RISKWEST
MANAGEMENT CONSULTANTS

Privacy Breaches: *Taking a risk-based approach*

SecureIT 2017 Securing your Privacy
ISACA Perth Chapter Annual Conference

Note & Disclaimer

Note: The material is © Riskwest. As an attendee at the presentation, you may use, with proper attribution, this material personally & within your organisation for educational purposes. This includes making copies, in whole or in part, of the material. Use of this material for purposes other than those indicated requires written prior consent from Riskwest. All requests should be emailed to admin@riskwest.com.au.

Disclaimer: Whilst care has been taken in the preparation of this presentation, Riskwest does not accept any liability to any person for the information or advice (or the use of such information or advice) which is provided in this material or incorporated into it by reference. The information is provided on the basis that all persons accessing this material undertake responsibility for assessing the relevance and accuracy of its content. No liability is accepted for information or services which may appear in any other format (e.g. video), or for any information or services which may appear on any referenced websites.

Speaker Biography

Mark Humphreys has over 20 years of experience encompassing logic mapping, strategic, operational and project risk, liability and insurable risk management with blue chip companies in the UK, and across the Australian private and public sectors. Mark has been a Board Director, and is a graduate and member of the Australian Institute of Company Directors. In addition, he is a '*Certified Insurance Professional*' (CIP) and 'Fellow' of the Australian and New Zealand Institute of Insurance & Finance, a '*Certified Practising Risk Manager*' (CPRM) and former National Director of the 'Risk Management Institution of Australasia', a '*Chartered Member*' (CMIOSH) of the Institution of Occupational Safety and a '*Member & Approved Trainer*' (MBCI) for the Business Continuity Institute.

Mark holds an MSc 'Insurance and Risk Management' and an MSc in 'Emergency Management' majoring in risk and business continuity management.

Email: mark.humphreys@riskwest.com.au.

RISK

Top 10 threats

1st Cyber attack

2nd Data breach

3rd Unplanned IT and telecom outages

4th Security incident

5th Adverse weather

6th Interruption to utility supply

7th Act of terrorism

8th Supply chain disruption

9th Availability of talents/key skills

10th New laws or regulations

Source: Business Continuity Institute, Horizon Scan 2017

What is *Risk* & *Risk Management*?

It is concerned with those risks which can **impact** any or all aspects of operations:

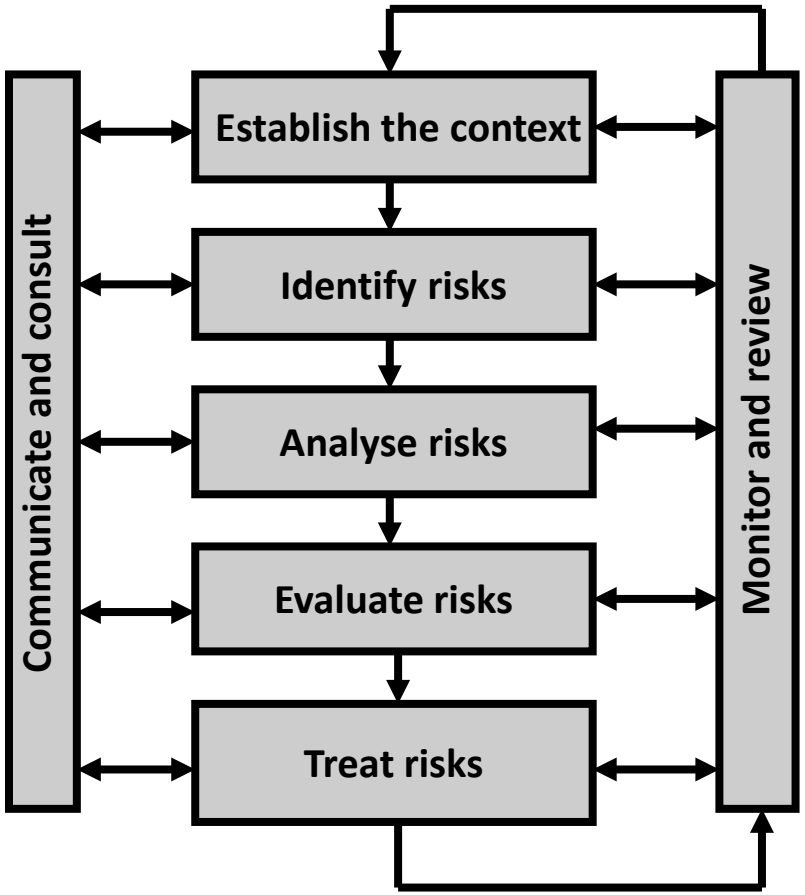
People / Safety & Health
Reputation & Image
Performance
Service Delivery
Interruptions to Service
Compliance
Financial Loss
Etc…..

The management of risk is about **understanding and responding to uncertainty** that could substantively impact an organisation's ability to create or preserve value for stakeholders over the short, medium or long term.

Based on Corporate Governance Principles and Recommendations, 3rd Edition, *ASX Corporate Governance Council.* Definition of *material risk.*

"the systematic application of management to the activities of communicating and consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk"

What does our activity involve?
In what internal and external context is it happening?



Source: WA State Government RM Guidelines (July 2016)

What will be critical to it's success?

What could go wrong?

How might that happen / what will cause it?

How are we going to manage it to make sure it doesn't happen?

But, if it happens what will result?

What is the consequence level if it happens?

How likely is it to happen with that consequence level?

Is that level of risk acceptable to us?

If not what else are we going to do about it?

Are we taking the appropriate amount of risk?

- Risk Measurement Criteria / Risk Reference Tables
- Defined risk tolerance and appetite statements
- '*Precautionary*' and '*As Low As Reasonably Practicable*' principles
- Clear Maximum Possible & Probable Losses

What is ‘reasonable’ ?

- What are the potential consequences of actions/inactions/decisions?
- What is the likelihood of such consequences?
- What is the burden of preventative/mitigative controls?

What happens if it goes '*pear shaped*'?

Crisis Management Plans

Business Continuity Plans

Contingency Plans

Data Breach Response Plans

What factors should I consider in identifying and assessing *privacy* risks?

Type of activity

Scope

Venue or location

People involved

Duration of activity

Technology involved

Am I using the *right* risk tools and techniques?

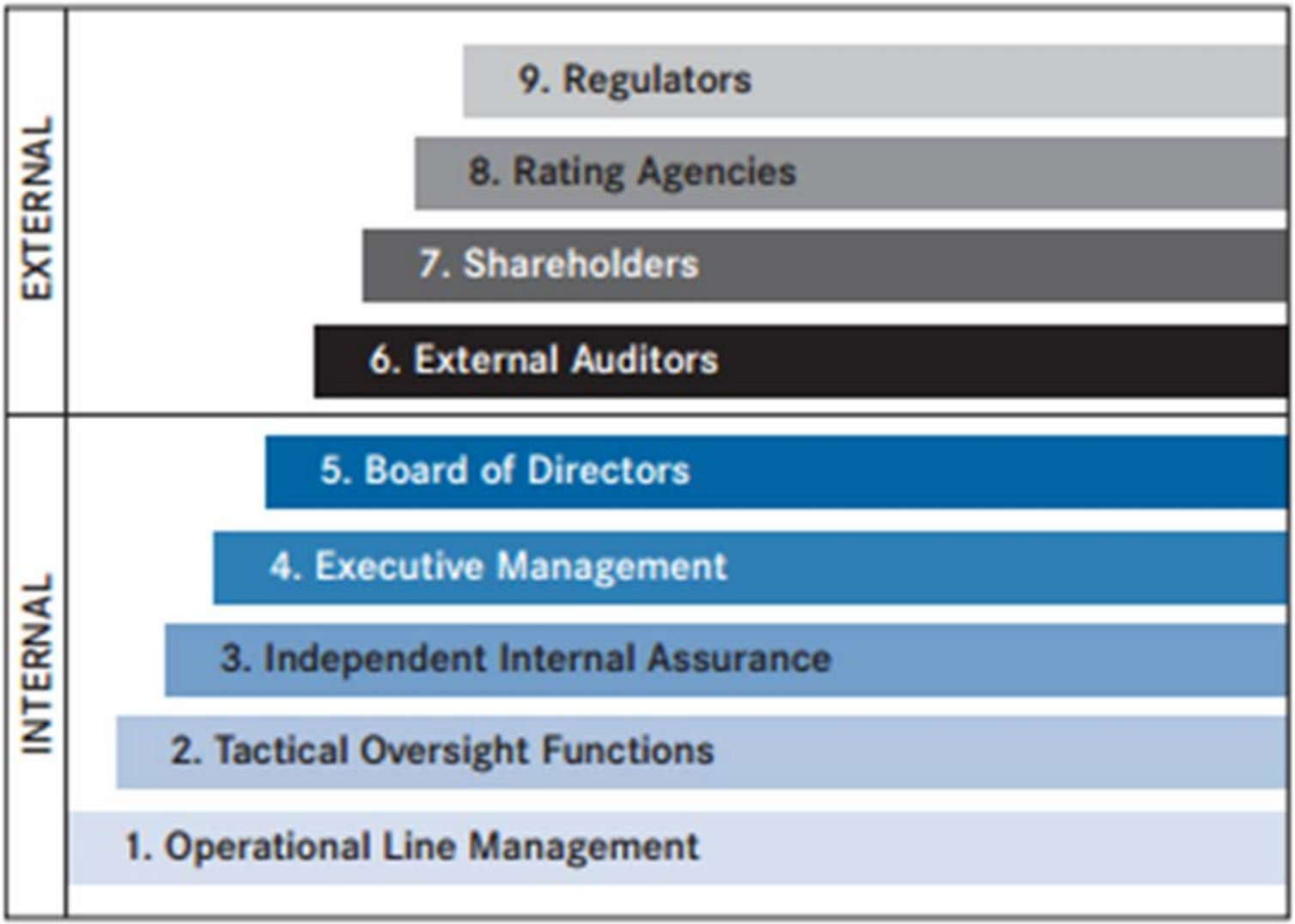
Where will I obtain the information I need?

- Past records/history
- Committees and teams
- Legal – compliance findings and expert judgements
- Experience – yours and other organisations
- Reports & Guides
- Brokers & Insurers
- Stakeholders

How do we know that we are doing all things reasonable?

- Controls identification
  - *'Hierarchy of Control'* principle
- Lines of Defence
  - Oversight

…is there enough oversight?



Source: Extract from 'Corporate Oversight & Stakeholder Lines of Defense – S Lyons (2011)

Thank You