www.pwc.com.au

The Great Reboot

What will Corporate Treasury look like in the future?

June 2020

pwc

Agenda

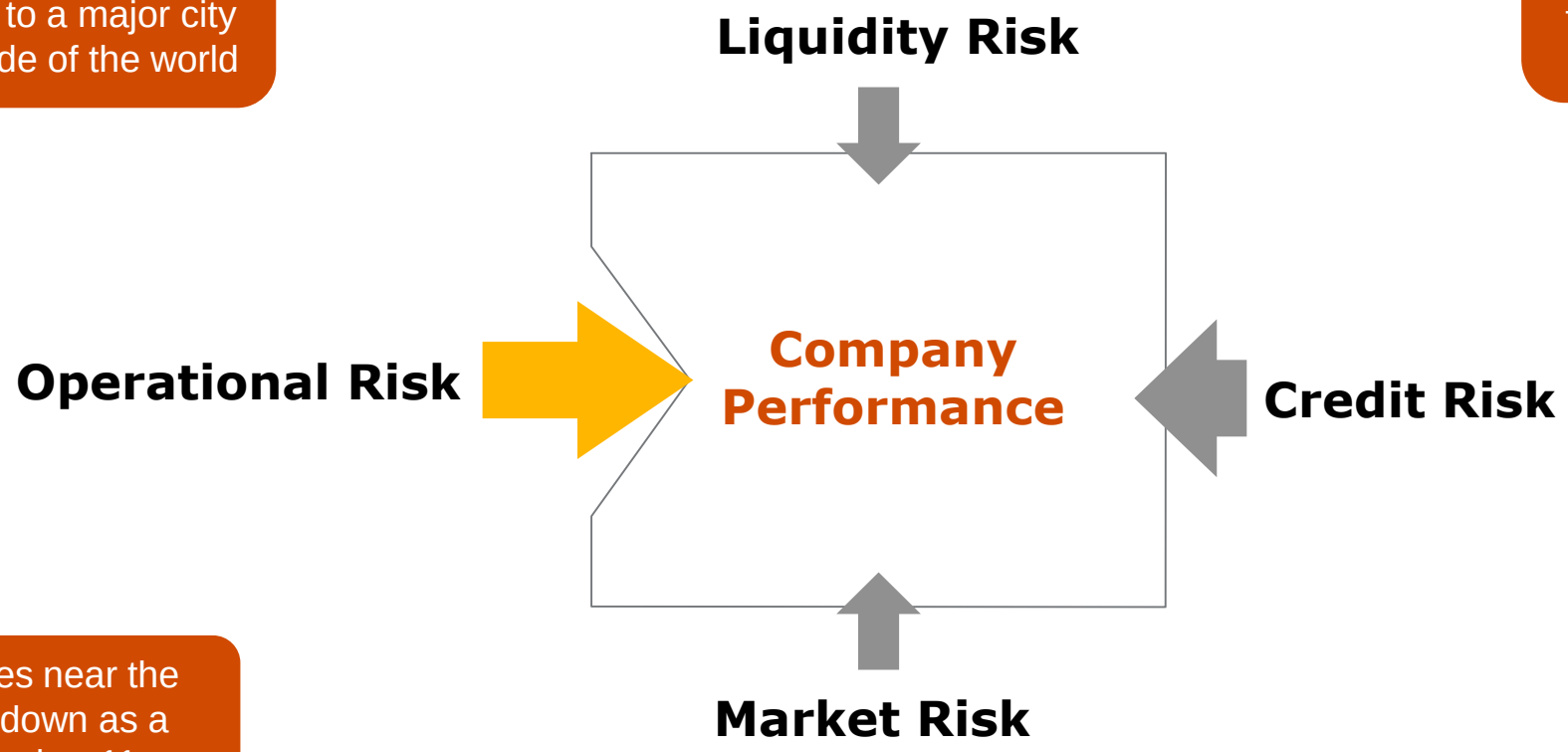
1 Introduction

What headwinds could a Corporate Treasury face?

<36 hours for infectious disease transmission from a remote village to a major city on the other side of the world

Over 300% increase in natural disaster frequency since the 1960's

7,000 signals of potential pandemic outbreaks per month



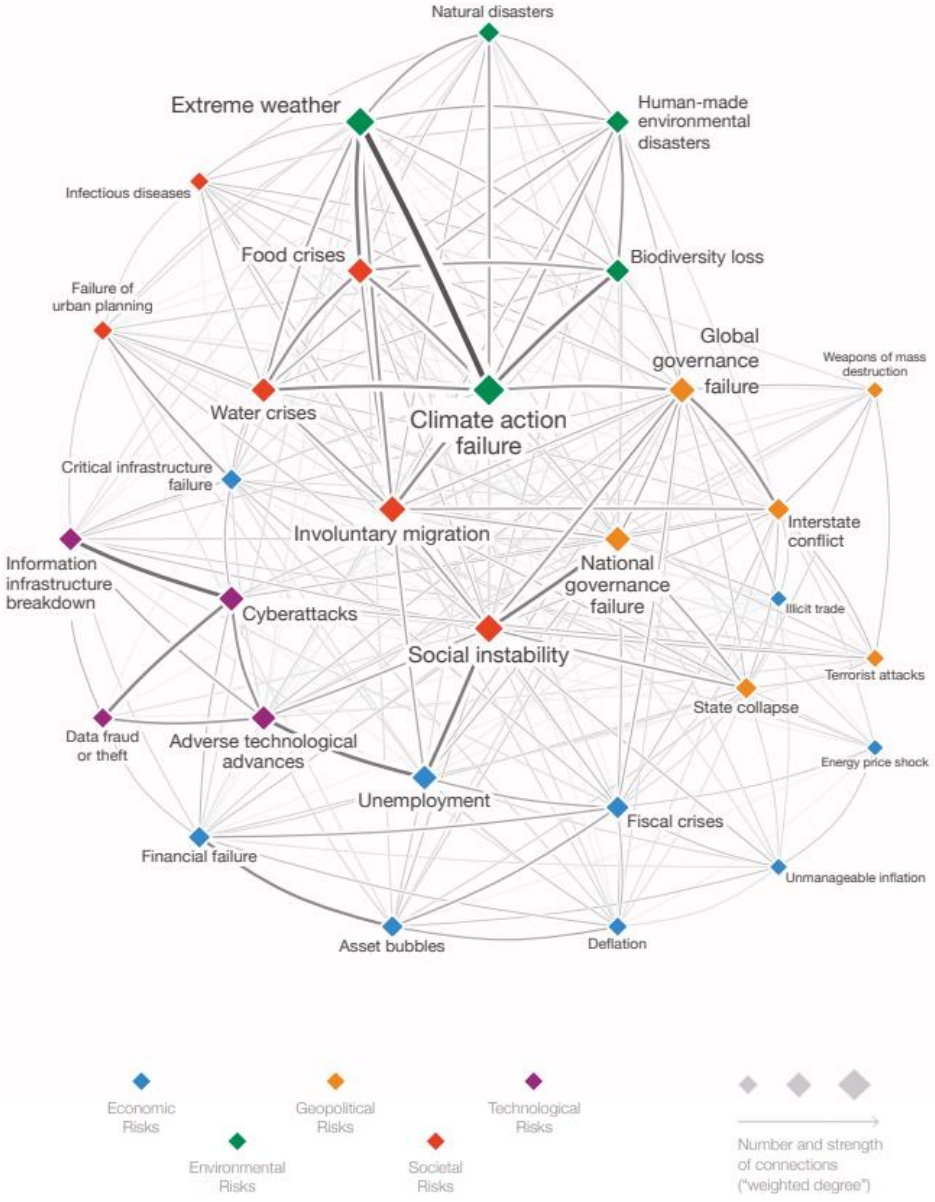
Australia's terrorism level is **Probable**, that "individuals or groups possess the **intent** and **capability** to conduct a terrorist attack in Australia"

18,000 businesses near the WTC were shut down as a result of September 11

3.1 million deaths per year due to decreased food production & supply chains

Source: World Economic Forum, European Commission, Australian Department of Home Affairs, Harvard Global Health Institute, Risk Frontiers and World Health Organisation

Interdependencies of Risk



Source: World Economic Forum

As shown, there is a known correlation between risks, both financial and non-financial.

We recognise that when we manage one risk, we can introduce another (e.g using an IRS to manage interest rate risk increases the counterparty & settlement risk).

These principles apply in our responses to disruption (e.g reduce operational risk through technology but introduce cyber & third party risks).

What do these risks mean for your Treasury? How do you directly or indirectly for manage and deal with it?

Under these scenarios, the ‘natural hedge’ is to build and increase strategic **Operational Resilience**.

Operational Resilience in a Corporate Treasury

"The ability of firms and the financial system as a whole to absorb and adapt to shocks, rather than contribute to them" – Bank of England

The ability of an Treasury department to continue to deliver Treasury services and activities in the face of adverse operational events by; anticipating, preventing, recovering from, and adapting to such events.

Operational resilience is the foundation of a strategic treasury

Governance	Integration	Measurement	Vigilance
• Have resilience incorporated into the Treasury risk appetite statement, framework and metrics. • Regular and actionable reporting to drive continuous improvement.	• Detailed view of dependencies of critical Treasury services and enablers. • Embed resilience considerations into Treasury workflows	• Defined tolerances for Treasury disruptions, based on the risk appetite statement. • Consideration of Treasury disruption scenarios against critical services	• Treasury plans and services monitored, tested and adapted on an ongoing basis. • Singular response programme for any incident.

2 Observations & Considerations

What have we seen?

Inability to sign legal documents digitally

Systems and network drives not available remotely to those who require it

Increase in bespoke and/or enhanced reporting requests. Difficult where reporting is manual and excel based.

Significant increase in cyber security risks especially with payments

Centralised contact lists and BCP were out of date or insufficient

Multiple physical versions of documents and confirmations

Limited resources to cover key treasury roles

More frequent requests reporting and analysis made difficult by lean teams and remote working

Dealing with documents arriving in the mail/fax

Shared services teams at capacity and can only provide minimal assistance

Staff wellbeing and mental health impacts, as they manage work, children, partners, isolation etc.

VPN or internet bandwidth limitations

Reduced availability or accuracy of exposures from the business units

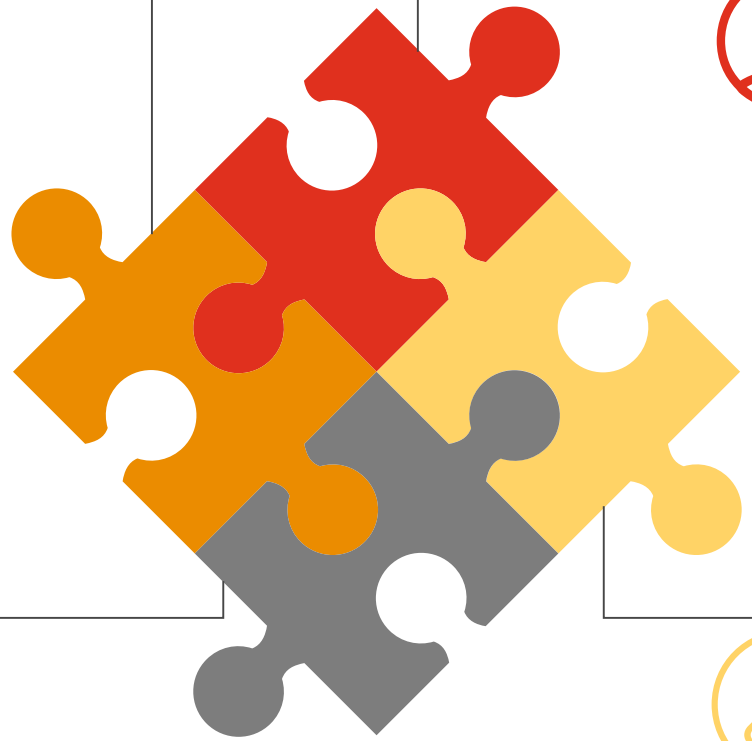
How can Treasury embed operational resilience?

Need to look at it from two perspectives:

- Tactical – what are the quick fixes that can be implemented to ensure you are better prepared next time
- Strategic – what from a policy, technology and process perspective needs to change to improve operational resilience

Treasury Technology
Review the treasury technology stack with a focus on supporting extended remote operations and surges in analytics and reporting.

People
Prioritise the enablement of people, through the consideration of the operating model and team size.



Treasury BCP
Development of a strong and robust Treasury BCP that can include emergency treasury policy and procedures.

Legal & Governance Frameworks
Assessment of the legal and governance frameworks covering transaction banking, debt and derivative execution, etc.

Treasury Technology

Over 80% of Treasurers agree cost is the biggest hurdle of technology adoption

Treasury A

Description

- 1-3 dedicated Treasury staff
- Excel and paper based
- Smaller counterparty panel
- Cash management focused
- Outsourced Treasury tasks
- Minimal &/or vanilla derivatives

Challenges

- Limited bandwidth to stretch
- Excel file management
- Manual cash visibility & operations
- Increased risk of manual error
- Limited remote working capability
- Treasury administered solutions

Potential Solutions

- Integrate an Excel user framework
- Leverage the existing broader stack
- Adopt complementary technology
- Consider cloud or co-authoring
- Engage IT & other business units
- Perform gap analysis

Treasury Technology

3x more likely to upgrade a TMS than change

Treasury B

Description

- 5-7 dedicated Treasury staff
- Likely TMS based
- Semi-integrated ecosystem
- Excel for cash & reporting
- Dedicated Treasury Accountant/s
- Increased use of derivatives

Challenges

- Older or Phase I TMS implemented
- “Black box” solutions & connections
- Workflow for the sake of workflow
- Manual data tasks still exist
- Outdated Excel models
- Irritating amount of paperwork

Potential Solutions

- Review & document the ecosystem
- Reconcile the TMS & capabilities
- Implement a task scheduler
- Standardise & consolidate
- Adopt specialised technology
- Undertake digitisation review

Treasury Technology

92% consider Operational Resilience an important driver for Treasury technology adoption

Treasury C

Description

- 8-15 dedicated Treasury staff
- Integrated TMS backbone
- Well developed ecosystem
- Enhanced STP enabled
- BI reporting & analytics
- More integrated into the business

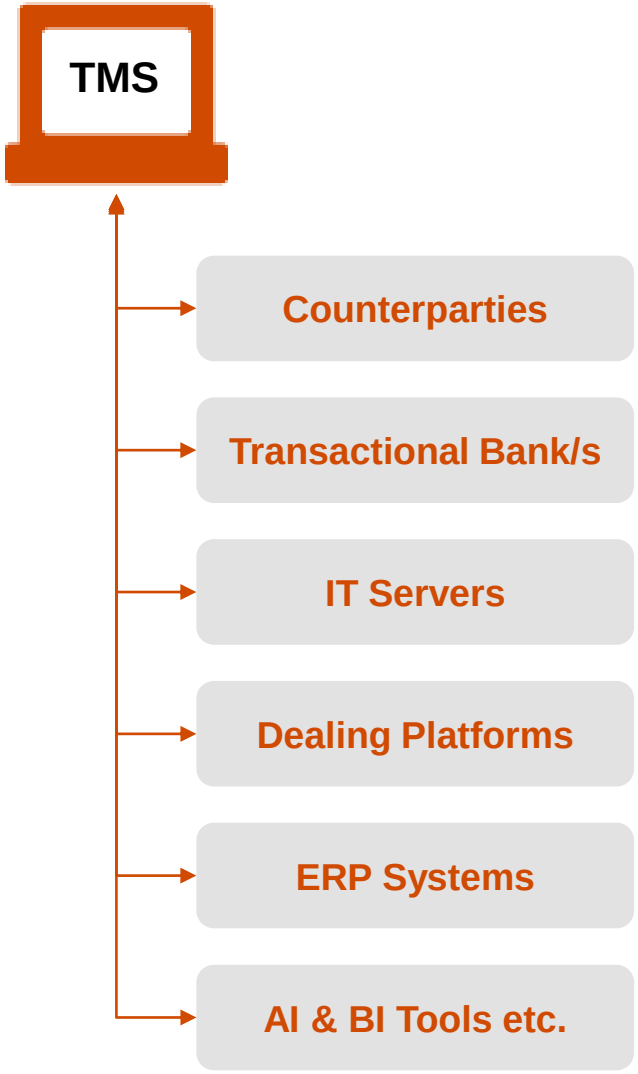
Challenges

- Multiple vendors & upgrades
- System interdependencies
- Cyber & 3rd (or 4th) party risk
- Increased ecosystem management
- Hosting & DRP obligations
- Data quality & management issues

Potential Solutions

- Develop an ecosystem map
- Add multiple data validation checks
- Dedicated ecosystem resourcing
- Conduct regular cyber reviews
- Potential solution consolidation
- Alignment of hosting & DRP duties

Considerations for enhancing the Treasury ecosystem



- How does each vendor/touch point's DRP relate?
- What happens if a system vendor is taken over or goes under?
- What are the connections between the systems?
- What are the fall backs for services (usually DRP) and connections in the short and long term?
- What is the process and activation triggers for a DRP or BCP and the relationship to the business, IT, 3rd parties?

A cyber hack occurs every **39 seconds** on average

Cyber threats have increased almost **500%** for some industries, experts expect a **30-40% increase** in cyberattacks due to increased remote working

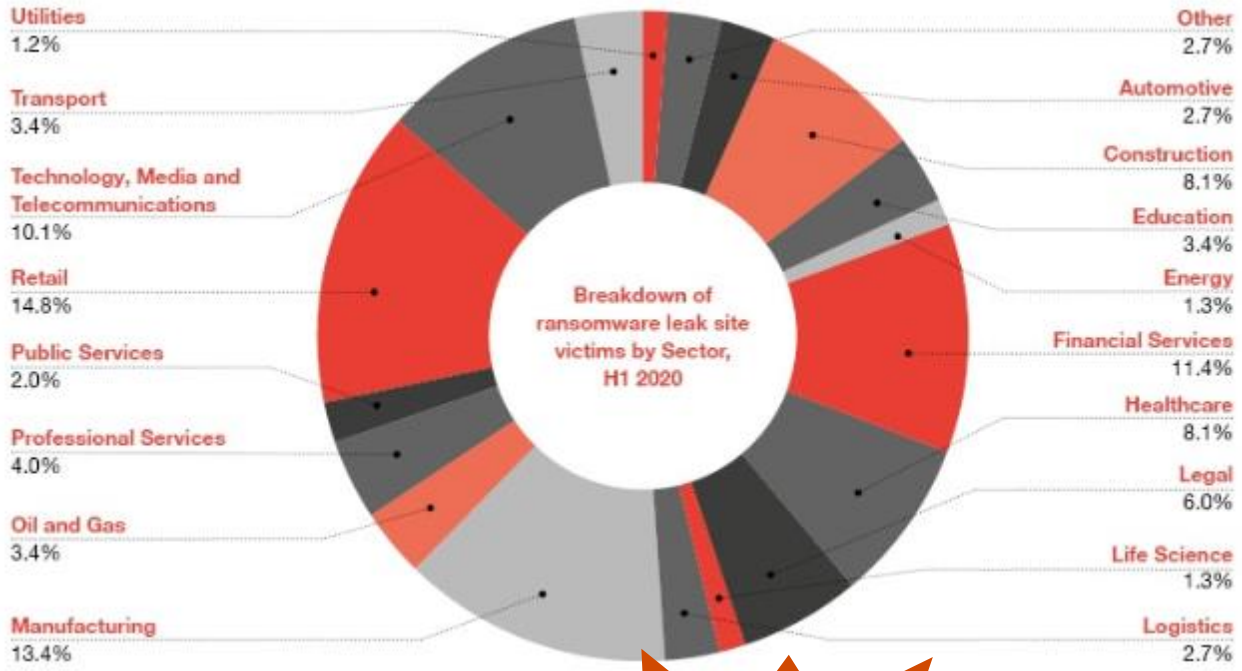
Increased Cyber Threats

Between 11th March - 20th May, over 150 global organisations had their data leaked online.

$3t estimated cost of cyber crime against businesses

What's caused the increase in cyber incidents?

- Espionage actors operating for governments with economic interests at play or increased geopolitical tensions
- Reduced spending from consumers means groups that traditionally go after credit card details need to find new income sources
- Increased opportunity to target organisations in desperate situations
- Ransomware run as affiliate programmes, have triggered growth in the number of affiliates participating in their programmes. Ransom demands are growing, encouraging other actors to enter the market
- Opportunistic reconnaissance identifying vulnerabilities, possibly related to rapidly stood up remote working practices



Source: PwC, Juniper Research

This will impact Treasury!

What cyber threats will you face?

78% of treasury organisations surveyed were hit with payment fraud in 2017

Type of Cyber Threat	Definition	Example
Malware	Leverages a vulnerability to install 'non-approved' software. Includes ransomware, spyware, viruses etc.	Fraudulent email with hidden malware attachment.
Phishing	Involves fraudulent communications that appear to come from a reputable source, usually through email.	Counterfeit request for a payment to a cybercriminal's account.
Zero Day Exploit	A vulnerability is announced but before a patch is implemented.	Treasury software is not immune, and often upgrades are delayed.
Man in the Middle	Hacker inserts themselves into a two-party channel.	Treasurer using airport Wi-Fi.
Denial of Service	Attack systems, servers, or networks with traffic to drain bandwidth.	External attack on Treasury servers.
SQL Injection	Attacker targets a SQL server to extract information.	TMS is likely an SQL database.
DNS or HTTP Tunnelling	The hacker utilises DNS or HTTP protocols to disguise data theft or remote access.	Attackers hide Treasury data to look like browser traffic to a remote web site.

75% of CFOs view cyber security as a critical concern vs **28%** of Treasurers

Source: PwC, CISCO, The Global Treasurer

People – What's the issue?

Examples of critical treasury processes

The average corporate Treasury size is **4** dedicated staff

Treasury 1

4 dedicated Treasury staff

Treasury 2

8 dedicated Treasury staff

Treasury 3

8 dedicated Treasury staff

How will each company deal with staff not being available?

People – Potential solutions

Key Considerations & Observations:

- Safety of staff and customers will remain paramount.
- Acknowledge individual requirements are unique to enable staff.
- Establish strong and effective communication lines.
- Standardise and prioritise workflows where possible.

78% of people want to continue working from home in some part

Potential Solution	Definition	Pros	Cons
Internal to Treasury	Onboard a new Treasury professional or Treasury Graduate.	• Dedicated and specialised team member to assist. • Ability to develop with the team.	• May not have budget. • Hiring, training and development time/requirements.
External to Treasury	Utilise people from the finance team or business.	• Familiar with the business and currently established. • Ability to invest in career progression & diversify.	• Currently untrained and required to keep them current. • Consideration around their priorities during busy periods.
Outsourcing	Utilise another firm to supplement the Treasury team and perform selected Treasury functions.	• Access to qualified staff. • Ability to leverage as required.	• Potentially reduced control and synergies. • Introduces 3rd party and alternative operational risks. • Unable to select staff.

The Legal & Governance Frameworks

What challenges could I face moving forward?

Considerations

- What process do I have for digital signatures (including their use and storage)? Will all my counterparties/banks accept these? What about my auditors?
- How will a robust document management process be maintained?
- How can business documents and their certified true copies be supported?

Example: Transactional Banking

- How do I add new users?
- Who can witness documents remotely?
- Will I need to change the process for opening new bank accounts?
- How will I manage KYC compliance remotely?
- What implications do FATCA, CRS, AML etc. have?

Engage with your stakeholders (including bank counterparties) with a view to digitise and optimise the process

Treasury BCP

A good Treasury Business Continuity Policy (BCP) will enable the elements of technology, people and the legal/governance frameworks to cohesively work together under alternative operating parameters.

Example considerations of a BCP for Treasury

- **Document management** – approval, history, assumptions.
- **Definitions** – scope, purpose, roles, priorities/systems, activation criteria & authorities, relationship to business BCP.
- **Loss of functions/services** – Detailed actions under each scenario.
- **Contacts** – Embedded or linked internal & external contact lists.
- **Related documents** – Embed (and have embedded) the BCP to necessary supporting documents and templates.

Consider emergency delegated authorities

A strong Business Continuity Policy is supported by a well-structured Business Continuity Programme

1. Business Continuity Policy
2. Identify Critical Treasury Processes
3. Risk Assessment
4. Build Resilience Plans
5. Training & Awareness
6. Exercising & Monitoring

3 The Return

The Return

The first 30 days…

1

Staffing

Will staff return at once, staggered or on an alternated roster? What structures will be needed to support this?

How do you continue to maintain social distancing at work? Can you physically do it or will you have to continue as a split team?

2

Delegation and system access

Likely that system access was modified to support the remote operating environment. Should this be removed and/or linked to the BCP?

Preparing for staff members getting sick for extended periods of time. What is the backup process and what is required to support it? e.g. system access, training etc.

3

Physical document control

Compile and reconcile hard copies of physical documents issued during the WFH period e.g. confirmations, compliance certificates, facility documents etc.

4

Communicate with 3rd parties

Advise counterparties and vendors of when the return of staff will occur. Also important to communicate any immediate changes, especially if a split team approach is taken or new staff are assigned as back ups.

5

The honest appraisal

Review how treasury performed during the WFH period and assess if any breaches, missed tasks, unnecessary costs or missed opportunities occurred?

Assess the risk and reporting models to see how they can be improved to incorporate a COVID-19 scenario impact

6

Focusing the team

The world moves on including regulation. Assess all projects put on hold to determine if they need to be restarted. What new issues need to be dealt with e.g. LIBOR replacement.

The Return – Embedding Operational Resilience in Treasury

Medium term…

1. Conduct a high level scan

Perform an end-to-end benchmark scan and gap analysis to identify the structural opportunities.

2. Embed operational resilience

Develop a plan and implement solutions to the structural opportunities identified. Ensure that changes consider any other risks that may be introduced.

3. Run a scenario testing

Perform multiple scenario analyses to test the end-to-end capabilities of the Treasury department's operational resilience.

Operational Resilience

Operational resilience is embedded from ongoing investment into:

- Treasury Technology
- People
- Treasury BCP
- Legal & Governance Frameworks

These entrench a Treasurer as a strategic partner and an anchor through disruption.

"Operational resilience is another area that we should never take for granted"
– Wayne Byres, APRA Chair

Contact

Chris Nelson

Senior Manager – Treasury Advisory

Email: Christopher.A.Nelson@pwc.com

Phone: 0432 020 895

Thank you

www.pwc.com.au

© 2020 PricewaterhouseCoopers. All rights reserved. PwC refers to the Australia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. Liability limited by a scheme approved under Professional Standards Legislation.