

Business Continuity Management in 2021

- Simon Jordan Business Continuity Institute – Auckland BCI Forum Leader
- Andrew Curlewis Director Future Programmes, Babcock New Zealand
- Andy Horne Partner Dispute Resolution and Litigation, MinterEllisonRuddWatts



BCI Horizon Scan Report 2021

Launch

BCI Auckland Forum - Launch

PROFILE: SIMON JORDAN

- Bachelor of Sciences (Earth Sciences) – Waikato University 1997
- Member of the Business Continuity Institute – Auckland BCI Forum Leader
- ISO22031/ISO27001 Lead Implementer, IRCA Certified ISO727001 Information Security Lead Auditor
- Over 20 years of business experience in both NZ and the UK
- Business/technical mix covering Business Continuity, Disaster Recovery, Information Security, Risk, Information Technology and Networking and Business
- BSI External Trainer – Business Continuity, Information Security, Risk and Asset Management Systems



| Company | Role | Responsibilities |
|---------------|---|---|
| Resilient IT | Managing Director/Principal Consultant - Auckland | <i>Business Continuity, Information Security and Risk Consulting</i> |
| Plan B | Key Account Manager – Wellington/Auckland | <i>Top 35 Accounts - Insurance, Banking, Retail, Legal, Logistics, Distribution</i> |
| IBM | Key Accounts - Systems & Technology - Wellington | <i>BNZ, ANZ, MoH, Police, Customs, Southern DHB's, NIWA</i> |
| Gen-i/Spark | Business Solutions Specialist - Wellington | <i>Infrastructure and WAN specialist - Enterprise and Government</i> |
| Itegrity (UK) | Director/Security Specialist - London | <i>Banking, Legal and Government</i> |
| ComputerLand | Account Manager - Hamilton | <i>Corporate Accounts & Education Sector</i> |

About the Horizon Scan 2021 Report



Risk and Threat Assessment: Last Twelve Months



The top three disruptions in 2020 were all health and safety focused



Top Three Disruptions by Risk Score: 2020

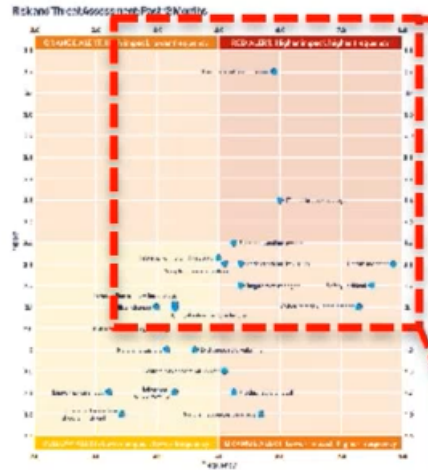
Non-occupational disease had the highest risk score ever noted for “past risks”

Risk and Threat Assessment: Past Twelve Months

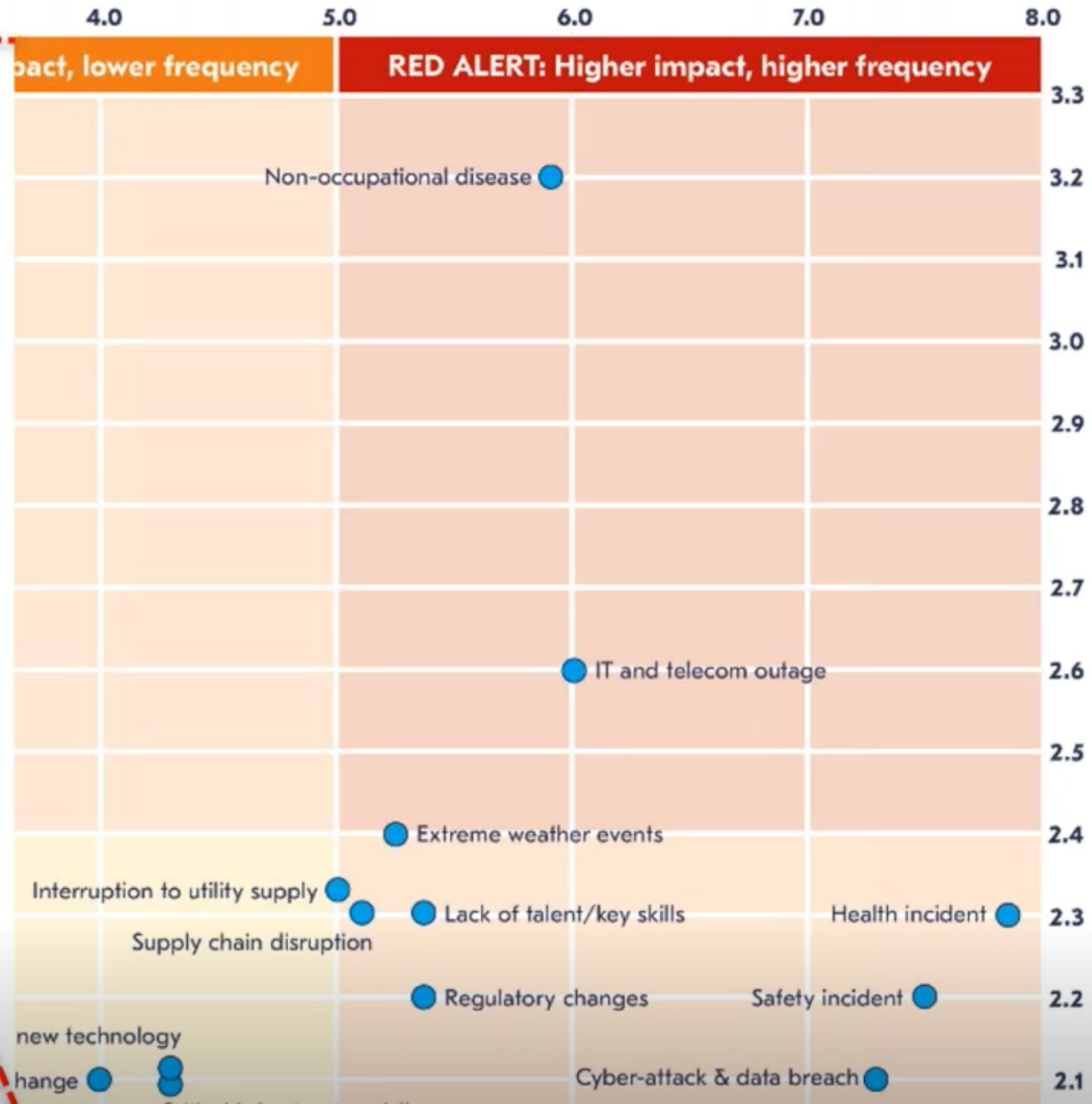
| Ranking | | Frequency | Impact | Risk Index |
|---------|---|-----------|--------|------------|
| 1 | Non-occupational disease (e.g. pandemic) | 5.9 | 3.2 | 18.6 |
| 2 | Health incident (occupational disease, reportable occupational disease, stress/mental health, increased sickness absence) | 7.8 | 2.3 | 18.2 |
| 3 | Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident) | 7.5 | 2.2 | 16.1 |
| 4 | IT and telecom outage | 6.0 | 2.6 | 15.8 |
| 5 | Cyber attack & data breach | 7.3 | 2.1 | 15.3 |
| 6 | Extreme weather events (e.g. floods, storms, freeze, etc.) | 5.2 | 2.4 | 12.3 |
| 7 | Lack of talent/key skills | 5.3 | 2.3 | 12.1 |
| 8 | Supply chain disruption | 5.1 | 2.3 | 12.0 |
| 9 | Regulatory changes | 5.3 | 2.2 | 11.7 |
| 10 | Interruption to utility supply | 5.0 | 2.3 | 11.3 |

| Ranking | | Frequency | Impact | Risk Index |
|---------|--|-----------|--------|------------|
| 11 | Political violence/civil unrest | 5.1 | 1.8 | 9.4 |
| 12 | Natural resources shortage | 5.7 | 1.6 | 9.3 |
| 13 | Introduction of new technology (IoT, AI, Big data) | 4.3 | 2.1 | 9.0 |
| 14 | Exchange rate volatility | 4.6 | 1.9 | 8.8 |
| 15 | Critical infrastructure failure | 4.3 | 2.1 | 8.7 |
| 16 | Product safety recall | 5.2 | 1.7 | 8.7 |
| 17 | Enforcement by regulator | 4.2 | 2.0 | 8.3 |
| 18 | Political change | 4.0 | 2.1 | 8.1 |
| 19 | Natural disasters (earthquakes, tsunamis, etc.) | 4.2 | 1.9 | 7.8 |
| 20 | Higher cost of borrowing | 4.3 | 1.7 | 7.3 |
| 21 | Lone attacker/active shooter incident | 3.4 | 1.6 | 5.7 |
| 22 | Energy price shock | 3.2 | 1.7 | 5.4 |

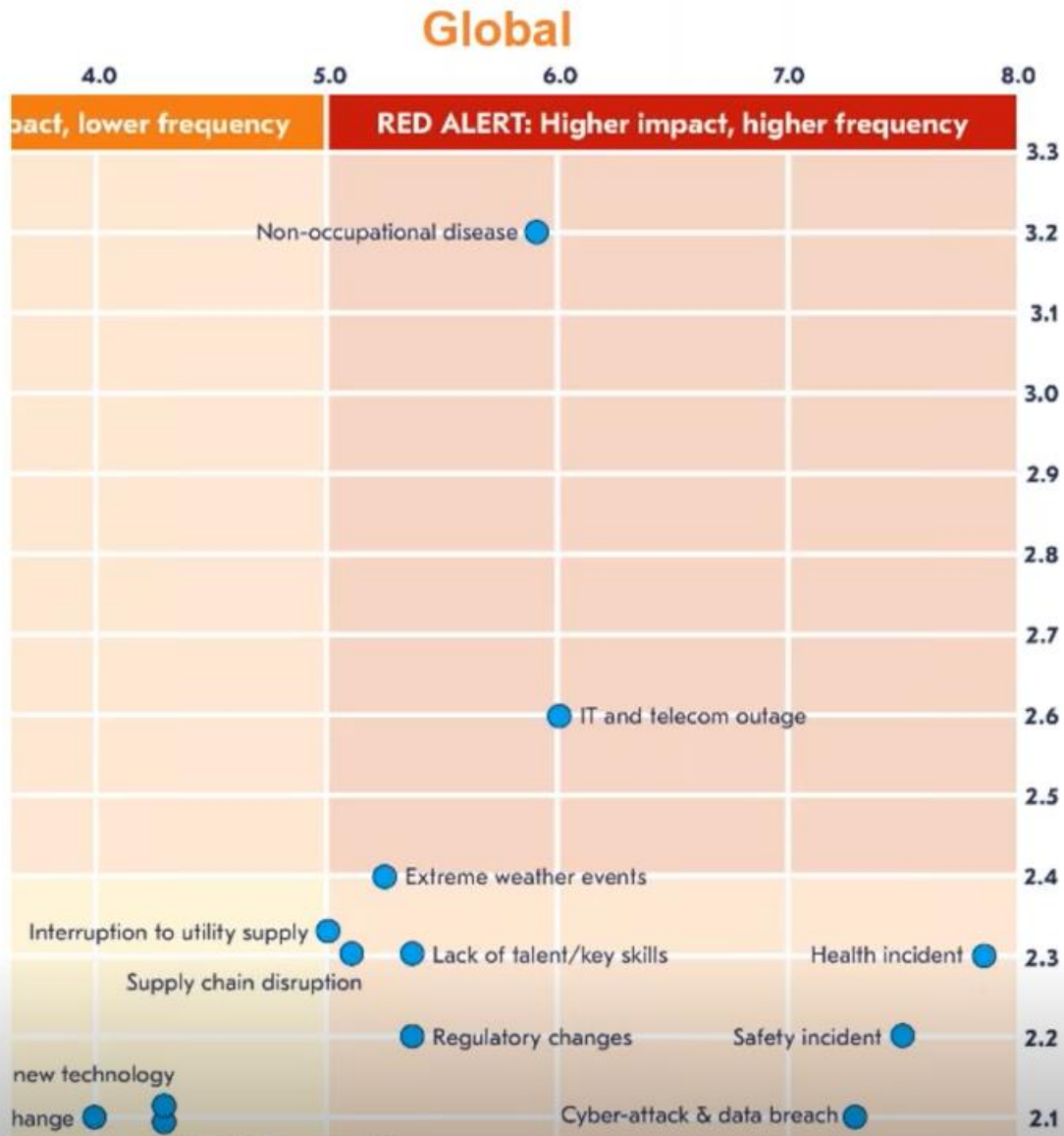
The impact of COVID-19 has been extreme, but “traditional” disruptions remain frequent



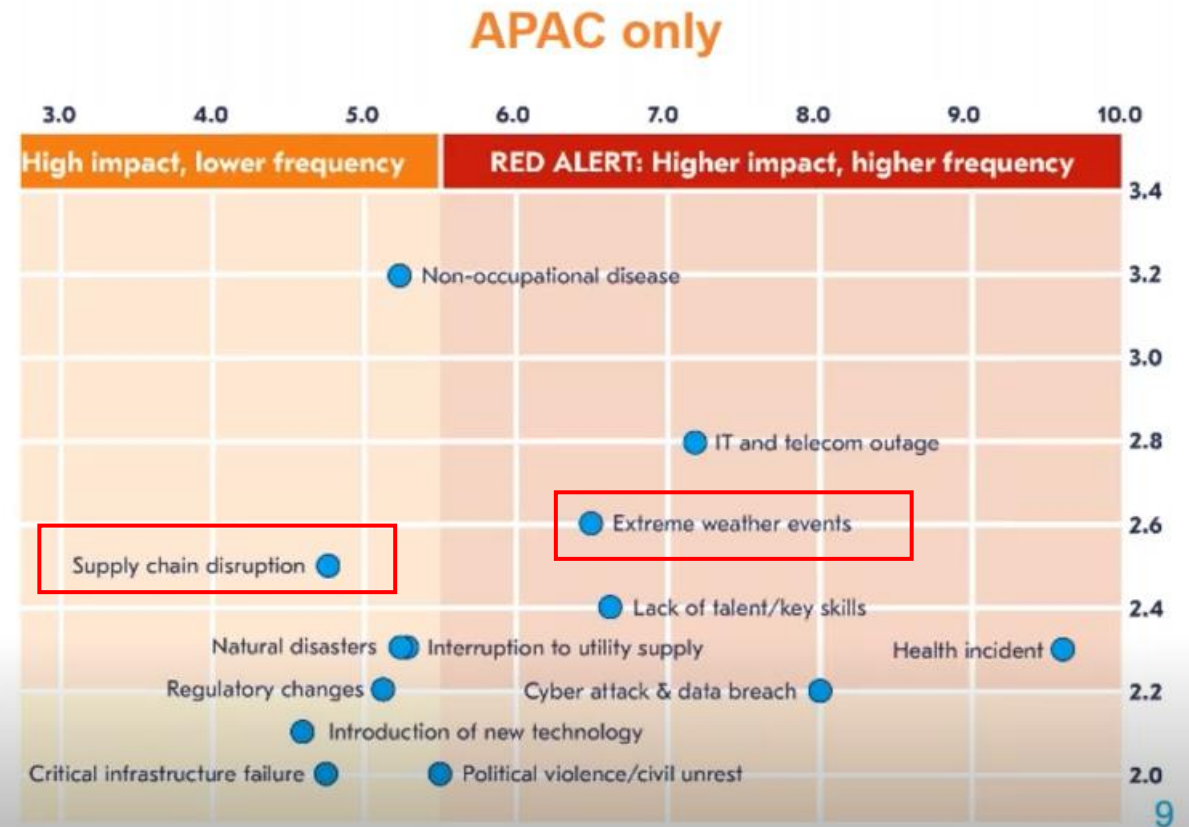
Risk and Threat Assessment: Past Twelve Months



Extreme weather and IT/telecom outage were more disruptive than COVID in APAC



Risk and Threat Assessments: Past Twelve Months



33% of organizations reported COVID-19 was not their most severe disruption in 2020

Which event was the cause of your most major disruption in 2020?



Risk and Threat Assessment: Next Twelve Months



COVID-19 still dominates concerns for 2020, but risk landscapes are being broadened



Top Three Anticipated Disruptions by Risk Score: 2021

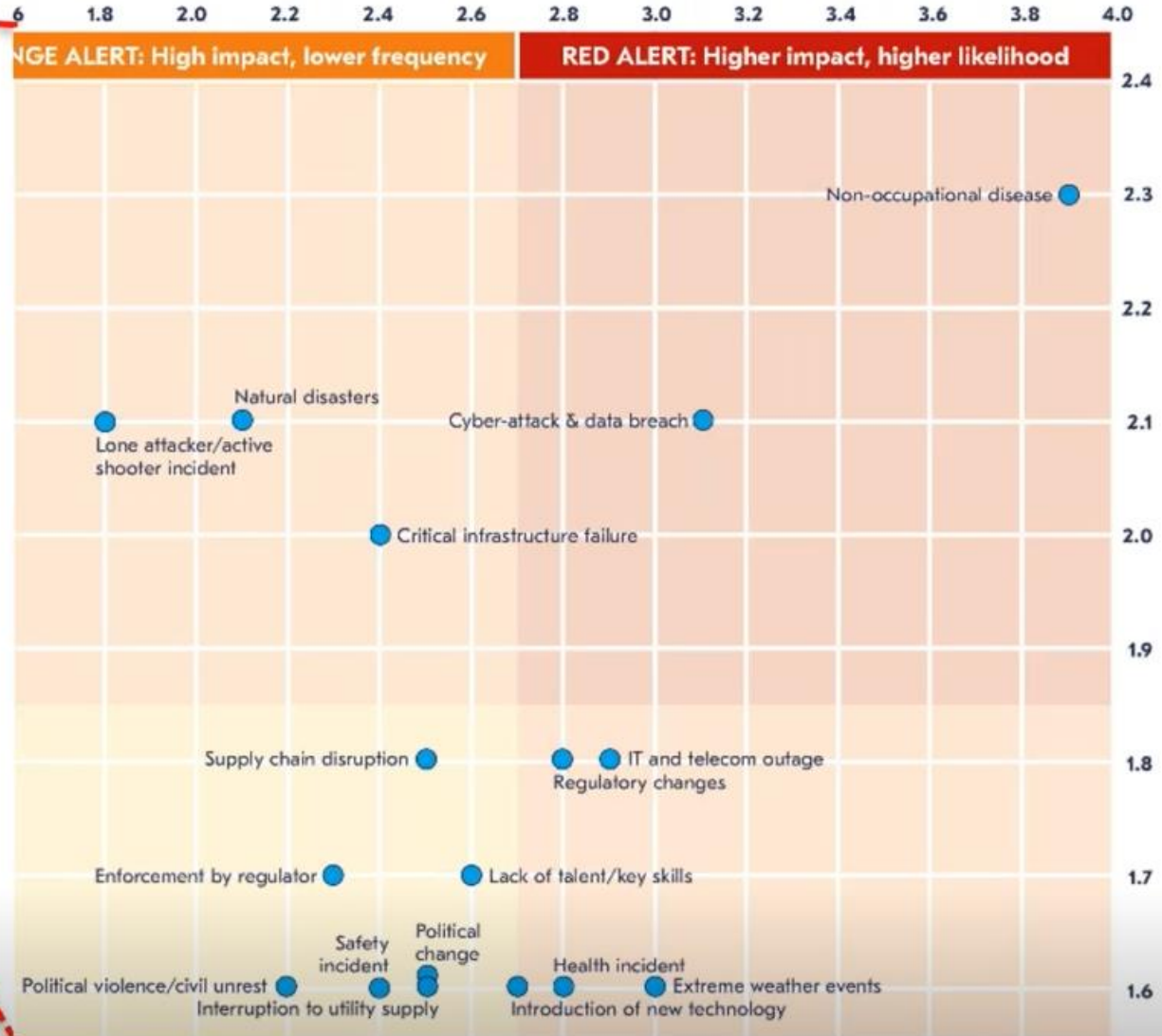
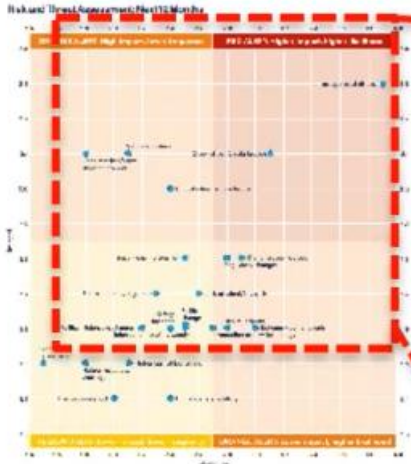
Organizations now more aware of the need to plan for “grey rhinos” & “black swans”

Risk and Threat Assessment: Next Twelve Months

| Ranking | | Likelihood | Impact | Risk Index |
|---------|---|------------|--------|------------|
| 1 | Non-occupational disease (e.g. pandemic) | 3.9 | 2.3 | 9.0 |
| 2 | Cyber attack & data breach | 3.1 | 2.1 | 6.6 |
| 3 | IT and telecom outage | 2.9 | 1.8 | 5.2 |
| 4 | Regulatory changes | 2.8 | 1.8 | 5.0 |
| 5 | Extreme weather events (e.g. floods, storms, freeze, etc.) | 3.0 | 1.6 | 4.8 |
| 6 | Critical infrastructure failure | 2.4 | 2.0 | 4.8 |
| 7 | Supply chain disruption | 2.5 | 1.8 | 4.5 |
| 8 | Health incident (occupational disease, reportable occupational disease, stress/mental health, increased sickness absence) | 2.8 | 1.6 | 4.5 |
| 9 | Lack of talent/key skills | 2.6 | 1.7 | 4.4 |
| 10 | Natural disasters (earthquakes, tsunamis, etc.) | 2.1 | 2.1 | 4.4 |

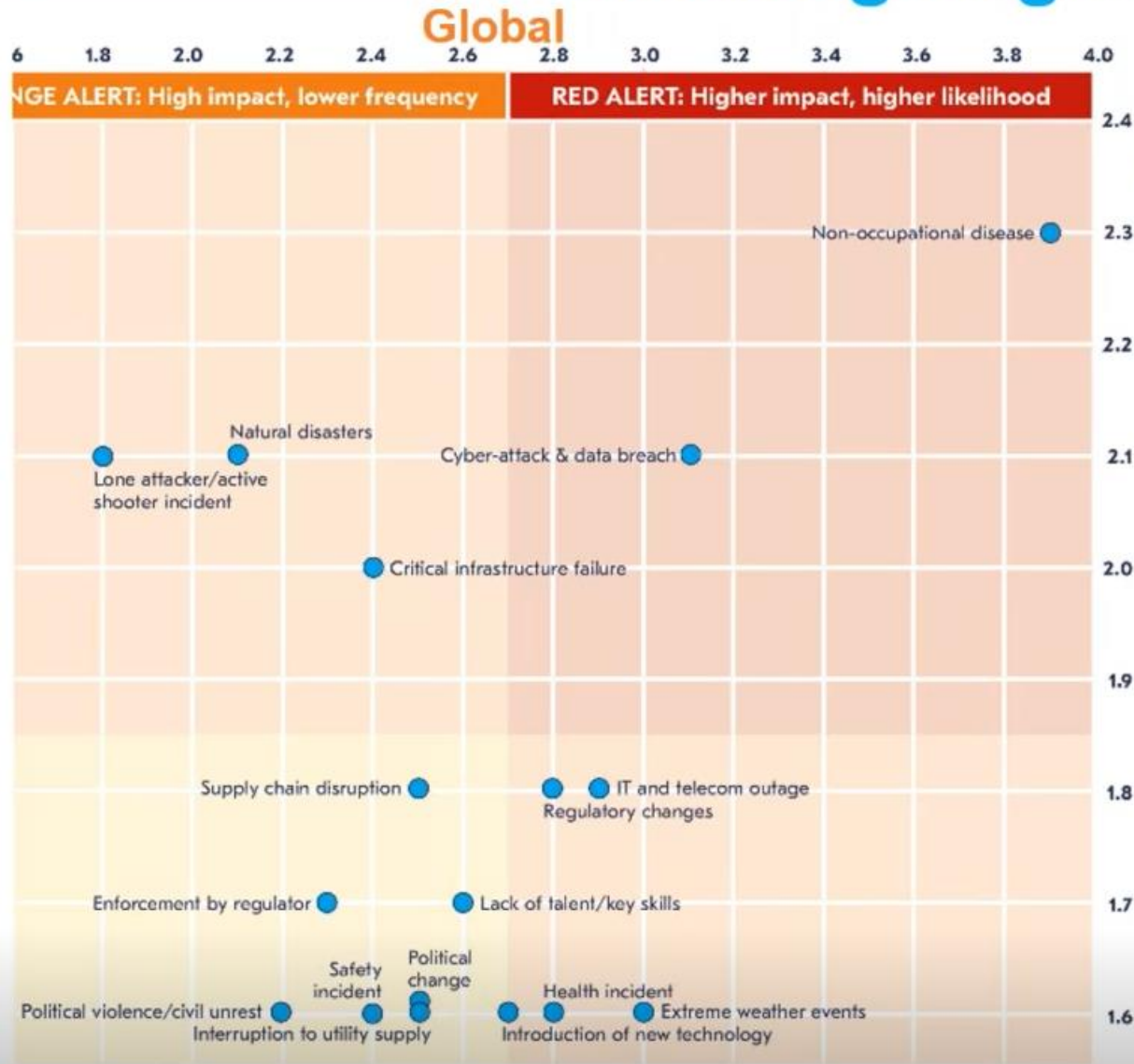
| Ranking | | Likelihood | Impact | Risk Index |
|---------|--|------------|--------|------------|
| 11 | Introduction of new technology (IoT, AI, Big data) | 2.7 | 1.6 | 4.3 |
| 12 | Interruption to utility supply | 2.5 | 1.6 | 4.0 |
| 13 | Political change | 2.5 | 1.6 | 4.0 |
| 14 | Enforcement by regulator | 2.3 | 1.7 | 3.9 |
| 15 | Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident) | 2.4 | 1.6 | 3.8 |
| 16 | Lone attacker/active shooter incident | 1.8 | 2.1 | 3.8 |
| 17 | Political violence/civil unrest | 2.2 | 1.6 | 3.5 |
| 18 | Exchange rate volatility | 2.4 | 1.4 | 3.4 |
| 19 | Higher cost of borrowing | 2.1 | 1.5 | 3.2 |
| 20 | Energy price shock | 2.0 | 1.4 | 2.8 |
| 21 | Natural resources shortage | 1.8 | 1.5 | 2.7 |
| 22 | Product safety recall | 1.5 | 1.5 | 2.3 |

Risks which have laid dormant for years are re-emerging on the risk landscape

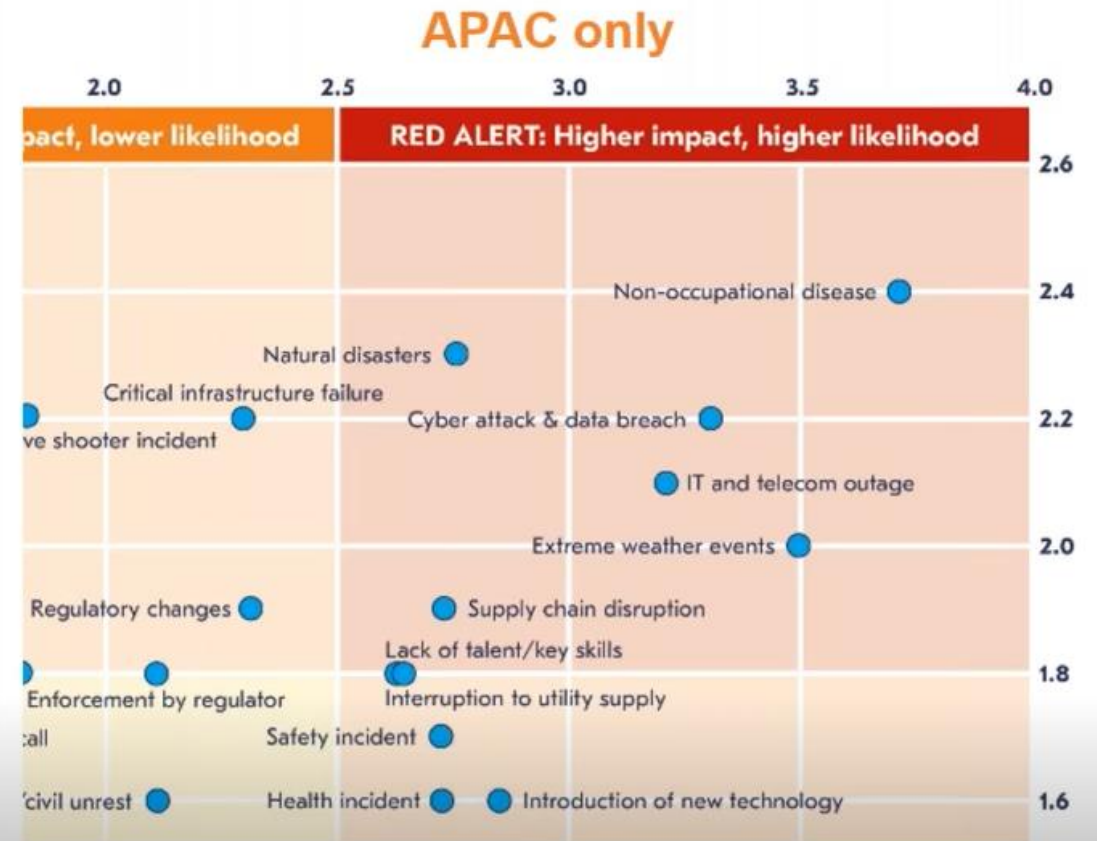


**Risk and Threat
Assessment: Next
Twelve Months**

APAC has greater concerns for other types of events going into 2021



Risk and Threat Assessments: Next Twelve Months



Consequences of Disruptions



2020's impact on staff morale/wellbeing has resulted in a renewed focus on "people"

Top five impacts or consequences of disruptions over the past twelve months



Loss of productivity:
64.8%



Negative impact on staff
morale/wellbeing:
61.4%



Loss of revenue:
51.7%



Increased cost of working:
43.6%



Staff loss or displacement:
40.3%

Benchmarking Business Continuity



2020 has delayed ISO 22301 certification for some, but more now using it as a framework



47.6%
We use ISO 22301 as a framework but are not certified to it.

5.1%
We use ISO 22301 as a framework, are not certified to it, but are in the process of getting certified.

12.5%
We use ISO 22301 as a framework and certify against it.

6.4%
We don't currently use ISO 22301 as a framework but we intend to move towards this during 2021

28.3%
We don't use ISO 22301 as a framework and have no plans to move towards this during 2021

The Organizational Resilience guidance standard enters the top 10 for the first time

Other management system standards used to manage risk/resilience: Top 10

| | | |
|----------|-----------------------|-------------------------------|
| 1 | ISO 27001 | IT Governance |
| 2 | ISO 31000 | Risk Management |
| 3 | ISO 9001 | Quality Management Systems |
| 4 | ISO 14001 | Environmental Management |
| 5 | NFPA/CSA Z1600 | Disaster/Emergency Management |

| | | |
|-----------|------------------|--|
| 6 | ISO 45001 | Occupational Health & Safety |
| 7 | ISO 14971 | Risk Management for Medical Devices |
| 8 | ISO 13485 | Quality Management Systems for Medical Devices |
| 9 | ISO 20000 | IT Service Management |
| 10 | BS 65000 | Organizational Resilience |

Certification to ISO 22301 has helped to bring balance sheet gains in a turbulent year

What benefits does certification provide to you and your organization?
(selected answers)



It increases our
organization's resilience:
71.8%



It enables consistent
BCM measurement
and monitoring:
69.0%



Ensures alignment
with industry peers:
56.3%



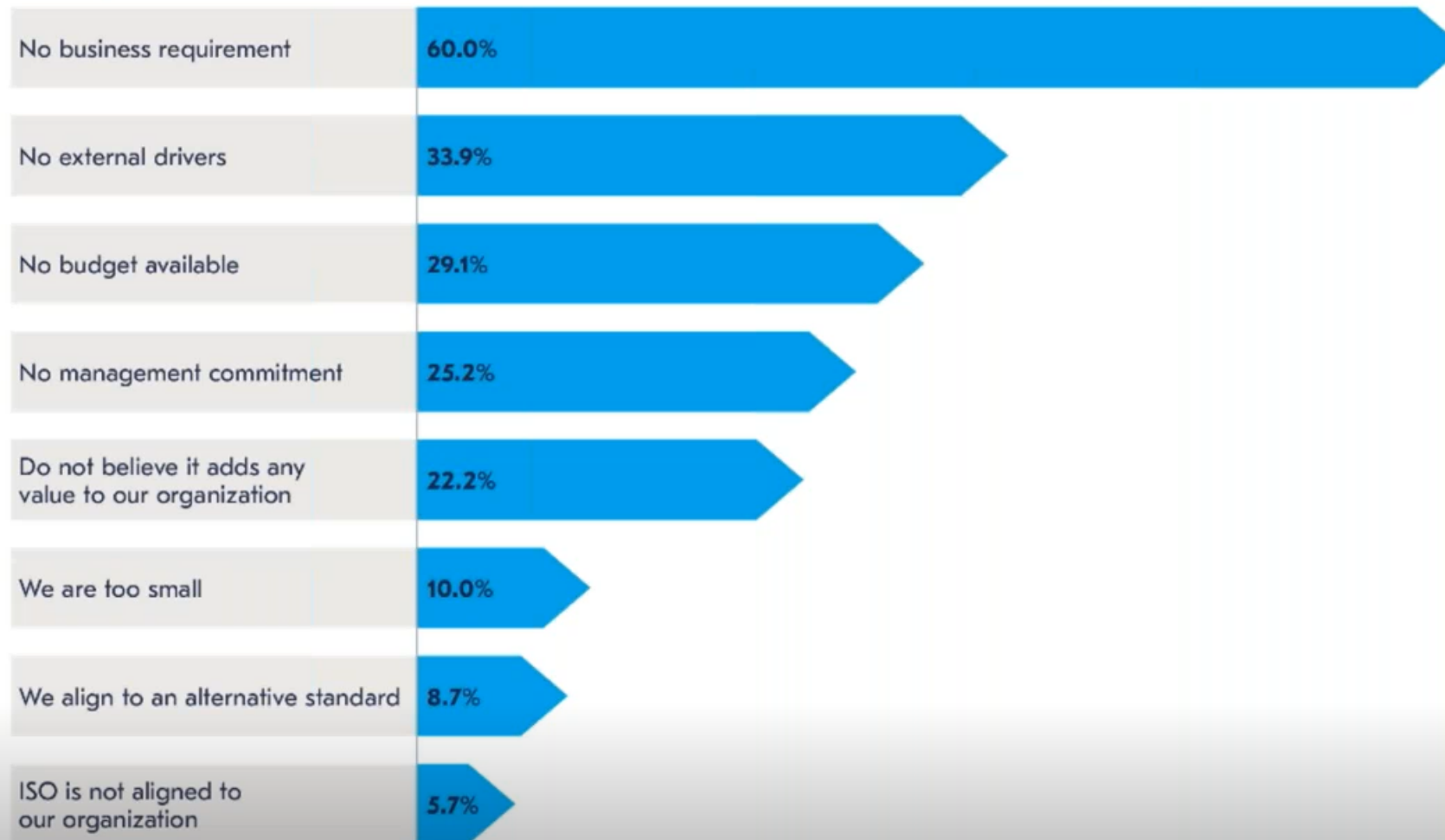
Helps to reduce
insurance costs:
40.9%



Supports international
trade:
36.6%

More organizations are now aligning to ISO 22301, but many feel little need to certify

What are your reasons for not being certified or having no plans to certify to ISO 22301?



Benchmarking longer term trend analysis



COVID-19 has prompted organizations to take a more structured approach to trend analysis



52.8%
Yes, this is conducted by a central, corporate function or department (e.g. Business Continuity, Strategy or Risk).

28.5%
Yes, but many different departments do this according to their own needs.

16.6%
No, we don't do this.

2.1%
Unsure

Usage of *all* sources has increased, with external reports seeing the strongest rise

How do you conduct a trend analysis of the risks and threats to your organization?

Top 5 answers



Internal risk and threat assessment:

91.7%



External reports/industry insight (e.g. Horizon Scan):

71.7%



Risk registers:

71.7%



Participation to industry events/conferences:

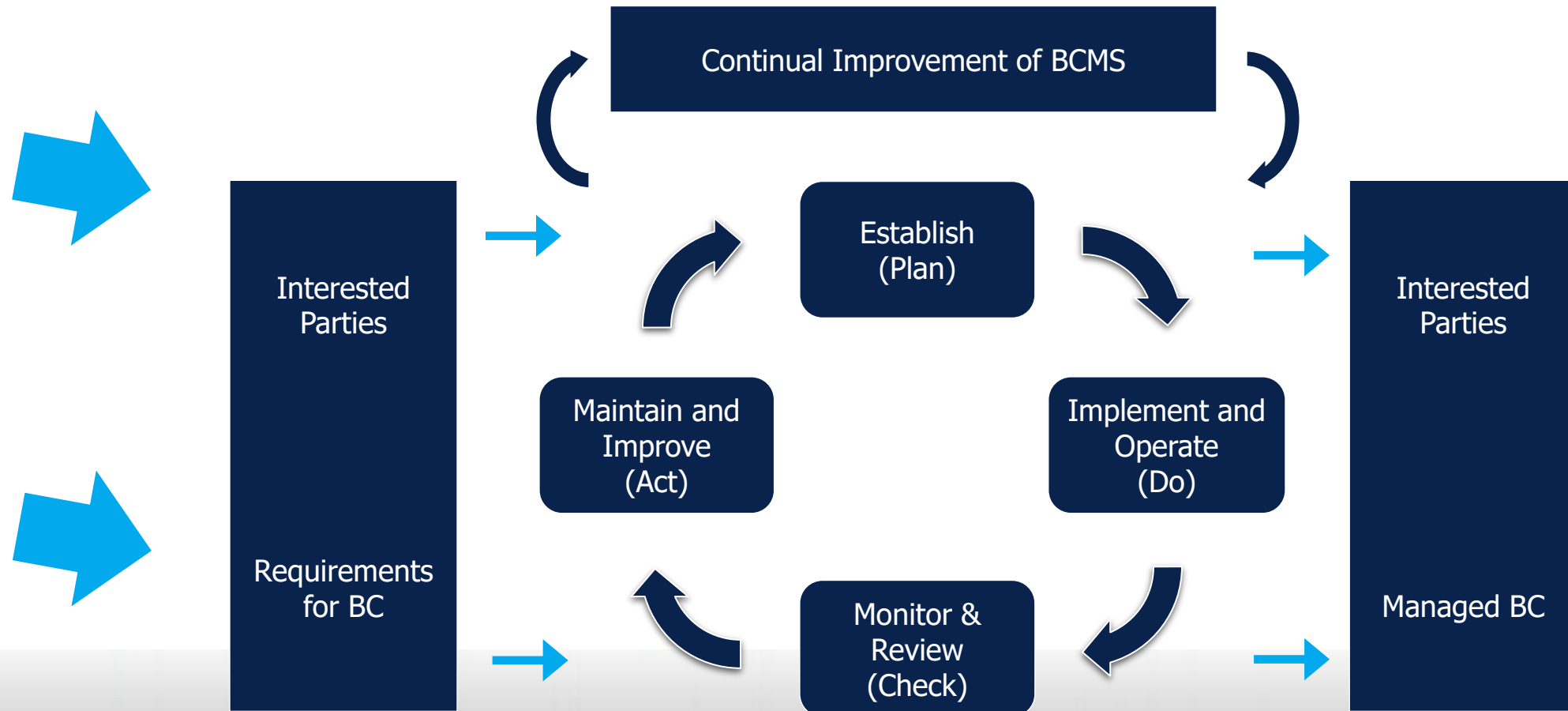
58.7%



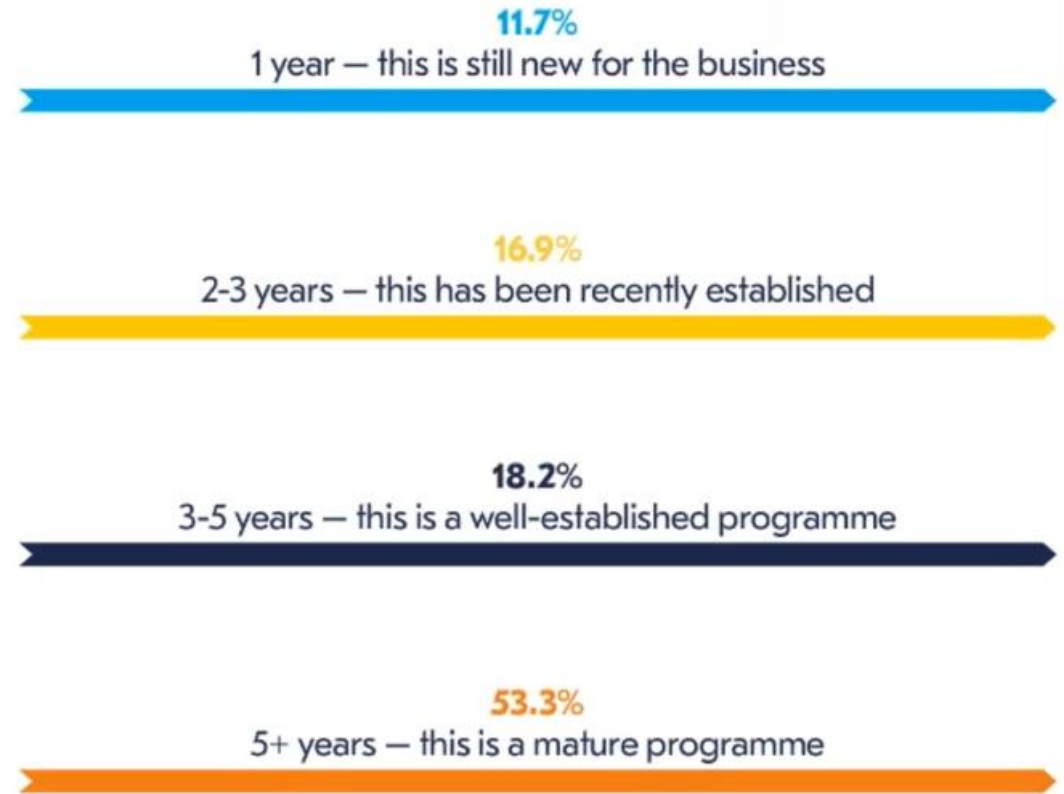
Social media monitoring:

44.4%

How does Horizon Scanning influence Business Continuity Management



More than half of organizations have been engaging in BCM for over five years



Key Lessons

- **The experience of 2020 has served as a lesson in the importance of horizon scanning and a broadened risk awareness.**
- **COVID-19 remains top of mind for many professionals, but the importance of being aware of emerging risks is crucial.**
- **The primary impact of COVID-19 has been on people rather than profits.**
- **Capitalise on management's heightened attention on horizon scanning and business continuity.**
- **Start to prepare consider longer-term risks in planning.**
- **Consider the bottom line gains that can be made from ISO certification.**

Business Continuity

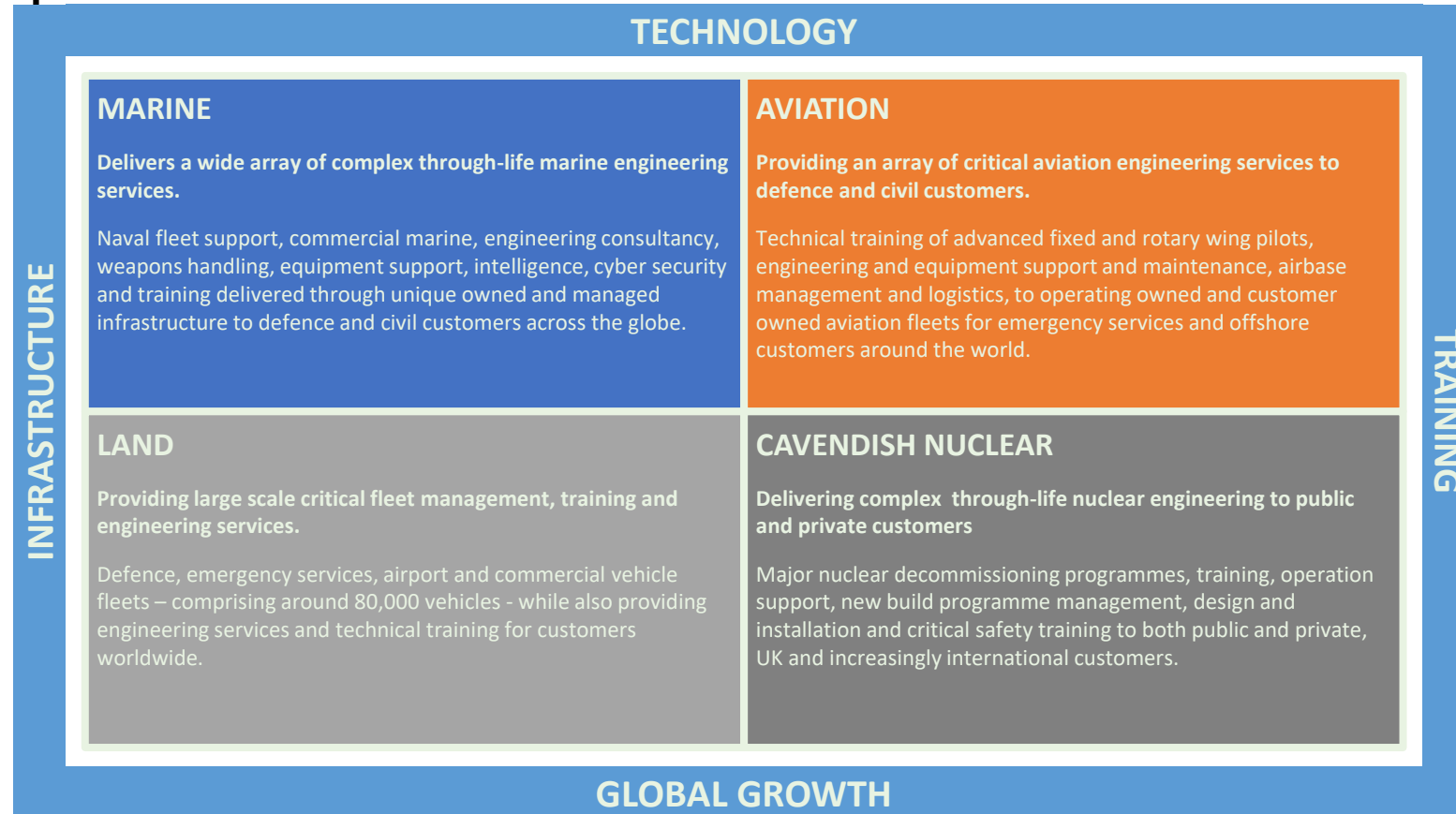
- › Andrew Curlewis Director Future Programmes
 - › Babcock New Zealand

babcockTM

At a glance



Group Structure – How We Operate





babcock

Devonport

**Marine
Industrial
Design**

**Air New Zealand – Ground
Support Maintenance Contract**

Dockyard
Management
Contract,
Royal New Zealand
Navy

Supply Chain
delivering
\$40M/yr

**Asset
Management**

37 naval
vessels under
management

Fixed High
Frequency
Radio contract

**490 Employees
(Incl 42 Navy
personnel)**

Largest
Calibration
Centre in NZ

**Commercial marine
services**

NZ Largest
Graving Dock
1888 (160m)

*“Those who protect or serve our
Nation rely upon us for their
support”*

49 Design
Engineers



Understand the Issue

Risk Realisation - March 2020

- Watching the world react
- Tested large scale working from home
- Separation of workforce concept - Red/Green Teams
- Understanding the customers immediate needs



Derive Solution

Command & Control

- Saturday 21st March 2020
- Command Huddle
- Establish Immediate actions
- Establish a Battle Rhythm



Customer

Derive Solution

- Use of common language
- What was the Command Aim?
- All subsequent activity was conducted collaboratively



babcock **NAVY** **MINISTRY OF DEFENCE** **DEFENCE FORCE**

PARTNERSHIP CHARTER

Our Purpose
Working together to sustainably deliver available, capable and safe ships and maritime systems to advance New Zealand's interests from the sea.

Our Pillars

| | | | |
|--|---|---|--|
| Integration The act of combining into an integral whole across the maritime enterprise | Agility The ability to respond rapidly to changes in the internal and external environment, without losing momentum or vision | Trust Transparency Relationships Understanding Shared successes Truth telling | Mana Demonstrate prestige; authority; control; power; influence; status; spiritual power; and charisma |
|--|---|---|--|

Our Promises

- Partner and plan for mutual success
- Engage regularly to align communication and requirements
- Promote moral courage
- Tell the unvarnished truth
- Protect our integrated plan
- Hold each other accountable
- Celebrate and share success

David Ruff CEO Babcock Australasia
CDRE Mathew Williams DCN RNZN
John Finderup DMD MoD
AIRCDRE Darryn Webb ACCAP NZDF
BRIG Rob Krushka COMLOG DLG

Promote Vision

Consultation & Comms

- Consultation with 3 Unions
- External Stakeholders – Wellington, Adelaide, London
- Our People
- Our Supply Chain
- Documentation of the plan
- Txt, email, video, briefings



Do Activity

Implementation



- Separation of Workforce
- Working from home
- Visible Leadership on site and virtually
- MBIE Inspection & Accreditation
- Virtual on boarding of new staff
- Docking/Undocking/Docking
- FaceTime/Zoom/MS Teams

Review



- Daily/Weekly review meetings
- Our People
- Business Leaders H&S forum
- COVID Level Changes

Learn

Business as Better

- IT budget takes a hit!
- Learning from experience
- Implementing Agile working across business
- Use of augmented reality to solve the NZ Border issues



Recognition

Babcock NZ - winner of the Strategic Partnership Award, one of the 2020 Minister of Defence Awards of Excellence to Industry.

“Your work during the lockdown in developing a business continuity plan that split the entire Navy dockyard up into teams helped to keep the Navy running through the pandemic.”



Key Take a ways

- Understand the Issue
- Derive a solution
- Promote vision
- Do Activity
- Learn

Andrew Horne | MinterEllisonRuddWatts



Andrew co-heads MinterEllisonRuddWatts' national dispute resolution practice. He also leads the firm's insurance practice.

With more than 25 years' experience as a lawyer and advocate, he regularly represents clients in mediation and at all levels of the New Zealand courts. He has extensive experience in corporate and commercial disputes, regulatory, insurance, financial services and technology disputes.

Cyber and business interruption risks



A typical cyber event

Malicious hacker data breach

Types of loss

- Your own costs
- Lost profits
- Liability to other people
- Fines and penalties

A photograph of the Reserve Bank of New Zealand building, featuring a large glass facade and a prominent sign that reads "RESERVE BANK OF NEW ZEALAND". The building is reflected in the glass windows. In the background, a circular building with a tiered roof and green trees are visible under a clear blue sky.

RESERVE BANK OF NEW ZEALAND

Cyber insurance

Typically covers:

- Cost of expert help
- PR costs
- Data restoration costs
- Ransom costs

May cover:

- Hardware and software repair costs
- Business interruption costs – lost profit
- Liabilities to third parties and contract penalties
- Fines, penalties and defence costs
- Digital media claims – e.g. defamation



Cyber insurance ...

Typical exclusions:

- Misdirected payment losses
- Damage to computer system from usual perils
- Loss caused by an authorised person
- Loss caused by a system failure
- Natural disasters
- Fines and penalties other than data protection



Professional Indemnity Insurance

- Breach of confidence – client data
- Loss of client data
- Conduct by employees – social media
- Misdirected funds (beware exclusions)
- Breach of client privacy
- Breach of client IP rights
- Transmission of computer virus



Fidelity and Crime insurance

- Data breaches by employees
- Theft of money by employees
- Intentional damage to systems
- Ransom demands



Statutory Liability insurance

- Fines for privacy breaches
- Fines and penalties under industry or regulatory schemes
- Defence costs



Hints and tips

- Identify key risks for your business
- Ask broker which policy covers
- Consider any gaps in cover
- Consider any sub-limits of cover
- Think about reducing risk

Recommendation

1

2

3

4

5

6

7

8

