Loss Entities

Corporate Investments

2 Improper business or market practices

10/04/2008 16:50:43

11/04/2008 14:00:35

25/03/2009 12:15:11

25/03/2009 12:18:35

27/01/2010 09:37:01

Funds

Correct/Improve

Notifications

Details

Financials

Commentary

Additional Info

Event Date: 01/04/2002

RAG: N/A

Recorded By: Database Administrator, DBA

On 10/04/2008 at 16:50:42

Is Active

Notify Regulator

Exclude Fund Losses

Area of Detection

Entity: ENT00001 Corporate Investments

Sub-Entity: None

Detection Date: 01/04/2002

Area of Origin

Entity: ENT00005 Deal signing

Sub-Entity: None

Description: Failing to act in its customer's best interests

Detailed Description:

Morgan Grenfell was fined by the Financial Services Authority (FSA) for breaching FSA Principles by failing to act in its customer's best interests and failing to manage its conflicts of interests in the course of a blind bid principle program trade.

The FSA found that Morgan Grenfell commenced proprietary trading in seven of the constituent securities of a client's programme trade, prior to its award, based on limited information provided to enable the firm to quote for that business. The proprietary trading resulted in the client paying more for the programme trade than they would otherwise have done.

This financial penalty was imposed in respect of the firm's conduct towards a customer and the management of conflicts of interest in the course of a blind bid principal programme trade in April 2002 which was in breach of FSA Principle 6 and Principle 8. The firm's programme trading desk engaged in trading in some of the component securities of the customer's programme trade between the provision of limited information to enable the firm to provide a quote for that trade and the strike time of that trade. The customer paid more than they would otherwise have done for this trade due to the firm's trading in these securities. The firm had previously carried out programme trades with the customer who was classified by the firm as an intermediate client. The customer was an experienced fund manager with in excess of GBP 30bn funds under management as at June 2002. The firm failed either to notify the customer in advance that it may trade in the component securities based upon the information supplied by the cust

Approved Date: 11/04/2008

Closed Date:

Personnel:

Owner: DBA Database Administrator

Nominee: DBA Database Administrator

Reviewer:

Review Date:


Documents

Save And Approve

Save Event

Cancel Edits

Close Window



82



Risk Events (Aggregation)

Accelerate Analyser - Risk Event

File Windows Help

Event Ref: EVT00001

Current State: APPROVED

Current Locks:  

Description: Failing to act in its customer's best interests

Total Losses: 459,488.31 USD

External Ref: 5

Amend

Delete Event

Unlock Origin

Close Event

Print Single Event Report

Failing to act in its customer's best interests

Actions

Loss Entities

Corporate Investments

2 Improper business or market practices

10/04/2008 16:50:43

11/04/2008 14:00:35

25/03/2009 12:15:11

25/03/2009 12:18:35

27/01/2010 09:37:01

Funds

Correct/Improve

Notifications

Details

Financials

Commentary

Additional Info

Head Office Currency: USD

View Currency: USD

Hard Impact Matrix

Soft Impact Matrix

Direct for Event

	Compensation	Regulatory Fines	Legal Fees	Interest & Charges	Other	Total
Actual Loss	0.00	459,148.90	1,449.28	339.13	0.00	460,937.31
Expected Loss	25,000.00	0.00	0.00	0.00	0.00	0.00
Actual Insurance Recovery	0.00	0.00	0.00	0.00	0.00	0.00
Expected Insurance Recovery	0.00	0.00	0.00	0.00	0.00	0.00
Actual Other Recovery	0.00	0.00	1,449.00	0.00	0.00	-1,449.00
Expected Other Recovery	0.00	0.00	0.00	0.00	0.00	0.00
Potential Loss	0.00	0.00	0.00	0.00	0.00	0.00
Total	0.00	459,148.90	0.28	339.13	0.00	459,488.31

Indirect for Event

	Other Indirect	Staff Time	Total
Actual Loss	0.00	0.00	0.00
Expected Loss	0.00	0.00	0.00
Actual Insurance Recovery	0.00	0.00	0.00
Expected Insurance Recovery	0.00	0.00	0.00
Actual Other Recovery	0.00	0.00	0.00
Expected Other Recovery	0.00	0.00	0.00
Potential Loss	0.00	0.00	0.00
Total	0.00	0.00	0.00
Fund Losses			0.00

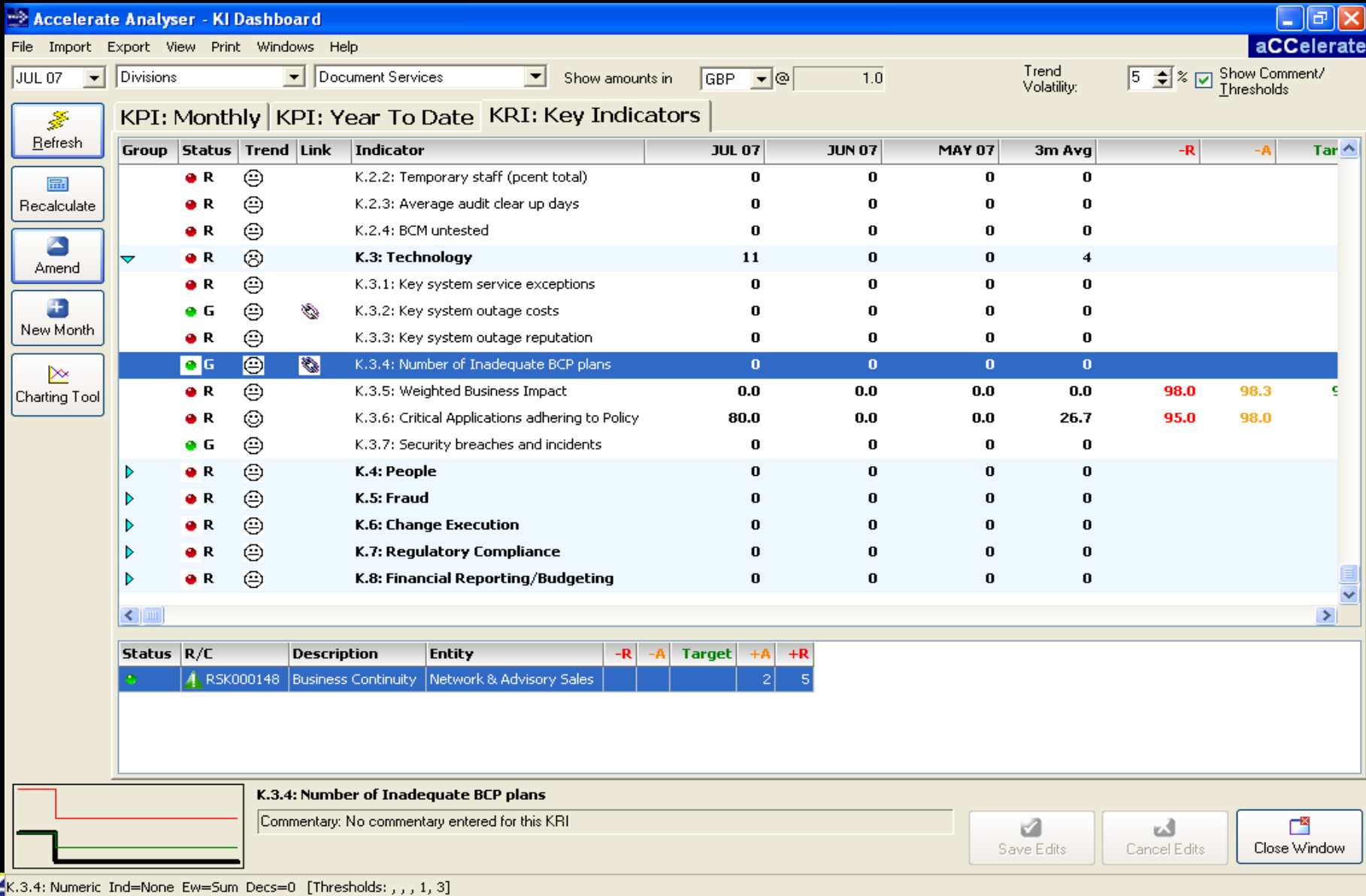
Save And Approve

Save Event

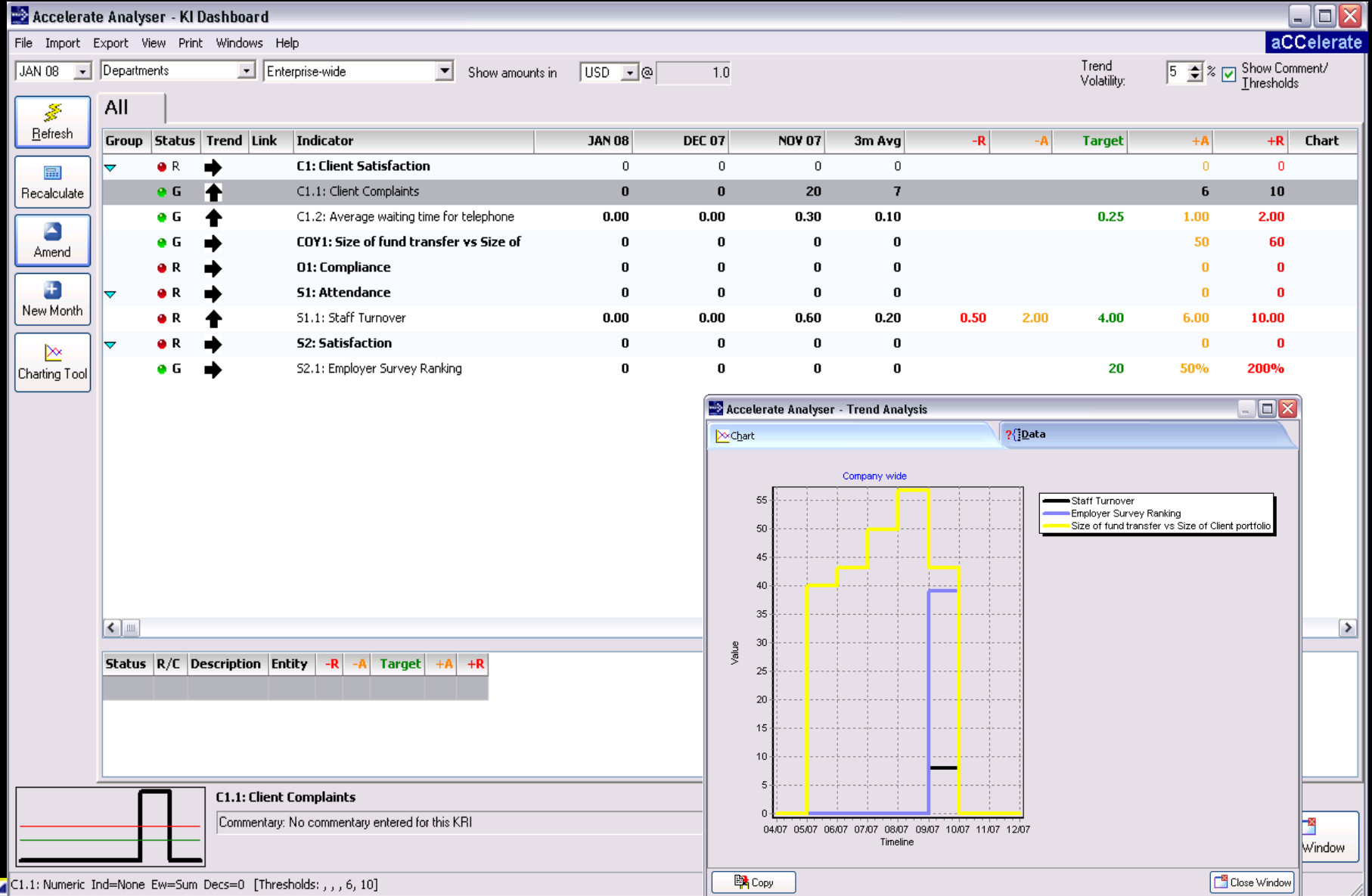
Cancel Edits

Close Window

















































KRI Dashboard



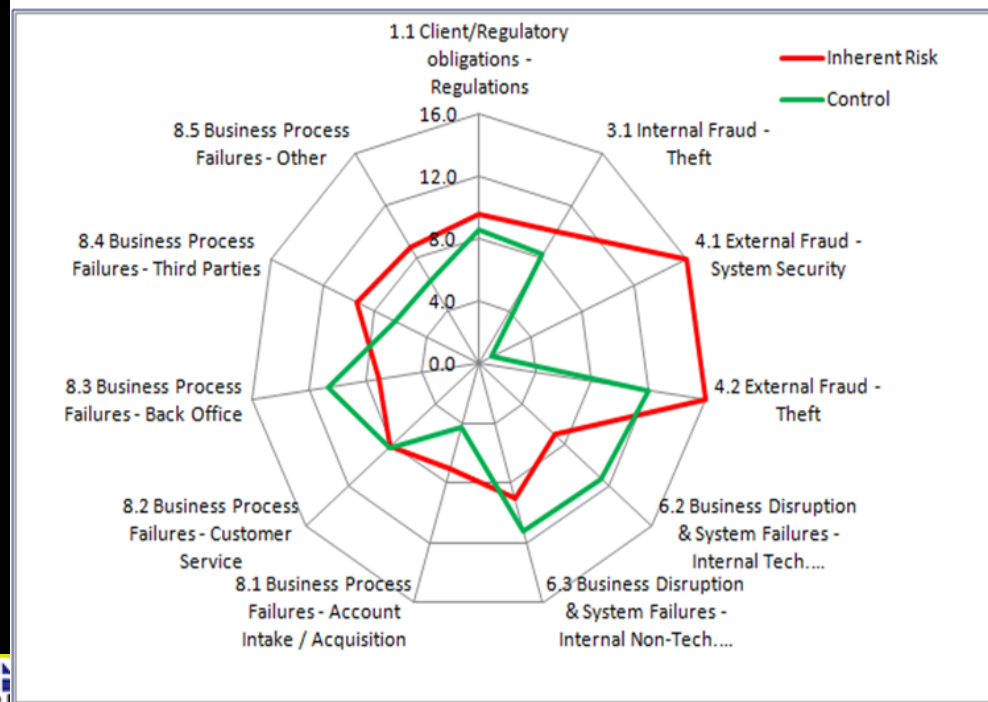
KRI Dashboard Charts



Top risks and their KRIs

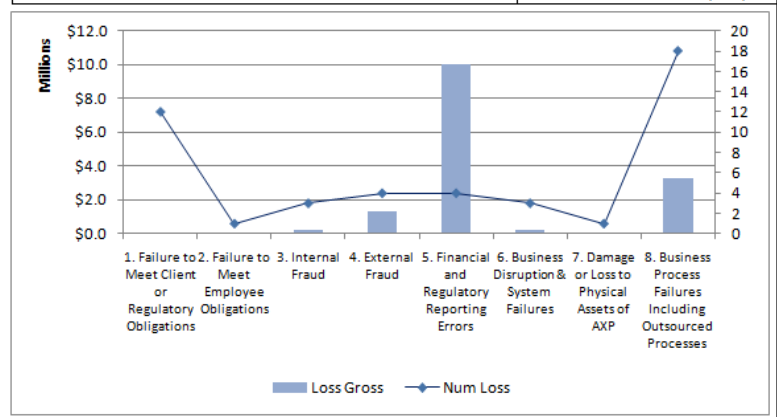
Risk/Risk Cat	Inherent Risk	Loss NUMBER	Loss VALUE	Indicator s	Direction	Action status	KRI Breakdown - Number per Risk/RiskCat
6.2 Business Disruption & System Failures - Internal Tech. Infra		2	1.2			A	
3.2 Internal Fraud - Unauthorised Activity		1	0.1				
4.1 External Fraud - System Security		2	0.3				
8.1 Business Process Failures - Account Intake / Acquisition		7	2.0				
5.2 Financial & Regulatory Reporting - Internal Reporting		18	3.3			A	
8.4 Business Process Failures - Third Parties		2	0.8			A	
6.3 Business Disruption & System Failures - Internal Non-Tech.		0	0.0				
4.2 External Fraud - Theft		5	4.8			A	
7.2 Damage or Loss to Physical Assets - Controllable Events (In		2	0.0			A	
8.1 Business Process Failures - Account Intake / Acquisition		1	0.0				
1.1 Client/Regulatory obligations - Regulations		1	1.5			A	
8.5 Business Process Failures - Other		3	1.0				
Other		2	0.3				
		46	15.2				

RISK CATEGORY 2 - INHERENT RISK VS AVERAGE CONTROLS SCORES

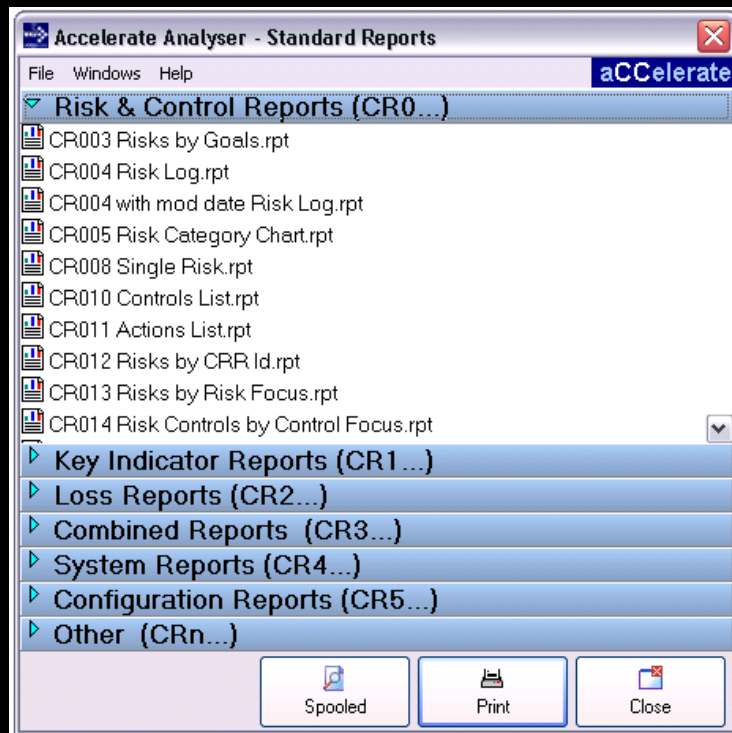


LOSS EVENT DATA FOR THE PERIOD


Risk Event Category	Num Loss	Loss Gross
1. Failure to Meet Client or Regulatory Obligations	12	45,000
2. Failure to Meet Employee Obligations	1	0
3. Internal Fraud	3	228,064
4. External Fraud	4	1,315,025
5. Financial and Regulatory Reporting Errors	4	10,058,125
6. Business Disruption & System Failures	3	220,367
7. Damage or Loss to Physical Assets of AXP	1	0
8. Business Process Failures Including Outsourced Processes	18	3,309,074
Grand Total	46	15,175,655



Reports (Parameter selection)



Accelerate 2.88 - MyCapital Page:1



CR008 Single Risk

Risk Ref: RSK00034:Fraudulent fund transfers through SWIFT.

Release of funds through SWIFT: ENT00040

Operational Models:					
Division	Legal Entity	Location	Mega/Major Process	Micro Process	Minor Process
Corporate Management	All	Bahrain	Funds Transfers	Release of funds through SWIFT	Deal funding

Central Risk Description:
Detailed Description: Fraudulent fund transfers through SWIFT. ;Causes:Motive to embezzle Consequences:Cash loss
Risk Category: IF.1. - Internal Fraud, Unauthorised Activity
Causal Category: N/S. - Not Set

Personnel:		Assessment:	
Owner: DBA Database Administrator	Email Owner: N	Freq:	
Nominee: DBA Database Administrator	Next Review Date:	Remind on:	02-Apr-08
Reviewer: DBA Database Administrator		Risk is Active:	Y

Latest Risk Assessment: ASM00100

Period End Date: 04-Sep-08 NOT ATTESTED RAM: MyCapital 09

Commentary:

Impact(Loss per Event)	INHERENT	RESIDUAL	TARGET
Likelihood:	Medium Once a year	Medium Once a year	Low Once every 3.33 years
Likelihood Score:	2	2	1
Impact Score:	3	2	2
Risk Score:	6	4	2

	High: \$,000,000	Medium: 2,600,000	Medium: 2,600,000
Financial			
Financial (Extreme)	N/A: 0	N/A: 0	N/A: 0
Reputation	Medium: 0	Medium: 0	N/A: 0

	\$,000,000	2,600,000	2,600,000
Total Exposure (USD):			
Ann. Exposure (USD):	\$,000,000	2,600,000	780,000
Severity:	Critical	Major	Minor

Average Control Design: 2.0	Average Control Performance: 3.0	Average Control Score: 6.0
------------------------------------	---	-----------------------------------

Goals:

Example of Multi Chart Reporting



V1.7 Rev 237

Printed by: DBA Database Administrator on 08/11/2009 10:45:31

Example of Dashboard Reporting

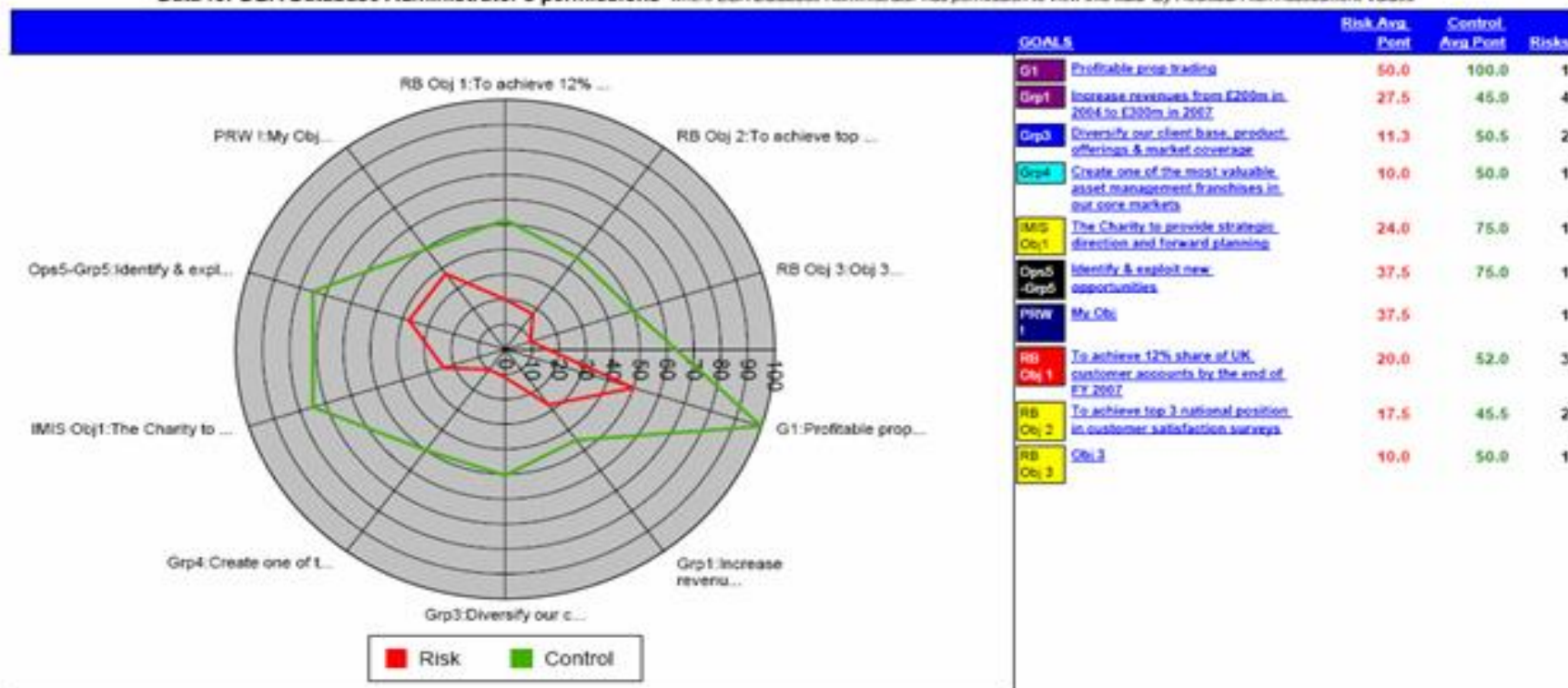
Company Name and app version from database - will be overwritten by application

Page:1



CR066 Goal Performance(DD)

Data for DBA Database Administrator's permissions where DBA Database Administrator has permission to view this data By Residual Risk Assessment Values



Inherent Risk = Gross Risk and Residual Risk = Net Risk

Printed by: DBA Database Administrator on 26-Mar-07 1:37 pm

Workflow Diary

Accelerate Analyser - Workflow Diary

File Day Windows Help

21 Day Summary

Daily Detail (click item to view)

Jan 2010

Mon	Tue	Wed	Thu	Fri	Sat	Sun
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Today: Tuesday 26 January 2010

Selection Criteria E-mails

Nominee equal to

DBA Database Administrator

☒ Risks
☒ Risk Events
☒ Actions
☒ Risk Controls
☒ Dashboard Thresholds
☒ Memos

E-Mail Status:

E-mail Trigger: 0 days

Refresh

Tue 26 Jan	CTR00086/RSK00092 Dual Control	RSK00092 Failure to present/present ...
Wed 27 Jan	CTR00086/RSK00092 Dual Control	
Thu 28 Jan	RSK00092 Failure to present/present ...	CTR00086/RSK00092 Dual Control
Fri 29 Jan		
Sat 30 Jan		
Sun 31 Jan		
Mon 01 Feb	ACT00020/RSK00092 Improve communication lines between Deal Funding an...	
Tue 02 Feb		
Wed 03 Feb		
Thu 04 Feb		
Fri 05 Feb		
Sat 06 Feb		
Sun 07 Feb		
Mon 08 Feb	ACT00020/RSK00092 Improve communication lines between Deal Funding an...	
Tue 09 Feb		
Wed 10 Feb		
Thu 11 Feb		
Fri 12 Feb		
Sat 13 Feb		
Sun 14 Feb		
Mon 15 Feb		

Tuesday 26 January 2010

CTR00086/RSK00092 Dual Control

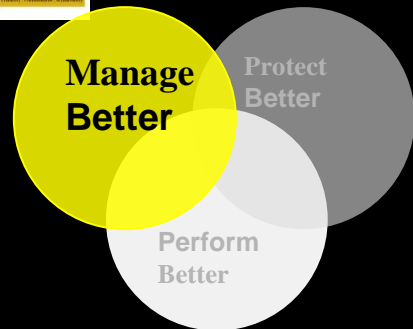
RSK00092 Failure to present/present accurately deal information
Failure to present/present accurately deal information;Causes:Errors/...

Right-click on item to set email status

+ Add Memo Item Export Appointments 2 Items

Close

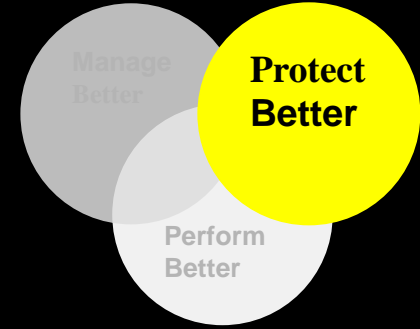
Technology can improve ERM: -



- ▶ Risk culture is sponsored from the top and cascaded throughout the organization
- ▶ Comprehensive risk assessment performed to identify all risks – responsibility for risk coverage is clearly defined
- ▶ Gaps in risk coverage are identified
- ▶ Common risk management technology platform aligns all risk functions
- ▶ Risk reporting is provided to stakeholders to support decisions and enable performance



- ▶ Risk overlaps and redundancies are rationalized or eliminated
- ▶ Risk coverage focused on high priority risks versus low risk areas
- ▶ Technology and knowledge management is leveraged to improve productivity
- ▶ Proficient resources minimize the time required to assess, test and report risks



- ▶ Risk functions provides confidence to take risk as opposed to avoid risk
- ▶ Risk provides process improvement suggestions to improve security, privacy, availability
- ▶ Risk function provides identification of risks and assists in determining boundaries
- ▶ Risk function contributes to oversight and ongoing assessment of the most strategic initiatives (e.g., new systems, acquisition integration, etc.)

Draw Gaps in your programme





Are u sure?



Yes we Can