



Society of Actuaries in Ireland

Risk Management Perspectives Conference

18th November 2014

A banker's perspective on risk management

Peter Rossiter

**Former Chief Risk Officer – AIB, IBRC, Citi
Handlowy**

**Society of Actuaries in Ireland
18 November 2014**

Risk Management six years after the crisis

Reminder: any crisis can be divided into four phases, e.g. the Irish banking crisis:

1. Diagnosis: combination of an extreme liquidity and credit stress event caused by over-reliance on wholesale funding to finance imprudent property-related lending
2. Quantification: ECB/EBA Comprehensive Assessment indicates the impact now largely accounted for within lenders' balance sheets, including impact of NAMA, but final 'cost' not yet determined

Risk Management six years after the crisis - *contd.*

3. Correction: loan restructuring and recovery processes
now largely in place
4. Prevention: lessons learned? Policy response?
Preparations for next 'crisis'

Where are we now?

Somewhere between 3 and 4 – loan recovery processes in place but re-default rates undetermined. Unprecedented policy response largely developed and under implementation

Diagnosis – key findings from Nyberg *

- '...unhindered expansion of the property bubble financed by ...wholesale market funding'
- '...speed and severity of the crisis was made worse by world-wide economic events...'
- '...banks set aggressive targets for profit growth....without the necessary corresponding strengthening of governance, procedures and practices'

* Report of the Commission of Investigation into the Banking Sector in Ireland. March 2011

Diagnosis – key findings from Nyberg * - *contd.*

- ‘...quite generally accepted that - traditionally volatile - market funding would continue to be available ...’
- ‘...totally unprepared for both of their key risks (property loan impairment and funding problems) occurring simultaneously’
- ‘...it appears now, with hindsight, to be almost unbelievable that intelligent professionals in the banking sector appear not to have been aware of the size of the risks they were taking’

* Report of the Commission of Investigation into the Banking Sector in Ireland. March 2011

Diagnosis - roles of business and risk management – more from Nyberg...

Business (first line of defence)

- *'...management had forgotten the very nature of credit'*
- *'...emphasised loan sales skills above risk and credit analysis skills'*
- *'...governance, systems and processes were also inadequate, exposing the covered banks to significant but often unrecognised operational risk'*

Risk (second line of defence)

- *'...In Anglo, credit risk management structures were inadequate'*
- *'...INBS's credit management was unusual in many respects'*
- *'...The Risk function in Anglo was inadequately resourced and did not have the conviction necessary to ensure compliance with credit policy'*



**Risk
Culture**

Correction phase – key components

- NAMA formed to manage land and development loans – showing strong progress in restructuring and recovery and repayment of NAMA bonds expected ahead of schedule
- Private Equity funds injected liquidity, helped establish a market for distressed assets and restore confidence in asset values
- Banks formed significant restructuring and recovery functions for other real-estate, SME and mortgage related debt
- Legal infrastructure initially held back by Dunne judgment but now becoming a credible threat to non-cooperative debtors

Correction phase – key components *contd.*

While the scale of the above should not be under-estimated, banks are also expected to support viable enterprises and economic recovery – and are largely doing so

*The challenge for risk management is to ensure optimum focus on both **front book lending** and **back book recovery***

Prevention phase – key components

Unprecedented scale of policy response, including:

- CRD IV / CRR – sets out rules for quality and quantity of capital, liquidity, leverage, remuneration, risk governance, etc. and is part of the ‘Single Rule Book’ to ensure a uniform legislative framework across Europe
- European Markets Infrastructure Directive (EMIR) – increasing the transparency over derivatives in Europe
- Central Bank of Ireland initiatives, including Fitness & Probity regime, macro-prudential proposals on mortgage lending, etc.

Prevention phase – key components *contd.*

Unprecedented scale of policy response, including:

- Central Bank of Ireland initiatives, including Fitness & Probity regime, macro-prudential proposals on mortgage lending, etc.
- European initiatives, including Banking Union (Single Supervisory Mechanism, Single Resolution Mechanism, Deposit Guarantee Scheme)
- Enforcement impacts, e.g., on Anti-Money Laundering, Sanctions, Payment Protection Insurance, mis-selling of derivatives, LIBOR rigging etc.

What does this mean for Risk Management in 2015

Three broad themes:

1.Regulatory:

- Demands on risk and control functions are expected to continue to increase, putting pressure on costs and business returns
- The Single Supervisory Mechanism will have a profound impact in expecting 'best practice' risk management across Europe, including in the area of data governance
- Huge fines / low (zero) tolerance for regulatory breaches will continue to curtail risk appetite, with some risk of unintended consequences.

What does this mean for Risk Management in 2015

1.Regulatory – *contd.*:

- Recovery and resolution planning (living wills) will result in structural changes to banks' operations (to protect critical functions) and balance sheets (to ring-fence Total Loss Absorbing Capacity)

What does this mean for Risk Management in 2015

2. Consumer Protection

- Conduct risk management is not only a regulatory imperative but a business necessity to protect reputations, enhance customer satisfaction and build sustainable franchises
- Typically linked to high profile mis-selling scandals such as Payment Protection Insurance in the UK, conduct risk management now incorporates other risks such as IT resilience, data protection, cyber crime or market rigging

What does this mean for Risk Management in 2015

3. Risk Culture

- Most bankers accept that a change in risk culture is desirable - it will take time to complete
- An increasing area of focus for risk management – developing measurement tools etc. – but ultimately the ‘tone is set from the top’

Thank You



Society of Actuaries in Ireland

Managing Cyber Risk

18 November 2014

Managing Cyber Risk

Phil Whittingham, XL Group

Head of Risk Policy, Process and Model Validation

Disclaimer:

The material, content and views in the following presentation are those of the presenter and do not necessarily represent those of XL Group plc.

Agenda

- Context “traditional view” v “new view”
- Definition
- Cyber Security in context of ERM Framework
- Some detailed examples
- Conclusions

Traditional view of 'IT Security'

- World of IT technology and networks
- Behind the scene – seen as back office operations
- Worms – viruses – spam – patches
- Keeping the technology safe – keeping the lights on
- Down time due to security glitch
- Taken for granted
- NOT a business issue – someone else's problem to fix it for the business

x . Π=ks□7rβUâÿ0f\»±' □π™%ã*–” }çX□f¥s*%çM-\$æ^%LQVô{òGÓ†À` □0ØΠPq⊗©~ □z•F£Bh□□⊗□≤úêá,,ó
??□Ǣ;□□=>□~ÿìÁ8' »q□□ç£□□□□%ÇávÿÙ∞⊗ÿ§áæ“ □l x□B□GÍF` □ôòf>{>◇İ□□B>9□j ä, | àÑ“ İ□<ü/nçô
>ì%Â□´“;©à≤` |xvÿß•□=üfl□□^ΠÃ«ï?{>|Ã¶ÿ9<ûá“□B□□□5µ6#€9€´~≤□, W□†áYwøÀÍÎY`uH`□í F·c2
ôÇ-Ω€Wóïf©[BñİÔæ;·gbs·;y±⊗1lİäæéç”Ë-≥~À“óí□c”-<ΠØ...Ímc□≠«†”ÓovÆ!J´æ8ÅN8@wÜÏH, <⊗“U
“€€=ôñ, °/⊗j□, éXÿ8ÿ⊗□â5]ÊxÉ·ÚBb1Ø2úuóÇòİø[; &~†¶f...ñ`M»Ô□;□#□wÂìΠ≥□j`Öì, ÂÙY, âÂí´√□È
[□□Ê`≠□Σ9b□ÿÂTâ\ö°?-tA=üñâæÕ°ÙB. †íé¶À. †ÿ□†´;£í αÙqM#¤%Ã<ÒÖÏìNVÂì´>□/°†)\□#İ{ÅÙ/!

New View

“In the 2014 survey most organisations (67%) said they are facing rising threats from information security, but over a third admit (37%) they have no real-time insight on cyber risks in order to combat these threats.” EY Global Information Security Survey

“Cybersecurity is now a persistent business risk. It is no longer an issue that concerns only information technology and security professionals; the impact has extended to the C-Suite and boardroom.” PwC Global State of Information Security Survey 2015.

Centre for Strategic and International Studies annual estimate of cybercrime cost (globally) is \$375Bn-\$575Bn.

“20% of all cyber crime impacts financial services.” IBM Cyber intelligence Report 2014.

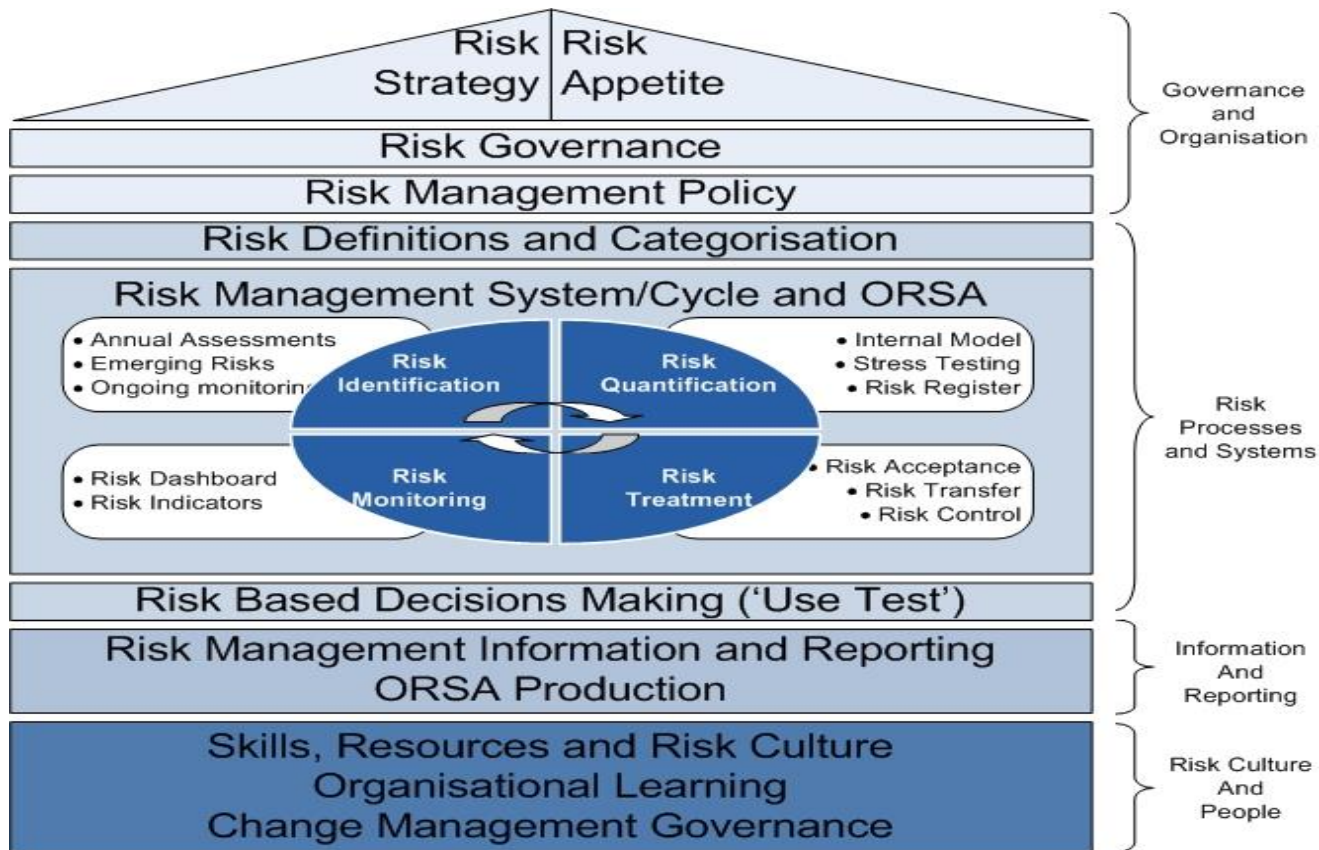
Average cost of a data breach investigation and clean-up is USD 620k (IBM)

Most companies do not detect even 1% of the security attacks every year....

Definition

“Cyber risk is loss or damage arising out of unauthorized access to, use of, disclosure of, disruption of, modification or destruction to information and information systems.”

Cyber Risk in the ERM Framework



Cyber Risk and Information Security at XL Group

Strategy

Defense-in-depth program that integrates people, process and technology to prevent, detect, respond to, and recover from information security events, threats, and risks.

Mission

Design, implement and maintain an information security program that:

- ensures the secure operations of our businesses
- supports business entry into new products, services, and applications
- protects XL's data, customers, and colleagues
- ensures the confidentiality, integrity, and availability of XL information
- complies with regulatory requirements

Tactical solutions

	Confidentiality	Integrity	Availability
Prevent	Policies – Training & Awareness - Network Access Control – Procurement		
	Network firewalls Vulnerability Assessment User Authorization Secure Email Remote Access (VPN) Laptop Encryption Data Loss Protection	Code Review Anti-Malware Software Laptop Firewall Intrusion Prevention (IPS)	DMZ Architecture User Provisioning Intelligence Alerts 3 rd Party Connectivity Content Filtering
Detect	Annual External Testing		
	User Authentication Audit Logs Intrusion Detection (IDS) Internet Monitoring Data Loss Protection	Server Monitoring Database Monitoring	Managed Security Service Provider Network Operations Center
Respond	eDiscovery		
	Patch Management Forensics	Forensics	Vulnerability Scanning CSIRT – Incident Response
Recover			
	Password reset	Back up procedures	Disaster Recovery

People Process Technology

Cyber Security Risks & Mitigation at XL

Risk	Mitigation at XL Group
Data Mobility (Laptops, Smart phones, USB tokens) Physical loss Data loss	Laptop full disk encryption Encrypted USB devices Blocking external storage devices (USB, CD, DVD) Smart Phones access and use governed by Mobile Device Management (MDM) Software including remote wipe capabilities
Cloud services, third party providers and other outsourced arrangements	Private cloud solutions only (public cloud prohibited) Contracts with Service Level Agreements (SLAs) and policy enforcement including strong authentication Audits
Insider threats including malicious and accidental	Data loss prevention (DLP) software Access & entitlement reviews Awareness & Training
Phishing Attacks Spear Phishing (specific target attack) Whaling (specific target attack against senior executives)	Spam filters Anti-malware, anti-virus Training & Awareness
Hacked system, network, or application including Hactivism, Cyberterrorism, Nation State Attacks, and Advanced Persistent Threats (APTs)	Managed Security Service Provider (MSSP) Intrusion Detection (IDS) & Intrusion Prevention (IPS) Mandatory External Testing for internet facing apps Audit logs
Malicious code (Malware)	URL Filtering Software Development Lifecycle policy & program Code Reviews
Data Transmission	Encrypted internet transmissions Network authentication Encrypted file transfer capabilities
Paper records	Data loss prevention (DLP) software
Electronic back-up	Full back up tape encryption

C level risk issue - Fiduciary responsibility

- US President's 2013 Executive Order – National Institute of Standards and technology (NIST) Cyber Security Framework.
- SEC Guidelines
- EU Data protection Regulation (2015)
- Link risk and security to corporate performance
- CEOs, BoDs need to take a leading role in protecting the organization
 - Protect reputation, bottom line, share price
 - Need to know enough to ask the right questions of the CISO/CIRO

Formalized Risk Register for Cyber Risk

Stage of process	Activities undertaken
1. Identify risks	<ul style="list-style-type: none"> • Identify all material risks • Identify risk owners for each risk • Risk owners to confirm the risks and inform the ERM team of any new risks • Risk owners to update the Group Risk Assessment template
2. Quantify inherent risk	<ul style="list-style-type: none"> • Assess the inherent risk exposure for each risk (i.e. consider the impact of the risk without any controls or other mitigation strategies in place) • Use the scoring criteria to score the risk for its financial and reputational impacts, the potential impact of the risk and the likelihood of it occurring
3. Identify controls	<ul style="list-style-type: none"> • Identify the key controls for each risk (minimum of one key control per risk and maximum of five) • Provide an overall rating for the effectiveness of the top 5 controls • When rating control effectiveness, focus on how well the control reduces the impact of the risk in question as opposed to its probability and whether the control is operating as planned
4. Quantify residual risk	<ul style="list-style-type: none"> • Residual risks are to be scored using the same scoring criteria as inherent risks but bearing in mind the controls being used to manage the risk

It doesn't stop with the risk register – use other tools also – scenarios, loss data tracking, etc...

Conclusions

- While Cyber Risk isn't a "new" risk or an "emerging" risk, it is genuinely a risk where the risk profile is changing.
- C Level interest is increasing.
- Risk frameworks don't need re designing, but they do need to ensure that the components are sufficient to address the specific risk.



Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem

Whistleblowing / Protected Disclosures

Joe Gavin, General Counsel

18 November 2014



-
- Protection of Sources
 - The case of journalist's privilege: Mahon Tribunal v Keena & Anor
 - The Public Interest Test



-
- Central Bank (Supervision and Enforcement) Act 2013
 - Protected Disclosures Act 2014
 - SSM Regulations 2014



-
- Central Bank (Supervision and Enforcement) Act 2013 (“the Act”) introduces protections for persons making disclosures of breaches of financial services legislation to the Central Bank
 - This is the first piece of legislation to offer such protection in Ireland
 - The Act does not use the word “whistleblowing” but introduces the term “Protected Disclosure”



What is a Protected Disclosure under the Act?

A disclosure is a protected disclosure when a person makes a disclosure:

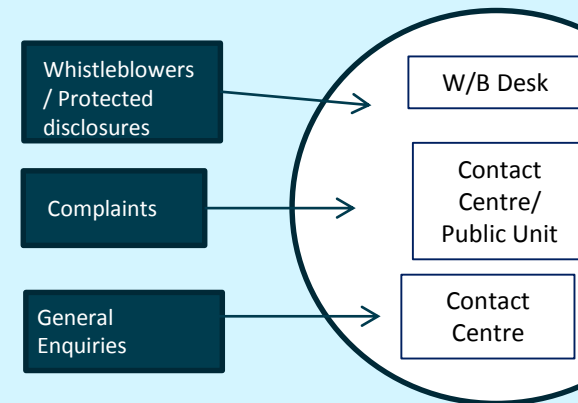
1. To an “appropriate person” (the Bank or an employee or authorised officer of the Bank)
2. In good faith
3. Has reasonable grounds for believing that either:
 - a) Financial Services law has been or is being broken or
 - b) Evidence is being/has been destroyed
4. They give their name

This is a very broad definition. It could encompass:

- A serious breach of financial services legislation
- A minor inadvertent breach of financial services legislation
- A complaint by a customer about a breach of the Consumer Protection Code by a regulated firm

How the Bank deals with Protected Disclosures:

Protected Disclosures go through separate channels, as this allows for special treatment for whistleblowers / protected disclosures



What protections are afforded to a Protected Disclosure?



Protections afforded to a Protected Disclosure

Protected Disclosure made by an Employee

1. The Bank may not disclose identity of employee except
 - With consent or
 - In so far as it may be necessary to ensure proper investigation
2. Employer cannot penalise employee (but not prevented from running business efficiently)
3. Employer may be prosecuted
4. Whistleblower protected from civil liability
5. Whistleblower has right of action in tort

Protected Disclosure made by a Person

1. The Bank may not disclose identity of person except
 - With consent or
 - In so far as it may be necessary to ensure proper investigation
2. Whistleblower protected from civil liability
3. Whistleblower has right of action in tort

What is the Bank required to do?

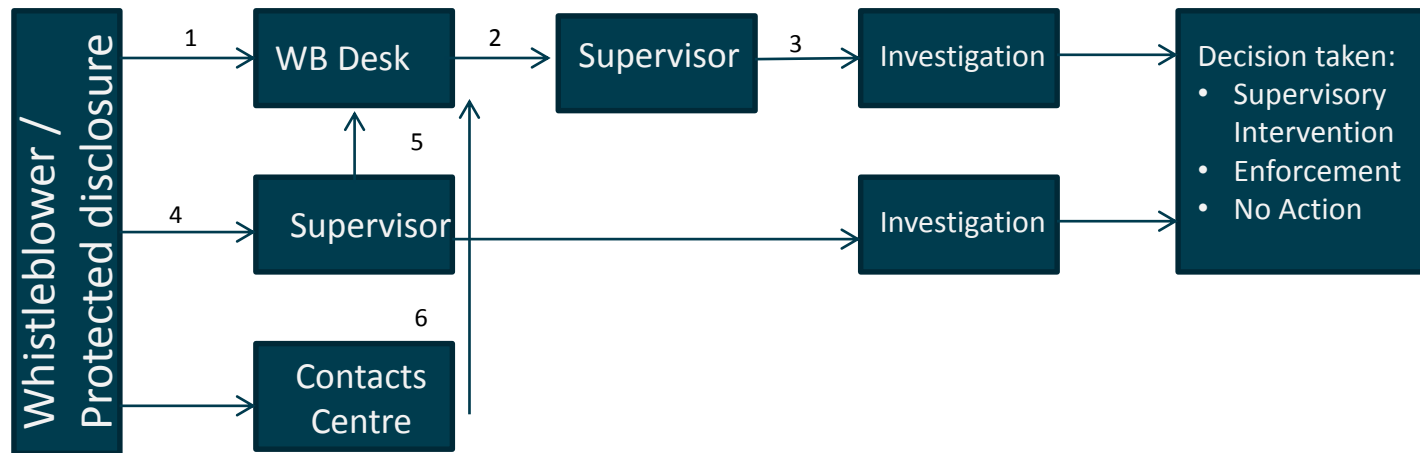
What does the legislation require the Bank to do in relation to Protected Disclosures?

The legislation is silent as to what action the Bank should take, other than not to disclose the identity.

Bank has established dedicated policies and processes to deal with whistleblower reports



Handling protected disclosures in the Bank



1. Dedicated Whistleblower telephone number and e-mail address set up. All contacts are handled by the Whistleblower Desk .
2. Having obtained the information from the Whistleblower, and provided some assistance, the Whistleblower Desk will forward the intelligence to the Supervisor.
3. The supervisor will review and decide whether to investigate the matter.
4. In some cases, a protected disclosure may be made directly to a Supervisor who can deal with the WB disclosure through to investigation if they wish.
5. The Supervisor informs the Whistleblower Desk of the contact so that a record can be maintained.
6. Contacts made via the Contact Centre which are from Whistleblowers will be forwarded to the Whistleblower Desk.



- Under S. 38(2) of the Act, a person performing a pre-approval controlled function (“PCF”) is required to disclose to the Bank information “which he or she believes will be of material assistance to the Bank” relating to:
 - A breach of financial services legislation
 - Evidence is being/has been concealed or destroyed
- Such a disclosure is a Protected Disclosure and the person making the disclosure is afforded the same protections as a whistleblower
- A PCF does not have to make a S. 38(2) disclosure if they have a “reasonable excuse”. A reasonable excuse for a person to fail to make a disclosure on the ground that the disclosure might tend to incriminate the person
- There is no offense/penalty for failing to make a S. 38(2) disclosure under the Act, but other actions may be taken by the Bank as part of Fitness and Probity assessment



- There will be some overlap between whistleblowing and PCF S.38(2) disclosures
- However the two disclosure mechanisms are kept separate in the Bank –
 - whistleblowers can call, email or send letters to the W/B Desk and may make anonymous disclosures. A telephone number and email address for whistleblowers are published on the Bank website: confidential@centralbank.ie
 - PCF's are required to complete a disclosure form providing information on the offence that was or is being committed, giving their contact details and PCF role. A separate email address is used: protecteddisclosures@centralbank.ie

Differences between Protected Disclosures Working Definitions



	Whistleblower	PCF Mandatory Disclosure	Personal Complaint	Personal Complaint on a systemic issue
Differences:	It is about an organisation	It is about a S38(2) disclosure and my organisation	It is about me	It is about me and maybe others
Contact might say:	“I want to report some wrongdoing in an organisation”	“As a PCF I am reporting a breach of financial services law in my organisation”	“I want my money back / I have been treated badly / in dealing with me the firm has breached financial services legislation”	“I want my money back / I have been treated badly by an organisation....and others may be affected too”

Differences between Protected Disclosures Working Definitions



	Whistleblower	PCF Mandatory Disclosure	Personal Complaint	Personal Complaint on a systemic issue
Differences:	It is about an organisation	It is about a S38(2) disclosure	It is about me	It is about me and maybe others
Contact might say:	"I want to report some wrongdoing in an organisation"	"As a PCF I am reporting a breach of financial services law in my organisation"	"I want my money back / I have been treated badly / in dealing with me the firm has breached financial services legislation"	"I want my money back / I have been treated badly by an organisation....and others may be affected too"
CBI Process	WB Desk	WB Desk	1. Complain to firm 2. Apply to FSO 3. CBI captures trends	CBI investigates or CBI captures trends
Protected Disclosure?	✓	✓	Yes if we are dealing with it	✓
Heightened protection of identity in CBI	✓			

All these disclosures are Protected Disclosures and require the Bank not to disclose the identity of the person making the disclosure

However a higher standard of confidentiality is applied for WB internally in the Bank



- Under the Act, the Bank may not disclose the identity of a person who has made a protected disclosure without first obtaining the person's consent except in so far as it may be necessary.....
- The Bank will maintain the confidentiality of the identity of the person making the protected disclosure
 - This is subject to some exclusions – e.g. where disclosure is necessary for the effective investigation of any matter by Bank or is required by law.
- While there is no legal requirement to keep a Whistleblower's identity confidential within the Bank, the Bank endeavours to maintain the confidentiality of the source in internal correspondence and discussions



- Public Consultation:
 - Consultation Paper CP79 : Handling of Protected Disclosures by the Central Bank of Ireland.
 - opened on 19/3/2014 and closed on 19/6/2014
 - Nine submissions received and considered
 - Feedback Statement and copy of submissions available on our website
- Industry letter:
 - Letter re: Protected Disclosures issued to all regulated firms on 5 November 2014. Outlines main provisions in the legislation and also the obligations on PCFs. Copy on Bank website.
- Website
 - <http://www.centralbank.ie/regulation/processes/protected-disclosures/Pages/Introduction.aspx>



-
- New Legislation implemented in July 2014
 - Focus of this legislation is to protect all workers from being penalised for whistleblowing
 - Central Bank is a prescribed person under the Act to whom workers can submit report in relation to breaches of financial services laws
 - Overlaps with Central Bank legislation on protected disclosures
 - Central Bank use same processes to deal with reports submitted under this legislation
-



- SSM Regulations introduced requirement on ECB to have mechanism for reporting of breaches of EU banking laws and ECB decisions
- Dedicated reporting channel established on SSM website for persons to submit reports
- Focus on anonymous reporting
- Objective is to stop misconduct in banks
- Investigation of reports conducted either by ECB or National Authority
- Co-ordination between ECB and National Authorities on breach reports



- Legislation enacted providing protection to persons making reports.
- Infrastructure now set up in Bank to receive and process Protected Disclosures from the public and from PCFs.
- Increase awareness of protection afforded to persons
- Encourage employees in firms, especially PCFs, to bring to our attention any breach of financial services legislation.
- Reports received assist the Bank's in fulfilling our mandate in protecting consumers.



-
- **Whistleblowing:**
 - **Whistleblowing contact line:** 1890 130014
Email: confidential@centralbank.ie
Post: Whistleblowing Desk
Central Bank of Ireland
Block D, Iveagh Court
Harcourt Road
Dublin 2
Website: centralbank.ie
 - **PCF reporting:**
Email: Protecteddisclosures@centralbank.ie
-



Thank you



Society of Actuaries in Ireland

Pharmaceutical Sector Risk Management

Risk Management as competitive advantage

18th November 2014

Introduction



- David Staunton
- Aerospace Engineer
- Risk Management in Bio-Pharma




Disclaimer:

The material, content and views in the following presentation are those of the presenter

Today

- Two real examples –
Directly affecting competitive advantage
- Illustrating Risk Management as a decision making process
 - Making decisions that matter
When they matter

Decisions
that matter



*1st Example
Focusing*



12 *Innovative Medicines*

4
Biosimilars

15
New Competitors

50%
Revenue
Patent Exposed



\$3 to \$5 bn

Per Successful Drug

95%

Failure Rate



Simple Solution

Introduce the new
drugs quicker –
Twice as quick actually

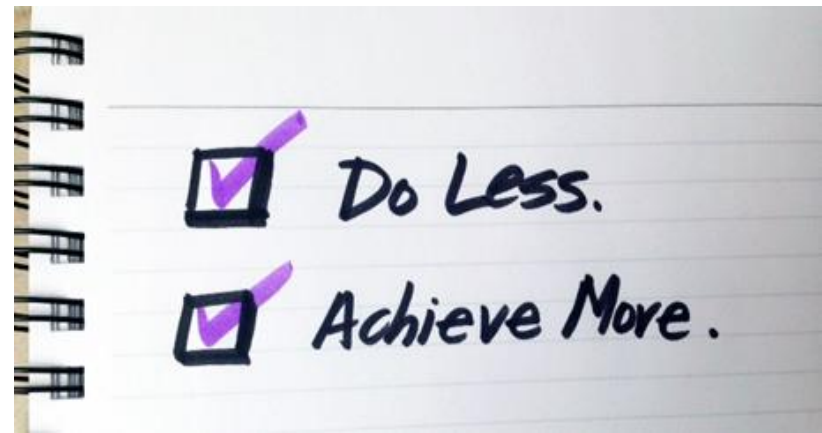
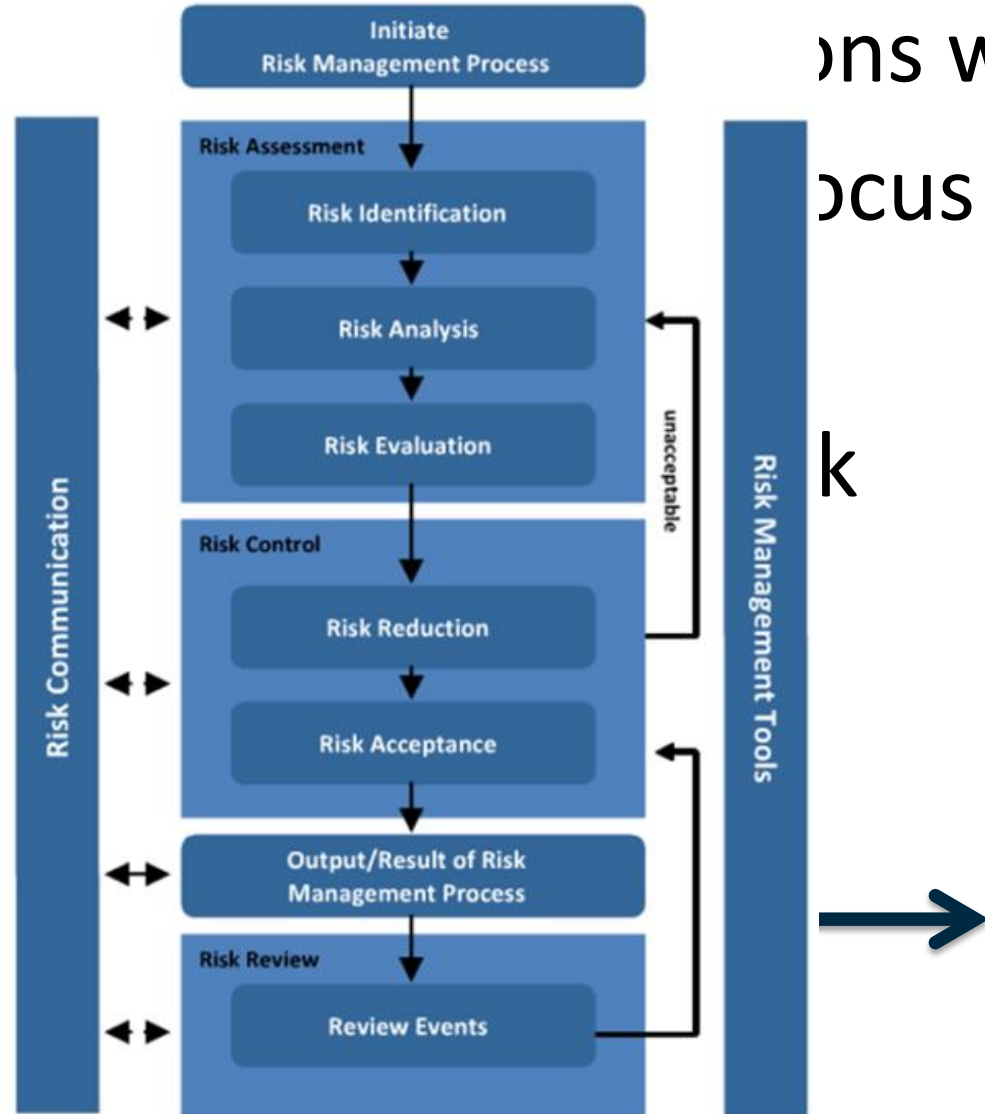


What's done

ions were to determine

OCUS

k





Regulations as an Advantage

- ICHQ8 Pharmaceutical Development QbD (Quality by Design)
- ICHQ9 Quality Risk Management QRM (Quality Risk Management)
- ICHQ10 Pharmaceutical Quality System (Management Review)

ICH
GUIDELINES



Start from the beginning

- As the drug is being developed in the lab there are people that know what is tricky about making the drug
- Focus
- Retain
- Develop





Shouldering Risk

- Prevenar in Grange Castle
Injecting babies
- Be more rigorous with what matters
- Rely on the industry experts for the rest





Terminology

- Critical Quality Attributes
 - Yield
 - Proteinaceous Particles on Oxidation
- Critical Process Parameters
 - Dissolved oxygen
 - Light exposure levels





Reduced time to market

- Reduced time to market by half
- Improved organisational knowledge retention
- Failing faster and cheaper

Risk Management as
a decision making
process



A female scientist in a cleanroom environment. She is wearing a white lab coat, a white hairnet, safety glasses, and yellow gloves. She is looking down at a tablet device she is holding. The background shows industrial equipment, including pipes, valves, and a blue motor. A dark blue semi-transparent box is overlaid on the right side of the image, containing white text.

*2nd Example
Prioritising*



Threat to Public Health

- In the United States drug shortages almost tripled between 2005 and 2010
- Shortages are becoming more severe as well as more frequent.





Call to Action

- There is a call to action from the US and EU Governments to solve the problem of drug shortages



- Executive Order 13588 -- Reducing Prescription Drug Shortages
- ISMP Medication Safety Alert, Special Issue Drug Shortages.
- EMA: Reflection paper on medicinal product supply shortages caused by manufacturing / GMP compliance problems



This is what was done

- 4 Questions
- What are the supply risks?
- Which risks erode the most value if not pursued?
- Which risks, if pursued, create the most value?
- Which actions should be pursued?



Framing the risk

- In order to answer the first question...
The risk must be framed correctly

Tipping point of material consequence



Description	Richter	Witness Observations
Instrumental	1 to 2	Detected only by seismographs
Feeble	2 to 3	Noticed only by sensitive people
Slight	3 to 4	Resembling vibrations caused by heavy traffic
Moderate	4	Felt by people walking; rocking of free standing objects
Rather Strong	4 to 5	Sleepers awakened and bells ring
Strong	5 to 6	Trees sway, some damage from overturning and falling objects
Very Strong	6	General alarm, cracking of walls
Destructive	6 to 7	Chimneys fall and there is some damage to buildings
Ruinous	7	Ground begins to crack, houses begin to collapse , pipes break
Disasterous	7 to 8	Ground badly cracked and many buildings are destroyed. There are some landslides
Very Disasterous	8	Few buildings remain standing; bridges and railways destroyed; water, gas, electricity and telephones out of action.
Catastrophic	8 or greater	Total destruction; objects are thrown into the air, much heaving, shaking and distortion of the ground



7 Numbers

7 key numbers

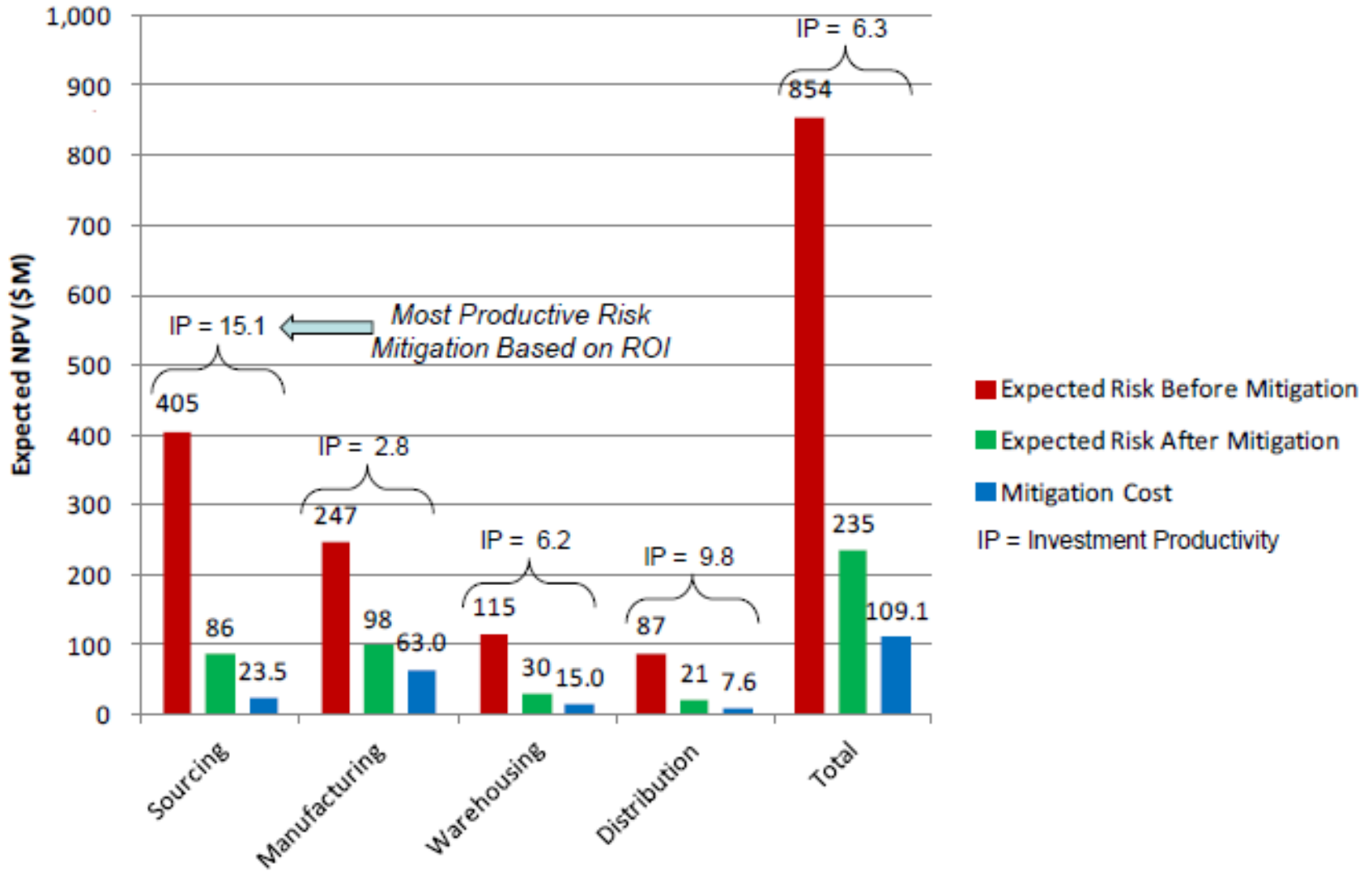
We are in the world where the risk has materialized...

- What would be surprisingly good
- What would be surprisingly bad
- What is most likely
- Applies to Sales and Cost
- What is the probability

7
Numbers



Portfolio Risk



Decisions that Matter

- Two real examples –
Directly affecting competitive advantage
- Illustrating Risk Management as a decision making process
 - Making decisions that matter
When they matter

Decisions
that matter

Making decisions that matter
When they matter

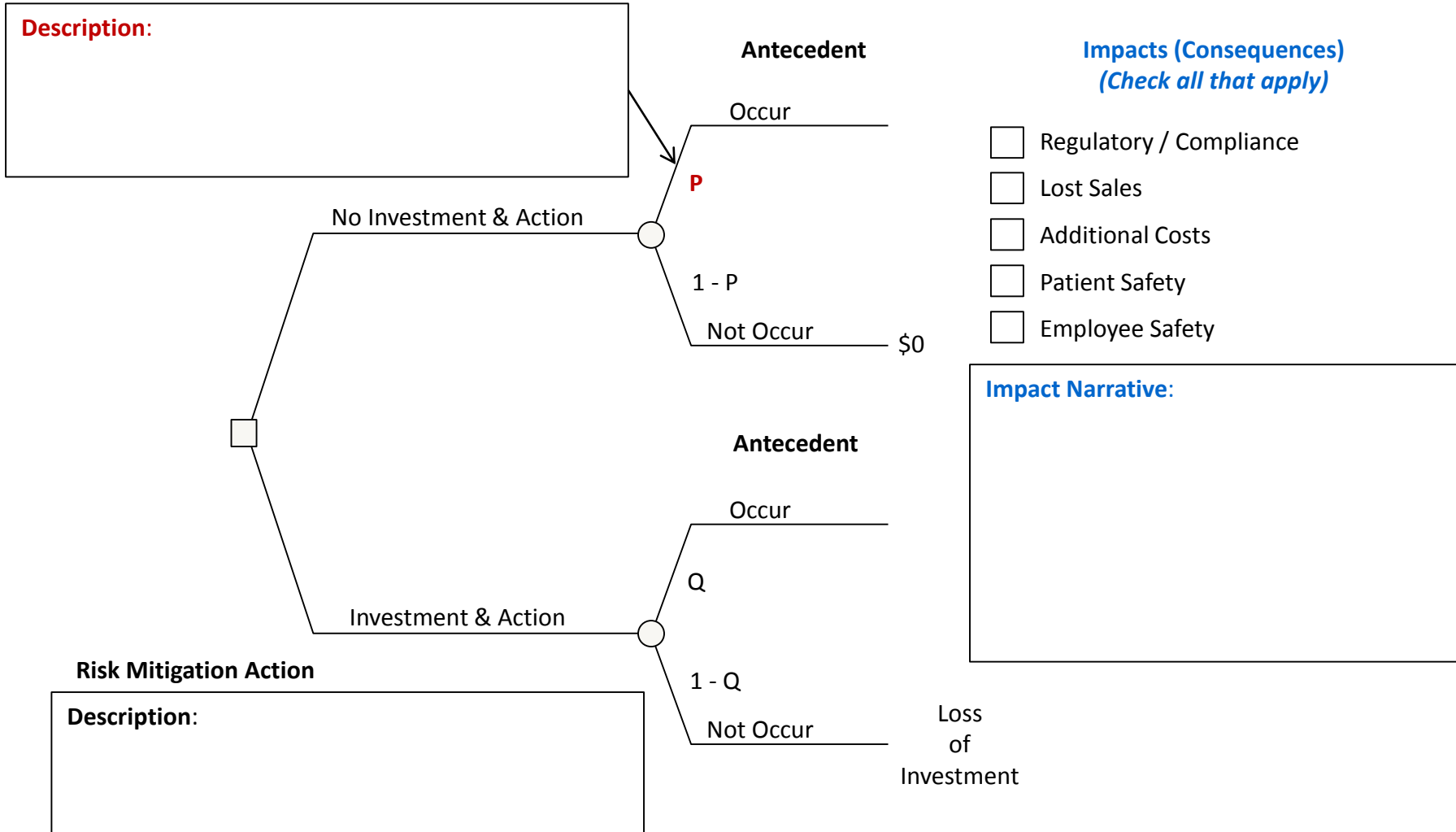
Questions?

Decisions
that matter

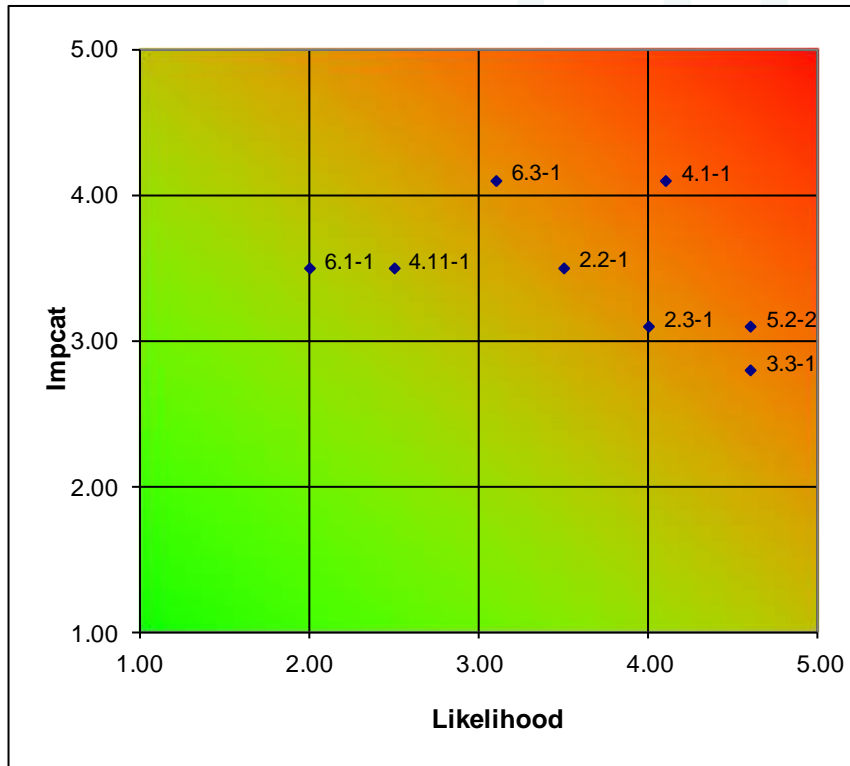


Template

Antecedent: *"Tipping Point of a Material Consequence"*



Heat Map – Very Pretty – Useless



Probability Impact Matrix

Ref	Risk	Imp	Like
4.1-1	Access to the Suite for CIP commissioning & The affect on the Plan of Record (4.1-2)	4.10	4.10
6.3-1	Clarity on the sequence of commissioning & validation activities (6.4-1)	4.10	3.10
5.2-2	I&C and Electrical resource holidays at the same time & for VPE IFC Pack	3.10	4.60
3.3-1	Changes on P&IDs between IFC & IFD can cause re-work	2.80	4.60
2.3-1	Field device interfaces on QBMS Panel & delay to panel delivery (2.5-1)	3.10	4.00
2.2-1	QBMS FS review by VPE owners & Daldrop (1.31-1)	3.50	3.50
4.11-1	Access to the CIP phases during coding by multiple groups	3.50	2.50
6.1-1	Failure testing on MCS must test every branch	3.50	2.00

- Total Number of Risks Identified 29
- New Risks Identified 7
- Risks Materialised 2
- Closed Risks 5



Society of Actuaries in Ireland

Risk Culture and Communications

Brid Horan - 18 November 2014

Topics

- **What is risk culture?**
- Building an effective risk culture
- Communication – not just information
- Monitoring
- The ‘Ask’

Disclaimer:

The material, content and views in the following presentation are those of the presenter.

Since 2000, competition has been transformational

Other Generators



Interconnectors



ESB Generation

Generation Market



ESB Networks

Transmission System



Distribution System



Regulated & Ringfenced Networks

Customers eligible to choose their Supplier



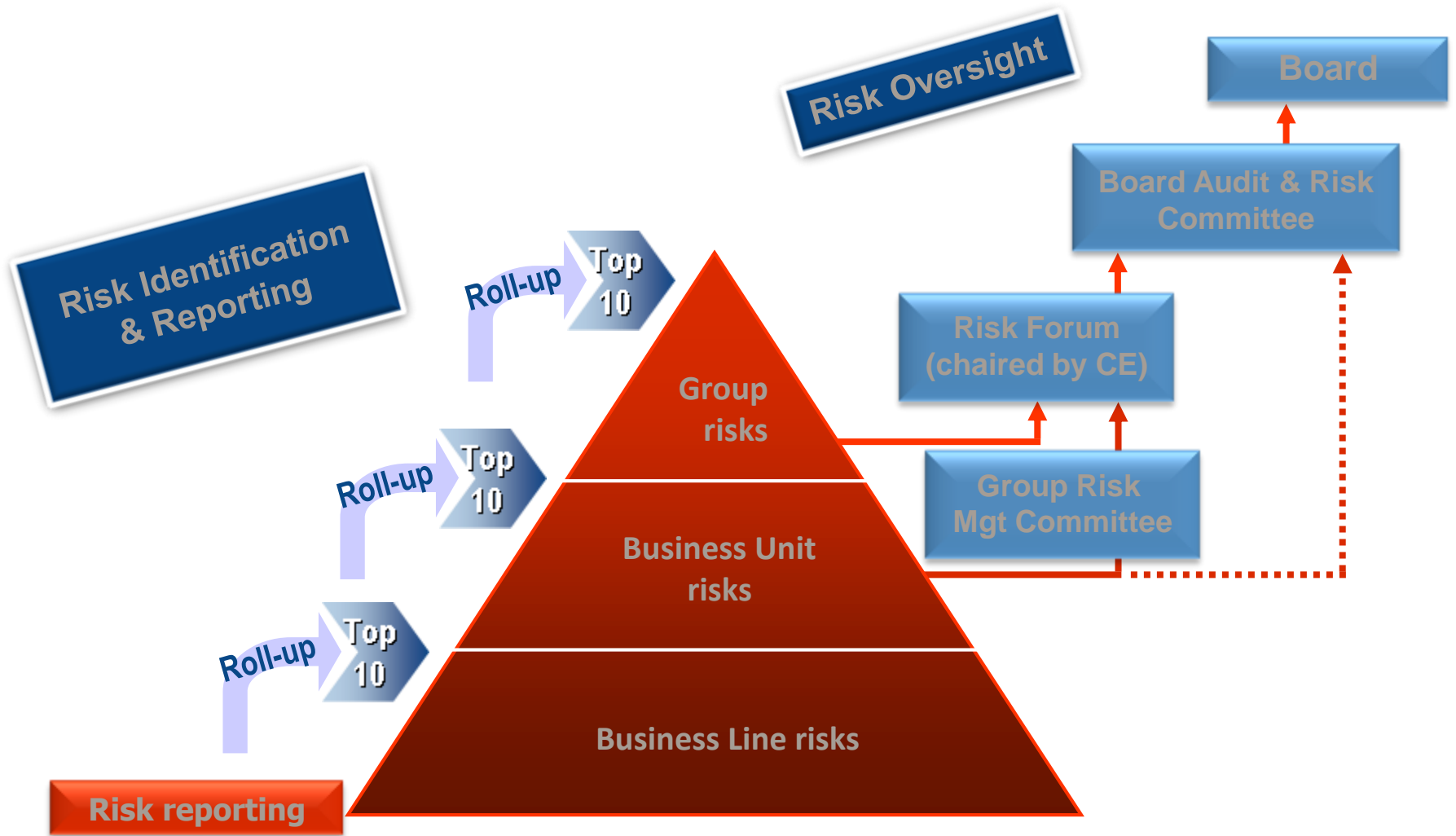
Others



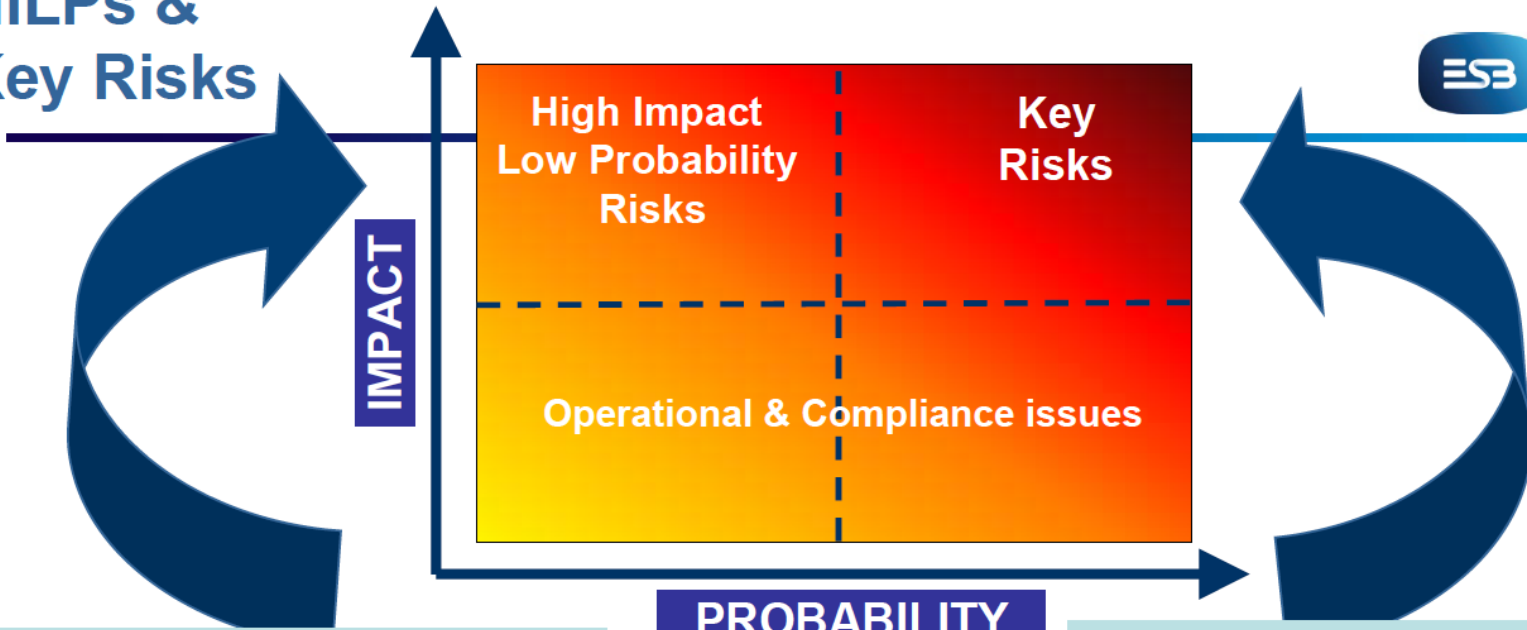
Retail Market



Risk Management Applies at all levels of the company



HILPs & Key Risks



HILP Risks

- Explosion / fire in plant
- Major safety incident
- Major environmental incident
- Sabotage / Terrorism
- Major IT virus attack (malware)
- Security incident overseas
- Failure of OMS(NW Distrib system)
- Dam failure/major flooding
- Major data security breach
- Major Supply Failure

PROBABILITY

Top Ten Group Risks

- Health & Safety incident
- Regulatory / Stakeholder decisions
- Change programmes are delayed
- Trading / operational risk
- Investment / Project Execution Risk
- Competitive / Economic pressures
- Reputation & Public standing
- Pensions DB scheme
- Difficulty securing appropriate Funding
- Failure of critical Infrastructure



When it all goes wrong....

BBC NEWS WORLD EDITION

You are in: **Business**
Thursday, 22 August, 2002, 16:59 GMT 17:59 UK

News Front Page



- Africa
- Americas
- Asia-Pacific
- Europe
- Middle East
- South Asia

Enron scandal at-a-glance

Click on headings below for details

- Investigators

Fifa Officials Embroiled in More Scandal After Receiving \$25,000 Watches at World Cup Finals

... given to Fifa's executive committee members at Brazil World Cup

Whistle-blower controversy 'most damaging' in Garda history

AGSI delegate warns conference morale in force at a dangerously low level

Gap, Next and M&S in new sweatshop scandal

– Indian workers are paid just 25p an hour
overtime in factories on street

k
high

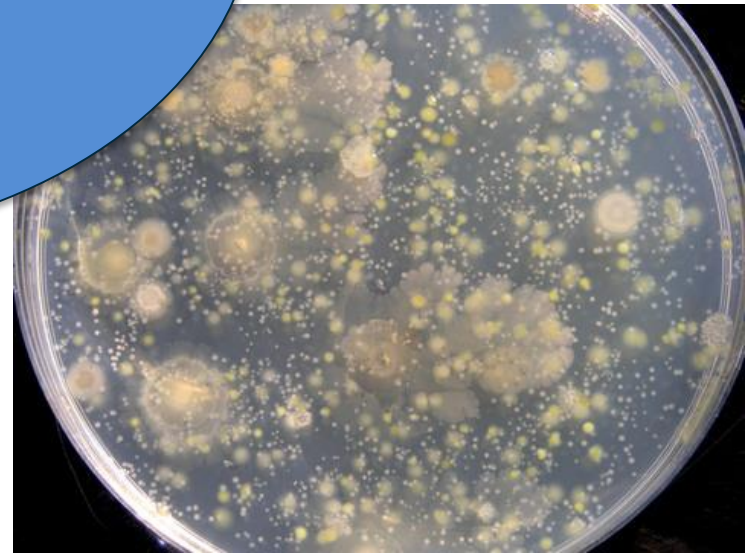


These examples demonstrate the impact that the “wrong” culture can have on the reputation of an organisation and on the morale of the people in that organisation.



What is risk culture?

*Culture is an environment,
a petri dish in which certain
behaviours and
characteristics are allowed
to flourish or not.*



John Harvie

Director Protiviti Insurance and Business Operations Improvement



Risk Culture

Risk Attitude

- Position adopted by individuals and group towards risk
- Disposition to risk
- Perception of risk

Risk Behaviour

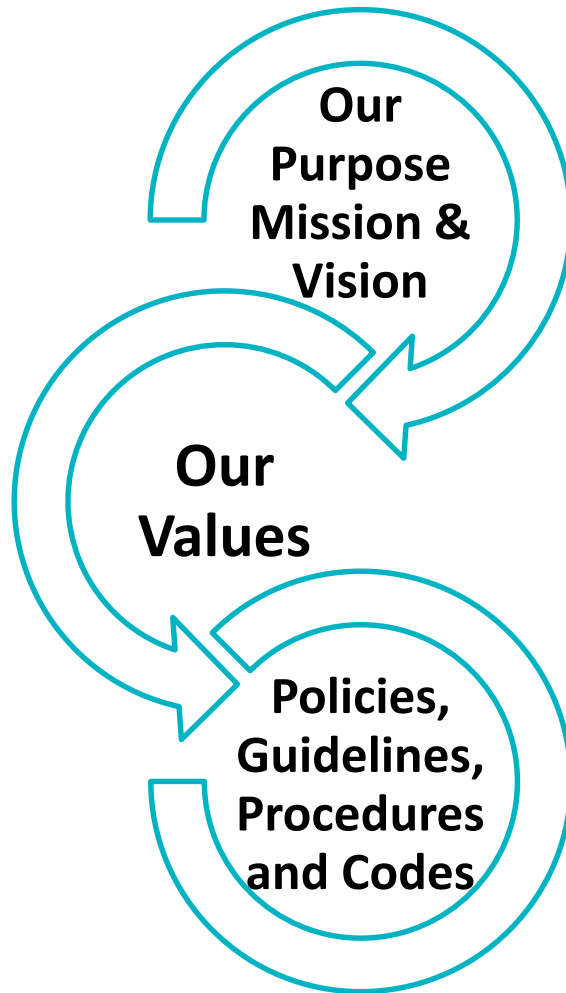
- Risk based decision making
- Risk processes
- Risk communications

Risk Culture

- Values, beliefs, knowledge, understanding of risk
- Explicit and implicit
- Shared by leaders and staff



Helping Culture Flourish



Who are we and what are we about?

What do we believe/stand for?

These support managers and staff by helping them to behave in a way that is consistent with our values and our purpose

Topics

- What is risk culture?
- **Building an effective risk culture**
- Communication – not just information
- Monitoring
- The 'Ask'

Disclaimer:

The material, content and views in the following presentation are those of the presenter.

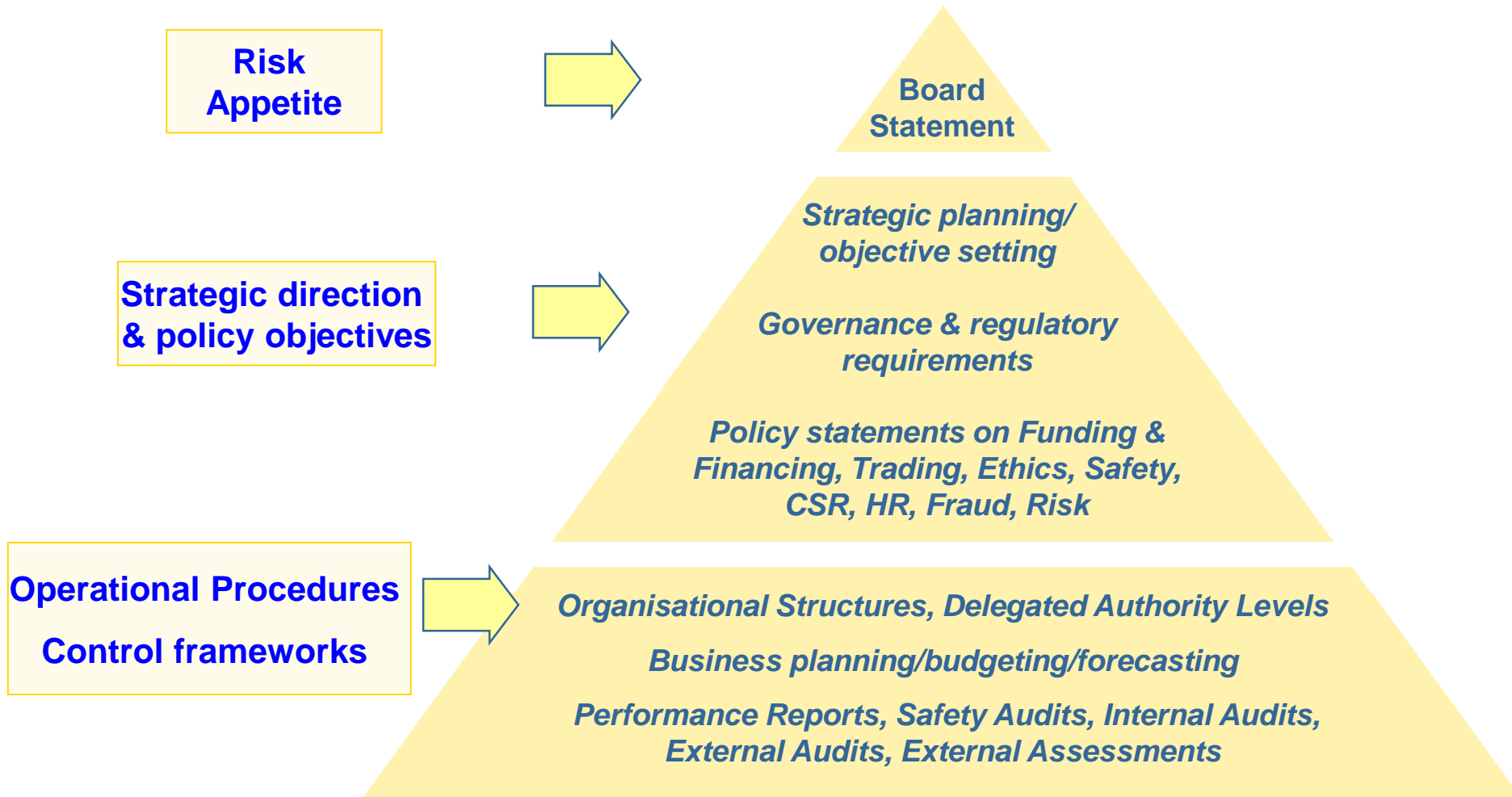


Linking Strategy and Risk





Cascading risk appetite





Roles and responsibilities

**“Top-Down”
Oversight,
Identification/
mitigation of risk
@ Group level**

Board			
<i>Overall Group responsibility for risk management and internal controls system</i>	<i>Sets strategic objectives and defines risk appetite</i>	<i>Monitors nature/ extent of risk exposure against risk appetite for principal risks</i>	<i>Provides direction on importance of risk management and risk culture</i>

**“Bottom-up”
Identification/
assessment/
mitigation
of risk @
business
unit level and
business lines**

Management Risk Forum
<ul style="list-style-type: none"><i>Assess and mitigate risks Company wide</i><i>Monitor risk management process and internal controls</i>

Board Audit & Risk Committee
<ul style="list-style-type: none"><i>Support Board in monitoring risk exposure against its risk appetite</i><i>Review effectiveness of risk management and internal controls systems</i>

Internal Audit
<ul style="list-style-type: none"><i>Support Audit & Risk Committee in reviewing effectiveness of risk management and internal controls systems</i>

Business Units		
<i>Risk management process and internal controls embedded across business lines</i>	<i>Risk identification, assessment and mitigation performed across the business</i>	<i>Risk awareness and safety culture embedded across the business</i>



Risk Management Process



- Strategy
- Objectives
- Risk Appetite
- Risk tolerance
- Risks

- Risk Owner
- Risk Manager
- Impact
- Likelihood
- Velocity
- Financial impact
- Within risk tolerance

- Current Activities
- Additional Activities
- Status

- ✓ Board
- ✓ Audit & Risk Committee
- ✓ Other Board Committees
- ✓ Group Risk Management Committee

Topics

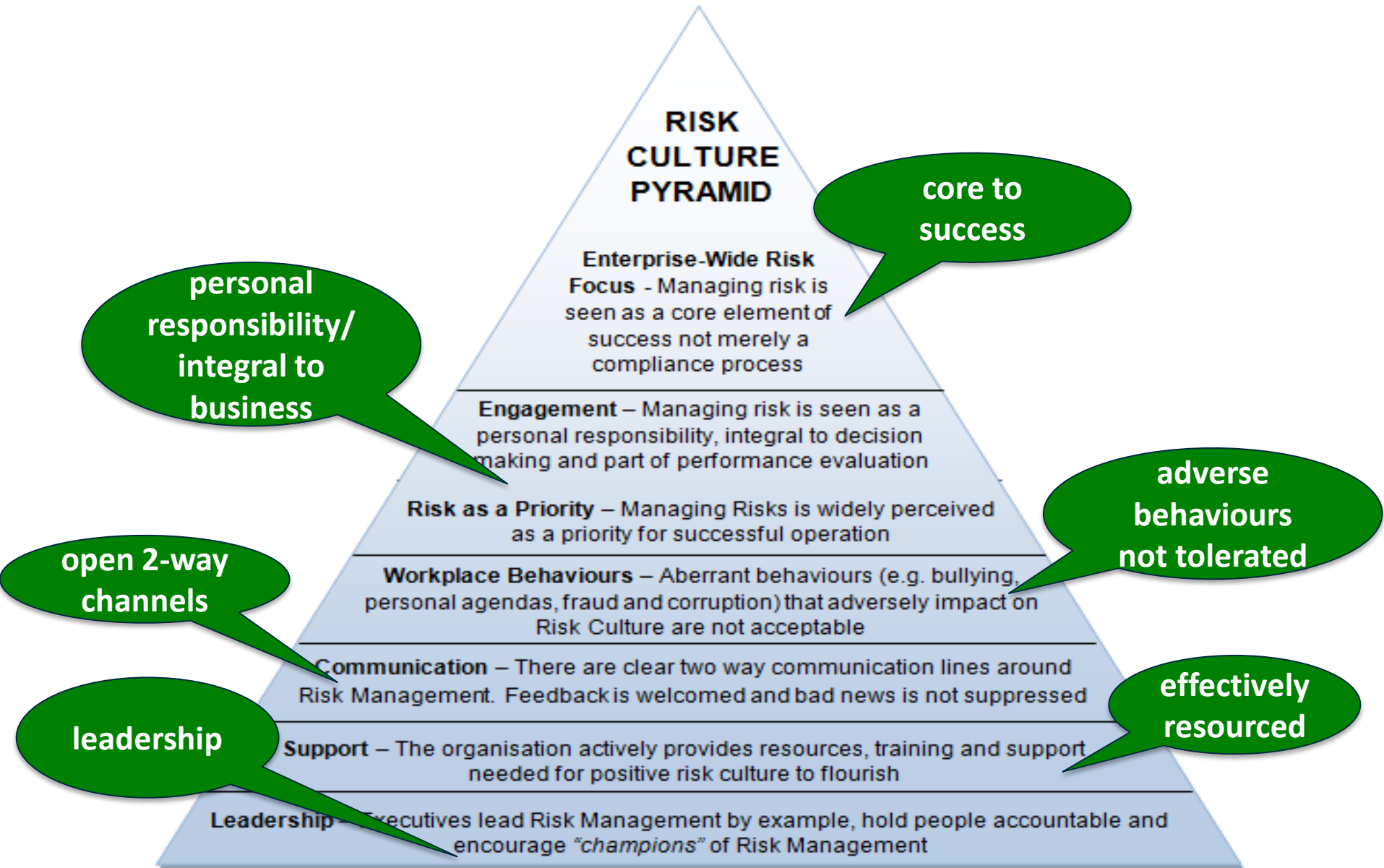
- What is risk culture?
- Building an effective risk culture
- **Communication – not just information**
- Monitoring
- Challenges
- The 'Ask'

Disclaimer:

The material, content and views in the following presentation are those of the presenter.



Risk Culture

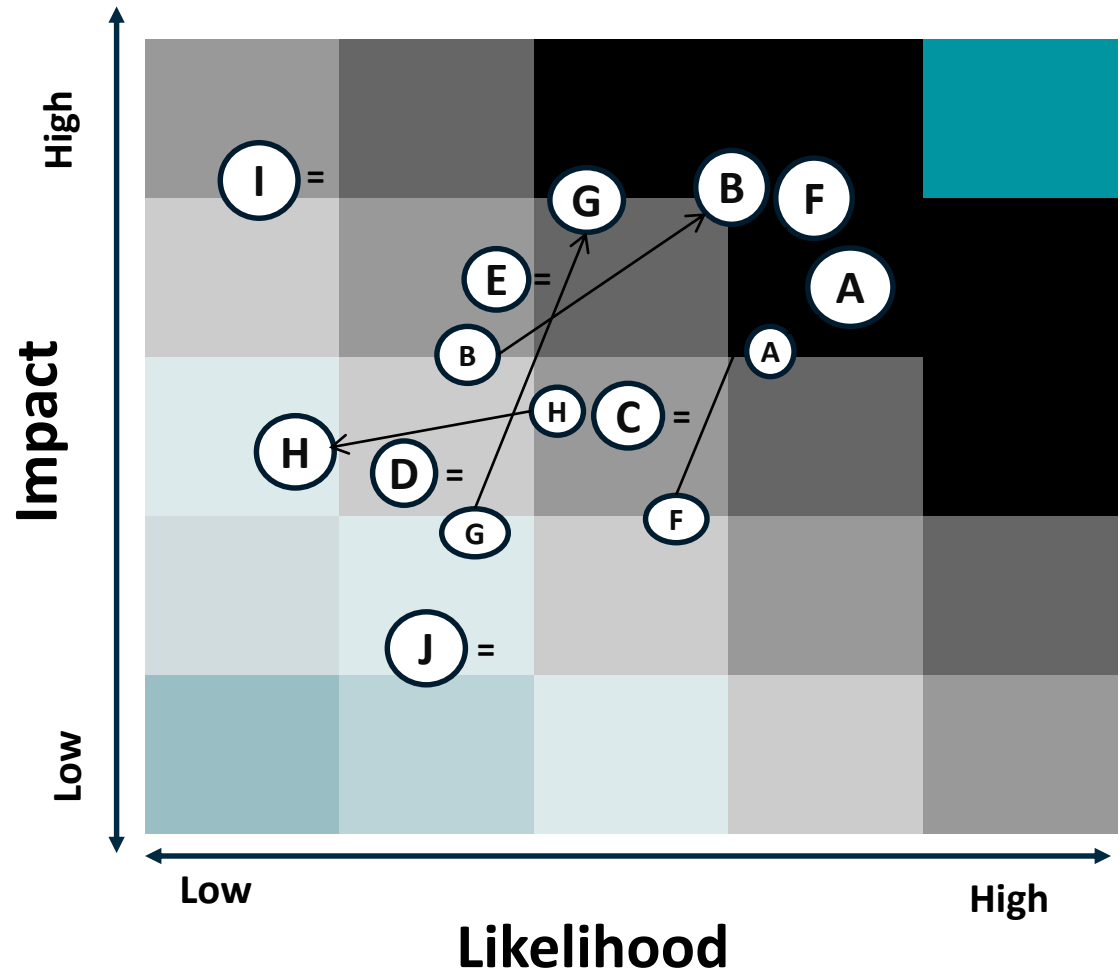




Communicating - Transparency

This heat map represents relative positioning of principal risks with indicative movement (where relevant) through the year

- A Regulatory/Stakeholder decisions
- B Delivery of Change
- C Trading/Operational
- D Investment/Project Execution
- E Commercial and Market
- F Pensions
- G Reputation and public standing
- H Funding and Liquidity
- I Safety and Environment
- J Infrastructure



Topics

- What is risk culture?
- Building an effective risk culture
- Communications – not information
- **Monitoring**
- Challenges
- The 'Ask'

Disclaimer:

The material, content and views in the following presentation are those of the presenter.



Monitoring - Sources of Assurance

1st Line

Line Management

Primary responsibility for adequate, effective & sustainable system of internal controls

2nd Line

Risk Compliance/ Financial Control

Formulates risk & compliance policies & procedures, monitors integrity

3rd Line

Internal Audit External Audit Other 3rd Parties

Independent assessment/reassurance re governance, risk management & control



Board and Board Committees

- Audit & Risk Committee supports Board in monitoring and reviewing effectiveness of risk management and control systems
 - Challenge received wisdom
 - “Skip” Briefings – meet with Business Units directly
 - Propose specific topics for Management and/or Board consideration
- Joint Committee initiatives
 - All Board Committees contribute to risk oversight
- Visit “shop floor” – see how risk awareness embedded across organisation

Topics

- What is risk culture?
- Building an effective risk culture
- Communications – not information
- Monitoring
- Challenges
- **The 'Ask'**

Disclaimer:

The material, content and views in the following presentation are those of the presenter.



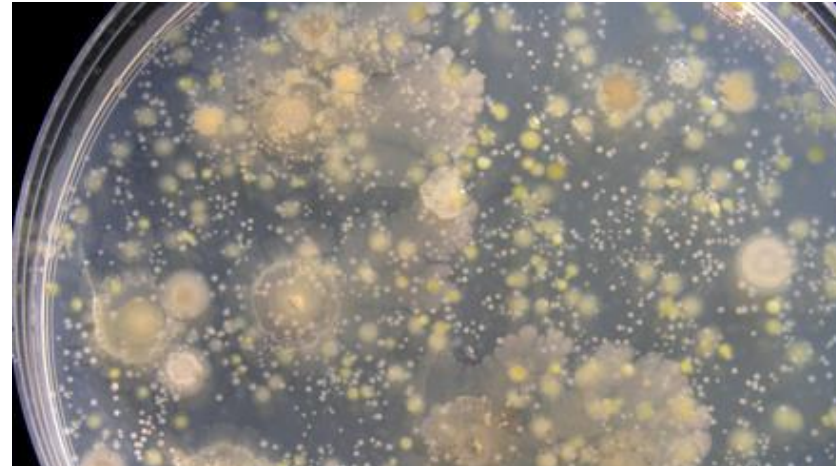
Effective risk culture REALLY matters

- Institute of Risk Management:
Risk culture under the Microscope: Guidance for Boards
2012
- Financial Reporting Council:
Guidance on Risk Management, Internal Control and Related
Financial and Business Reporting
September 2014
- Society of Actuaries in Ireland:
Embedding a Risk Culture: Behavioural Aspects of Managing Risk
Professor Niamh Brennan
September 2013



The 'Ask'

- Effective risk culture is essential for effective risk management
- Risk culture is an element of organisation culture
- Organisation culture is deep-rooted but can be changed
- Really know your culture and what drives it – harness the power of Middle Management
- Work on all those drivers, especially yourself





Thank you.....

“Hey..... Let’s be careful out there”

Hill Street Blues (1981 – 1987)