WISE2019

Whole Industry Simulation Exercise Evaluation Report

General

December 2019

Hong Kong Financial Services Business Continuity Management Forum

Control Risks Pacific Limited | 2501-02, Level 25 | The Centrium | 60 Wyndham Street, Central, Hong Kong | China

+852 6963 0040 hongkong@controlrisks.com

Table of contents

Executive summary

WISE (Whole Industry Simulation Exercise) is a biennial market-wide crisis simulation exercise for Hong Kong's financial services industry, organised by the Hong Kong Financial Services Business Continuity Management (HKFSBCM) Forum. As in 2017, Control Risks was retained to plan, provide secretariat support and deliver WISE2019. HKFSBCM is a not-for-profit industry-group of business continuity management professionals employed in the financial sector in Hong Kong. WISE2019 was the third exercise of its kind in Hong Kong and served the following key objectives:

- Provide crisis and stress management skill training;
- Familiarisation with crisis management process;
- Familiarisation with business continuity plans and facilities;
- Test coverage and feasibility of business continuity plans, and stress testing of plans;
- Create a sense of urgency;
- Promote business continuity management;
- Practice interbank and interagency coordination;
- Practice crisis communication, internal, external and with regulators;
- Fulfil regulatory requirements;
- Build confidence in the banking sector with clients, regulators and society at large.

The scenario of WISE2019 included African swine fever, market volatility, a swine flu pandemic, critical national infrastructure failure, insider-led cyber-attack, and deep-fake media. The senior crisis management teams (CMTs) of 42 financial institutions participated from their own offices in a simulated three-hour crisis scenario on 18 October 2019. Every CMT was connected to the central command and control centre (CCC), which released newscasts, emails, social media and market data in real-time, as well as providing telephone injects, and to which CMTs sent their responses, such as updates to regulators and responses to external clients.

Key observations

- There continues to be high interest for an industry-wide crisis management exercise;
- The scope of participating organisations, this year, widened with the inclusion of virtual banks;
- Crisis management capabilities vary across the industry;
- Structuring the exercise to better reflect how organisations respond to crises demonstrated increasing maturity of the exercises and organisations taking part;
- Participating organisations demonstrated effective communication with various stakeholders;
- Most organisations provided a timely and adequate response to the regulators' request for information;
- Most organisations believe they are well prepared for a pandemic crisis;
- Cyber security responses are integrated with crisis management responses, but insider threat response and integrating this with crisis management responses presents an ongoing challenge;
- Some organisations are not well prepared for telecommunications connectivity issues.

Suggestions for future exercises

- Ensure exercise content is more relevant to all participants, such as expanding on the participant lead generation of absenteeism data for the pandemic scenario;
- Consider further improvements to exercise delivery format such as adding distinct breaks and considering how to provide time for regulatory submissions and follow up actions from the crisis management meetings;
- Allow more time and resources for facilitator preparation;
- Make further tweaks to exercise portal for enhanced user experience;
- Increase the involvement of the regulators;
- Further enhance the structure of the command and control centre;
- Revisit the costing model for participation.

Please refer to section 4 for detailed observations and section 5 for detailed suggestions for future exercises.

1. Introduction

WISE is an industry-wide initiative conceived and organised by HKFSBCM, a group of senior business continuity management professionals employed in a wide cross-section of firms in the banking and securities industry. HKFSBCM aims to collaboratively support business continuity professionals in the financial services sector. Through regular meetings, HKFSBCM discusses current affairs, emerging threats, regulatory requirements and best practices in the areas of business continuity and crisis management.

WISE2015 provided the first secure and managed platform for participating organisations to test and improve their crisis management and business continuity procedures. The CMT of each participating organisation faced a variety of primary operational disruptions to exercise their decision-making abilities and deliver a coordinated response to key stakeholders. The exercise was aimed at increasing industry resilience in addition to exercising individual organisations' responses to specific threats. 25 organisations participated in the exercise, including Hong Kong and International banks, asset managers, as well as securities firms. Following the success of WISE2015, WISE2017 was delivered with similar objectives and grew to 45 participating organizations.

In October 2019, HKFSBCM organised WISE2019. The fundamental objective to enhance the crisis resilience of the Hong Kong financial services sector with opportunities to evaluate and strengthen the capabilities of CMTs remained unchanged, and the general set-up and delivery methods remained the same. However, the third instalment of WISE had some key differences:

- Stability and efficiency of exercise portal back-end software
  - During WISE2015 and WISE2017, some participants reported they experienced a delay in receiving injects and the exercise portal became unstable at certain stages. For WISE2019, Ruder Finn, Control Risks' partner, developed a customised exercise portal (Sonar 3.0) with innovative features to ensure smooth operation and better interaction between participating organisations.
- Exercise scenarios were more comprehensive
  - Since not every firm is equally affected or challenged by the different scenario storylines, more bespoke scenario elements were created to ensure specialist companies, such as asset management firms, were challenged and engaged.
- Adjustment in the exercise delivery structure
  - During WISE2015 and WISE2017, some participants claimed the scenario pace was too fast, and there was insufficient time for impact analysis and discussion. In WISE2019, the exercise delivery structure was revamped to better reflect how organisations respond to crises in real life. The scenario included time for two 30-minute crisis management meetings to ensure enough time for incident response and assessment, information processing and team discussion.
- Active participation by the regulator
  - As industry wide exercising has evolved, participants have recognised the important role regulators will play in a major incident potentially or actually affecting the Hong Kong market. In 2019, the Hong Kong Monetary Authority (HKMA) was able to exercise its role in supporting the financial services industry. The HKMA engaged actively with three participants during the exercise: UBS, HSBC and WeLab Digital Ltd.

2. WISE

2.1 Why WISE?

WISE creates a unique opportunity for participating organisations to exercise their response strategies to a potential crisis situation, where the whole industry is affected. The first, smaller scale exercise was conducted in 2013, when a group of financial institutions individually but simultaneously responded to a simulated unfolding pandemic crisis. In 2015, a full-fledged exercise (WISE2015) simulated a wide-scale transport disruption, followed by serious internet disruption and data leakage. WISE2017 focused on cyber and physical threats. WISE2019 focused on rehearsing various financial institutions' response to a pandemic followed by internet instability and insider-led cyber-attack. An interesting element added to the scenario was the use of deep fake videos, which entailed adding the voice of the REBEL to three well-known public figures. Similar market-wide exercises are organised in other major financial hubs, including Quantum Dawn in the US, Waking Shark in the UK and Raffles/IWE in Singapore.

2.2 What is crisis management?

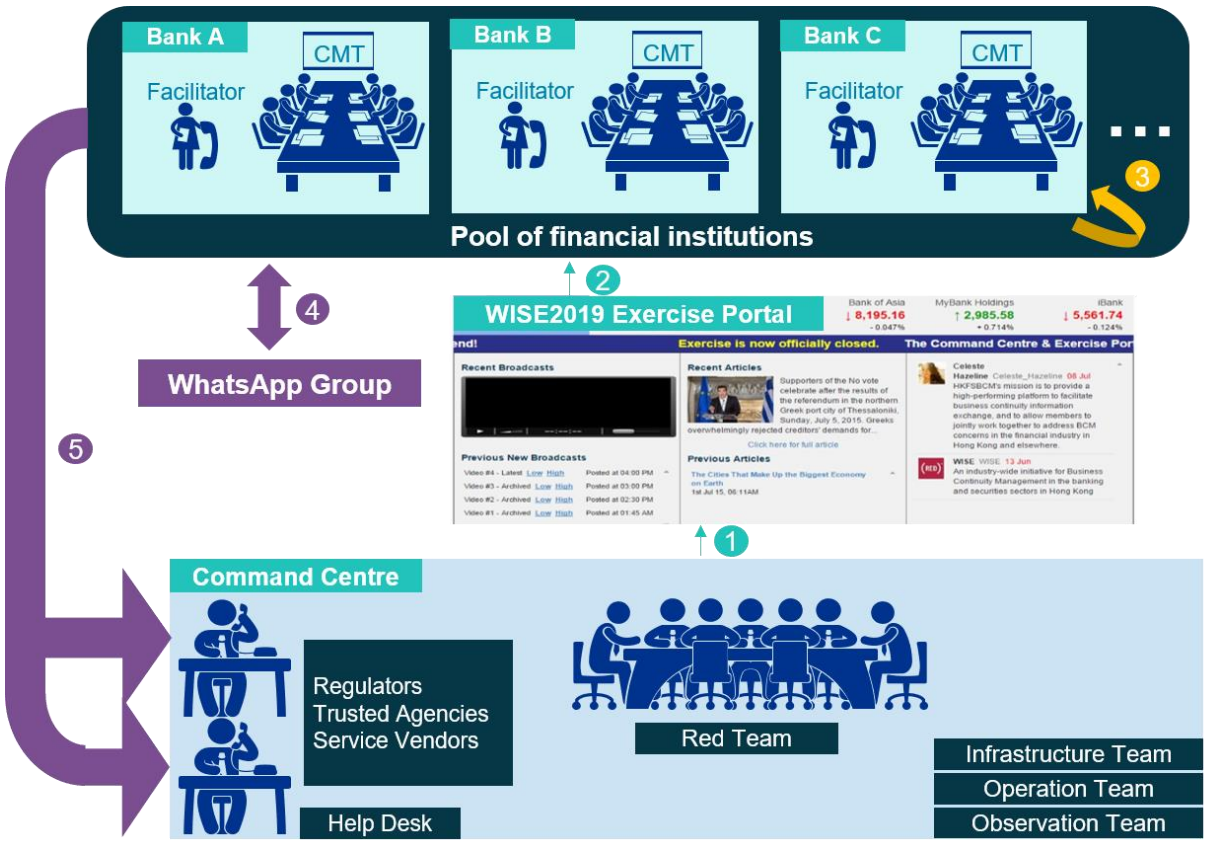
Crisis management is the process by which an organisation responds to a significant event/issue that has the potential, if not managed appropriately, to harm the organisation, its stakeholders, or the general public. The issues are typically so important, unexpected, extraordinary, urgent and sometimes emotional that normal management is insufficient. It involves procedures and plans, but also individual skills and practices. In many countries, banks jointly engage in industry-wide table-top exercises, where the CMT from each organisation discusses the response to a challenging hypothetical situation, or scenario, which unfolds from a central simulation centre. WISE is an industry-wide crisis management exercise where participating organisations jointly exercise their abilities to respond to different crisis scenarios.

2.3 How is WISE delivered?

WISE is delivered in a simulated exercise format to CMTs at a pre-announced date and time. What participating CMTs do not know, however, is the scenario that will unfold. Through so-called 'injects', which can be situation reports, emails, phone calls or newscasts, the CMTs are informed of developments of a crisis. The Command and Control Centre (CCC) in another location controls these injects through a specially designed web portal, to which each firm has access. The CMT members will then respond to the situation as if it was real. As this is a simulated exercise, no actual physical actions, such as evacuating a building or activating a recovery site, are taken. However, such commands are relayed to the CCC, who will, in real time, role-play several parties and respond as if the actions were real. This includes the confusion and misinformation that generally occurs in such situations.

2.4 Practical setup

Figure 1: Practical setup of WISE



- Each participating bank's CMT gathers in their own office.
- Through the exercise web portal, they see the crisis scenario unfold through injects. The portal shows an ongoing sequence of general news reports, news videos, stock market developments and social media.
- The developments presented on the portal are supported by phone calls and emails sent from the central command centre, creating an immersive scenario reality.
- The central command centre is staffed with subject matter experts to direct the events. Its proceedings are observed by a range of invited interested parties.
- The CMTs are expected to discuss the developing situation and decide on actions. These can include:
  - Calling or emailing parties such as the authorities, police and other organisations. To this end, the subject matter experts in the CCC impersonate these entities to provide realistic responses.

- Sending out corporate or social media statements. Through the portal, posted statements are visible to all participating CMTs.
- Taking internal actions, which are confined to the exercise.

2.5 WISE portal

The WISE portal is the main interface between the central command centre and every participating CMT. HKFSBCM owns the URL www.hkwise.org, which was also used for the 2015 and 2017 exercises, although Ruder Finn provided the portal back end software and hosting. Access to the portal is password protected and ample time is given for testing, as several companies need to white-list the portal for functionality.

The portal automatically refreshes and gives access to all released injects throughout the scenario. Injects can take different forms, but typically include newscast videos, news articles, social media and stock exchange ticker. In addition, the portal contains static data, such as a directory of phone numbers to be used in the exercise including contact numbers for every participating organisation, as well as the numbers on the simulated parties in the central command centre.

WISE2019 included two major improvements to the platform:

- Redesign of entire interface
  - The interface this year was designed with both war room-like interaction in mind (three/four screens) and for one-screen usage (laptops) and mobile access for participants. There was more information per post, such as a clearer name, category and post time. In addition, there was a visual highlight notifying participants that a specific post has appeared which requires heightened attention.
- Usability & customisability for participants
  - After participants log in, the dashboard immediately presents the three default panels which includes the News, Social Media and Corporate tab. Participants can choose to collapse or expand any panel. This allows each participant to focus on the screens that are relevant to their role. When a new inject appears, a small notification would appear next to that panel. Also, participants this year could directly reply to the social media posts.

3. WISE2019

3.1 Participants

WISE2015 and WISE2017 attracted respectively 25 and 45 different financial institutions to participate. 42 institutions participated in WISE2019, demonstrating a continuous interest in an industry-wide exercise.

The scope of the exercise was limited to banks, securities firms, asset management firms, and clearing houses with operations in Hong Kong. The following organisations participated in WISE2019:

- Australia and New Zealand Bank
- AXA Investment Bank Managers (Asia)
- Bangkok Bank Public Company Limited
- Bank Julius Baer & Co. Ltd.
- Bank of America Merrill Lynch
- Bank of China (Hong Kong) Limited
- Bank of Communications (HK) Limited
- Barclays
- BNP Paribas
- BNY Mellon
- China CITIC Bank International Limited
- China Construction Bank (Asia) Corporation Limited
- Chong Hing Bank Limited
- Citi Bank
- CMB Wing Lung Bank
- Credit Suisse
- Dah Sing Bank
- Deutsche Bank AG
- Fubon Bank (Hong Kong) Limited
- Goldman Sachs
- Hang Seng Bank Limited
- HSBC Ltd.
- ICBC Asia
- JP Morgan
- Livi VB Limited
- Macquarie
- Mizuho Securities Asia Limited
- Morgan Stanley
- Nanyang Commercial Bank, Limited
- Natixis
- OCBC Wing Hang Bank
- Public Bank (Hong Kong) Limited
- SC Digital Solutions Ltd
- Shanghai Commercial Bank Ltd.
- Société Générale
- Standard Chartered (Hong Kong) Limited
- State Street Bank Hong Kong
- The Bank of East Asia, Limited
- UBS AG
- Union Bancaire Privée, UBP SA Hong Kong Branch
- WeLab Digital Limited
- Wells Fargo Bank, N. A.

3.2 WISE2019's objectives

The key objectives of the WISE2019 programme included:

- Provide crisis and stress management skill training;
- Familiarisation with crisis management process;
- Familiarisation with business continuity plans and facilities;
- Test coverage and feasibility of business continuity plans, and stress testing of plans;

- Create a sense of urgency;
- Promote business continuity management;
- Practice interbank and interagency coordination;
- Practice crisis communication, internal, external and with regulators;
- Fulfil regulatory requirements;
- Build confidence in the banking sector with clients, regulators and society at large.

The benefits of participating for individual firms included:

- Cost efficient way to deliver a high-quality crisis management scenario exercise;
- Full participation in a simulated exercise involving the CMT;
- Access to subject matter expert briefing sessions in the months leading up to the exercise;
- Regular briefings on crisis management and crisis communications;
- Complimentary train-the-trainer seminars for facilitators on effective crisis management;
- Company-specific confidential debriefing, benchmarking and industry report;
- Complimentary access to Control Risks' cyber threat intelligence reports.

3.3 Preparations

The organisation was structured into an Organising Committee and a Scenario Development Committee, where HKFSBCM volunteers and specialists teamed up with Control Risks.

3.3.1 Organisation

The Organising Committee was formed in May 2019 to oversee project development and designation of tasks for WISE2019. The Organising Committee comprised the board of HKFSBCM and the Control Risks project team. Meetings were held fortnightly throughout the project to ensure preparations for WISE2019 were on schedule.

The initial planning phase of the exercise involved driving awareness of WISE2019 across the industry. HKFSBCM board members and Control Risks team members met with a variety of organisations and officials to explain and promote the initiative. This included the relevant authorities, financial industry-wide associations, and media.

Industry engagement was initiated in July with two industry-wide briefing sessions, hosted by the HKMA and SFC. Registration for WISE2019 was open from June to the end of August. A total of 42 organisations registered to join the exercise. The fee for WISE2019 was set at HKD 50,000 per participating organisation, a marginal increase compared to WISE2017. HKFSBCM is a not-for-profit organisation; the fees were used to cover costs associated with the delivery of WISE exercises.

3.3.2 Training workshops

Two training workshops were held to prepare all participating institutions for the exercise and to give them more information about what to expect and how to prepare.

- The first briefing was held on 2 July 2019 at HKMA's office. This was a chance for participants to understand more on readiness for the exercise in October and gain insight into crisis management best practice. Leigh Farina, Board Member of HKFSBCM, opened the session with a reminder of WISE 2019's objectives, and Nadav Davidai of Control Risks led the briefing with a session on "Crisis management – the contemporary challenge and a health check".
- The second briefing was held on 26 July 2019 at SFC's office. In this session, Ben Wootliff and Mikk Raud of Control Risks presented on the topic of "Cyber threat trends in Asia Pacific and beyond".

3.3.3 Facilitation

Every participating CMT had to identify a facilitator, who played a crucial role in the delivery of WISE. Their tasks included:

- Arranging logistics: ensuring the CMT members are invited, a room is available, the technical facilities, such as phones, web portal and projectors, are in place and tested.
- Ensuring CMT discussions do not stall: although facilitators should not be part of the CMT or provide answers or solutions, it is the facilitator's role to keep the CMT engaged. For example, by injecting prompting questions or giving immediate feedback on the proceedings in the CMT. Although they do not help the CMT to respond, they do ensure members stay focused and the scenario does not leak into the "real world".
- Being the eyes and ears for the CCC: if the injects overwhelm or are too slow, are misunderstood or fail to engage, the CCC has some flexibility to change course or pace for that specific CMT.

Two briefing sessions were organised to prepare the facilitators for their role: introduction of the portal for delivering injects, run through of the high-level scenario and discussion on logistics to ensure the successful delivery of the exercise within their organisation.

- The first briefing was held on 13 September 2019 at the Admiralty Conference Centre, the venue of the CCC.
- The second briefing was held on 26 September 2019 at UBS's office.

These briefing sessions were supported by a comprehensive facilitator information pack, which included an outline of the scenario and a range of supporting information. The pack also included materials and a contingency pack with all injects in case the live portal could not be accessed.

3.3.4 Command and Control Centre (CCC)

The CCC is the heart of every large-scale crisis management exercise. During WISE2019, the CCC oversaw the delivery of the unfolding scenario injects and simulated the outside world. Volunteers took up positions in the telephone

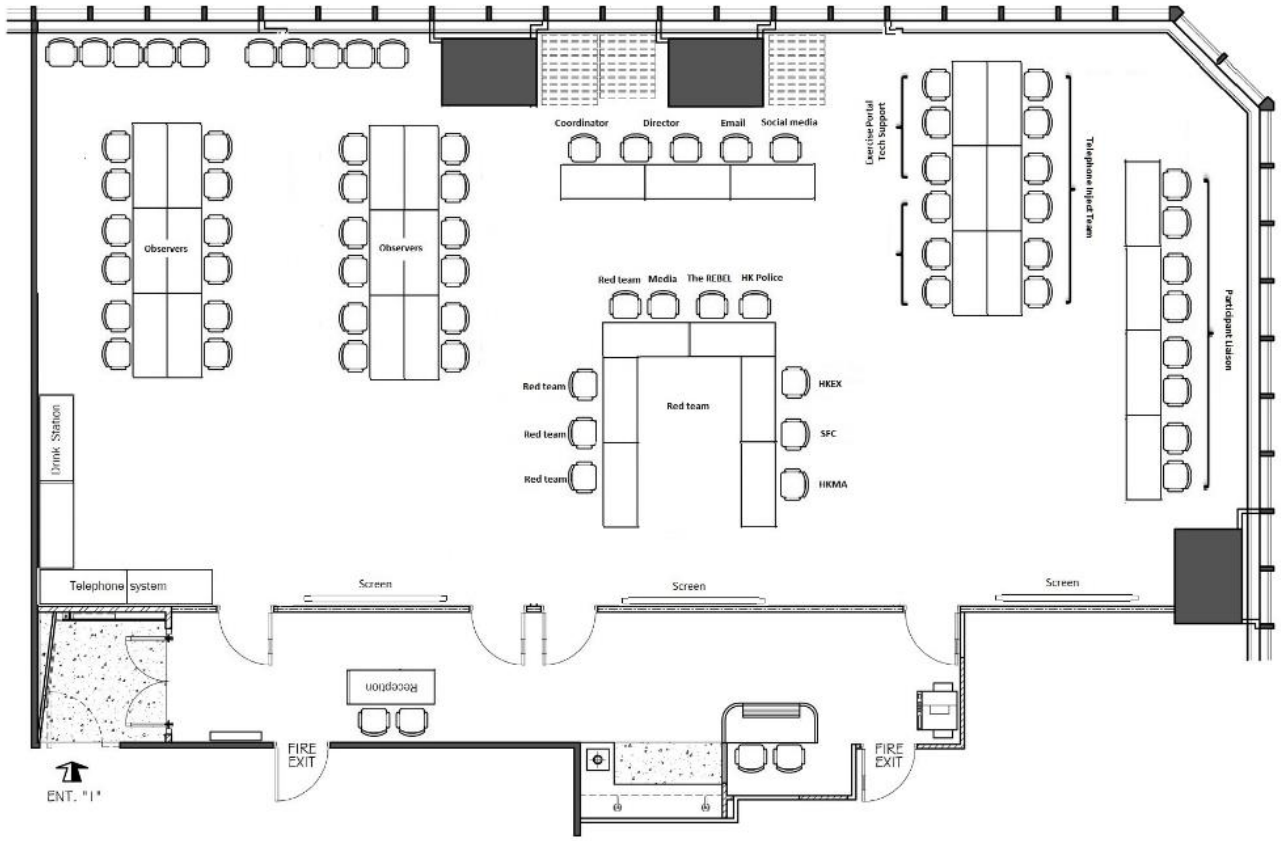
injector team, participant liaison team and role-played various authorities, including law enforcement, regulators and journalists. This also included a red team that could deliver more challenging or customised injects where needed.

Several observers joined the CCC to witness the delivery of the exercise including:

- Asia Securities Industry and Financial Markets Association (ASIFMA)
- Bank Negara Malaysia
- Dubai Financial Services Authority
- Hong Kong Exchanges and Clearing Limited (HKEX)
- Hong Kong Monetary Authority (HKMA)
- Securities and Futures Commission of Hong Kong (SFC)
- Singtel / Trustwave

The CCC was equipped with 27 desks with laptop and dedicated phone lines, plus 24 seats for external observers. Because of its pivotal importance, the CCC set-up was rehearsed a month in advance, in parallel with an exercise dry run.

Figure 2: CCC layout



3.3.5 Scenario development

The Scenario Development Committee (SDC) was established in May 2019. The team was tasked to develop the scenario, as well as manage the production of the various injects. The exercise scenario included three main challenges: pandemic, internet connectivity issues, and an insider-led cyber-attack.

The design and development of each scenario thread was allocated to a member of the SDC. Once a thread was drafted, this was shared with the full committee for feedback and revisions before being split into injects and aggregated into the master events list. The scenario threads were divided into several independent sub-events or incidents, with each inject allocated its own time segment. The scenario injects were based on the exercise objectives and requirements and alluded to topical trends and incidents. For instance, sophisticated insider attack and deep fake elements were included to reflect recent emerging cases of cyber criminality. The aim was to offer participating organisations the opportunity to estimate potential impacts of each incident and provide an initial response within a short period of time. To add to the realism and stress within the CMTs, some injects were released simultaneously, such as the internet becoming unavailable while the absenteeism rate and home-working was on the rise due to pandemic. Importantly, this year's exercise took place during Hong Kong's ongoing civil unrest, which had already posed various real-life challenges to the participating organisations' business continuity before the exercise. Bearing that in mind, the organisers ensured that WISE2019 allowed the participating organisations to exercise a different set of procedures than what they had already been implementing in real life in relation to the civil unrest.

The following factors were considered during the development of the scenario:

- Level of realism;
- Type of threat;
- Location of the threat;
- Optimal date and time for delivery within the exercise timeframe;
- Differing levels of crisis management 'maturity' in the participating organisations.

All parts of the scenario needed to be realistic, plausible and challenging. The scenario was designed to be extensive and challenge each participating CMT, helping organisations to identify potential areas of weakness. In addition, the exercise was structured to encourage interaction and cooperation with external parties and seek advice and collaborate under challenging circumstances.

During the inject production period, the SDC considered the following criteria:

- Ensure the scenario is sufficiently challenging to incite in-depth discussions within the CMT;
- Ensure the scenario covers the specialisations of all participating organisations, e.g. securities, asset management, retail, private banking;
- Confirm whether the scenario is credible and topical for the Hong Kong financial services sector, while managing geopolitical tensions or sensitivities;
- Estimate the consequences of disruption caused by the scenario to avoid overwhelming the industry, which might lead to closure of the market. One of the key aims of the exercise is to challenge the industry without closing the market;

- Ensure the scenario is sufficiently diverse to encompass systemic risks across the market, rather than risks that could be managed by a single organisation in isolation.

In preparing a realistic timeline for the scenario, it was important to allow enough time for participants to understand and respond to the various injects.

To ensure the effectiveness and credibility of the scenario, the SDC invited several trusted organisations to provide advice and review the master events list, including industry professionals from HKFSBCM, HKMA, SFC, HKEX, and Control Risks. This approach presented valuable insights and reinforced the credibility of the exercise.

3.3.6 Inject production

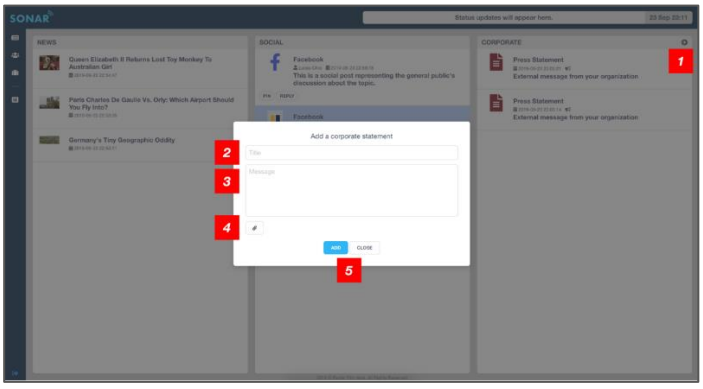
Individual scenario injects were designed for delivery to participating organisations through the WISE2019 online exercise portal. The communications consultancy Ruder Finn was subcontracted by Control Risks to provide the exercise portal platform and design the aesthetic aspects of the scenario injects. Each organisation was provided with three unique login credentials to access the portal.

Examples of scenario injects delivered through the portal included:

- News videos and articles;
- A “live” ticker to update participants on market movements, simulating the Hang Seng Index;
- Dynamic social media posts, e.g. Twitter, Facebook posts;
- A “live” ticker to highlight important scenario information (e.g. breaking news) and important exercise announcements (e.g. commencement of the exercise);
- Press releases/corporate statements.

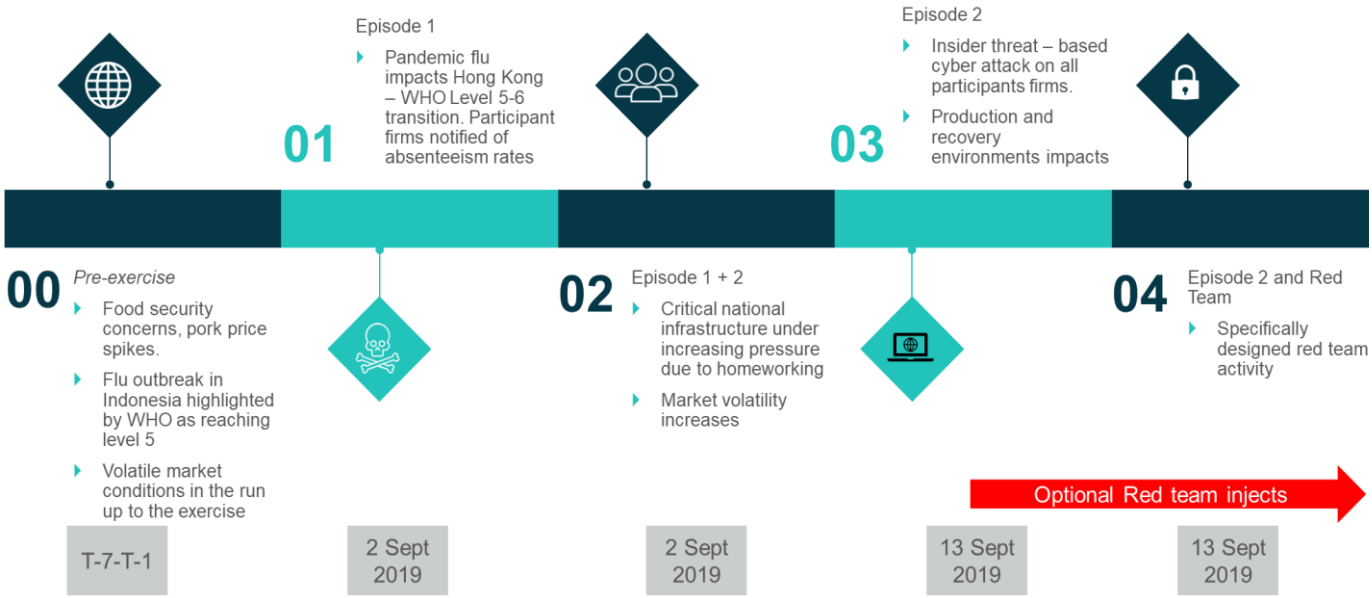
In addition to receiving scenario injects, participants could post press releases and corporate statements in the exercise online portal to simulate their crisis communications strategy. Any press releases or corporate statement posted on the portal could be viewed by other participants and members of the command centre. Once a post had been made, it was not possible for the organisation to edit or delete it, which reflects the process in a real-life crisis.

Figure 3: User interface of the exercise portal



3.4 Scenario

Figure 4: Key scenario elements



Before the exercise, participants could access the portal and read news about the African swine fever outbreak. However, this served as a 'red-herring' and would not have a significant impact on the financial industry, as African swine fever does not spread to humans.

Once the exercise commenced, the first episode included the spread of a swine flu (H2N3) pandemic from Indonesia to Hong Kong where people could not purchase the essentials to prevent the spread of the contagious disease. This resulted in a spike in absenteeism at work. Moreover, signs of users having difficultly accessing the internet started to emerge. As the swine flu contagion unfolded many financial institutions implemented homeworking. In order to challenge homeworking as a solution, the scenario included widespread issues with internet connectivity. As a result, this scenario tested how financial institutions would react to a crisis involving multiple different simultaneous issues.

The second episode was characterised by an insider cyber-attack. This was caused by a group of frustrated employees who were forced to work during the pandemic and risk becoming infected. The cyber-attacks led to various customers receiving false bank statements, which eventually resulted in customers losing confidence in their banking institutions. At the same time, large numbers of customer enquiries were received by institutions which were simultaneously short of staff to handle these enquiries. In a situation like this, participants were challenged to restore customer confidence and solve the data integrity issue.

Figure 5: Exercise phases experienced by the CMT

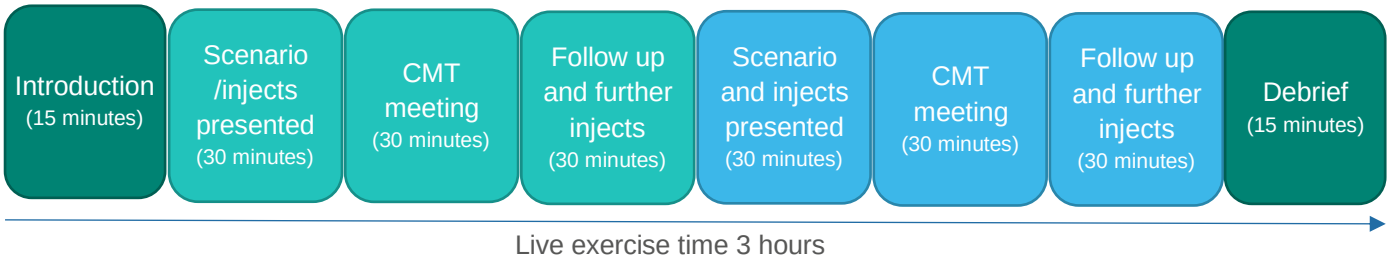


Figure 6: key inject delivery timeline

Exercise time	Actual time	Inject
Pre-exercise	Pre-exercise	Video 1: “Swine Flu - is it a repeat of 2009?”
Period 1	13:00	Checkpoint 1: Pre-exercise health check
Period 1	13:30	Exercise commencement
Period 1	13:30	Video 2: “Swine flu having a huge impact on Hong Kong”
Period 1	13:30	Checkpoint 2
Period 1	13:35	Video 3: “Most severe flu outbreak since 2009”
Period 1	13:50	Video 4: “Hong Kong employers struggling to cope with absenteeism”
Period 1	13.59	1st regulator’s request for information
Period 1	14:00	Crisis management meeting 1
Period 1	14:10	Video 5: “Global flu - update”
Period 1	14:30	Video 6 (deep fake): “This is the REBEL”
Period 1	14:45	Checkpoint 3
Period 1	14:50	Video 7 (deep fake): “We told you”
Period 2	15:02	Video 8: “Friday 13th September - Flu ravaging the financial sector!”
Period 2	15:29	2nd regulator’s request for information
Period 2	15:30	Crisis management meeting 2
Period 2	15:28	Video 9 (deep fake): “We are still in your systems”
Period 2	16:00	Video 10: “Global Flu mortality rate averaging 3%”
Period 2	16:15	Checkpoint 4
Period 2	16:20	Video 11: “Hong Kong financial sector suffers coordinated cyber attack by the REBEL”
Period 2	16:45	Checkpoint 5: Exercise close

4. WISE2019 – observations

4.1 WISE2019 has led to a variety of key observations

Key observations and lessons identified from WISE2019 are summarised in the following sections.

4.1.1 There is a continuously high interest in an industry-wide crisis management exercise

- WISE2019 took place during a challenging time for Hong Kong, with various real-life incidents for the business continuity management teams and CMTs in the financial industry. However, a participation rate close to that of WISE2017 demonstrates a continuous demand for industry-wide crisis management exercises. A crisis may occur through different avenues, and exercises like WISE help CMTs train their response to a variety of low likelihood, but high impact scenarios.

4.1.2 The scope of participating organisations is widening with the inclusion of virtual banks

- WISE2019 included three virtual banks as participants. The presence of Livi VB Limited, SC Digital Solutions Ltd., and WeLab Digital Limited, demonstrates both the changing nature of the financial industry as well as the similar needs and challenges virtual banks face in managing crises.

4.1.3 Crisis management capabilities vary across the industry

- In an exercise bringing together 42 financial institutions of different sizes and expertise, it is natural that some organisations will find the scenario more challenging than others. Most of the organisations reported the tempo was satisfactory throughout the exercise. However, while the proportion of organisations perceiving the tempo as too fast increased from 22% to 30% between the middle and the end of the exercise, the proportion of organisations perceiving the tempo as too slow also increased from 7% to 13% within the same time period. This shows that as the exercise became increasingly challenging for some, other organisations felt the challenge decreased.
- The convergence of various scenario elements unfolding simultaneously posed additional challenges to organisations, which, like exercise tempo, were perceived differently. For example, while the absenteeism caused by the flu pandemic was rated as the most challenging for 12% of organisations, 47% or almost half of the organisations considered it the least challenging. Similarly, while the critical national infrastructure outage was perceived as the most challenging for 32%, another 30% found it the least challenging. These figures demonstrate that even though the participants belong to the same financial industry, their varying size and competencies expose them to different challenges.

- While almost all CMT members indicated that the exercise increased their confidence as a CMT member, the personal skills of CMT members also vary across organisations. Close to half of CMT members identified that they need more training to better respond to a crisis, while almost another third indicated full confidence in their current capabilities.

4.1.4 Structuring the exercise to better reflect how organisations respond to crises demonstrated increasing maturity of the exercises and organisations taking part

- To better reflect the way in which organisations respond to crises, the exercise was structured to allow CMTs to assess incoming information, conduct a CMT meeting and conduct follow up actions. This format was repeated twice and CMTs were given 30 minutes to complete their CMT meeting. This allowed CMTs to practice their ability to manage their response in a way that reflects how they will respond in a genuine incident and identify improvements in their internal processes.
- Some of the key lessons learned from WISE2017 included not logging and summarising the incoming and outgoing information and actions taken, and not having a clear understanding of the CMT members' roles and responsibilities. This year's feedback suggests that almost all organisations made a record of incoming and outgoing information, as well as had a clear understanding of roles and responsibilities of CMT members. Furthermore, almost all CMT members were reportedly forthcoming with sharing information and providing relevant knowledge for their business area updates, which led to effective and well-communicated decision-making. We believe these improvements are due to the opportunity to properly practice crisis management meetings, which allowed the organisations to effectively assess the ongoing crisis and decide on the relevant actions.

4.1.5 Participating organisations demonstrated effective communication with various stakeholders

- Most organisations indicated they have developed communication plans and procedures to effectively communicate with internal and external stakeholders. Most organisations communicated with internal staff, media, customers and the regulators.
- Only 55% of organisations indicated that they communicated with industry peers during the exercise. While this demonstrates that more than half of the organisations took advantage of the chance to liaise with their peer organisations, there is room for development in industry-wide collaboration for responding to an industry-wide crisis.

4.1.6 Most organisations provided a timely and adequate response to the regulators' request for information

- As part of the exercise, participants were required to respond to two requests for information from their respective regulators, either the HKMA or the SFC. These requests were issued right before each designated CMT meeting to ensure that the CMTs have an opportunity to discuss the response to the questions, as well as offer an agenda for those organisations with no structured CMT meeting procedures. Most organisations were able to respond to

their regulator's request for information within the allocated 45 minutes, with the response times ranging from 5 minutes to 70 minutes. Several organisations got in touch with their regulator to report the ongoing incidents even before receiving the regulator's request, which displays mature engagement procedures.

- The quality of the responses to the request for information was largely adequate. While some organisations provided short, one sentence responses to the regulators' questions, others drafted more detailed responses, outlining the exact steps taken along with action plans. While both options are acceptable if the requested information is captured, industry best practice is to have an established protocol in place to communicate important information to regulators in a timely fashion.

4.1.7 Most organisations believe they are well prepared for a pandemic crisis

- One of the objectives of introducing the pandemic thread to the scenario was to test the industry's readiness for a crisis that has not impacted Hong Kong since SARS in 2003. All organisations indicated they have an existing pandemic plan with a prioritised list of departments and functions, which they also used to respond to the pandemic scenario. Almost all organisations also indicated they have a social distancing policy included in the pandemic policy, which is crucial to effectively contain the rate of absentees while maintaining operations. However, based on the observations from the CCC, several organisations communicated much lower absentee figures than others during the exercise. This is due to the alphabet-based absenteeism calculation formula used to determine the absentees from each organisation, which led to a different impact in each organisation.
- Even though almost half of the organisations found the pandemic as the least challenging scenario thread, several organisations also rated it as the most challenging, which indicates not all institutions are well prepared for pandemic challenges.

4.1.8 Cyber security response is integrated with crisis response, but insider threat response integration with crisis management presents a larger challenge

- Nearly all organisations stated they have a specific cyber response element integrated to their crisis management plan. Participants indicated that this was effectively used during the exercise, which suggests that the industry has understood cyber threats and is well prepared to respond to a cyber-incident. However, the cyber-attack introduced in the exercise originated from an employee, further testing the organisation's readiness to tackle malicious insiders, who have been behind an increasing number of cyber incidents over the past year. Only 60% of participating organisations reportedly have an insider threat response plan, which may reduce the effectiveness of an organisation's response to this type of threat.

4.1.9 Some organisations are not well prepared for telecommunications connectivity issues

- The critical national infrastructure outage introduced together with the pandemic posed an additional challenge to participants' resilience. For a third of the organisations, the telecommunications connectivity issues that prevented homeworkers from completing their duties proved the most difficult to respond to out of all scenario threads. At the same time, another third of the organisations considered this thread as the least challenging, pointing to both

different levels of readiness among the industry, as well as the differing operational requirements within the industry.

4.2 Benchmarking

Each participating organisation will receive an individual report which helps them assess their effectiveness as compared to the industry and best practice.

The detailed report will cover the following topics:

- Crisis management skills
  - The internal organisation of the CMT and the CMT facilities for the exercise.
- Communication
  - The communication practices of the organisations from a high-level understanding of formal procedures to activities taken during the exercise, including the submission of public statements and social media posts and response times. This covers internal and external communications from an information vetting perspective to information dissemination.
- Information management
  - Information can be an advantage and disadvantage in a crisis. The process of understanding, communicating, discussing and recording information is key to ensuring a CMT effectively manages itself and the situation.
- Decision-making
  - An effective CMT allows effective management of an incident. This area will look at the effectiveness of CMT members' involvement in the discussion and decision-making process. It also helps show the integration of the cyber element into response plans, as well as staff welfare and the recording, review and execution of decisions and tasks.

5. Considerations for WISE2021

Most participants gave positive feedback to the exercise, commending the scenario and logistical arrangements as thoroughly thought through and well executed. This means WISE2019 was well received and should be continued in a similar format in 2021. However, through the post exercise survey and a post exercise briefing session held on 2 December at UBS and delivered by Ben Wootliff of Control Risks, the Organising Committee has identified the following considerations for WISE2021:

5.1.1 Ensure exercise content is more relevant to all participants

- The scenarios chosen for WISE 2019 were considered appropriate and realistic, with greater complexity than previous exercises. The addition of the Deep Fake videos was considered a useful mechanism to educate CMTs on emerging threats. The scenarios were also considered helpful in prompting CMTs to work with subject matter expert departments within the organisation such as the cyber teams. Participants would like to see a greater push for this in future.
- Participants appreciated the ability to tailor injects to their organisation, such as the absenteeism data. This can be explored further by allowing greater flexibility to customise local injects. Admittedly, most of the injects were designed for retail and commercial banks. Thus, some participants thought some of the injects were irrelevant to them since they were investment banks with a different business structure. Therefore, it is suggested to develop and categorise more tailored injects especially for investment banks, to avoid CMTs being underutilised during the exercise. Facilitators would also appreciate having red team injects available to them, with the command centre providing additional injects as checkpoint feedback identifies a need.
- Many participants thought the cyber scenario was confusing since limited details of the attack were provided. Thus, some organisations had to come up with assumptions to respond to the situation, which is not ideal from the exercise delivery perspective. Therefore, participants recommended that more detail and direction be provided, such as which exact banks are compromised, how much information had been compromised, etc.
- For future WISE exercises it is recommended participating organisations provide greater input to the scenario development work stream.

5.1.2 Consider further improvements to exercise delivery format

- The delivery of WISE2019 introduced two allocated time slots for each CMT to conduct a 30-minute CMT meeting. This opportunity was considered a useful improvement in the delivery format. However, the industry would also like to see clear breaks in the exercise.
- Some elements of the exercise were considered unrealistic. This included the need to complete the regulatory update during the CMT meeting as well as the inconsistent pace of injects, with multiple injects arriving simultaneously in some parts, and at a much slower pace in others. Injects also sometimes did not reflect organisational structures.
- Some participants indicated three hours was too long for the exercise, although this length was chosen based on majority feedback prior to the start of WISE 2019. This feedback, in addition to other feedback on the need to

include more realistic and localised injects, and the need for extra time to prepare for and follow up on action post CMT meetings, should inform the format of future exercises. These needs could well be met with a real time exercise conducted over 1-2 days allowing participating CMTs to manage an incident in a more realistic setting.

5.1.3 The exercise delivery model should be reviewed to ensure it meets the objectives of organisations and learnings from WISE 2019

Facilitators are key stakeholders in delivering WISE and are relied upon to undertake a significant number of tasks from conducting portal testing to coordinating the internal setup and internal delivery of the exercise. To better support this community, the following improvements are suggested:

- A longer lead in time allowing facilitators to be fully briefed prior to them needing to undertake internal briefing sessions. Facilitators would also prefer to receive materials such as the run book and handbook earlier to fully understand the exercise. This would need to be balanced with the risk of the scenario being leaked, either to CMT participants or the wider world.
- Roles and responsibilities for the facilitator and other roles should be provided at the outset, to ensure the most appropriate person is identified. This would help them balance the workload across the facilitator and point of contact.
- A structured dry run of the scenario, allowing facilitators to understand the scenario and their role in supporting the delivery of the exercise should be held. This could involve facilitators undertaking the role of the CMT to better embed the exercise outcomes.
- Facilitators identified that proactive communications about the exercise, rather than ad hoc updates, would help them in their role, and allow them to manage their stakeholders better. These communications should include forward looking dates and tasks to be undertaken by the facilitators.
- In addition to extra facilitator training, some organisations identified a need for greater best practice training in crisis management for senior management. This was offered as an additional service by Control Risks, but the opportunity was not taken. Future WISE exercises may consider changing the delivery/pricing model to incorporate professional crisis management training.

These improvements would ensure facilitators are comfortable advising internal senior management on the exercise delivery, purpose and overview. This ensures internal participants are properly engaged and ready to undertake their role fully during the event.

5.1.4 Make further upgrades to the exercise portal for an enhanced user experience

- Participant feedback was positive on portal design and stability. However, facilitators identified that it would be helpful if incoming injects could be accompanied by an audio cue that can be switched on and off.
- Facilitators noted the ticker is no longer a useful update tool. Material updates should be included in the core injects. The fact that the ticker prompts are no longer relied upon reflects increasing maturity in participating organisations. This should be removed in future and replaced with the audio cue, as detailed above.

- To allow better monitoring of the unfolding scenario, some organisations would like to see unread news items with a different colour or highlighted.
- Although the exercise portal was introduced with various upgrades since WISE2017, some organisations still experienced connectivity issues, especially with video playback. This may have to do with participants' network bandwidth, resulting in a few organisations using the prepared contingency pack.
- Finally, in addition to the portal, facilitators identified a need to consider additional communications channels such as WhatsApp for future exercises. This would have to be balanced with the risk of information leakage.

5.1.5 Increase the involvement of the regulators

- There is a strong support among the participants to see more involvement from industry regulators HKMA and SFC, as well as industry-wide bodies like Hong Kong Association of Banks (HKAB) and ASIFMA where they provide greater guidance on a coordinated industry response. Participants especially expected more pressure, questions and guidance from HKMA and SFC both in the form of phone calls and emails during the exercise. This may include an industry wide call where participants are required to response to regulator questions.
- Participants also identified a wish for the regulator to continue their engagement in scenario development, like that observed in Singapore.
- Participants questioned the role of HKAB in a major incident. HKAB's involvement should be considered in future WISE exercises, and participants should also be discussing this gap with their internal HKAB representatives.

5.1.6 Further enhance the structure of the command and control centre

- The command and control centre operated well. Due to improvements in portal stability and a greater understanding of the scenario by facilitators, there were fewer calls to the Participant Liaison team. Conversely, the Red Team was better able to provide reactive injects and required additional support. Considering this, in future WISE exercises resources should be rebalanced.
- The CCC is resourced by volunteers. In future WISE exercises it is recommended that as part of their participation, each organisation provides a volunteer for the command centre. Volunteers do not need to be BCM professionals; rather, greater support from those in subject matter areas involved in the exercise (such as cyber professionals) provides a more enriched experience for participants.
- Volunteers undergo a training session before the exercise commences. However, from the CCC and survey, it was observed that some banks could not understand the messages from the telephone injectors. For example, not all the telephone injectors clearly stated which role they were representing. Therefore, telephone injectors should be given clearer instructions before the exercise commencement to avoid similar confusion in the future.

5.1.7 Revisit the costing model for participation

- Participants considered the fee of HKD50,000 per institution good value for money. It was recommended the fee should be benchmarked against Singapore Raffles exercise.
- The engagement model between HKFSBCM, participants and vendors should be reviewed for future WISE exercises. The current model has the potential for a vendor to complete the planning for the exercise, and

participants to withdraw with little consequences. The cost of the exercise would be borne by HKFSBCM, suggesting that the engagement model should be refined.

5.1.8 Ideas for future scenarios

Prior to WISE 2019 initiation, a survey was issued to HKFSBCM members to gather feedback on scenarios. This was useful, however, can be further improved by issuing to participants who have signed up for WISE. By targeting participants directly, the scenario development group will have data relating to each participant which can help with tailoring the exercise content. Ideas for future scenarios provided by the participants include:

Cyber	Physical	Sector-specific
Man-in-the-middle attack	Attack by terrorist or disgruntled staff	Money laundering
Electronic theft of intellectual property	Natural disaster (flood, severe storm, etc.) affecting CNI	Credit and liquidity crisis
Attack on a cloud service provider	Electricity failure	Global financial crisis resulting in bank run
Data integrity	City-wide curfew	
Network isolation	Military deployment to Hong Kong	
Non-availability of offshore recovery solutions		
Attack impacting internal and external key vendors and/or parts of global business		

Annex A. Credits

WISE2019 would not have been possible or a success without the generous help and contributions of an army of determined professional volunteers, assisted by numerous professionals.

Table 1: WISE2019 Organising Committee

HKFSBCM (Board)		
Hozefa Badri (UBS AG)	Etta Lo (Société Générale)	Margaret Goodchild (HSBC Ltd.)
Leigh Farina (HSBC Ltd.)	William Fawcett (HSBC Ltd.)	John Chan (Morgan Stanley)
Control Risks		
William Brown	Mikk Raud	Nadav Davidai
Ben Wootliff	Gordon Wong	Harmanbir Kaur

Table 2: WISE2019 Scenario Development Committee

HKFSBCM		
Angus Lee (HKEX)	Elizabeth Tam (HSBC Ltd.)	Margaret Goodchild (HSBC Ltd.)
Karen Lee (Macquarie)	Hozefa Badri (UBS AG)	Martin Eber (HSBC Ltd.)
Prasad Shetty (Bank of America Merrill Lynch)	William Fawcett (HSBC Ltd.)	Matthew Mollenkof (Morgan Stanley)
Kitty Lim (CMB Wing Lung Bank)	Leigh Farina (HSBC Ltd.)	John Chan (Morgan Stanley Asia Ltd.)
Etta Lo (Société Générale)		
Control Risks		
William Brown	Mikk Raud	Nadav Davidai
Ben Wootliff	Gordon Wong	Harmanbir Kaur
Ruder Finn (production)		
Joshua Wang	Terry Tong	Kenneth Chan
David Ko		

Table 3: Regulatory and industry support

Name	Organisation
Brian Lee	HKMA
Jacky Lau	HKMA
Kevin Yau	HKMA

Name	Organisation
Terence Chan	HKMA
Angela Cheung	SFC
Thomas Wong	SFC
Hokinson Ho	SFC
Emily Ngan	HKAB

Table 4: Observers

Name	Organisation
Clement Kwan	ASIFMA
Laurence Van der Loo	ASIFMA
Asha Baskaran	Bank Negara Malaysia
David Wong Tuong Hup	Bank Negara Malaysia
Noor Zanariah Mohammad	Bank Negara Malaysia
Shahril Nizam Abdollah	Bank Negara Malaysia
Siow Zhen Shing	Bank Negara Malaysia
Ken Coghill	Dubai Financial Services Authority
Angus Lee	HKEX
Dominic Polisano	HKEX
Jeff Yip	HKEX
Billy Lai	HKMA
Celine Chan	HKMA
Grace Tam	HKMA
Jennifer Tse	HKMA
Gordon Kao	HKMA
Polly Ngai	HKMA
Felix Law	SFC
Schenken Wong	SFC

Table 5: WISE2019 Command and Control Centre volunteers

Name	Organisation	Command Centre role
Derek Taylor	Control Risks	Participant Liaison Lead
Ling Jing	Control Risks	Participant Liaison

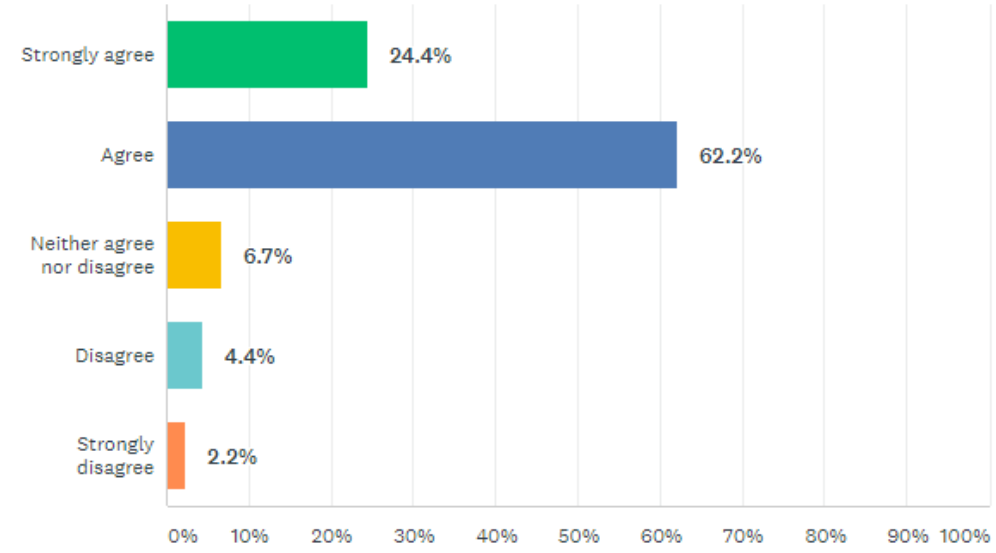
Name	Organisation	Command Centre role
Josiane Dresch	HSBC	Participant Liaison
Sean Robertson	Control Risks	Participant Liaison
Selina Tng	Prudential	Participant Liaison
Steven Wilkinson	Control Risks	Participant Liaison
Wendy Chan	APG Asset Management	Participant Liaison
Wai Meng Choong	Control Risks	Police and the REBEL
Joshua Wang	Ruder Finn	Portal tech support
Kenneth Chan	Ruder Finn	Portal tech support
Terry Tong	Ruder Finn	Portal tech support
Nadav Davidai	Control Risks	Red Team Lead
Andy Lau	HSBC	Red Team
Angel Olausson	Wells Fargo	Red Team
Polly Choi	Fubon Bank	Red Team
Simon To	State Street	Red Team
Edwin Lee	Shanghai Commercial Bank	Red Team: HKEX
William Fawcett	HSBC Global Banking & Markets	Red Team: HKMA
Angela Har	HSBC	Red Team: SFC
Kanika Sethi	HSBC	SurveyMonkey Control
Simon Lowth	SL Services	SurveyMonkey Control
Alexandre Beaumont	Société Générale	Telephone inject
Edward Ip	ZA Bank	Telephone inject
Felix Lin	ZA Bank	Telephone inject
Peter Chen	Control Risks	Telephone Inject
Smith Fung	Chong Hing Bank Limited	Telephone Inject
Sonia Chung	HSBC Global Banking & Markets	Telephone inject
Tammy Cheung	HSBC Global Banking & Markets	Telephone inject

Special thanks

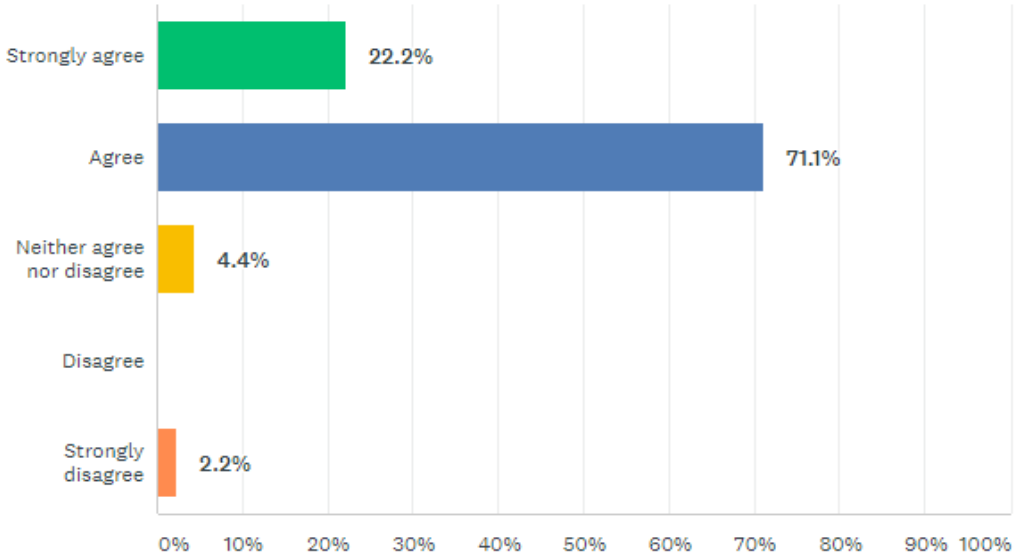
HKFSBCM would like to thank the HKMA, SFC, ASIFMA and HKAB for their invaluable support in driving awareness of WISE2019 by hosting information sessions and/or sharing information on the exercise with their membership.

Annex B. Data collected after the exercise

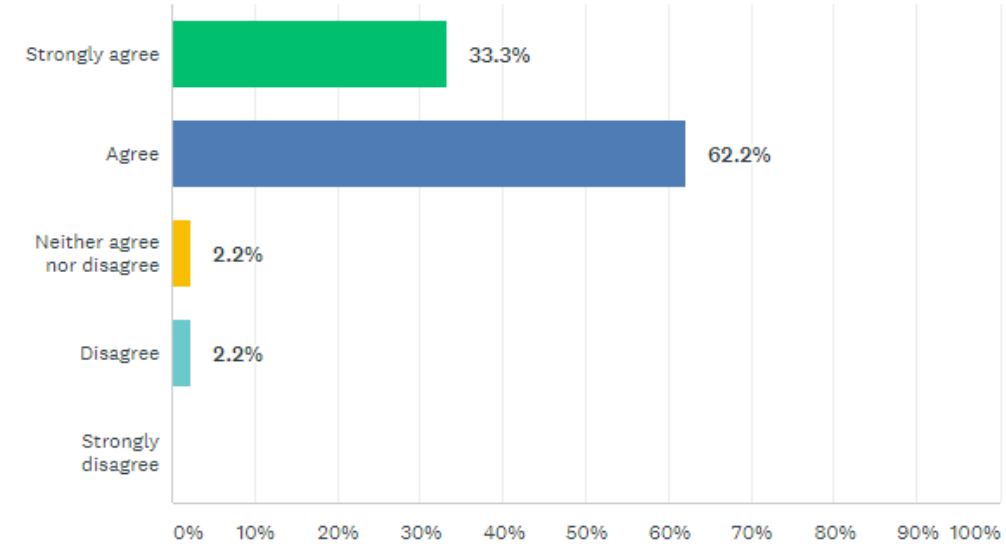
1. You have formalised procedures and processes for communicating with clients effectively, e.g.: communication channels, procedures and decision-making processes are in place



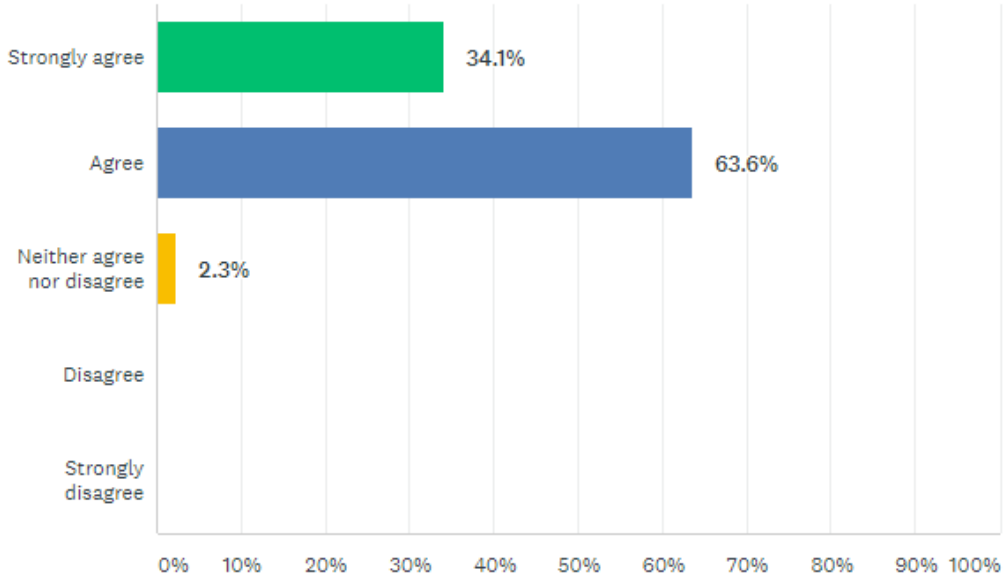
2. Key external audiences, messages and preferred communication channels have been identified, e.g.: regulators, vendors, media, law enforcement, social media, press release etc.



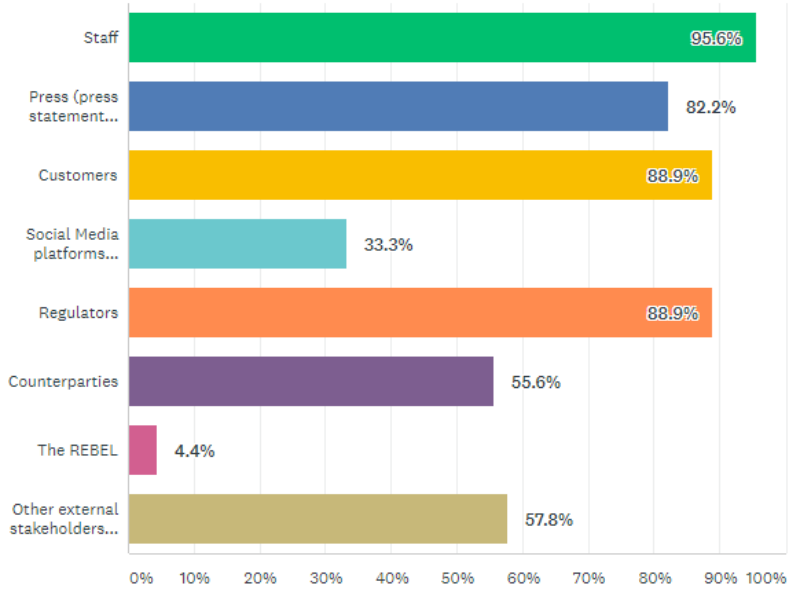
3. You have effective media engagement protocols, e.g.: approved media spokespersons are identified and known to Crisis Management Team members and have the right skills for media interactions.



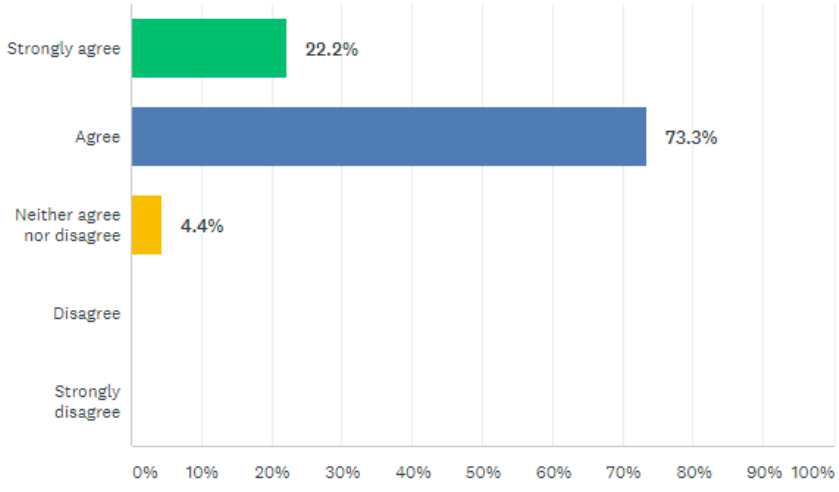
4. Effective internal communications channels and protocols for disseminating information to staff were identified, e.g.: intranet, text message, call cascade, manual or automated call trees, etc.



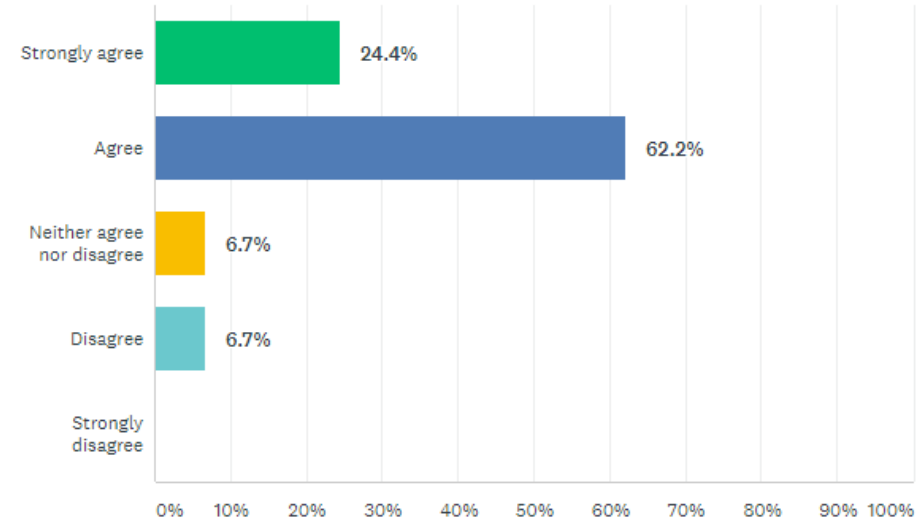
5. During the exercise, you initiated communications (i.e. make the decision to communicate, or release communications) with:



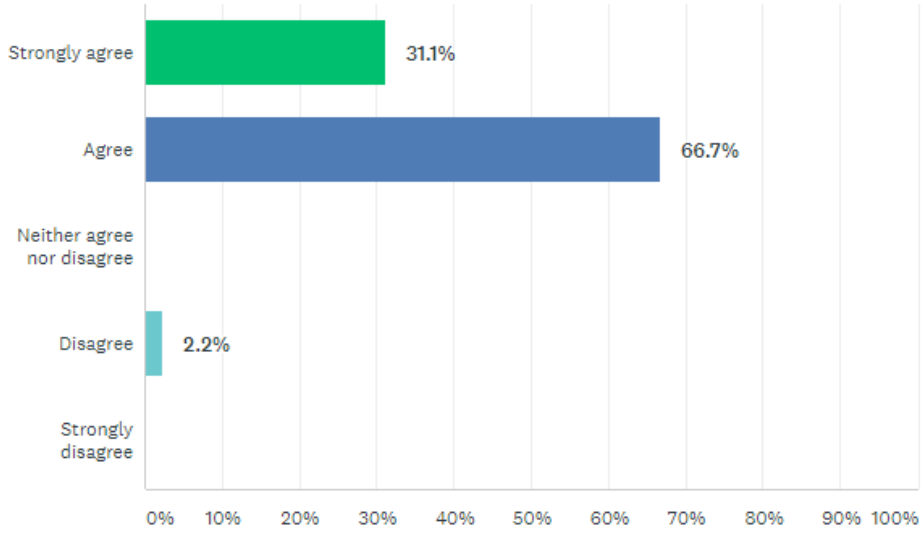
6. The Crisis Management Team can effectively assess and respond to the situation, e.g.: you are confident that in a real incident there are protocols in place to provide you with business impacts, management information / performance statistics – there are sufficient tools available to support effective decision making.



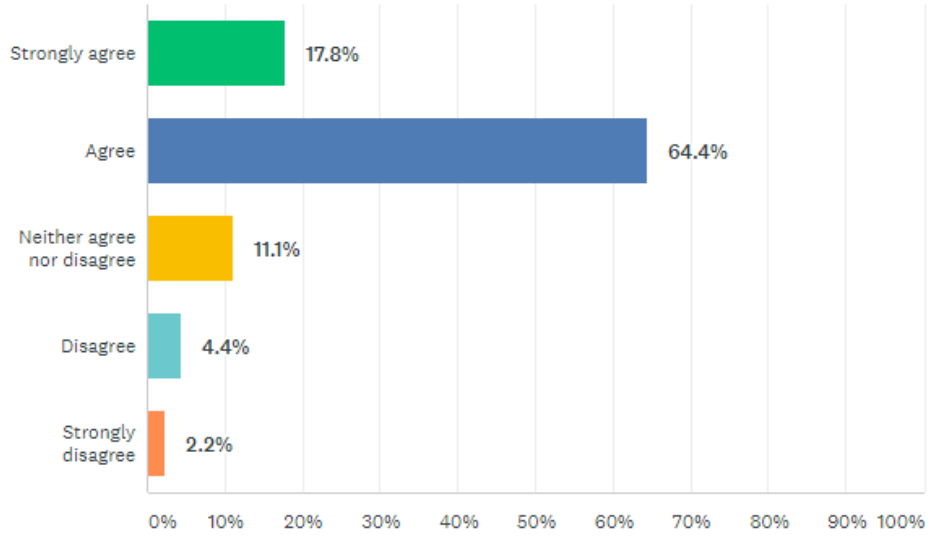
7. A record was made of all incoming and outgoing information, along with internal discussions, e.g.: actions/ information log (manual or automated), meeting minutes, etc.



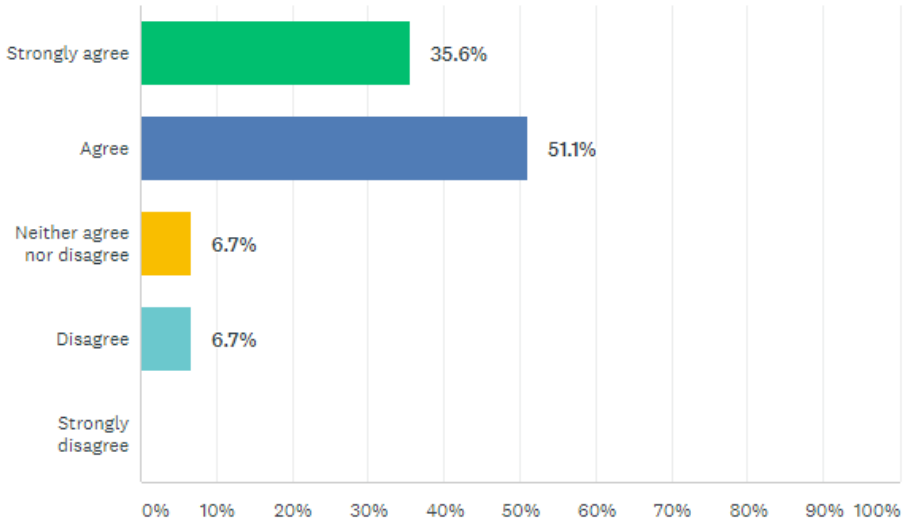
8. All Crisis Management Team members shared information effectively, e.g.: members were forthcoming with sharing information and providing relevant knowledge for their business area updates.



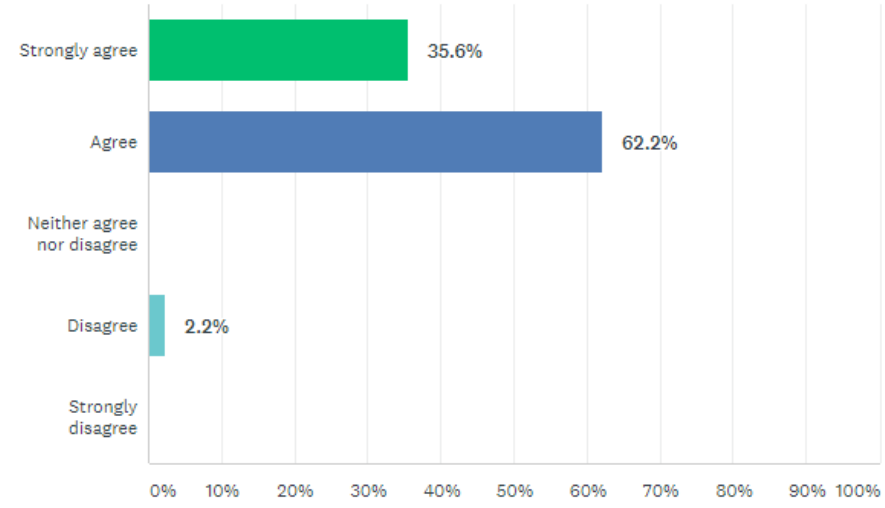
9. The Crisis Management Team regularly set aside time throughout the course of the incident/meetings to summarise and review current information/actions, etc.



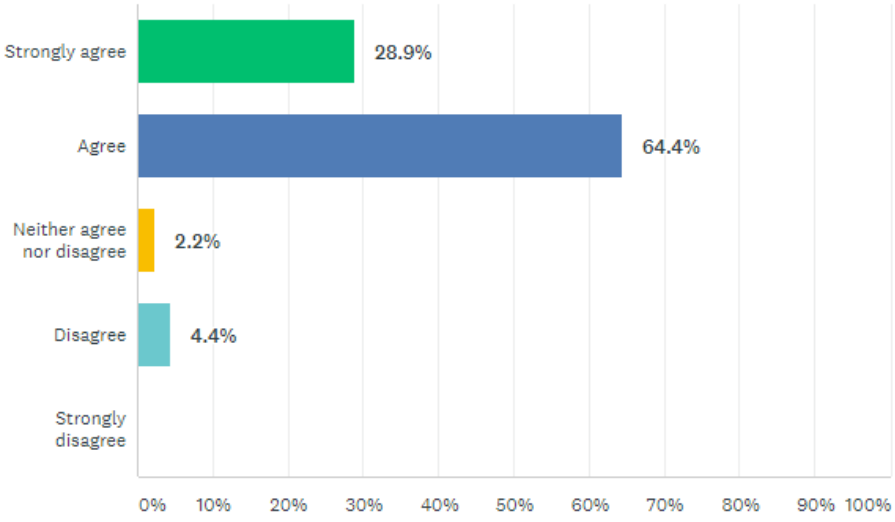
10. My organisation has a standardised crisis management team agenda, which was used to conduct the crisis management meetings.



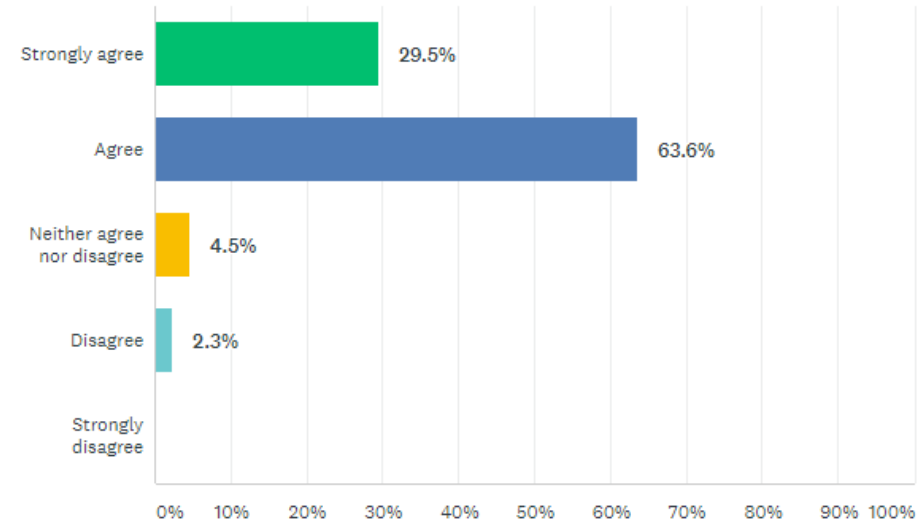
11. All members of the Crisis Management Team understood their roles and responsibilities.



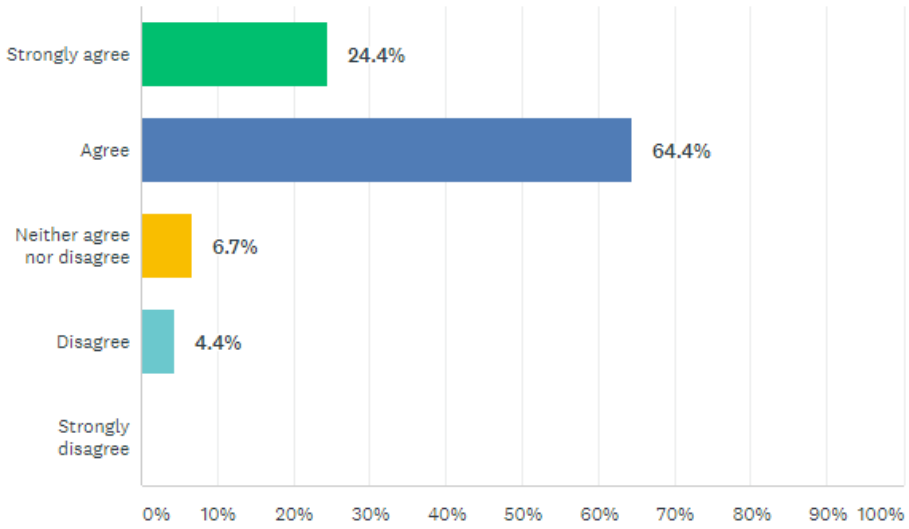
12. Cyber Incident Response is integrated into our Crisis Management Team and protocol.



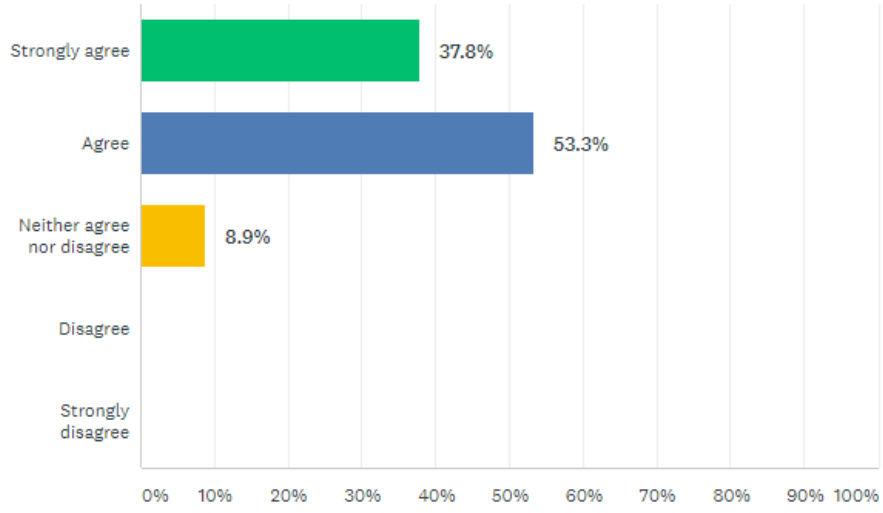
13. The Crisis Management Team's approach to decision making was effective, i.e. decisions were made and communicated clearly.



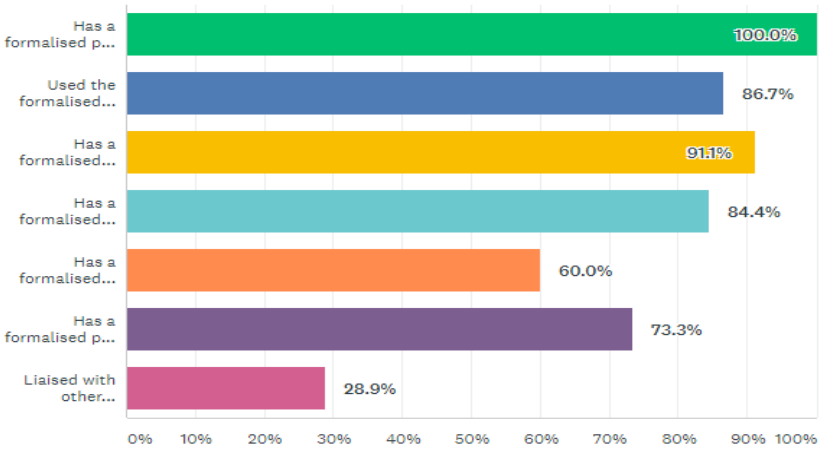
14. Crisis Management Team decisions were translated into actions and tasks, recorded, tracked and followed up by the Chair throughout the exercise.



15. The current Crisis Management Team membership is appropriate – the correct people were around the table or available to support effective decision making.

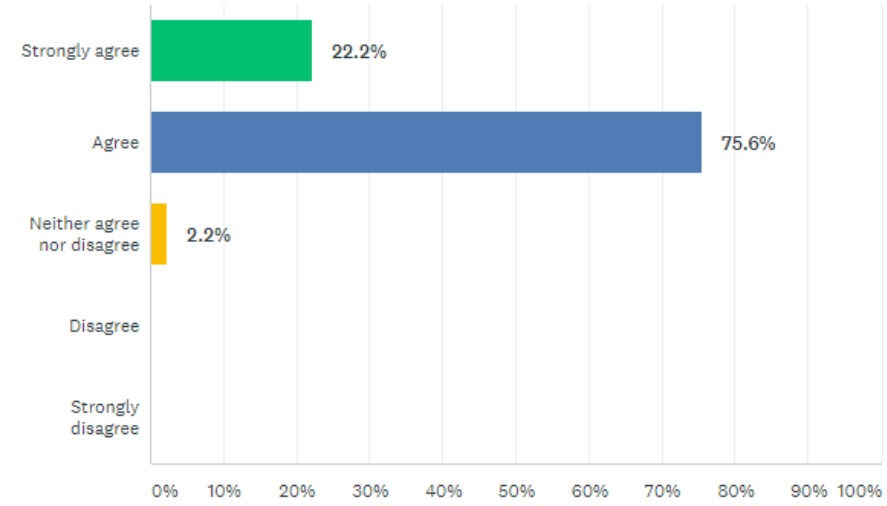


16. Your organisation:

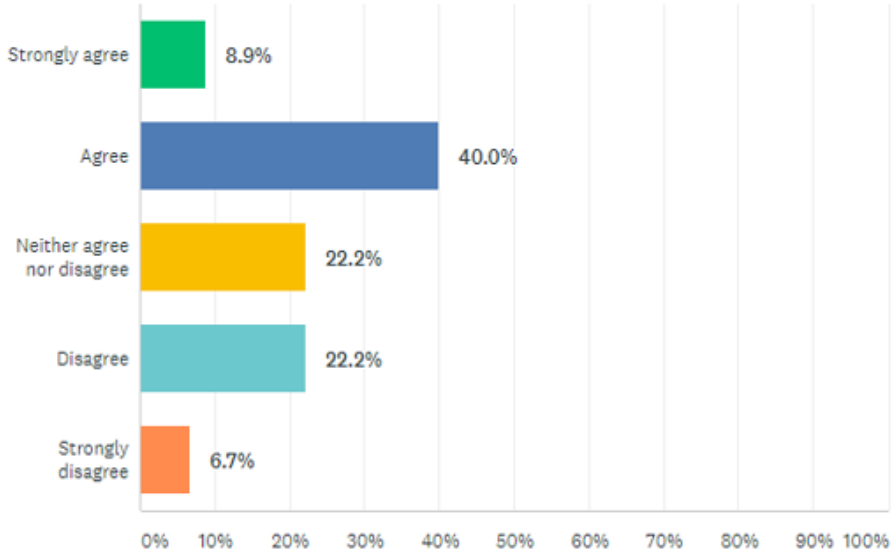


ANSWER CHOICES	RESPONSES	
Has a formalised plan for pandemic	100.0%	45
Used the formalised pandemic plan as part of the exercise	86.7%	39
Has a formalised pandemic plan that includes policies around social distancing and home working	91.1%	41
Has a formalised cyber response plan	84.4%	38
Has a formalised crisis response to specific insider threat attack	60.0%	27
Has a formalised plan for data integrity issues	73.3%	33
Liaised with other participants to see if they had also been targeted by the REBEL	28.9%	13

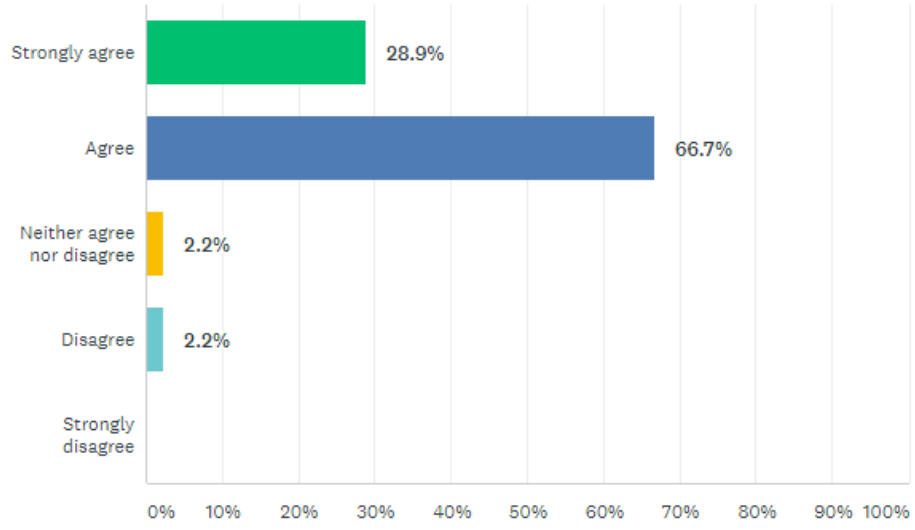
17. The exercise helped develop my personal confidence as a Crisis Management Team member.



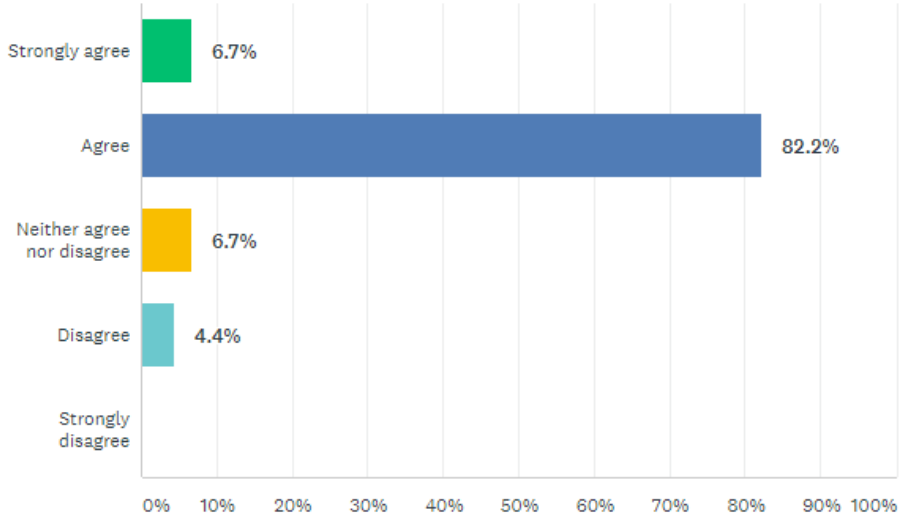
18. The exercise identified that I need more training in my role and responsibilities.



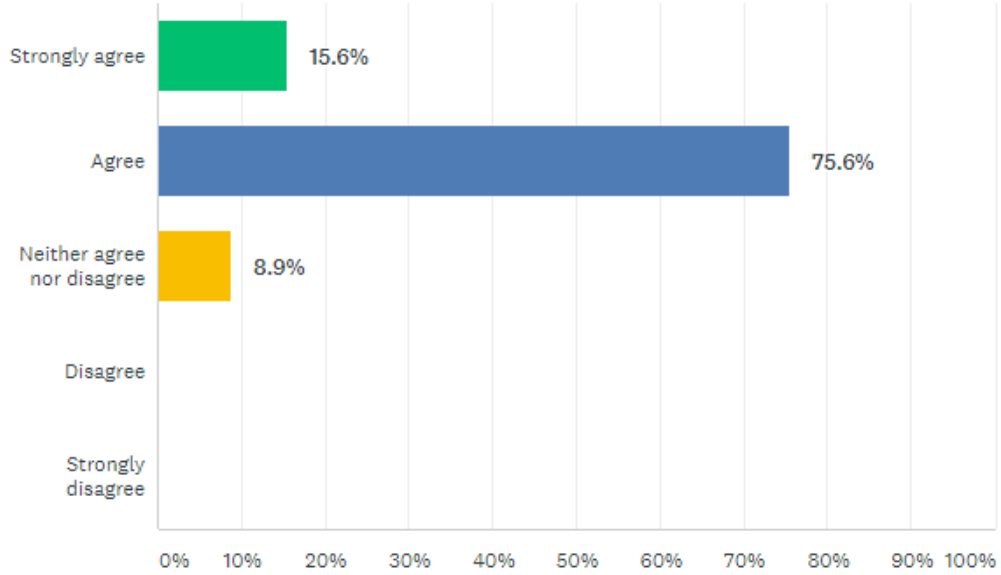
19. The exercise was well organised (internally).



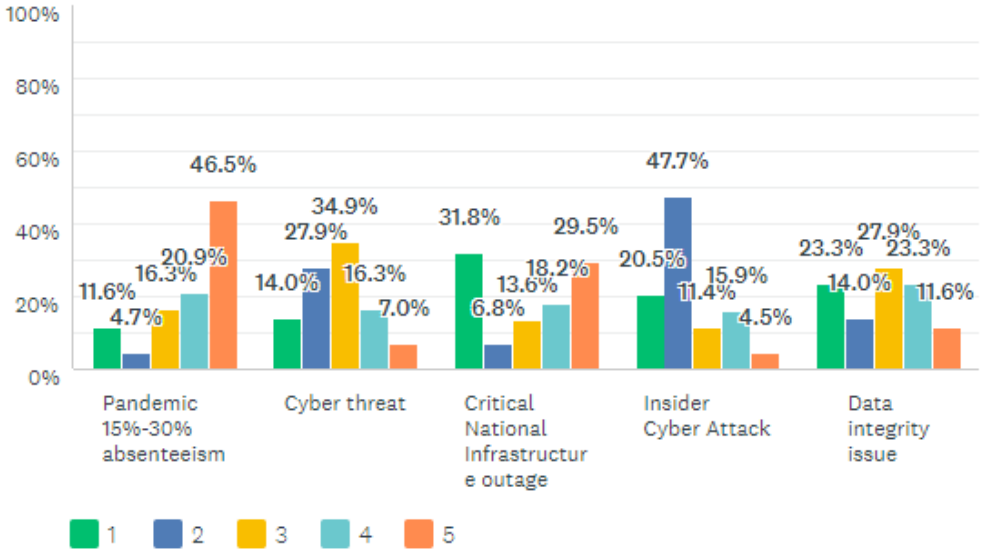
20. The information I was provided with before and during the exercise was sufficient.



21. The hot debrief/feedback session was useful. (Did it capture our areas of strengths and weaknesses? Did you feel it was a good assessment of the exercise?)



22. Which scenario did you find most challenging during the exercise? (Rate the most challenging as '1' and the least challenging '5' – use each rating only once).



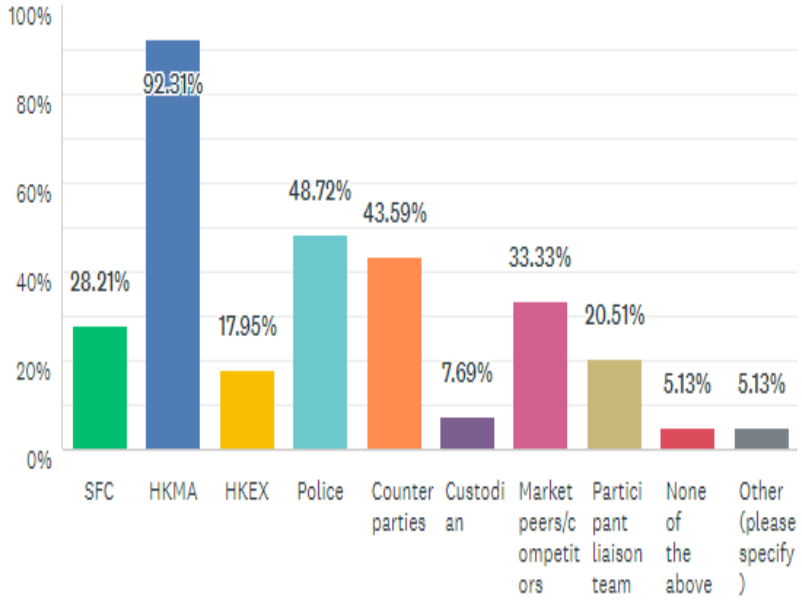
Annex C. Data collected during the exercise

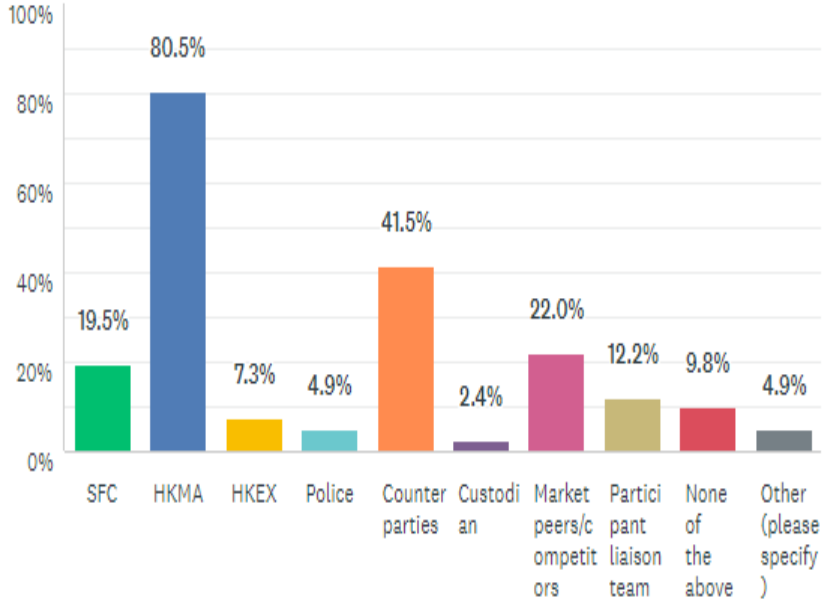
Pre-exercise health check at 1.00 pm

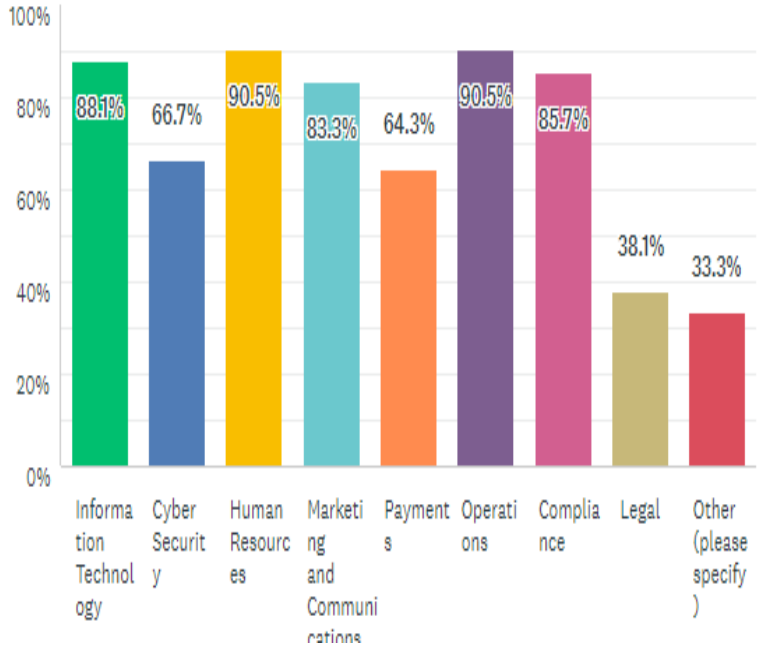
- 100% of the participating organisations tested their portal and telephone for WISE2019 and ensured that it works well.
- 90% of the Crisis Management Team members were present and ready for the commencement of WISE 2019 at 13:30.
- 98% of the participating organisation's CMT could successfully login into portal.
- 79% of the participating organisation had whiteboard or flipchart available for deliberation.
- 95% of the participating organisation had multiple screens for the portal available for deliberation.
- 88% of the participating organisation had pens and papers available for deliberation.
- 58% of the participating organisation had post-it notes available for deliberation.

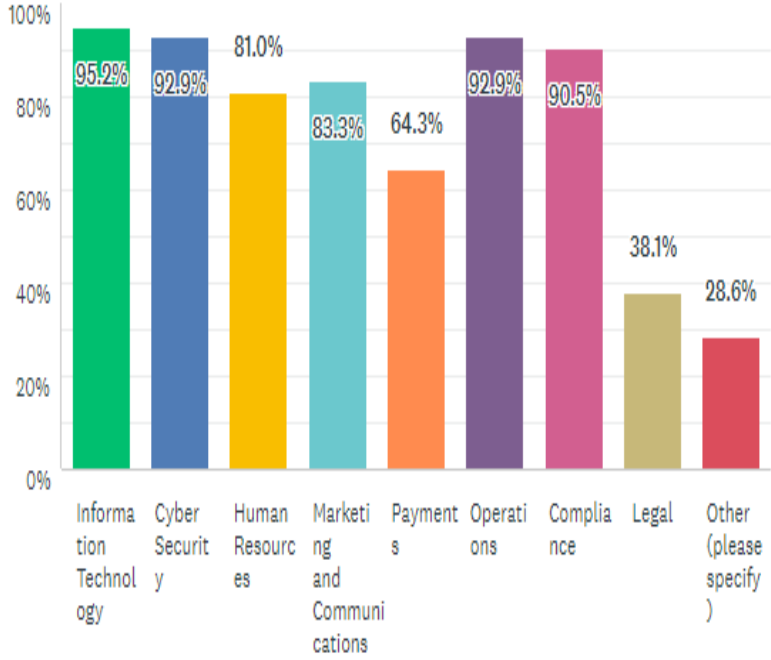
Exercise commencement at 1:30 pm

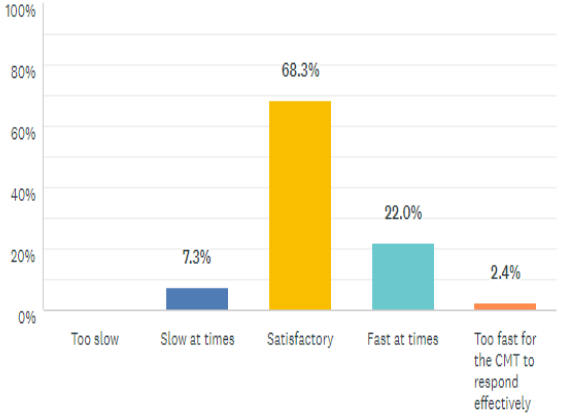
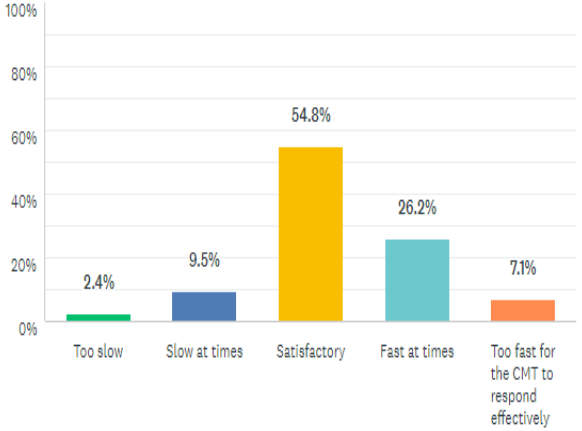
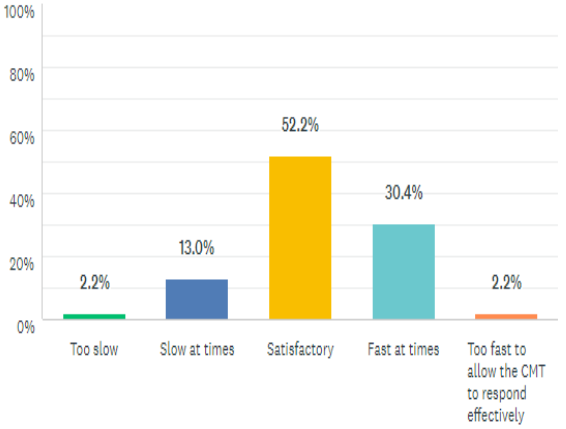
- 100% of the participating organisations said that their portal, email and telephone worked well.
- 100% of the participating organisations' CMT were present at 1:30 pm and started the exercise sharply.

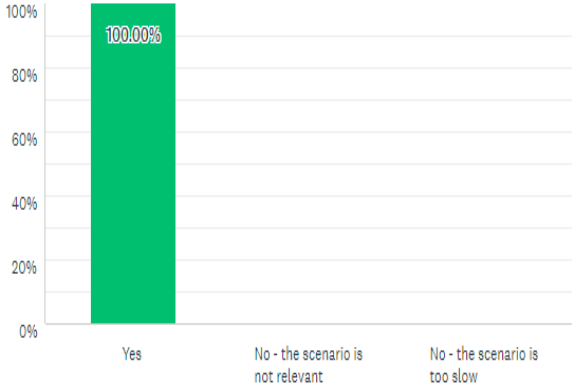
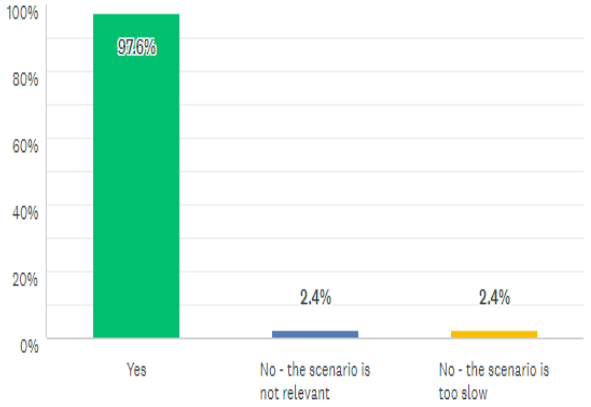
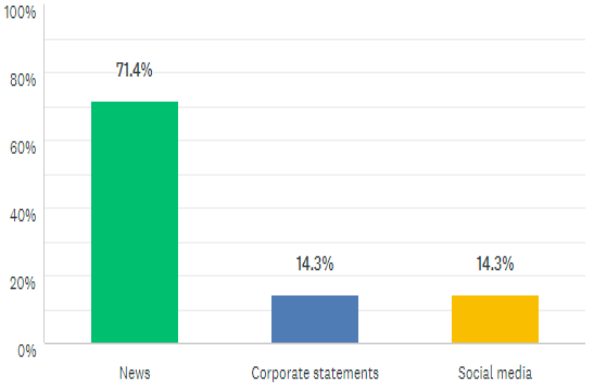
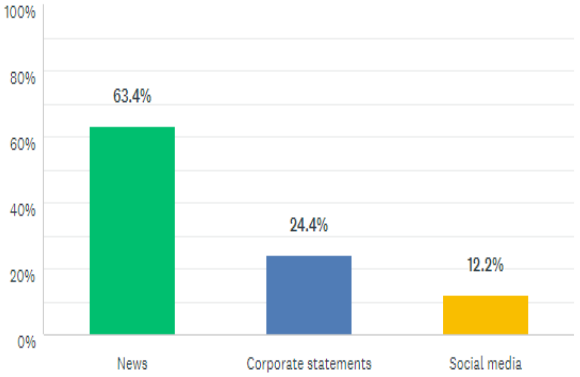
Time	Communications with external stakeholders
75 mins into the exercise	

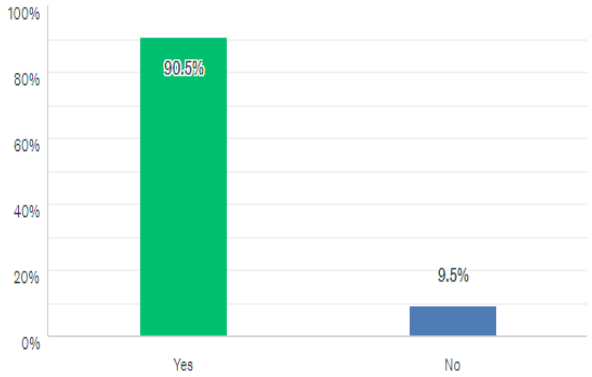
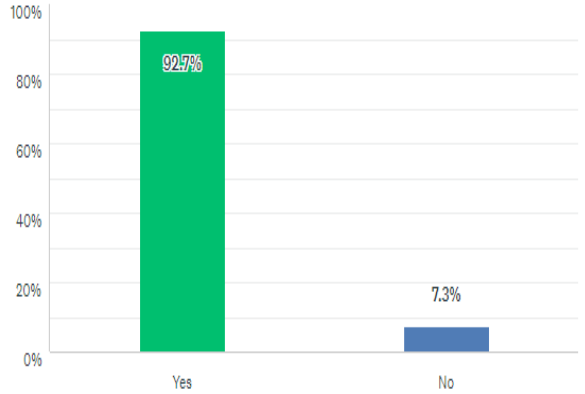
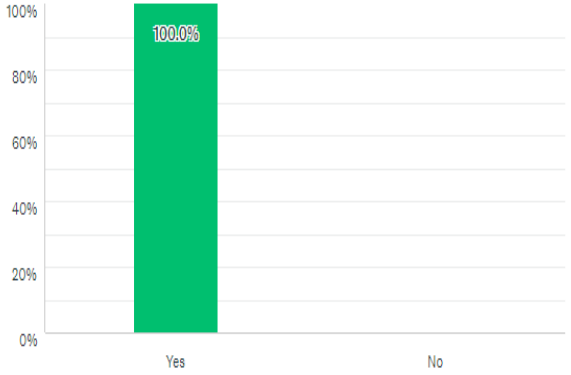
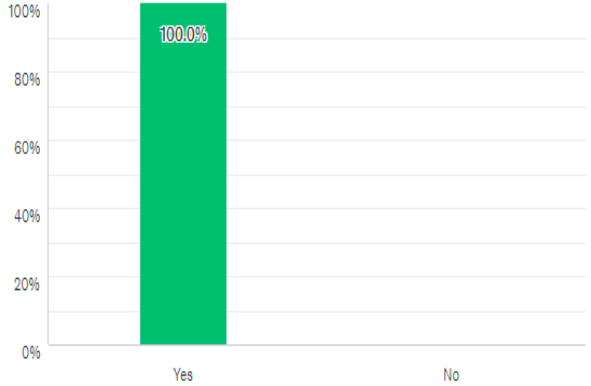
Time	Communications with external stakeholders
165 mins into the exercise	

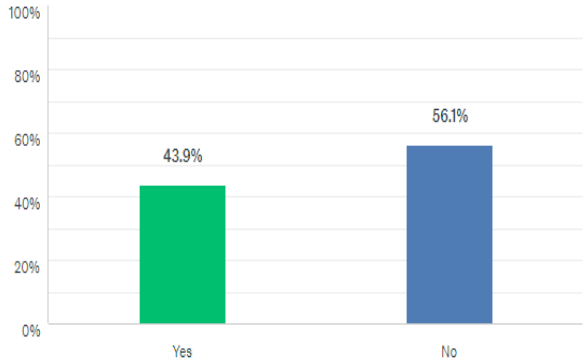
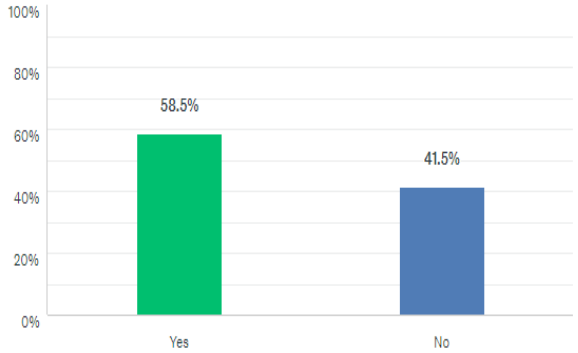
Time	Communication with specialist departments
75 mins into the exercise	

Time	Communication with specialist departments
165 mins into the exercise	

Area	75 mins into the exercise	165 mins into the exercise	Overall
Technology required for WISE2019 works; i.e. portal, CMT email and telephone	All the technology worked well for all the participating organisations.	The email worked well for all organisations. However, the portal did not work for 1 organisation and the telephone did not work for 2 organisations.	Overall, 89% of the participating organisations were satisfied with the technology, with the remaining being neutral.
Tempo			

Area	75 mins into the exercise	165 mins into the exercise
CMT is engaged and discussing the scenario		
Area of portal CMT is actively monitoring the most		

Area	75 mins into the exercise	165 mins into the exercise
CMT completed the CMT meeting		
CMT responded to the regulator's request for information		

Area	75 mins into the exercise	165 mins into the exercise
CMT communi-cated with other participating organisations		
Key decisions made	▸ Activated work from home and/or split office arrangements; some organisations made exceptions for IT staff and senior management. ▸ Invoked BCP and pandemic plan. ▸ Imposed travel ban or restrictions for staff travelling in and out of Hong Kong. ▸ Monitored absenteeism; conducted employee wellness checking. ▸ Monitored incoming customer inquiries; encouraged customers to use e-channels; limited physical interaction with clients. ▸ Communicated with regulators, third party vendors and internal departments to gain more information. ▸ Increased the sanitation of office and equipment. ▸ Elevated the monitoring of market volatility. ▸ Monitored the risk of potential cyber-attack; suspended e-banking; scan for malware, opened a recovery site. ▸ Tightened fraud parameters; isolated the statement platform; double confirmed large transactions, monitored ATM withdrawals; fact checked with corresponding banks on remittance and SWIFT issues; deployed	▸ Continued the home-working policy. ▸ Monitored absenteeism; ascertained the health condition of absent staff. ▸ Increased the sanitation of office and equipment. ▸ Provide more support to the call centre in order to be able to handle customer enquiries; shifted additional desks to overseas in order to field clients' queries. ▸ Communicated with staff, clients, regulators, police, vendors for situation updates, reporting of data integrity issues, and verification of statements; set up special hotline to handle customer enquiry pertaining to statement data problem. ▸ Invoked the Computer Security Incident Response Team (CSIRT); investigated the cause, impact of cyber-attack, health checked the supporting applications and network infrastructure; investigated who the insider is; worked on system recovery; suspended remote and physical access of suspicious staff; revoked access to data centre and keeping privileged access only for the bare minimum staff required; disabled compromised accounts to protect customer data/ privacy.

Area	75 mins into the exercise	165 mins into the exercise
	alternate payment for SWIFT and RTGS; reconciled statements; monitored transaction volume and system capacity. ▸ Issued corporate statement/messages on website; communicated with staff, regulators, other banks, police, and internal/regional critical functions; requested support from HQ. ▸ Checked with key correspondent banks on their current operations and ordered additional banknotes for liquidity purpose; closely monitored the bank's liquidity position and notified Head Office about the latest situation (for standby liquidity). ▸ Prepared scripts for frontline and customer service and phone banking. ▸ Closed some bank branches.	▸ Suspended the statement enquiry function of online banking and notified customers via online banking/ official website; suspended enquiries services across internet and mobile channels for retail and commercial customers. ▸ Ceased trading; discussed the potential of suspending trading if integrity of the data is a significant concern; ceased night-time services; closed branches due to cyber-attack. ▸ Issued a press release; issued an apology regarding incorrect bank statements. ▸ Worked with relationship managers to ensure successful payment execution; maintained only minimal level of remittance and payment services; rejected new requests for outward remittance; notified customers not to perform online real time transaction ▸ Discussed areas that can be improved in company policies. ▸ Continued to monitor the bank's liquidity.

Time into the exercise	Area	Results
75 mins	Pandemic plan	100% of the participating organisations had reviewed and used its pandemic plan. Moreover, they had a prioritised list of departments and functions within its pandemic plan.
165 mins	Cyber-attack response	95% of the participating organisations had a specific cyber response element to their crisis management plan. Among these organisations, 97% stated that the plan was referred to as part of to the response to the exercise.
165 mins	Absenteeism	60% of the organisations thought that the increasing absenteeism rate presented new challenges to their institution.
Overall	1st phase CMT discussion	Social Distancing ▸ 96% of the organisations' CMT discussed social distancing. Flu outbreak monitoring in the wider population ▸ 83% of the organisations' CMT discussed about the flu outbreak monitoring in the wider population. Flu outbreak monitoring in staff ▸ 98% of the organisations' CMT discussed about the flu outbreak monitoring in staff. Health & safety measures ▸ 100% of the organisations' CMT discussed Health & Safety measures that could be deployed. Work from home capacity ▸ 96% of the organisations' CMT discussed about working from home capacity.
Overall	2nd phase CMT discussion	IT/Data Incident Investigation ▸ 100% of the CMT discussed about IT/Data incident investigation Insider Threat ▸ 84% of the organisations' CMT discussed about insider threat Customer Communications for IT issues ▸ 98% of the organisations' CMT discussed about Customer Communications for IT issues Customer Communications to counter the deep fake threat ▸ 71% of the organisations' CMT discussed about the deep fake threat
Overall	CMT chair action	Roll Call ▸ 91% of the CMT chair conducted a roll call and checked all required areas were represented. Minutes

Time into the exercise	Area	Results
		▸ 80% of the CMT chair ensured that the minutes were being taken. Situation overview ▸ 100% of the CMT chair asked for or provided an overview of the situation. Impact on organisation ▸ 93.3% of the CMT asked the designated CMT members for the impact on their area.