



IMAS 16th Regulatory Roundtable



June 14 / Wednesday



2:15pm - 5:15pm



Deloitte Singapore
6 Shenton Way,
OUE Downtown 2 #33-00
Singapore 068809





imas

INVESTMENT MANAGEMENT
ASSOCIATION OF SINGAPORE

SESSION STARTS IN

1 MINUTE

Enjoy your session

IMAS 16th Regulatory Roundtable



imas

INVESTMENT MANAGEMENT
ASSOCIATION OF SINGAPORE

SESSION STARTS IN

30 SECONDS

Enjoy your session

IMAS 16th Regulatory Roundtable



imas

INVESTMENT MANAGEMENT
ASSOCIATION OF SINGAPORE

WELCOME REMARKS BY:

Carmen Wee

CEO, Investment Management Association of Singapore (IMAS)

IMAS 16th Regulatory Roundtable



imas

INVESTMENT MANAGEMENT
ASSOCIATION OF SINGAPORE

OPENING REMARKS BY:

Fann Teh

Chairman of IMAS Regulatory Committee

IMAS 16th Regulatory Roundtable



Navigating the Business Continuity Management Guidelines
by Monetary Authority of Singapore
IMAS 16th Roundtable 14 June 2023



MAKING AN
IMPACT THAT
MATTERS
since 1845

Speakers



Wong Nai Seng

Partner, Regulatory Strategy &
Regulatory Advisory, Deloitte
Member of IMAS Regulatory Committee



Lawren Poh

Subject Matter Expert – Crisis and
Incident Response
Director, Southeast Asia Cyber Incident
Response Lead, Deloitte & Touche LLP



Goh He Lin

Subject Matter Expert – Crisis
Management and Communications
Senior Manager, Crisis & Resilience,
Deloitte & Touche LLP

Testing & Exercises

Strengthen awareness and stress-test competency in all areas of crisis and resilience.

- Table-top
- Command Post
- Wargaming

Resilient Leadership

Develop crisis-ready leaders through training and workshops to set the tone right from the top.

Gap Analysis, Audits and Capabilities Assessments

Assess current state of and benchmark against industry peers for continuous improvements.

24/7 Crisis Management Office

Stay ahead of a crisis with real-time support and monitoring from our subject matter experts in:

- Communications
- Legal
- Incident Response
- Data Privacy

Business Continuity Programme Maintenance

Provide executive-level support as proxy BCM co-ordinator to guide the maintenance of programme and effect changes required to address regulatory updates.

Incident Investigation

Technical and project management support in containing the incident and root cause analysis.

Triage

Leverage Deloitte's Cyber Intelligence Centre to triage and neutralize threats

Investigation Review

An investigation review allows for an objective view of the steps taken

Resilience Program Development

Set frameworks and plans in place:

- Operational Resilience
- Operational Risk
- Business Continuity
- Crisis Management
- Crisis Communications
- Cyber Incident & Response
- Third-party Risk

Recovery Support

Shift mindsets from value preservation to value creation:

- Post-crisis recovery
- Reputation Management
- Scenario Planning
- Cyber Strategy Advisory
- Technology Rebuild
- Cybersecurity Governance Advisory



Programme Summary



2:15pm ▶ **Registration**

2:30pm ▶ **Welcome & Opening Remarks**
Ms Carmen Wee, CEO of IMAS
Ms Fann Teh, Chairman of IMAS Regulatory Committee

2:45pm ▶ **Presentation on the Overview of BCM guidelines by Deloitte & Touche**
Mr Wong Nai Seng, Partner, Regulatory Strategy & Regulatory Advisory, Deloitte, Member of IMAS Regulatory Committee
Mr Lawren Poh, Director, Southeast Asia Cyber Incident Response Lead
Ms Goh He Lin, Senior Manager, Crisis & Resilience

3:15pm ▶ **Networking Session and Refreshments**

3:30pm ▶ **Breakout Group Activity (Moderated by Deloitte & Touche)**

4:45pm ▶ **Individual Group Presentation and Summary**

5:00pm ▶ **Closing Remarks**
Ms Fann Teh, Chairman of IMAS Regulatory Committee

5:15pm ▶ **End**

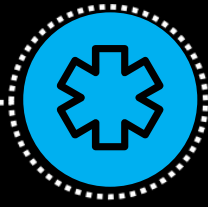
What is Operational Resilience?



Why Operational Resilience?

Operational Resilience

- **Ability to deliver critical operations through disruption.**
- **Ability to identify and protect itself from threats, adapt and recover from disruption with minimal impacts**
- **Understanding of the organisation's risk appetite**
- **Identify tolerance for disruption over a range of severe but plausible scenarios**



Pandemic-driven

Resilience was a pandemic response - from remote working measures to alternative delivery of services to customers.



Global regulatory movement

Key regulators have been seeking consultation and are underlining the importance of operational risk management across global markets.



Digital adoption

Ability of financial firms to safeguard their critical infrastructures and minimise customer harm with proliferation of new technology.



Supply-chain risks

Financial sector's interconnectedness and dependency on third parties.

MAS BCM Guidelines

01

End-to-end centric view in **ensuring the continuous delivery of critical business services** to customers.

02

All FIs should meet the new guidelines and **establish a BCM audit plan within 12 months of its issuance by June 2023**. First BCM audit should be conducted within 24 months of the Guidelines issuance.

03

The BCM guidelines **applies to all Financial Institutions:**

- Locally Incorporated and Branch
- Insurer, REIT Management
- Fund Management
- Product Financing
- Corporate Financial Advisory
- Credit and Charge Card Issuer and Licensee
- Major Payment Institution
- Credit Rating Agency
- Venture Capital Company
- Custodial Services
- Licensed Trust Company
- Market and Exchanges
- Money Changing Licensee
- Money Broker
- OTC Counterparties








Unpacking and Understanding MAS' BCM Requirements



1. What is a (Critical) Service?

Services deliver a specific outcome to an identifiable, external end user.

 Has a distinct outcome	 Is not channel-specific
 Is provided to an external end user	 Can be simply described from an end-user perspective
 Is a separate service	 Accountability is held by the organisation

Example: A baked goods manufacturer prepares a range of products for wholesale and retail customers, including national grocery stores, corporates, hospitals and small businesses.



■ Service ▶ Process

1. What is a (Critical) Service?

Identifying a service is important in order to create an inventory of business services across the organisation as a starting point.

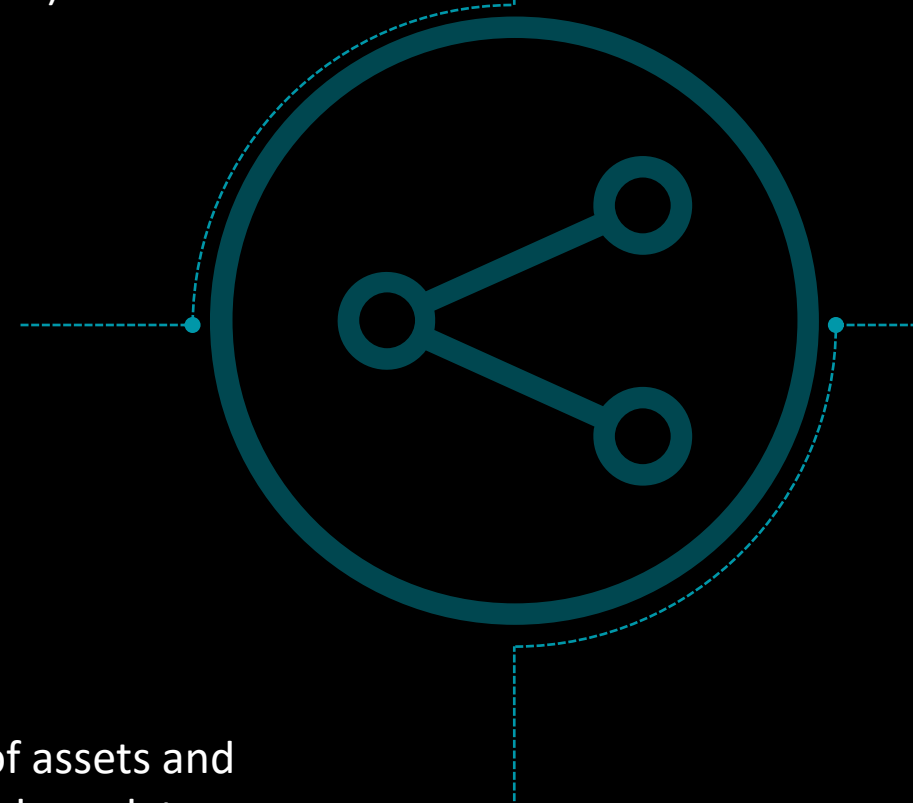
Asset Management	Banking	Insurance
Portfolio Management	Deposits	Purchase a policy
Trade Execution	Cash Settlement and Securities Trade	Policy renewal
Payments In / Payments out	Foreign exchange	Change or upgrade customer policy
Treasury	Execute payments	Claims submission
Regulatory Reporting	Access credit and cash	Receive claim payment/settlement
Fund Accounting / Valuations	Arranging, underwriting and distributing syndicated loan financing	Savings / Investment

1. Not all services are critical

Critical services are those whose disruption could cause an intolerable impact on the 'outside world' (e.g. customers, the broader market/economy, the environment, broader society) or the organisation itself (its financial viability, reputation, legal/regulatory position).

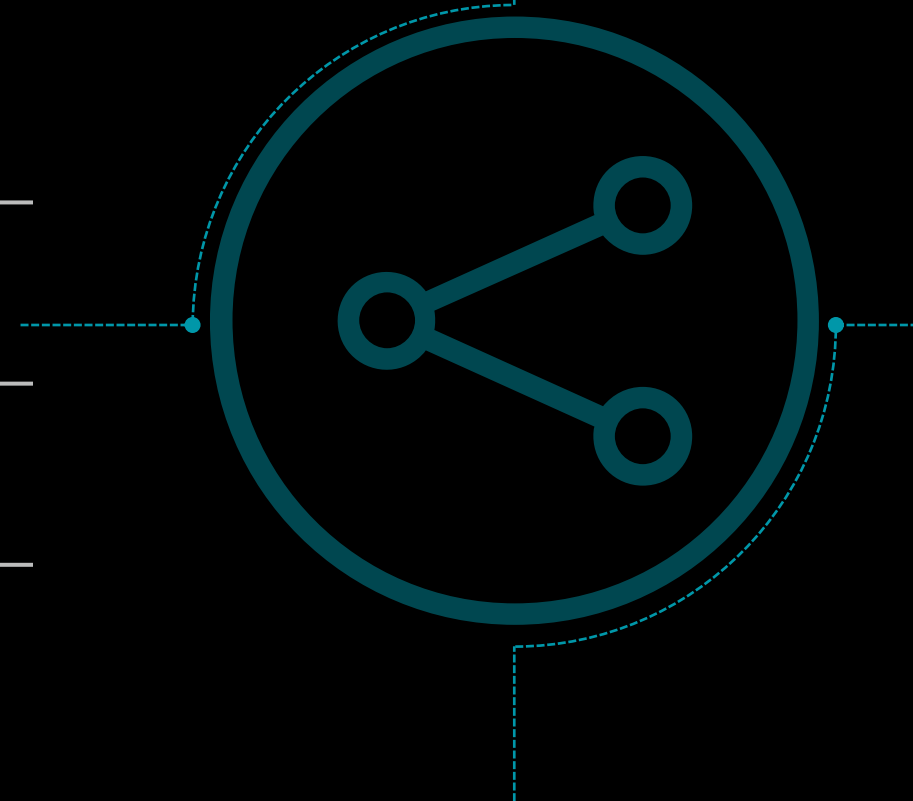
- a) The **FI's safety and soundness**¹;
- b) The **FI's customers**, based on the number and profile² of customers affected, as well as how they are impacted;
- c) Other **FIs that depend on the business service.**

1. Assess extent of damage to the FI's financial and liquidity position, any loss of assets and revenue, loss of business and investments, and any inability to meet legal and regulatory obligations
2. Type of customers (e.g. retail/corporate/interbank customers)



1. What is a (Critical) Service?

	Impact areas	Could disruption to the delivery of this service cause an intolerable impact?
External impacts	Stakeholder / end user harm	Harm to an external end-user or critical stakeholder. This includes a threat to life safety/financial security/livelihood or prevention from fulfilling daily life activities.
	Market instability	Threatens the stability of the market and other FIs that depend on the business service.
Firm impacts	Reputational damage	Results in a severe loss of confidence and trust in the organisation.
	Legal / Regulatory breach	Breaches in legal or contractual requirement resulting in severe regulatory action e.g. loss of license to operate
	Financial failure	Puts at risk the very existence or financial viability of the organisation.



Note: Critical activity does not automatically translate to a critical service.

2. Critical Services Mapping

Mapping' of critical services is an identification process where organisations identify and document the **1) necessary processes** and **2) resources** (people, technology, facilities and information etc.) end-to-end required to deliver a critical service.

Processes:



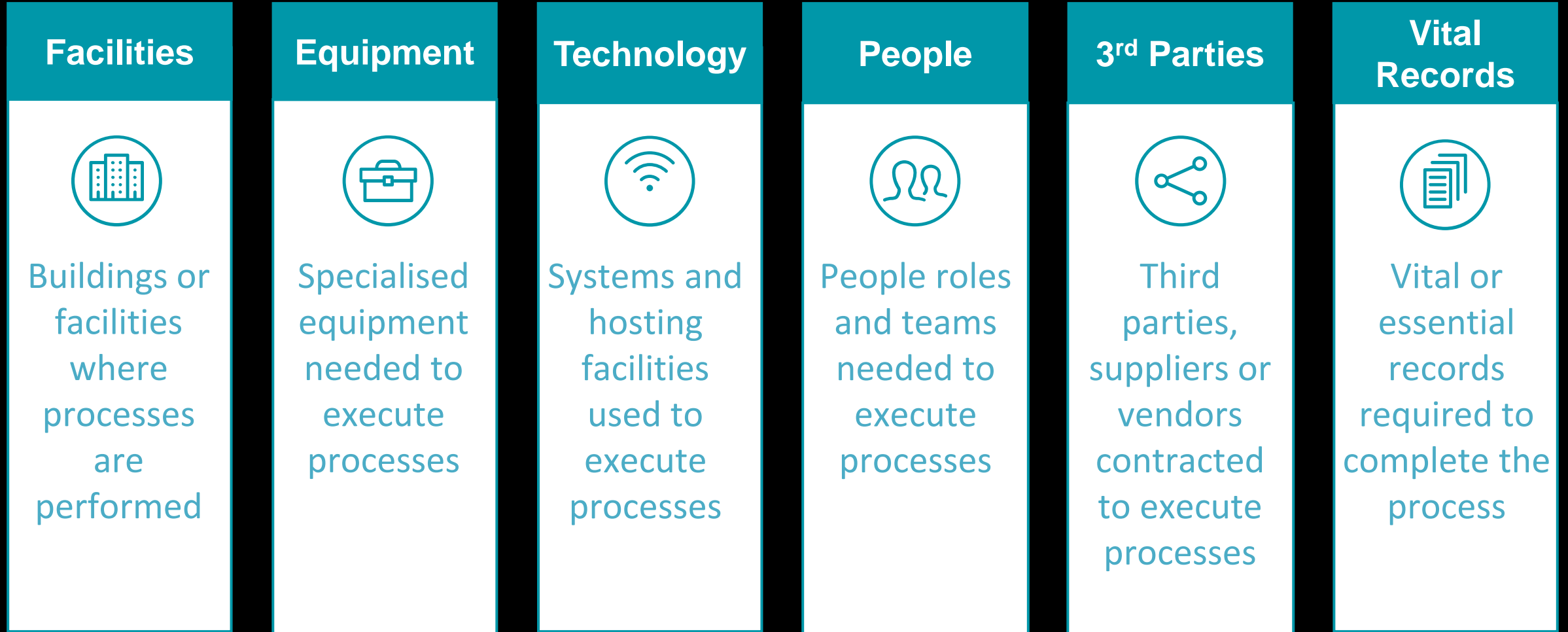
Considerations:

- Identifying the maximum impact on the success of a specific business unit or function, and focus on activities/tasks that transform inputs to outputs
- Compilation of activities/tasks performed by the organisation
- Compilation of activities/tasks, irrespective of the location in which they are performed
- Mapped to a critical service

Where to start:

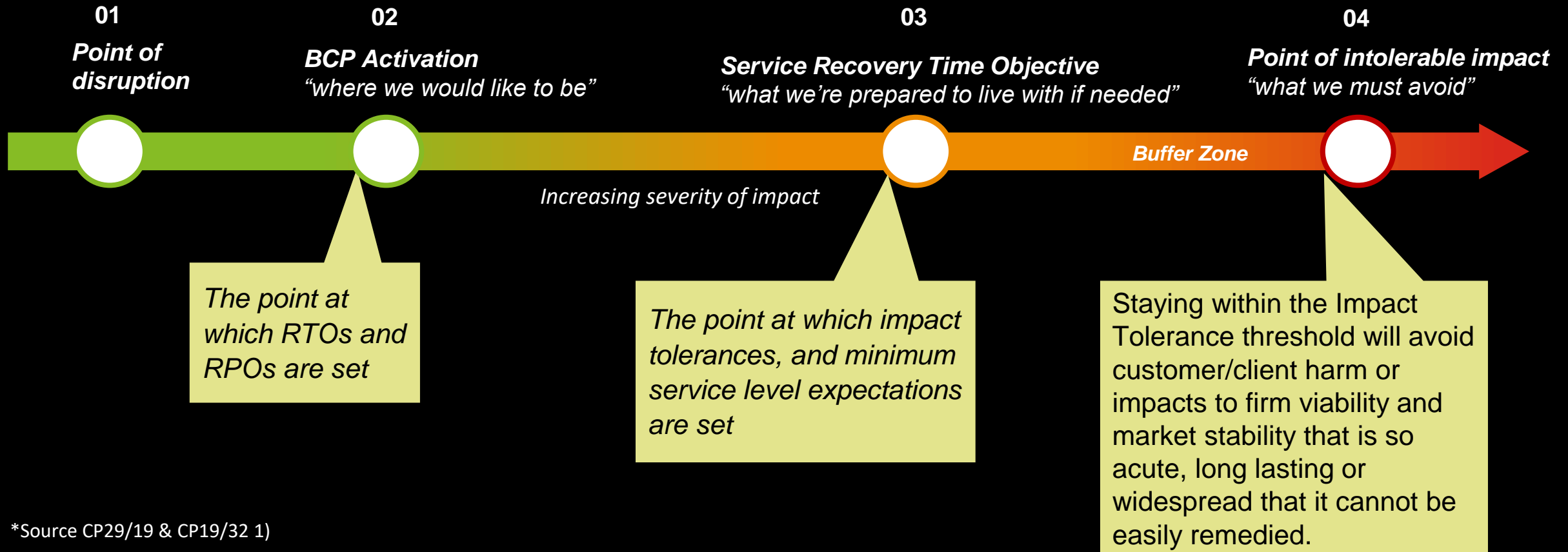
- Customer journey maps
- Target operating models
- Value stream documentation
- Operational process manuals
- Business continuity documentation
- Documentation from related frameworks (Incident Management, Crisis Management, IT Disaster Recovery)

2. Critical Services Mapping



3. Why Establish Service Recovery Time Objective?

In a move away from looking solely at the preservation of critical assets, service recovery time objectives comprise of two parts: one is agreeing on the impact tolerances and the other is RTO/RPO setting.



*Source CP29/19 & CP19/32 1)

** Source ISO 22301:2012

*** Source GPG 2018

3. What is Service Recovery Time Objective?

Steps for determining Service Recovery Time Objectives

1

Map end-to-end business functions and interdependencies required to provide critical services.

2

Consider and determine the scope of criticality to finalise business functions and interdependencies to map to critical service.

3

Establish the recovery time objectives (RTO) of all business functions and systems identified within the scope of criticality.

4

The SRTO of each critical service is the maximum amount of tolerable time for disruption by the all the business functions mapped within the scope of criticality.

Considerations

- People, systems, tools and third parties required to complete the critical service.
- Enabling services should feature how critical services are supported.

Prioritization

- a) Impacts to end customers
- b) Impacts to firm viability
- c) Impacts to market stability

Validation

- Recovery Time Objectives, and Service Recovery Time Objectives of should look beyond the recovery time of critical systems as the single factor. Considerations include:
 - a) Minimum service level expectations by customers and counterparties
 - b) Recovery time of processes, people, third parties and enabling services

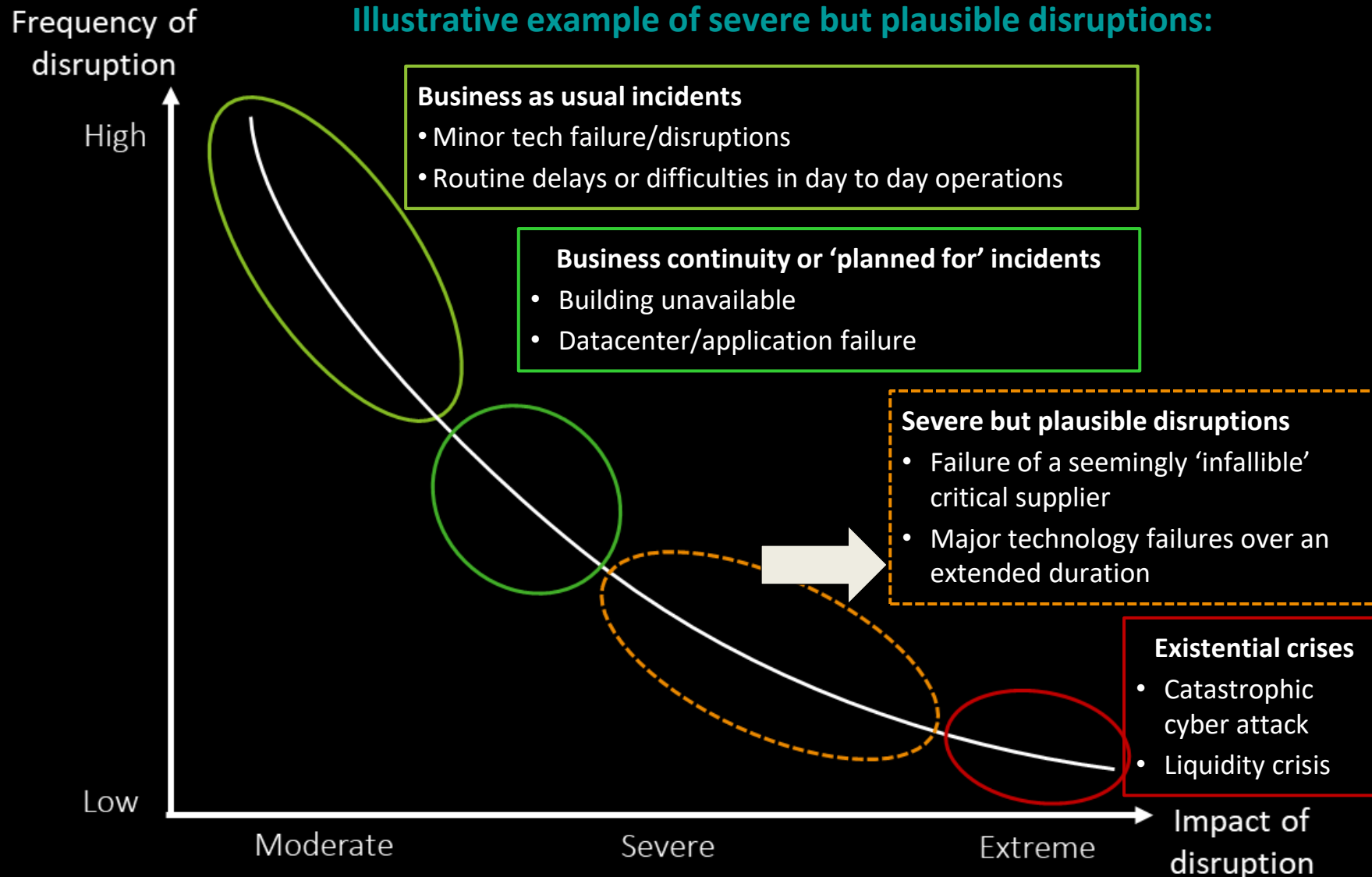
4. A Clear Understanding of Concentration Risks

Dependency	Description	Examples of Concentration Risks
People	Primary teams	<ul style="list-style-type: none">• Lack of alternates to assume key responsibilities to mitigate single points of failure (this may include delegated authorizations for key activities, succession planning etc.)
	Alternate teams (transfer of work)	<ul style="list-style-type: none">• Inadequate training and lack of access to necessary tools to perform essential tasks.
Facilities	Office sites / Data centres	<ul style="list-style-type: none">• Arrangements for operations and data centres which support critical business services have not been made to mitigate concentration.
Technology	Systems which support important business services	<ul style="list-style-type: none">• Systems which support important business services are not configured so that the services have access to mirrored data in real time
		<ul style="list-style-type: none">• Systems which support important business services are not separated from the main site
Processes	Key stages	<ul style="list-style-type: none">• Lack of manual workarounds or other means to execute key processes identified in the critical services mapping
Third Parties	Important outsourced products/services	<ul style="list-style-type: none">• Contingency arrangements and service level agreements with vendors for continued provision of services have not been established• Resilience of third parties have not been assessed and tested on a regular basis

5. Availability of Plans: A Clear Set of Standard Operating Procedures to Manage Incident Response and Guide Recovery



6. Tests and Exercises: Validation of Familiarity and Feasibility of SOPs



Why Test?






- To demonstrate that Critical Services can be delivered within the Service Recovery Time Objectives
- Identify where resilience measures require further enhancement
- Allows capabilities to be explored and improved in a 'safe' environment prior to a real disruption occurring

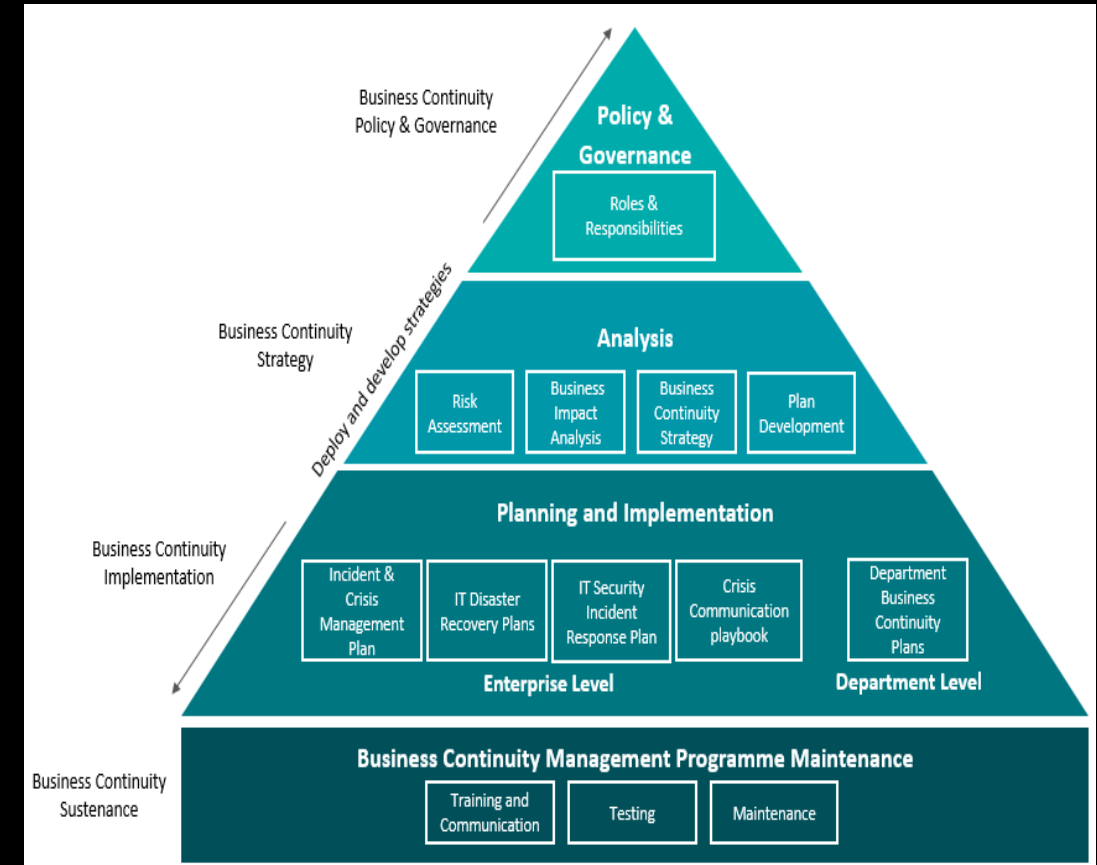
7. Significance of Board Oversight and Senior Management Sponsorship of BCM Programme

Responsibilities		
BCM Principles	Board	Senior Management
1. BCM Framework	<ul style="list-style-type: none">Review of framework’s effectivenessApproval, oversight and maintenance of BCM	<ul style="list-style-type: none">Implementation of the BCM frameworkPrudent and sound policies are put in place
2. Roles and responsibilities	<ul style="list-style-type: none">A BCM function is established and resourcedSenior management has sufficient authority and access to the Board	<ul style="list-style-type: none">Roles and responsibilities are establishedMeasurable goals and metrics are used to assess BCM preparedness
3. Identification and update of critical services		<ul style="list-style-type: none">Identify critical services and establish SRT0Setting and reviewing operational resilience parameters
4. Testing		<ul style="list-style-type: none">Plans tested regularly against severe but plausible scenariosServices can recover within SRT0 and RTOGaps identified are remediated in a timely manner
5. Annual Attestation	<ul style="list-style-type: none">Request for attestation from senior management	<ul style="list-style-type: none">Provide regular and timely reports to the Board
6. BCM Audit	<ul style="list-style-type: none">Ensure that independent audit is performed	<ul style="list-style-type: none">Gaps and weaknesses identified are remediated in a timely manner

8. Audit of BCM Framework and Critical Services Upon Implementation

An independent BCM audit is required once every three years to assess the adequacy and effectiveness of the BCM framework and the ability of identified critical services to recover within the stipulated service recovery time.

-  **Coverage of Business Continuity Planning** e.g identification of risk scenarios, impacts to stakeholders and the corresponding recovery strategies to include considerations for Critical Services
-  **Outline of roles and responsibilities** of the Board and Senior Management in alignment to new BCM framework
-  **Approach taken in the identification of critical business services** and the mapping of dependencies
-  **Availability of Plans** and adequacy of documentation for Critical Services
-  **Validation of BCPs**, Recovery Time Objectives and Service Recovery Time Objectives against severe but plausible scenarios



Common Challenges

Mindset Shift from BCM1.0 > BCM2.0

- Gaining buy-ins from stakeholders
- Driving the implementation top-down

Accuracy of mapping critical processes and resources to a service

- Differentiating between a function from a service
- All processes are critical and not prioritized
- Granularity of mapping commiserating with scale of operations

Determination of Service Recovery Time Objectives

- Lack of data and understanding to establish Service RTO
- Conflicting service level expectations with system RTO
- Complexities of system dependencies

Third Party Concentration Risks

- Strong reliance on head offices and key vendors for technology support and operational matters
- Unavailable Service Level Agreements (SLA)s with head office and key vendors

Resilience going forward...

TODAY'S OBJECTIVE...

What conventional BCM helped to do

- Identifying critical processes
- Developing contingencies and plans for 'well known' scenarios
- Testing business continuity plans together with incident and crisis management structures

TOMORROW'S OUTCOMES

What the recent focus on operational resilience endorses

- Identifying critical services (i.e. outcomes) needed by customers, and other stakeholders
- Setting impact thresholds for disruption
- Stress testing assumptions, and outcome recoverability against 'what if' scenarios

What we want BCM to look like

- Focus analysis and planning on the critical services
- Assume disruptions will happen and building readiness for a broad range of scenarios
- Identifying contingencies that go beyond a single Business Continuity Plan

Tea Break (15 mins)



Breakout Activity



Breakout Activity: Table-top Exercise

What is it?

A table-top exercise is the mode of conduct to facilitate today's discussions on the key requirements outlined by MAS. Through the introduction of a fictitious FI scenario and a series of incident injects, we will unpack and talk through the key areas shared in the earlier half of the Roundtable.

Why?

Through 'gamification', we hope to enhance everyone's awareness and understanding of the MAS guidelines, while also providing a platform to discuss and learn from one another.

How?

- Each group will be assigned to assume a role in the fictitious FI where they would discuss and respond to the injects brought to their attention.
- After the introduction of each inject, 10 minutes will be given to all groups to discuss before we go round the room to share our thoughts. Deloitte facilitators will be on-hand to support and guide group discussions.
- There will be a quick hot-wash after the exercise to summarise key observations and discussion points as take-away from the activity.



Table-top Exercise

Instructions:

- Enter presentation mode
- Walk through the injects and questions
- Discuss response and considerations required by the role assigned to your group

Start

About the Company

- DT Investment Global is a leading European asset management firm with presence in more than 30 countries.
- Serves both retail and institutional clients
- Offers active and passive management of a wide range of traditional and alternative assets to serve our clients and support our distributors.
- Singapore is one of the six international hubs, alongside Tokyo, Paris, London (Head Office), Luxembourg and New York.
- The Singapore office is a key investment and operational hub covering 10 countries in Southeast Asia, Australia and New Zealand.

Group 1

Senior Management /
Board

Group 2

Portfolio Management

Group 3

Trade Execution

Group 4

Finance

Group 5

Compliance / Risk
Manager

Next

Key Systems Used in DT Investment Global:

In house systems

SINTRADE	DTLog	DTFolio	DTInvestware
Input trade orders	Books and ledgers maintenance Input trade orders, settlement and reconciliation	Management of portfolio requests	Portfolio rebalancing and modelling
DTConnect	DTSync	DTNexis	DT Alliance
Front Office tool for account management / opening	Client register, Screening	Unblocking of codes	Internal messaging platform

Third party vendors

MS Office	Bloomberg	SmartAccess
Email and client comms	Equities, Structured Products, Cash Bonds	Cash Equities, OTC Derivatives
FXPro	SimCorp Dimension	DOW Jones
FX Spot, Forward / Swaps, Equity Options	Position keeping and monitoring	Account Screening and checks

Opening



Wednesday, 14 Jun
0900H



Next

Inject 1

Wednesday, 14 Jun
1012H

 An error occurred. Please try again later. If the error continues, contact your System Administrator. 



Management Console

Login:

username:

admin3264

password:

Go

Connection failed: Access Denied for admin3264

I am i

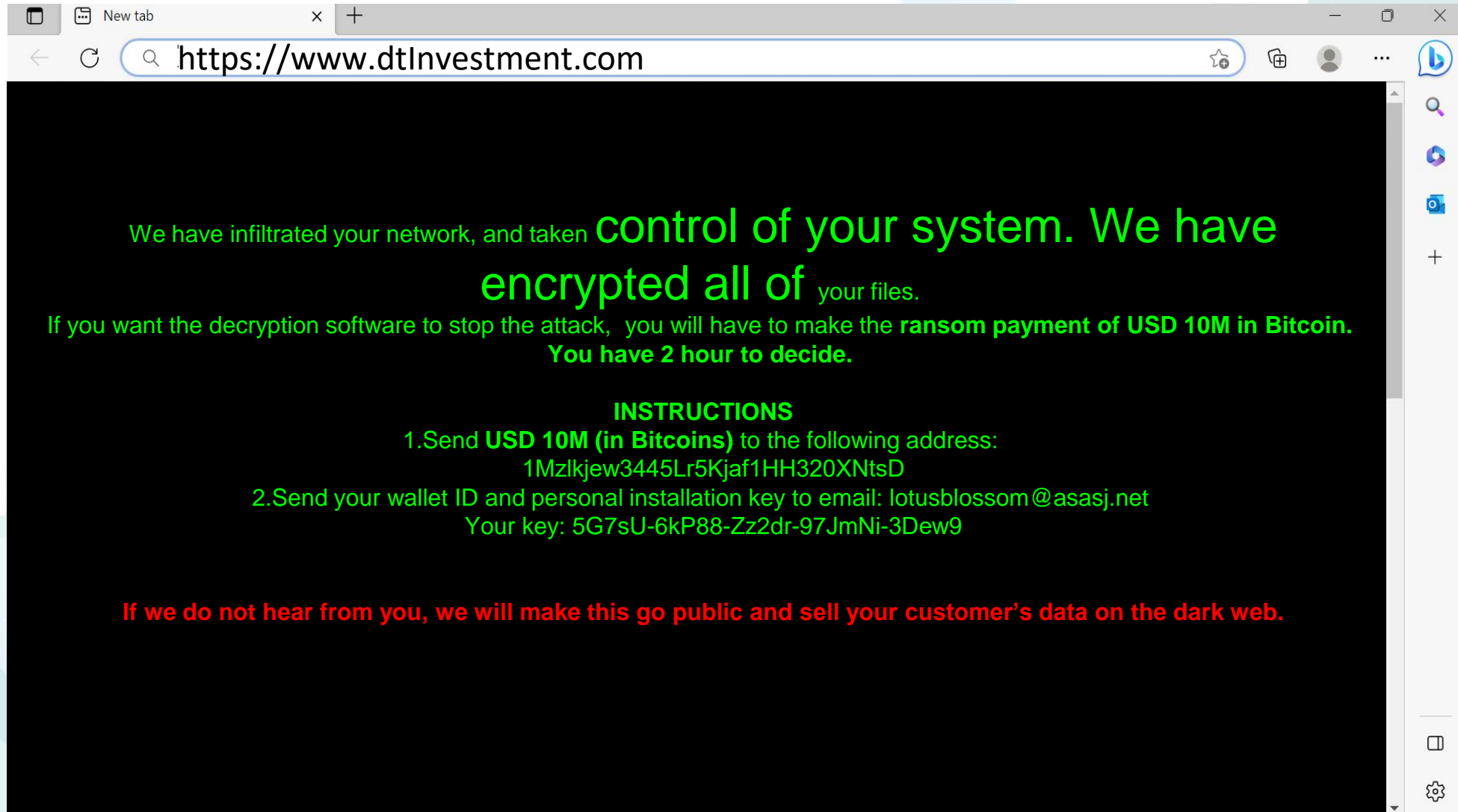
Please get it fixed immediately!
nothing that I've tried works!

tes and

Next

Inject 2

Wednesday, 14 Jun
1212H



Next

Discussion: Inject 1 and 2

1

Senior Management / Board:

Cyber attacks have become a top risk for the financial sector. As Senior Management and the Board, what other severe and plausible scenarios should DT Investment Global be considering? How would the severity and impact be established?

2-4

(Critical) Business Services:

From the inventory of business services shortlisted by the London Head Office, which are the ones that the Singapore team would consider as Critical Business Services locally? And why?

5

Compliance / Risk Management:

What are the key criteria that should be used to assess the adequacy of the list of severe but plausible scenarios?

Next

Inject 3

**Wednesday, 14 Jun
1245H**



Next

Discussion: Inject 3

1

Senior Management / Board:

In this scenario, what are some mitigation controls that could be put in place to minimize impacts to operations and client harm?

2-4

(Critical) Business Services:

Based on the mapping sheet provided, please identify the critical processes, systems, tools, people required to maintain critical services. Please also determine the Service Recovery Time Objective for your business service.

5

Compliance / Risk Management:

As part of the self-assessment checklist, what areas would you include based on the scenario?

Next

Inject 4

**Wednesday, 14 Jun
1300H**

 Reply  Reply All  Forward  IM



Sent: 2 minutes ago

CEO DT Investment Global

Cyber insurance and Activation of Cyber forensics team

To  **SG Crisis Management Team**

Hi,

We are consulting our cyber insurer on the possible claims.

We have also activated our cyber forensics vendor to investigate the root cause and suggest possible remediations. As of now, recovery is estimated to take around 3-4 weeks.

Please proceed with your business plans to bring up the services to continue operations. Keep us informed on the progress.

Global CEO

Next

Discussion: Inject 4

1-5

All groups:

What are some areas of concentration risks that you have observed thus far? What are strategies that DTInvestment Global has deployed or could have used to manage concentration risks?

Next

Inject 5

Wednesday, 15 Jun
1030H



BREAKING NEWS: DTInvestment Global suffers ransomware breach



Screenshot of ransomware note demanding US10M. Investigators and customers concerned over potential leak of personal data.

Next

Discussion: Inject 5

1

Senior Management / Board:

How would the role and responsibilities of crisis communications be split between head office and the senior leadership team in Singapore?

2-4

(Critical) Business Services:

What forms of communication – notification, reporting etc do you think the firm needs to provision for to help manage the stakeholders impacted by your critical business service?

5

Compliance / Risk Management:

As part of the self-assessment checklist, what would be the areas that should be included based on the requirements of this inject.

Next

End of Table-top Exercise

Hotwash:

Share your learnings and observations

- What went well for the groups? Your own team?
- Areas that were challenging
- Any other key observations

End

Table-Top Exercise Observations

	Good practices raised
	Opportunity for enhancement

Observations
There were good sharing from best practices around the room on the types of mitigation controls that can be considered to manage concentration risks.
Participants in various group were able to brainstorm and establish with various methodologies to reduce concentration risk. This includes using of cloud computing to allow for cross-region backup and support, establishing split team and alternate site to reduce talent concentration risk, and globalising of workforce to reduce concentration risk arising from geographical instability in a particular country or region.
It was also mentioned that the pandemic had driven the industry’s ability to recover quickly from a prolonged disruption, especially where the front office can continue to deliver services remotely – thus minimising risks of dependency on office premises and systems.
Various considerations and perspectives were raised and discussed in guiding the groups in the identification of critical services and key processes and resources
Participants were able to identify a list of criteria to rate the impacts to the critical services. This included: <ul style="list-style-type: none">• Financial and business impacts, loss of assets.• Regulatory and legal obligations such as PDPA/European data protection (GDPR),• Likelihood of occurrence, past occurrences• Understanding of interdependencies with head office and third party vendors

Table-Top Exercise Observations

	Good practices raised
	Opportunity for enhancement

Observations
A wide range of recovery strategies were shared during the session.
<p>Participants in various groups took into consideration many valid factors when recovering services such as</p> <ul style="list-style-type: none">• The customer profile (New vs existing customers etc.)• Manual workarounds in place• Considering the options available and the cost of adopting such actions
<p>Several Participants suggested to establish a central party/team that would work round the clock to help with crisis management/ Disaster recovery efforts which is currently an industry best practice</p>
<p>Participants were able to identify certain key stakeholders such as the Cybersecurity Agency of Singapore (CSA) and Monetary Authority of Singapore (MAS) for reporting purposes.</p>

Table-Top Exercise Observations

	Good practices raised
	Opportunity for enhancement

Observations
Varying approaches were applied in the determination of the Service Recovery Time Objective (SRT0). It is key that service level expectations and considerations for system and resource dependencies are factored in before establishing the SRT0.
Participants understood the definition of RTO, but had some difficulties of identifying the SRT0. This led to some participants thinking that the SRT0 would be a summation of all RTO in the processes mapped.
Some participants only considered the RTO for the individual functions and did not take into account of the RTO of several systems or vice versa
Some participants did not take into account issues from various angles when discussing on the topic of SRT0 such as regulatory impacts or market effects.
When considering on processes to be kept during crisis, one of the team’s thought process was that as long as the process/function have a workaround (or can be done manually), the process can be kept; Having a workaround is crucial when a process is deem critical, but it should not be the main consideration to determine if a process is critical

Table-Top Exercise Observations

	Good practices raised
	Opportunity for enhancement

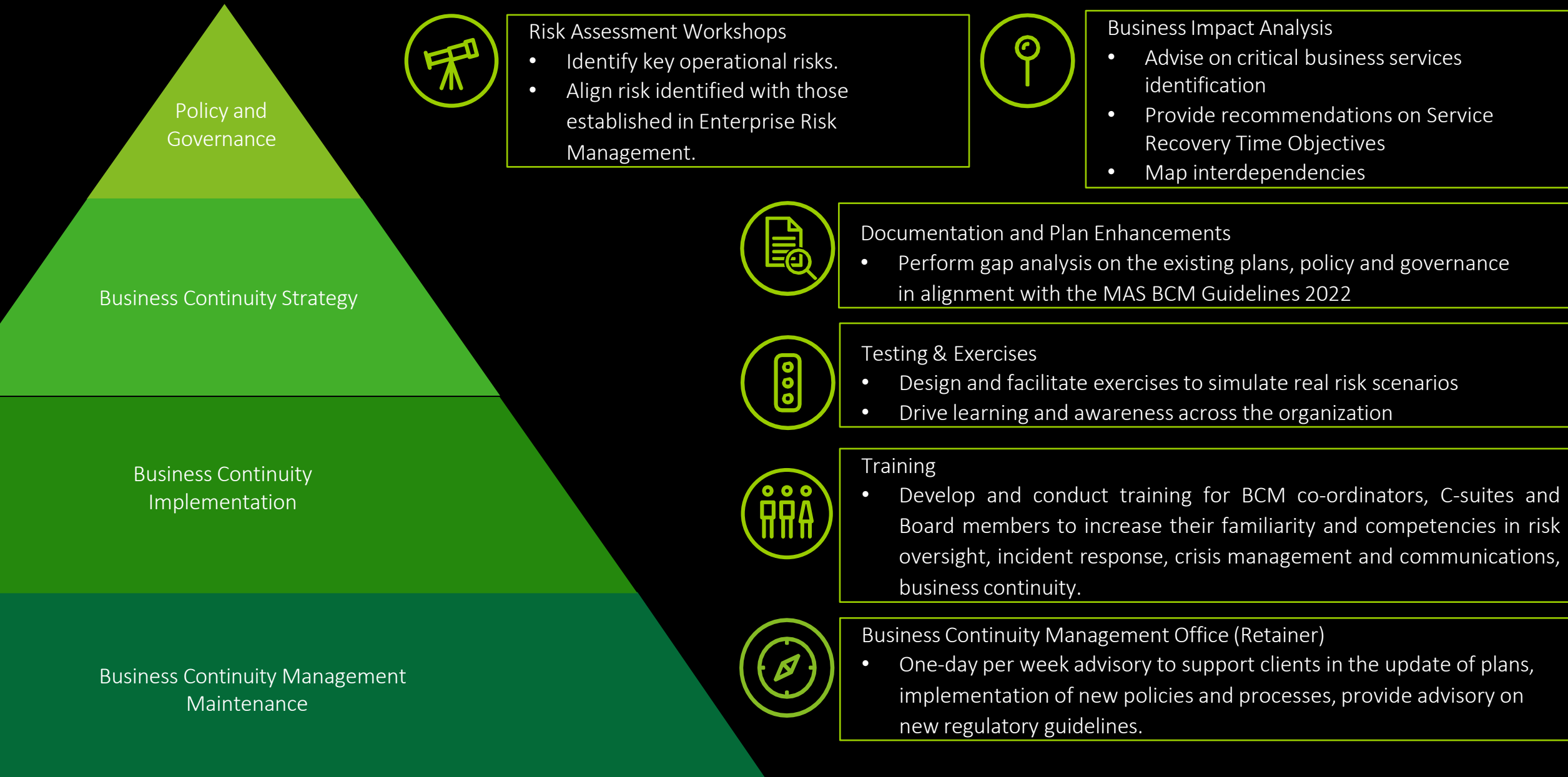
Observations

Impacts and response strategies from a possible ransomware attack can be further refined. While cyber insurance is a safety net for organisations, it is key for senior management and the Board to establish the organisation’s posture around ransomware payment.

Participants had considered the effects of the ransomware on the business functions and services. However, they missed a key point on the posture of ransom payment and what could possibly be the impacts from their decision.

The introduction of a severe but plausible scenario like a ransomware attack also challenged participants to consider more broadly what could possibly be the list of risk scenarios that could be of high impacts to their organisation.

Managing the Gap: How Deloitte Can Help



Thank You. Connect With Us.

Thio Tse Gan

Executive Director
tgthio@deloitte.com

Wong Nai Seng

Executive Director
nawong@deloitte.com

Lawren Poh

Lead Crisis & Incident Response
lapoh@deloitte.com

Goh He Lin

Business Continuity, Crisis Management and
Communications, Brand & Reputation
hgoh@deloitte.com



imas

INVESTMENT MANAGEMENT
ASSOCIATION OF SINGAPORE

CLOSING REMARKS BY:

Fann Teh

Chairman of IMAS Regulatory Committee

IMAS 16th Regulatory Roundtable

imas

INVESTMENT MANAGEMENT
ASSOCIATION OF SINGAPORE



Thank you for joining us today!

Please fill in the feedback form
before you leave



IMAS 16th Regulatory Roundtable