

The Global Evolution of Enterprise Risk Intelligence (ERI) and its Adoption and Maturity across Different Cultures

Presented by Andrew Howarth,
CEO & Founder, RMSS.



New Zealand Society for Risk
Management Conference 2012



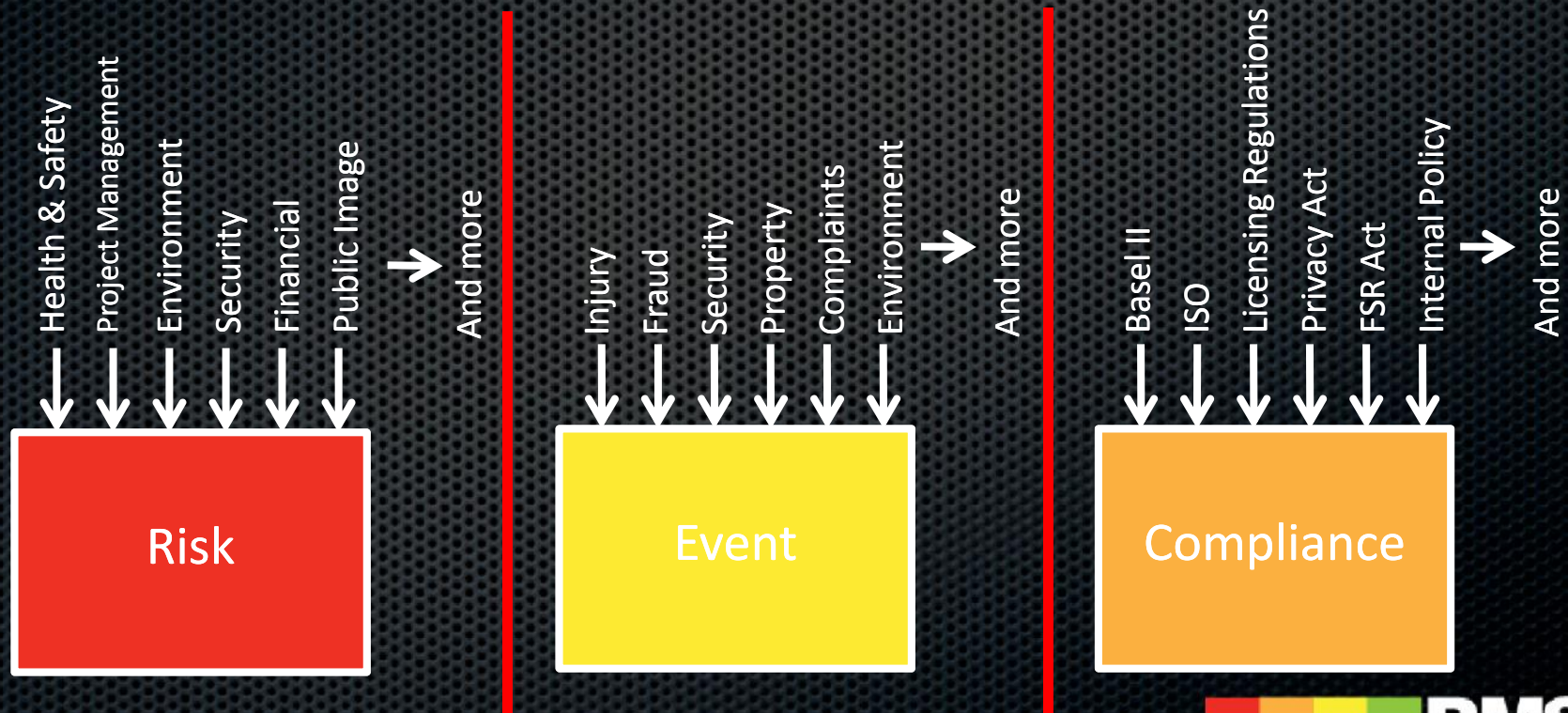
Agenda

1. Common Current State
2. What is ERI
3. ERI across organisational boundaries
4. Adoption of ERI in various nations and cultures
5. The operational and strategic benefits of ERI
6. Leading practice industry and case study examples



Current state

- There is compliance management, risk management, and event management



Enterprise Risk Intelligence (ERI)

- Integrates the key areas of risk, compliance and event management across an organisation / enterprise allowing analysis and collaboration to generate intelligence
- Enterprise - entire organisation (operation and strategic)
- Risk and Intelligence - best defined together

ERI... a quality circle

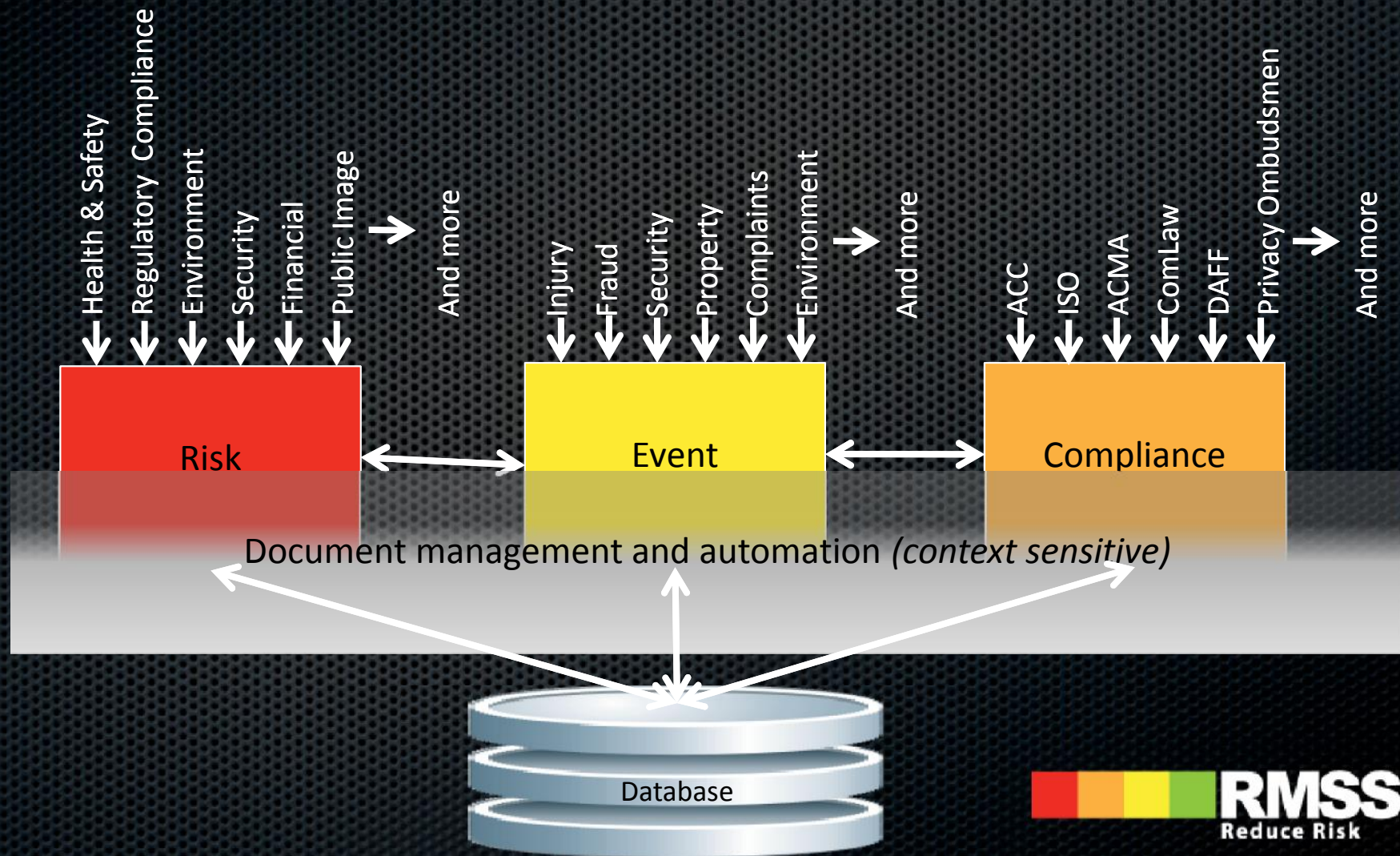


ERI... a quality circle



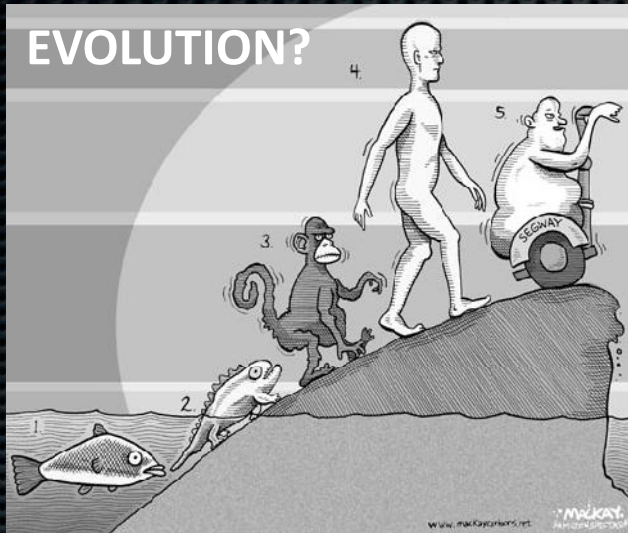
Interlinking of functions- ERI

True enterprise



ERI - evolution

↑
VALUE ADD FOR ORGANISATIONS



1

Risk management equals buying insurance

2

Regulators are demanding risk management activities

3

We need a sustainable process to monitor all risks

4

Risks need to be quantified comprehensively

5

We need to know the economic impact of our largest risks

6

Shareholders demand a risk/return framework

7

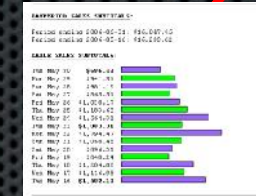
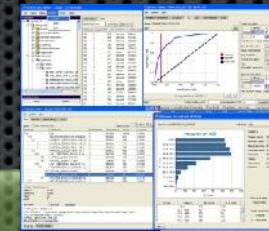
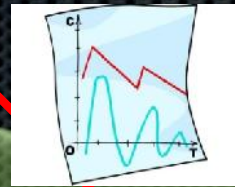
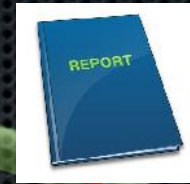
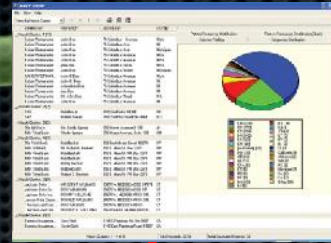
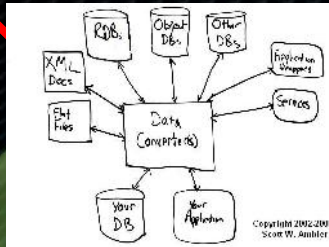
Decision making across firm is linked to building economic value

GRC lives here

ERI lives here

Current State – Challenges

- Organisations collect disparate information on risk, event and compliance from different sources in different formats at different levels of sophistication and accuracy
- 3 separate pieces of information
- Information must be collated to create something meaningful
- Reported to different levels of the organisation and different sections



Event Data

Risk Data



Compliance Data

ERI

With the right information:
Accurately understand the
factual condition, take
prioritised action to reduce the
adverse impacts and increase
the potential for success.



Current State – Market Challenges

- Following the latest global economic crisis, organisations are still operating in volatile, highly changeable risk and compliance environments
- In a Deloitte and Forbes 2012 survey of 192 executives, 91% planned to reorganise and reprioritise their approaches to risk management
- How will organisations handle increased volatility?
- Respondents indicated that a centralised approach will likely continue - **ERI**

Driving forces behind the adoption of ERI

External Factors

- Broader scope of risks arising from:
 - Globalisation
 - Industry consolidation and deregulation
 - Increased regulatory attention to corporate governance
 - Competition – more offensive and strategic approach to risk management
 - Technology etc.
- New technologies/systems to manage risk, event and compliance to facilitate ERI

Internal Factors

- Consequences and penalties for non-compliance to regulation
- Board and stakeholder requirements for information (corporate boards under regulatory pressure to address risk management)
- Link to shareholder value and achievement of organisation's goals.

ERI-Global Evolution

- Country risk management – different economic, political or environmental conditions that may adversely affect an organisation's exposure in that country
- These conditions also restrict the ability of organisation's ability to implement ERI particularly in low income countries:
 - Increased volatility
 - Commodity price risk
 - Global financial markets volatility
 - Political turmoil
 - Overall cost
 - Access to resources (and skilled resources).

What are the cultural variations and success of the evolution of ERI in different global regions?

- USA – financial and medical focus with public image considerations high
- Asia – true ERM compliance focus (ISO driven)
- UK – safety evolved risk plus insurance / finance focus
- Europe – soup mix (German and France leaders)
- Leaders come from the Commonwealth - Canada, Australia, New Zealand & UK

How does this 'quality circle' of Risk, Events and Compliance operate in business? (Event Management)



- Events tell us about our **Risk Management** processes, eg. An event is a risk that eventuated!
 - How effective are our controls?
 - Did we identify this as something that had the potential to happen?
 - Are our risk assessments accurate?
- Best Practice organisations analyse events and not only put in place Corrective Actions but Preventative (mitigating) treatments.

How does this 'quality circle' of Risk, Events and Compliance operate in business? (Event Management)



- They tell us about our **Compliance Management**, eg. An event is also a lack of; or break, in compliance to law, policy, procedure, licensing, standards, etc.
 - Were controls that should have been implemented actually in place?
 - Were there non-conformances or non-compliances?
 - Did we implement our policies and procedures?
- Events also identify and measure breaches in relevant compliance obligations that contributed to the event. This helps organisations prioritise compliance obligations.

How does this 'quality circle' of Risk, Events and Compliance operate in business? (Event Management)

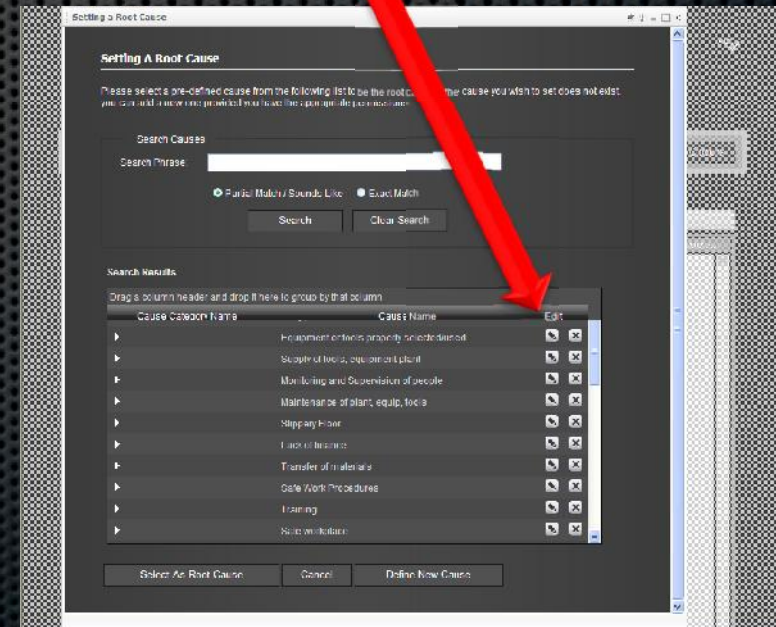
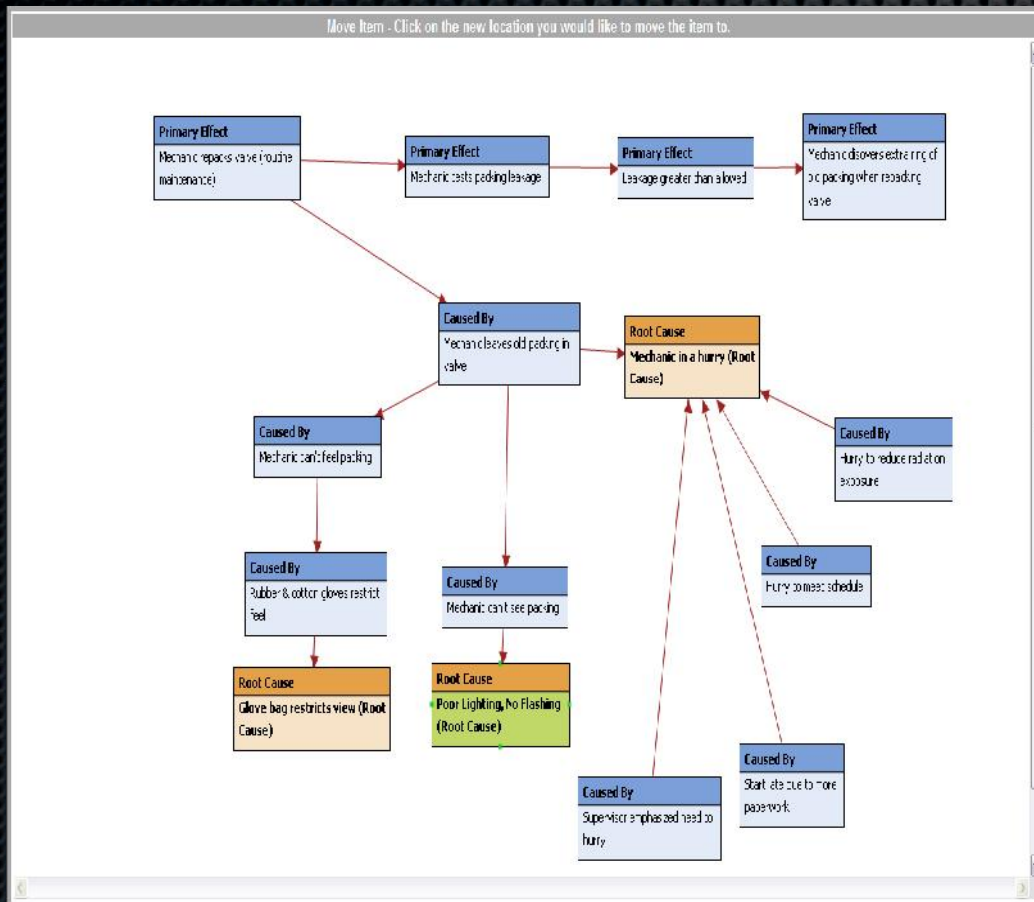


- Learning from Events is also about understanding why the event happened and linking it back to Risk and Compliance management
- Event causation and **Risk** mapping
 - The link is vital in becoming a Learning Organisation (prevention not reaction).
- Event causation and **Compliance** mapping
 - The link is vital in becoming a Learning Organisation (prevention not reaction)

Learning from events



Causation analysis links risk and compliance frameworkswhat obligations where non compliant that contributed to this event and what risks are associated?



Mapping Causation to Risk

RMSS **riskmanager** Logout Andrew Howarth

[risks](#) [compliance](#) [events](#) [enhancements](#)

[Risks | Identify](#) [Identify](#) [Assess](#) [Control](#) [Monitor](#)

[Add Risk Area](#) [Search Records](#) [Add New Risk](#) [Notes & Documents](#) [Identify Risks](#)

[Add Risk Type](#) [Clear Filters](#) [Copy Record](#) [Delete Record](#)

Assessment Record Number: 59

Operational Sector:

Port Location:

Division / Department:

Risk Area:

Risk Type: [Search](#)

Selected Risk

Risk Description
Created from Incident 1071

What are the consequences if this risk eventuates?

What controls are currently in place?

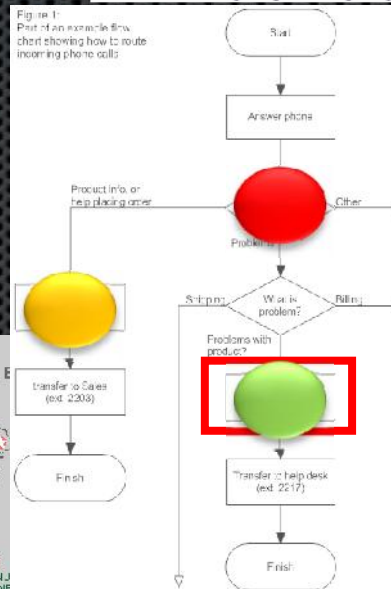
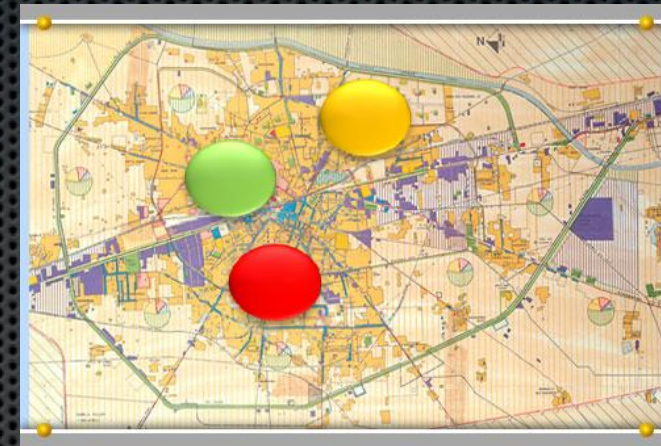
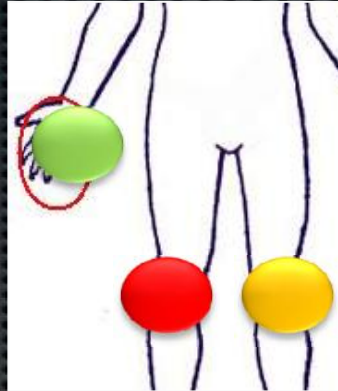
What additional controls do you recommend?

[Open Assessment Calculator](#) [Calculate Risk Scores](#) [Assign Actions](#) [Delete Selected Risk](#)

Risk	Consequence	Likelihood	Residual Risk
<input checked="" type="radio"/> Mechanic in a Hurry	<input type="text"/>	<input type="text"/>	<input type="text" value="- (0)"/>
<input type="radio"/> Poor Lighting, No Flashlight	<input type="text"/>	<input type="text"/>	<input type="text" value="- (0)"/>
<input type="radio"/> Glove Bag Restricts View	<input type="text"/>	<input type="text"/>	<input type="text" value="- (0)"/>

RMSS
Reduce Risk

Learning from events – the physical relationship

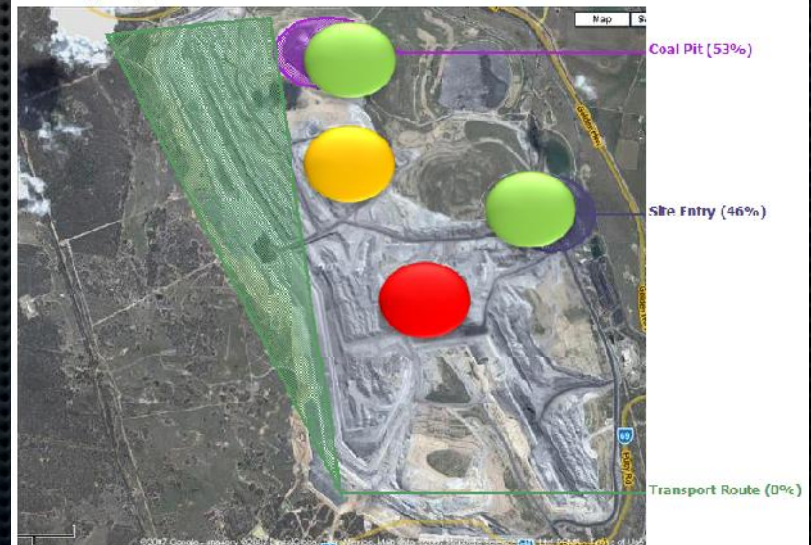


Victoria

Incident Image Hotspots

Occurrence Date: 1 Feb 2007 TO 17 Jun 2008

Incident Type: Injury



Escalating events on the basis of risk (potential outcome) not just severity (actual outcome)

Incident Classification

☒ HSE Incident ☐ Other Incidents (Excluding Hazards)

Incident Potential Risk Assessment

Assessment Model / Master Category: AS:1360 - Corporate

Consequence	Likelihood	Residual Score
Catastrophic	Likely	Extreme (24)

Incident Occurrence Details

Occurrence Date: 10 Feb 2011 06:42 AM

Incident Type: Injury / Illness

Incident Severity: C - Low

Incident Classification

☒ HSE Incident ☐ Other Incidents (Excluding Hazards)

Incident Potential Risk Assessment

Assessment Model / Master Category: AS:1360 - Corporate

Consequence	Likelihood	Residual Score
Moderate	Likely	High (17)

Incident Occurrence Details

Occurrence Date: 10 Feb 2011 06:42 AM

Incident Type: Injury / Illness

Incident Severity: A - High

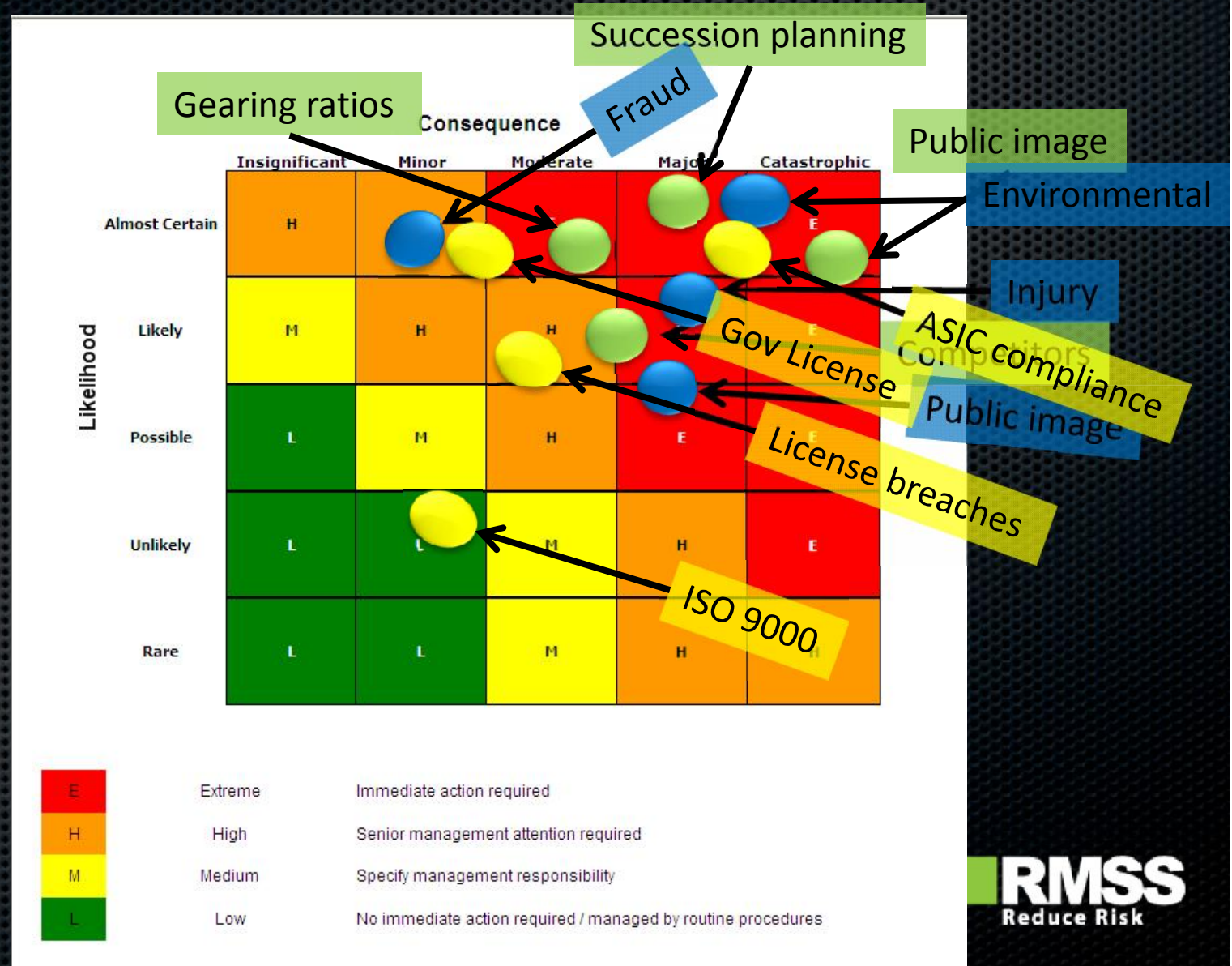
Learning from events – the functional relationship



Top Risks

Events with Highest Risk

Significant compliance breaches



How does this 'quality circle' of Risk, Events, and Compliance operate in business? (Compliance Management)



■ Compliance is a critical element of the **Risk Management** and **Event Management** process:

- Through the management of control frameworks
- Through identifying a lack of or a break in compliance obligations (control frameworks)
- By ensuring the delivery of critical actions (eg. disaster recovery, business continuity, corrective actions, etc.)

Using Compliance methodologies in Risk Management by auditing control frameworks



1. Are the processes needed for the quality management system in place throughout the organisation as identified?

Yes ☒ No ☐ Not Applicable ☐

Observations:

Actions:

2. Is the sequence and interaction of these processes being determined?

Confirmed ☒ Not Applicable ☐ Not Determined ☐

Observations:

Actions:

A negative response is automatically a risk...

RMSS riskmanager

Identify

Assessment Record of Hazard: 9

Selected Risk: **Terminated User Agreements**

Risk Treatments Required: Respond to users within required timeframes

Status of Risk Treatments: POC was in users on 14/01/03 regarding confirmation of language. POCs represent potentially exposed as funds committed to X80110. If project does not proceed, POC potentially exposed as funds committed to X80110 should project not proceed.

What are the consequences of this hazard? POC potentially exposed as funds committed to X80110 should project not proceed.

Risk	Likelihood	Consequence	Residual Risk
Terminated User Agreements	Unlikely	Minor	Low (10)
Terminated User Agreements	Unlikely	Catastrophic	High (10)

RMSS riskmanager

Control

ASIXLabel: Sydney Harbour - Port Project - Finance - Financial Management Plan

Risk: Terminated User Agreements Category: Financial Risk Management

Risk Description: User Agreements are terminated as fixed timeframes for approvals for X80110 not met, ie. 30/06/05 and 31/12/05.

Current Control Measures: Respond to users within required timeframes

What controls are currently in place? POC was in users on 14/01/03 regarding confirmation of language. POCs represent potentially exposed as funds committed to X80110. If project does not proceed, POC potentially exposed as funds committed to X80110 should project not proceed.

What are the consequences of this hazard? POC potentially exposed as funds committed to X80110 should project not proceed.

Assessment Date: 13 Jun 2008 Risk Score: 5 Moderate Projected Risk Score: 4 Low

Open Actions: Create New Action, Add Completed, Email Notification, Delete Action

Previous Control Statements for this Risk: User Agreements are terminated as fixed timeframes for approvals for X80110 not met, ie. 30/06/05 and 31/12/05.

Control Statement: User Agreements are terminated as fixed timeframes for approvals for X80110 not met, ie. 30/06/05 and 31/12/05.

Programme Statement for this Risk: User Agreements are terminated as fixed timeframes for approvals for X80110 not met, ie. 30/06/05 and 31/12/05.

Action: Respond to users within required timeframes

Progress And Notes:

Control Type: Action Due Date: 20 Jul 2008

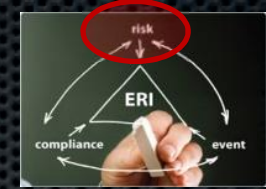
Programme Responsible: Responding Emergency Action/Change

%Reduction: 20 %

%Cost: 213221.0

Justification Score: 150 Must Be Done

What are we seeing in 'best practice' organisations?



RMSS Logout Admin Admin

riskmanager risks compliance incidents enhancements

➔ Risks | Identify Identify Assess Control Monitor

Add New Item Search Records Add New Risk Notes & Documents

Add Risk Type Clear Filters Copy Record Delete Record Identify Risks

Assessment Record Number: 8 Selected Risk Save Draft

State: New South Wales

Region: New South Wales Region

Location: Albury

Basel Level: Systems

Operational Risk Category: Search Policy Health & Safety

Risk Description

Unsafe Health & Safety - Work Practices or equipment in use due to poor understanding of responsibilities

Contributing Factors (what causes the risk to happen?)

Staff undertaking hazardous tasks or performing unsafe acts due to lack of knowledge and/or understanding of risks

Key Risk Indicators / Mitigating Practices

Staff awareness sessions provided; Managers required to monitor staff workplace

Consequences

Open Assessment Calculator
Calculate Risk Scores
Assign Actions
Delete Selected Risk

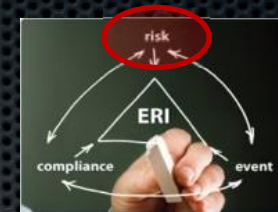
Risk	Likelihood	Consequence	Residual Risk
Illegal Acts	Almost Certain	Extreme	Very High (20)
Mismatch between growth and systems development	Likely	Moderate	High (15)
Poor Commitment to Control	Possible	Moderate	High (14)
Remote Locations	Possible	Minor	Medium (9)
Business Strategy	Unlikely	Moderate	Medium (6)
Complex organisational structures	Unlikely	Moderate	Medium (6)
Continuous profitability	Unlikely	Minor	Low (4)
Environmental Aspects	Rare	Low	Low (1)

RMSS Reduce Risk

A bank

- Risk identified (*using a Basel 2 checklist*) to regional business line (*operational*)
- The top risk (*highest*) meets the criteria (*either individually or collectively*) with the same risk
- Identifies across multiple regional business lines and is included in the strategic risk register while the other risks are not

Strategic risk is driven from business operations



RMSS
riskmanager

Home | Compliance | Incident | Performance

History | Analyse | Control | Monitor

Report

Risk Register

Individual Risk Treatments

Completed Risk Treatments

Overall Risk Treatments

Account Risk Treatments

Summary

Summary Completed Risk Treatments

Open Risk Treatments & Estimated Cost

Unassigned Risk

Uncontrolled Risk

Health & Safety

Top Risk

Today Summary

High-risk Internal

Risk Score

Completed Action Costs

Planned Action Costs

Risk Matrix

Action Report

Treatments Report

History

RMSS
Reduce Risk

Top Risks

Operational Risk Category	Communication - Health & Safety	Risk Level	People
Risk	Risk Description	Average Score	Times Identified
Communication	Inadequate/inappropriate work procedures and safety training	11	1
Communication	Inadequate/inappropriate supervision over third party contractors/operators	13	1
Communication	Office based staff carrying out repetitive admin based tasks	13	1
Communication	Loss of hearing to personnel due to noise exposure	6	1

Operational Risk Category	Control - Health & Safety	Risk Level	Systems
Risk	Risk Description	Average Score	Times Identified
Operational Control	Staff employed in screen based work suffering eye strain and/or injury	14	1
Operational Control	Inadequate maintenance on eyewear and portable showers	11	1

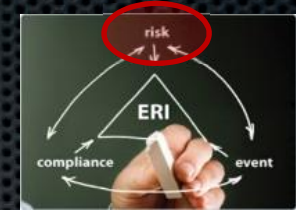
Operational Risk Category	Corporate - Operational	Risk Level	Systems
Risk	Risk Description	Average Score	Times Identified
Storage Market Share	Loss of market share to competitors	22	1

Operational Risk Category	Documentation - Health & Safety	Risk Level	People
Risk	Risk Description	Average Score	Times Identified
Environmental Management System Documentation	Staff are potentially exposed to rotating plant &/or machinery while carrying out duties &/or maintenance activities	22	1
Environmental Management System Documentation	Staff driving machinery (tractor, loader etc.) on public roads may be involved in an accident	22	1
Document Control	Accidents as a result of the lack of on-site safety training and awareness	20	1
Document Control	Staff driving machinery (tractor, loader etc.) on the airframe may be involved in an accident	17	1
Document Control	Staff performing maintenance are potentially exposed to HV Electrical Systems while carrying out maintenance activities	15	1

Thursday, 26 November 2009

Page 1 of 3

Operation risk is managed at the business 'coal face'



RMSS
risk manager

Logout Admin Admin

Identify Assess Control Monitor

Risk Worksheets Custom Reports

Number of Assessments: 81

State:

Region:

Location:

Report Level:

Operational Risk Category: Search

Master Category:

Risk:

Assessment Date:

Date Range: to

Responsible Person:

Risk Owner:

Risk Rating:

Legal Status:

Case Filter

Risk Register

Individual Risk Treatments

Completed Risk Treatments

Overdue Risk Treatments

Recurring Risk Treatments

Summary

Summary Completed Risk Treatments

Open Risk Treatments & Estimated Cost


Unassessed Risks

Uncontrolled Risks

Identified Risks

Top Risks

Holistic Summary


RMSS
 Reduce Risk

Risk Register

Location: Queensland - South East Queensland - Brisbane - Banking Centres - Banking Solutions

Assessment Type: Issue 2

Assessment Category: Fraud

Master Category: Internal Fraud

State / Branch / Business Unit	Queensland - Brisbane - Banking Centres	Region / Business Line	South East Queensland - Banking Solutions	
Assessment Record: 10	Risk Category: Internal Fraud - Fraud			
Risk	Risk Description	Contributing Factors (what causes the risk to happen?)	Residual	Risk Owner
* Continuous profitability	Continuous profitability in excess of organisation and industry standards	Customers and Staff	Significant (21)	Andrew Howarth

Mitigating Practices / Controls

Consequences

Risk Treatment Description	Control Statement	Responsible Person	Due Date	Cost Progress/Notes	Control Type
Risk	Risk Description	Contributing Factors (what causes the risk to happen?)	Residual	Risk Owner	
* Business Strategy	Clearly defined business strategy; no "buy in" by managers and staff		High (14)	Andrew Howarth	

Mitigating Practices / Controls

Consequences

Risk Treatment Description	Control Statement	Responsible Person	Due Date	Cost Progress/Notes	Control Type
Risk	Risk Description	Contributing Factors (what causes the risk to happen?)	Residual	Risk Owner	
* Complex organisational structure	Complex organisational structure		High (14)	Andrew Howarth	

Mitigating Practices / Controls

Consequences

Risk Treatment Description	Control Statement	Responsible Person	Due Date	Cost Progress/Notes	Control Type
Risk	Risk Description	Contributing Factors (what causes the risk to happen?)	Residual	Risk Owner	
* Poor Commitment to Control	Poor commitment to control and a bad reputation		Medium (10)	Andrew Howarth	

Generated on Monday, 2 March 2009 4:37:57 PM

Page 1 of 4

Risk	Risk Description	Contributing Factors (what causes the risk to happen?)	Residual	Risk Owner
* Remote Locations	Remote locations that are poorly supervised and the existence of secure related banking lines		Medium (10)	Andrew Howarth

Mitigating Practices / Controls

Consequences

Risk Treatment Description	Control Statement	Responsible Person	Due Date	Cost Progress/Notes	Control Type
Risk	Risk Description	Contributing Factors (what causes the risk to happen?)	Residual	Risk Owner	
* Absence of two or more (and) systems development	Absence of two or more (and) systems development		Medium (10)	Andrew Howarth	

Mitigating Practices / Controls

Consequences

Risk Treatment Description	Control Statement	Responsible Person	Due Date	Cost Progress/Notes	Control Type
Risk	Risk Description	Contributing Factors (what causes the risk to happen?)	Residual	Risk Owner	
* Illegal Acts	Illegal acts of any sort		Very Low (3)	Andrew Howarth	

Mitigating Practices / Controls

Consequences

Risk Treatment Description	Control Statement	Responsible Person	Due Date	Cost Progress/Notes	Control Type
Risk	Risk Description	Contributing Factors (what causes the risk to happen?)	Residual	Risk Owner	
* Illegal Acts	Illegal acts of any sort		Very Low (3)	Andrew Howarth	

Mitigating Practices / Controls

Consequences

Risk Treatment Description	Control Statement	Responsible Person	Due Date	Cost Progress/Notes	Control Type
Risk	Risk Description	Contributing Factors (what causes the risk to happen?)	Residual	Risk Owner	
* Illegal Acts	Illegal acts of any sort		Very Low (3)	Andrew Howarth	

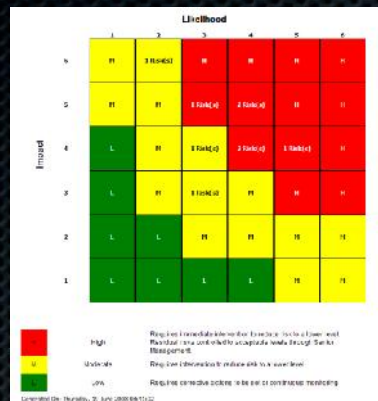
Generated on Monday, 2 March 2009 4:37:57 PM

Page 2 of 4

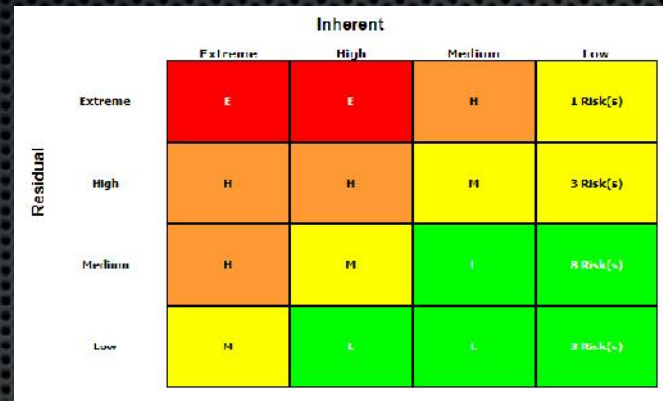
Disparate risk methodologies cascade into a strategic risk register



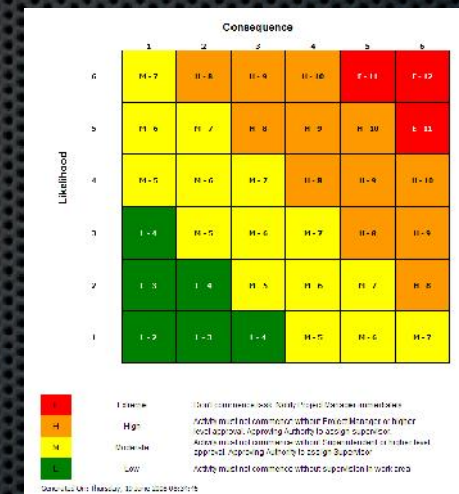
Health and Safety



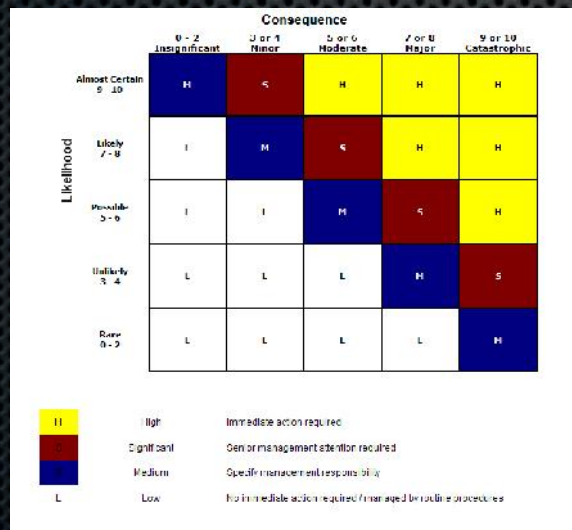
Environment



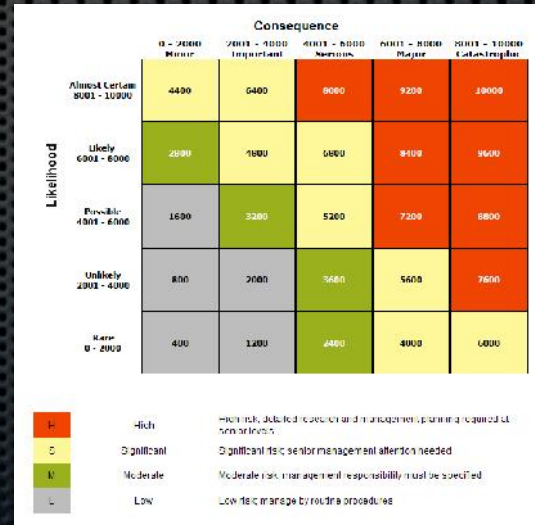
Major projects



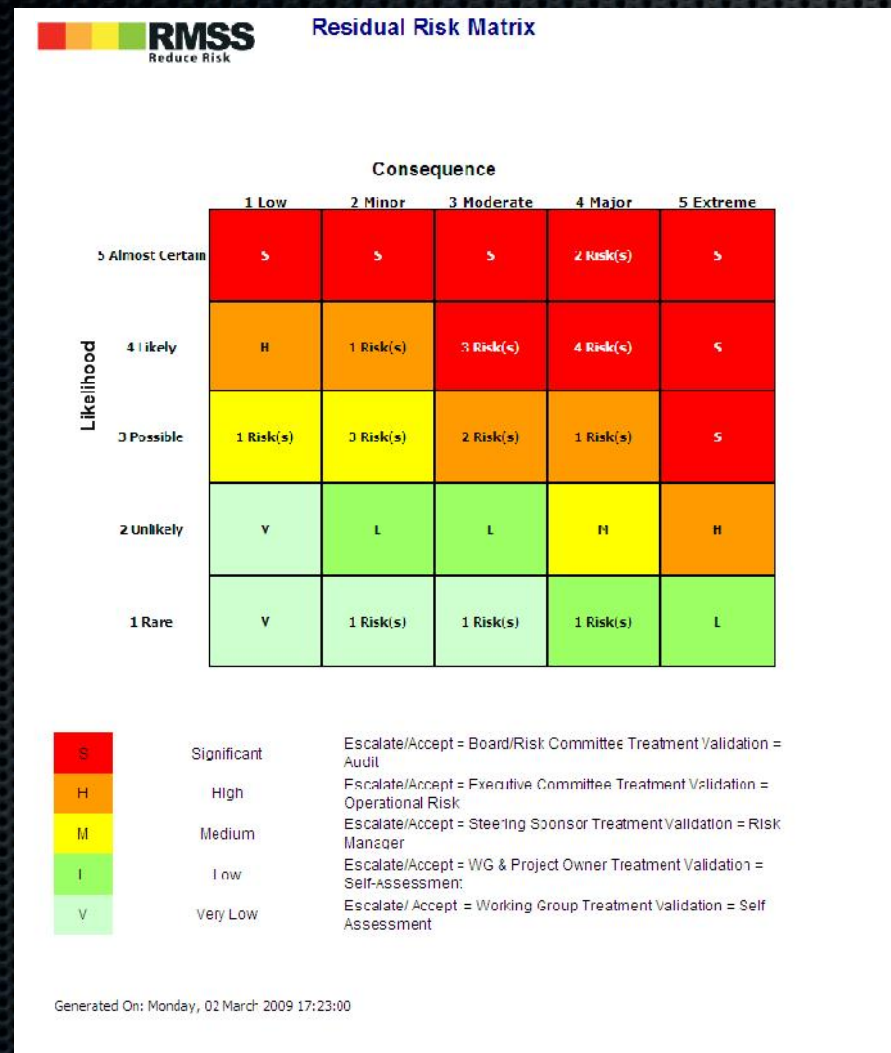
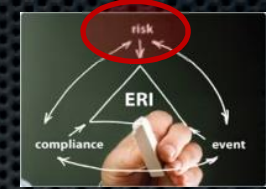
Finance



Security



Disparate risk methodologies cascade into strategic risk register



Different risk models with different consequence values allows operational risks to cascade UP the organisation to form a LIVE enterprise risk register which is capturing the current top risks of the business.

Enterprise Risk Intelligence Evolution

↑
VALUE ADD FOR ORGANISATIONS

Process to best practice ERI

Reaction

Prevention



Notify of events



Investigate events



Corrective actions to prevent further events from occurring



Compliance process to audit/test control frameworks/corrective actions



Introduction of risk – risks identified from investigations and auditing of control framework



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



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



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

TIME →



What about the separation of powers and practices between different functions?

- ERI involves extracting the intelligence or information out of the disparate areas and combining it at an enterprise level
- Where there is a **real** need for segregation, eg. the compliance team are audited by the audit team (organisationally separated), this can still exist through well designed security modeling of groups and roles.

Are there any additional costs associated with ERI?



■ ERI actually costs less than current state!

- One system vs. multiple systems
- Time saved in manually collating data
- Reduces incorrect information risk (better decisions, less cost to organisation)
- Flexibility in allowing multiple concurrent different work flows and terminologies meaning change management and training costs reductions.

ERI advantages – What are the Strategic benefits?

- More effective advance strategic and operational planning – one source of truth!
- A structured, more formal approach to decision making
- Greater confidence in decision making and achieving operational and strategic objectives (reduced information risk)
- Improved competitive standing.

Summary

- ERI integrates the key areas of risk, compliance and event management across an organisation/enterprise to unlock the following capabilities:
 - The ability to measure the organisation's risk management process through the analysis of events
 - The ability to identify breaches in compliance as a risk
 - Prioritise breaches and corrective actions through the risk assessment of compliance obligations
 - Escalate events on the basis of risk

Summary

- ERI is a process and a journey and can not be achieved overnight
- Organisations also face challenges such as:
 - Resistance to change
 - Traditional (restrictive) views of risk management
 - ERI is still an evolving process.

Presented by Andrew Howarth, CEO, RMSS

- Phone: +614 7 3252 1400
- Email: enquiries@rmss.com.au
- Web: www.rmss.com.au

Copyright and Disclaimer

Copyright© 2012 Risk Management and Safety Systems Pty Ltd, all rights reserved. The **riskmanager**, **eventmanager**, **compliance**manager, **claims**manager, **chemical**manager, **competency**manager, **content**manager, **health**manager, **permit**manager, are trademarks or registered trademarks of RMSS. All other trademarks acknowledged. Elements of the Risk Management and Safety Systems Pty Ltd applications described in this document are protected by Australian Registered Patent 2006100476 and other Australian and international patents pending.

