Senate Environment and Communications References Committee
Inquiry into the Triple Zero service outage

Questions on notice – Optus

1. **Provide a copy of the 40-page crisis management document referred to during the hearing.**

   Answer:
   Please refer to the attached document.

2. **How much does it cost Optus to run Triple Zero?**

   Answer:
   It is difficult to quantify the exact cost to Optus – and to the broader industry – of providing the Triple Zero service, as there are a range of indirect costs involved where the embedded portion specifically attributable to Triple Zero is not separated.

   The information below is provided in order to illustrate the primary elements of the costs to Optus.

   In terms of clearly visible direct costs, large telecommunications carriers including Optus contribute to the operations of Triple Zero Operator via the Telecommunications Industry Levy (TIL). This levy only applies to telecommunications carriers with annual revenue over $25 million and is based on eligible revenue. A proportion of proceeds from the TIL fund Telstra for operating the Emergency Call Person (ECP).

   In addition to the TIL, Optus pays Telstra (as the ECP) $1.80 for each call made from its network to Triple Zero. This is currently equivalent to approximately $8.5 million per year.

   To provide customers with access to Triple Zero, Optus relies on its broader network infrastructure and operations, which are the subject of significant ongoing investment. While the portion of these costs that could reasonably be allocated to Triple Zero would in most instances be relatively small, collectively the amount is more material. For example:

   - Optus Networks uses certain infrastructure and dedicated trunks towards the ECP that are built in order to support the handling of Triple Zero calls. In the IMS node (VolTE switch), there is a specific node for Triple Zero (known as the e-cscf), which is bundled within the IMS solution purchased from our vendor.
   - The cost of access to spectrum to allow Optus customers (and customers of other carriers who may need to camp on to our network) to access Triple Zero.

- Ongoing network improvement and maintenance costs to ensure reliability of coverage.
- Costs involved in monitoring network operations and responding as appropriate, regulatory compliance and reporting.

3. **In Mr Rue's opening statement, he mentions critical gaps highlighted by the outage. These "critical gaps" were later described as including escalations in call centres, alarming, crisis training drills. Optus to identify these critical gaps and how they have been addressed, and how real-time visibility and monitoring of Triple Zero performance has been changed.**

Answer:

Critical gap	How addressed
Escalations in call centres	• Since the outage on 18 September 2025, Optus has implemented additional compulsory escalation process following any customer reports of Triple Zero failure, ensuring concerns are referred directly to Networks for investigation, and Specialist Care to then manage the case with the customer. • Onshore Specialist Care coverage for customers is now available 24/7. • A safety net has also been implemented in the Optus Interactive Voice Response (IVR), with emergency related utterances triggering call routing to the onshore Specialist Care team • Optus has also implemented enhanced emergency handling training to support agents during critical incidents and enforce stronger escalation controls.
Crisis training drills	• Optus maintains a regular cadence of simulations which enables us to map, review and continuously improve our crisis management processes. The cadence of these simulations has been increased to support the continued uplift of our processes. • “Dry-run” simulations of key teams are now conducted every two months, or when there is a material change to our processes, which includes different scenarios or permutations of outages and crisis management, including disaster relief or major outage management, including welfare checks. • For completeness, Optus also participates in outage simulations run by NEMA, such as the NEMA Higher Risk Weather Season Preparedness Briefings, NEMA National

	Preparedness Higher Risk Weather Season Summit and the NEMA Exercise Convergence.

Alarming and how real-time visibility and monitoring of Triple Zero performance has been changed	• Optus' Network Service Experience Team (NSET) is located in the Optus Network Operations Centre, which operates 24 hours a day, seven days a week.
	• Optus has both automated and manual monitoring processes in its network monitoring and alarming ecosystem.
	• These processes are designed to identify outages based upon trends and behaviours that indicate a disruption to normal network operations.
	• NSET's role includes monitoring graphs that record various aspects of the operation and performance of Optus' services, including:
	  ○ call drop rate
	  ○ call setup failure volumes for voice calls generally,
	  ○ separate graphs for emergency calls to the 3 Emergency Call Service (ECS) specifically.
	• Prior to the Triple Zero outage of 18 September 2025, the system used by Optus NSET raised automated alerts for emergency calls based on pre-set triggers at a **national** level.
	• Since the 18 September 2025 outage, Optus has:
	  ○ Introduced enhanced 24/7 monitoring of Triple Zero call volumes and failure rates at a state and territory level down to SA3to enable early detection of anomalies or deviations from normal call traffic;
	  ○ Implemented daily Triple Zero test calls in every state and territory, pending industry-wide work on automated end-to-end testing;
	  ○ Implemented additional processes in Optus call centres to support customers who are unable to successfully make a call to Triple Zero, including an additional compulsory escalation process as outlined above.

4. **Provide a final breakdown of device type and brand for the calls that did not get through to Triple Zero during the 18 September 2025 outage.**

   Answer:
   There were 158 handset types across 17 handset manufacturers that did not connect to Triple Zero.

   Eighty-one per cent of the handsets were Apple and Samsung variants.

   Appendix 1 provides the detailed list of handsets and manufacturers.

   We note that some devices that did not connect to Triple Zero did also appear in the category where they did connect via Telstra and TPG camp-on. This suggests that there may have been an end-user behaviour that influenced the outcome (for example, some customers may have chosen to end the call before the camp-on process could complete).

5. **Provide further information status of steps taken to fix camp-on issues and establishing an effective backup system so emergency calls can camp-on to another network.**

   Answer:
   Network configuration changes
   Optus has increased the emergency call inactivity timer from 10 seconds to 600 seconds. In the event of a network scenario similar to that experienced on 18 September 2025, this adjustment will allow more devices to be able to connect to an Optus secondary voice gateway and complete an emergency call.

   Handset Improvements
   Optus has supported extensive device testing, (including testing conducted at the UTS test facility) to simulate complex, deep network failure scenarios. Handset manufacturers are using this information to work with industry to deliver enhancements through new software releases aimed at improving emergency calling behaviour, including more resilient camp on- logic and process.

6. **Confirm that Optus' testing of Triple Zero calls occurs in cooperation with the Emergency Call Service (ECS) and provide a view as to whether customers should be testing their own devices separately.**

   Answer:
   Optus has been engaged with the ECP on the volume of test calls undertaken by our network. This currently sits at 1,000 automated test calls daily. We will continue to work with Telstra and the ECP as this testing progresses.

To ensure that the ECP is not flooded with test calls (impacting legitimate calls), our automated test calls drop prior to going through to an operator. This is aligned with the industry standard and expanded to support additional volumes post-September 2025.

Optus does not encourage our customers to make test calls to Triple Zero. We do encourage customers to check their device compatibility on our website.

Optus continues to work with industry, government and the regulator on future device testing arrangements and public awareness activities in line with the recommendation of the Independent Review by Dr Kerry Schott AO.

7. **Can you please provide plain English definitions of the following terms/abbreviations used in Optus' submission:**

Answer:

Term/Abbreviation	Description
E000 trunk blocking	*This is a process of blocking / draining 000 calls before starting works.* *Optus has dedicated trunks for sending Triple Zero calls to Telstra. No other traffic uses these trunks.* *If there is planned work that has any potential to impact Triple Zero trunks at one of our sites, that site is removed from service.* *The process blocks any idle circuits first to prevent new calls from using those trunks. Calls in progress are allowed to complete between customer and Triple Zero. When the call is completed then the circuit is blocked.* *When the site is blocked calls to Triple Zero use one of the other Operating sites to deliver the calls to Telstra.*
Session Border Gateway (SBG)	*Security gateway that makes sure every call that enters the Optus Mobile Voice Core from the Radio Network is safe and allowed.*
Evolved Packet Gateway (EPG)	*Mobile Data Gateway that directs mobile voice and data traffic to and from the mobile device and the core network.*
Networks Technical Investigation Bridge	*A technical call that includes all relevant engineering and operational engineers that are required to resolve an incident.*
eCAB	*emergency Change Advisory Board.*

ExCo	*Optus Executive Management Committee made up of direct reports to the CEO.*
VP	*Vice President (job title)*
CTRE Escalations	*This should read CRTE Escalations and refers to a dropbox that was used to escalate matters to the Optus Customer Resolutions Team.*
OB Network SD	*Enterprise service delivery frontline service desk email Dropbox.* *Utilised for emails coming in from all Enterprise customer segments.* *It takes the emails received and then creates the service ticket.*
SMB Compliance	*Refers to a dropbox used to escalate matters to the Optus Small Medium Business Compliance Team.*

8. **Page 18 of Optus' submission states that the firewall upgrade started 24 hours earlier than originally planned. However, Appendix A states that the upgrade started 23 hours earlier than originally planned. Can you please confirm which number is correct?**

   Answer:
   23 hours as noted in the timeline appendix is incorrect; it should read 24 hours as reflected in the body of the submission.

9. **Does Optus' submission use the terms 'Optus Call Centre' and 'Optus Contact Centre' interchangeably? If these terms refer to different things, please explain the difference.**

   Answer:
   These terms are used interchangeably within the Optus submission.

10. **When was the final report of Dr Kerry Schott's Independent Review into the 18 September 2025 outage provided to Optus?**

    Answer:
    A copy of the final report was sent to the Optus Chairman on 12 December 2025.

11. **Were any draft versions of Dr Kerry Schott's report or draft findings provided to Optus? If so, how many drafts were provided and when?**

    Answer:
    A draft of Dr Schott's report was provided by her secretariat function on Wednesday 3 December for the purposes of factual review. Comments were provided by Optus on 8 December, with no further draft being provided for review and comment. On 12 December 2025, the secretariat function sent a copy of the final report to the Optus Chairman.

12. **Optus states in its submission that it was contacted by the SA Ambulance Service (SAAS) at 13:15, 13:17 and 13:25 AEST on 18 September 2025 regarding potential Triple Zero call issues:**

18/09/2025	13:15	Call from SA Ambulance to Optus Operational Architect - EB Delivery regarding possible Triple Zero issue.	SA Ambulance notifies Optus that there is a potential issue with emergency calls. Asks the Optus contact if there is an issue with Triple Zero of which the contact says they are not aware of any. SA Ambulance contact says they will confirm. Call duration 37 seconds.
18/09/2025	13:17	Call from SA Ambulance to Optus Operational Architect - EB Delivery confirming Triple Zero issue.	SA Ambulance confirms with Optus Operational Architect – EB Delivery that there are issues with emergency calls. Optus confirms they will escalate internally. Call duration 25 seconds.
18/09/2025	13:25	Call from SA Ambulance to Optus Operational Architect - EB Delivery asking for update.	SA Ambulance calls Optus requesting an update on the emergency call issue identified. Optus confirms the issue is being escalated. Call duration 15 seconds.

(Optus, *Submission 1*, Appendix A)

On the other hand, the SAAS's submission states that it attempted to contact Optus at 13:43 CST (14:13 AEST) on 18 September 2025, and does not mention any further communications with Optus that day:

- SAAS proceeded to attempt to contact an Optus representative via phone call to discuss the issue at 13:43 CST.

(SAAS, *Submission 27*, p. 2)

Could you clarify or provide any additional information on the nature of Optus' communications with the SAAS on 18 September 2025 concerning the Triple Zero call issues, including the timing of those contacts? Additionally, please specify the source or sources of the information relied upon by Optus.

Answer:
The three calls outlined in Optus' timeline relate to calls received from SA Ambulance Service (SAAS) to our EB Delivery team. This information was drawn from a review of call records.

The call at 13:43 CST (14:13 AEST) referred to in the SAAS submission was received by Optus' Director of Security and Public Safety. It was a very brief call (approximately 20 seconds) from a number that was unknown at the time. The issue was not discussed in detail and the caller agreed to a request to call back later.

At the time, as outlined in the Optus submission, a Major Incident had been declared (at 13:51 AEST) after the earlier calls from SAAS, and the Optus team was responding as a priority.

Appendix 1 – Question 4 - Handsets that did not connect to triple zero

Manufacturer	Device	Count of Unique Devices
3FeetSolutions Pty Ltd	BigButton M	1
3FeetSolutions Pty Ltd	Smart55R	1
Apple Inc	Apple iPhone 11 (A2221)	20
Apple Inc	Apple iPhone 11 Pro (A2215)	2
Apple Inc	Apple iPhone 11 Pro Max (A2218)	2
Apple Inc	Apple iPhone 12 (A2172)	1
Apple Inc	Apple iPhone 12 (A2403)	6
Apple Inc	Apple iPhone 12 mini (A2399)	2
Apple Inc	Apple iPhone 12 Pro (A2407)	6
Apple Inc	Apple iPhone 12 Pro Max (A2411)	9
Apple Inc	Apple iPhone 13 (A2633)	10
Apple Inc	Apple iPhone 13 Pro (A2638)	6
Apple Inc	Apple iPhone 13 Pro Max (A2643)	12
Apple Inc	Apple iPhone 14 (A2882)	13
Apple Inc	Apple iPhone 14 Plus (A2886)	2
Apple Inc	Apple iPhone 14 Pro (A2890)	4
Apple Inc	Apple iPhone 14 Pro Max (A2894)	11
Apple Inc	Apple iPhone 15 (A3090)	5
Apple Inc	Apple iPhone 15 Plus (A3094)	5
Apple Inc	Apple iPhone 15 Pro (A3102)	6
Apple Inc	Apple iPhone 15 Pro Max (A3106)	3
Apple Inc	Apple iPhone 16 (A3287)	6
Apple Inc	Apple iPhone 16 Plus (A3290)	2
Apple Inc	Apple iPhone 16 Pro (A3293)	6
Apple Inc	Apple iPhone 16 Pro Max (A3296)	14
Apple Inc	Apple iPhone 16e (A3409)	3
Apple Inc	Apple iPhone 6S (A1688)	1
Apple Inc	Apple iPhone 7 (A1778)	2
Apple Inc	Apple iPhone 7 Plus (A1784)	1
Apple Inc	Apple iPhone 8 (A1863)	2
Apple Inc	Apple iPhone 8 (A1906)	1
Apple Inc	Apple iPhone 8 Plus (A1864)	6
Apple Inc	Apple iPhone SE (A1723)	1
Apple Inc	Apple iPhone SE (A2296)	7
Apple Inc	Apple iPhone SE (A2783)	4
Apple Inc	Apple iPhone X (A1865)	4
Apple Inc	Apple iPhone XS (A2097)	3
Apple Inc	Apple iPhone XS MAX (A2101)	1
Google Inc	Pixel 6a	1
Google Inc	Pixel 7	2

Google Inc	Pixel 8a	1
Google Inc	Pixel 9	1
Google Inc	Pixel 9 Pro	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH1920 - AX5s	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2067 - A72	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2135 - A53s	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2185 - A15	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2195 - A54 5G	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2271 - A16s	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2273 - A54s	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2305 - Find X5 Pro	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2307 - Find X5	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2333 - A96	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2349 - A16k	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2577 - A58	4
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2579 - A38	2
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2591 - A18	3
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2631 - A60 4G	1
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2683 - A60 5G	4
Guangdong Oppo Mobile Telecommunications Corp Ltd	CPH2695 - A4 Pro 5G	2
Guangdong Oppo Mobile Telecommunications Corp Ltd	OPPO A17	1
HMD Global Oy	Nokia 2.2	1
HMD Global Oy	TA-1337 - Nokia 5.4	5
HMD Global Oy	TA-1362 - Nokia XR20	1
HMD Global Oy	TA-1452 - Nokia C2 2nd Edition	1
HMD Global Oy	TA-1486 - Nokia XR21	1
HMD Global Oy	TA-1549 - Nokia 110 4G	3
HUAWEI Technologies Co Ltd	HUAWEI P20 Pro	1

KVD International Group Limited	S41T	1
LG Electronics Inc.	LM-G900EM	1
LG Electronics Inc.	LM-X320ZMW	1
Mobiwire SAS	Optus X Lite 4	2
Motorola Mobility LLC, a Lenovo Company	Lamu24	2
Motorola Mobility LLC, a Lenovo Company	LamuLite24	2
Motorola Mobility LLC, a Lenovo Company	Macan24	1
Motorola Mobility LLC, a Lenovo Company	motorola edge 30 fusion	1
Motorola Mobility LLC, a Lenovo Company	motorola edge 50 fusion	1
NOTHING Technology Limited	A059P - Nothing Phone (3a) Pro	1
Samsung Korea	DM2 - Galaxy S23	1
Samsung Korea	Galaxy A04s	2
Samsung Korea	Galaxy A05s	4
Samsung Korea	Galaxy A12	6
Samsung Korea	Galaxy A13	5
Samsung Korea	Galaxy A14	1
Samsung Korea	Galaxy A14 5G	5
Samsung Korea	Galaxy A15 5g	14
Samsung Korea	Galaxy A16	2
Samsung Korea	Galaxy A16 5G	8
Samsung Korea	Galaxy A20	1
Samsung Korea	Galaxy A20s	1
Samsung Korea	Galaxy A21s	4
Samsung Korea	Galaxy A22	1
Samsung Korea	Galaxy A22 5G	1
Samsung Korea	Galaxy A23	3
Samsung Korea	Galaxy A25 5G	1
Samsung Korea	Galaxy A30	1
Samsung Korea	Galaxy A32	2
Samsung Korea	Galaxy A33 5G	2
Samsung Korea	Galaxy A34 5g	3
Samsung Korea	Galaxy A35 5G	1
Samsung Korea	Galaxy A50	2
Samsung Korea	Galaxy A51	2
Samsung Korea	Galaxy A52	1
Samsung Korea	Galaxy A52 5G	1
Samsung Korea	Galaxy A52s 5G	2
Samsung Korea	Galaxy A53 5g	1
Samsung Korea	Galaxy A54 5g	2
Samsung Korea	Galaxy A55 5g	6
Samsung Korea	Galaxy A56 5g	2

Samsung Korea	Galaxy A71	2
Samsung Korea	Galaxy A73 5G	1
Samsung Korea	Galaxy Note10+ 5G	1
Samsung Korea	Galaxy S10	2
Samsung Korea	Galaxy S20 5G	1
Samsung Korea	Galaxy S20 FE	1
Samsung Korea	Galaxy S20 FE 5G	1
Samsung Korea	Galaxy S20 FE LTE	4
Samsung Korea	Galaxy S20 Ultra 5G	2
Samsung Korea	Galaxy S20+ 5G	1
Samsung Korea	Galaxy S21 5G	5
Samsung Korea	Galaxy S21 FE 5G	2
Samsung Korea	Galaxy S21 Ultra 5G	1
Samsung Korea	Galaxy S21+ 5G	2
Samsung Korea	Galaxy S22	10
Samsung Korea	Galaxy S22 ULTRA	2
Samsung Korea	Galaxy S22+	2
Samsung Korea	Galaxy S23	2
Samsung Korea	Galaxy S23 FE	2
Samsung Korea	Galaxy S23 ULTRA	7
Samsung Korea	Galaxy S23+	3
Samsung Korea	Galaxy S24	3
Samsung Korea	Galaxy S24 ULTRA	9
Samsung Korea	Galaxy S24+	2
Samsung Korea	Galaxy S24FE	6
Samsung Korea	Galaxy S25	1
Samsung Korea	Galaxy S25 Edge	1
Samsung Korea	Galaxy S25 Ultra	10
Samsung Korea	Galaxy S25+	1
Samsung Korea	GALAXY S8 SM-G950F	1
Samsung Korea	Galaxy Z Fold5	2
Samsung Korea	SM-G960F GALAXY S9	1
TCL Communication Ltd	TCL 505	2
Umi Network Technology Co Limited	A9 Pro	1
Vivo Mobile Communication Co Ltd	iQOO 9 SE	1
Vivo Mobile Communication Co Ltd	iQOO Neo6	1
Vivo Mobile Communication Co Ltd	vivo T1	1
Vivo Mobile Communication Co Ltd	vivo V17 Pro	1
Vivo Mobile Communication Co Ltd	vivo V25 Pro	1
Vivo Mobile Communication Co Ltd	vivo Y12	2
Vivo Mobile Communication Co Ltd	vivo Y53s	1
Xiaomi Communications Co Ltd	Redmi Note 10S	1
ZTE Corporation	Blade A72s - Optus X-Max	1
ZTE Corporation	Optus X-Plus	1
ZTE Corporation	P503 - Optus X-Start 4	2

ZTE Corporation	P545 - Optus X-Power 2	1
ZTE Corporation	P601 - Optus X-Sight 3	6
ZTE Corporation	P656 - Optus X-Total	1
ZTE Corporation	P660 - Optus X-Tap3	1

Crisis Management Procedure

Document Control			
Document type: ☐ Policy ☐ Standard ✓ Procedure			
Version: 4.6	**Approval date:** N/A	**Effective date:** N/A	**Next review date:** N/A
Accountable Person (Owner): [redacted] / [redacted]			
Responsible Business Unit: Risk and Resilience / Corporate Affairs and Marketing			
Author: [redacted]			

Document Amendment List

Version	Date	Section	Nature of Amendment	Amendment Author
3.0	05 Jul 2022	All	Creation of Optus Crisis Plan	Optus - Group Risk Management
3.9	1 Sept 2022	General Review	Review and Update	Risk & Resilience
4.0	15 Feb 2023	All	Updated template and aligned with new crisis escalation process and criteria	Risk & Resilience
4.1	24 Aug 2023	All	Updated to reflect changes in BCPs and organisational structure	Risk & Resilience
4.2	15 Dec 2023	All	Updated to reflect changes in BCPs and organisational structure	Risk & Resilience
4.3	30 Oct 2024	2	Updated to reflect changes in organisational structure	Risk & Resilience
4.4	17 Feb 2025	2.1.1 and 2.1.2	Updated to reflect changes in organisational structure	Risk & Resilience
4.5	2 May 2025	2.1.1 and 2.1.2	Updated to reflect changes in organisational structure	Risk and Resilience
4.6	21 May 2025	2.1.1 and 2.1.2	Updated to reflect changes in organisational structure	Risk and Resilience

Contents

OPTUS

CRISIS MANAGEMENT PLAN SUMMARY

Crisis Definition

"Local, regional or global event that has the potential to cause personal harm or a major financial, operational, reputational, regulatory and/or legal impact on Singtel Group and its stakeholders"

Crisis Structure

Strategic	Crisis Mgmt Executive Committee (CMEC)
Operational	Crisis Management Team (CMT)
Tactical	BU Incident Mgmt Functions & Teams

Priorities & Objectives

- ✓ Maintain personnel safety
- ✓ Minimise customer impact
- ✓ Protect the environment
- ✓ Restore critical assets, processes & systems
- ✓ Protect our brand/reputation
- ✓ Meet regulatory requirements
- ✓ Minimise legal liability

Phase 1 Assessment & Activation

1. Identify & Assess

A crisis may be identified by:

- Business Unit incident management process
- Incident management team (e.g. Rapid Response Team)
- Referral by a CMT or CMEC member

Accountable BU Exec and **CMT Secretary** perform preliminary assessment and convene CMT for full assessment if required.

2. Declare & Notify

Only the Optus CEO (or authorised deputy) **can declare a crisis** on behalf of Optus

Optus CEO notifies GCEO.

Singtel MC, Optus Board and Singtel Board also notified

3. Activate & Convene

CMT and **CMEC** are activated and convene to assume control of the crisis. Supporting working groups established as required.

Phase 2 Crisis Response

The **CMT and CMEC regularly meet**, **make decisions** and **monitor the crisis**, including the effectiveness of any response activities implemented via BUs / incident teams

Manage Actions

The CMT iterates on the action plan, considering the need for: emergency protocols, containment activities, specialist advice, activation of disaster recovery and business continuity plans, minimising legal/regulatory risks and reprioritising and allocating resources

Manage Communications

Corporate Affairs lead both **internal and external** communication according to the crisis communications plan.

The CMEC appoints a **media spokesperson** for Optus.

Crisis updates including decisions, issues and actions are documented and communicated via regular situation reports (**SITREPs**)

Phase 3 Post Crisis Actions

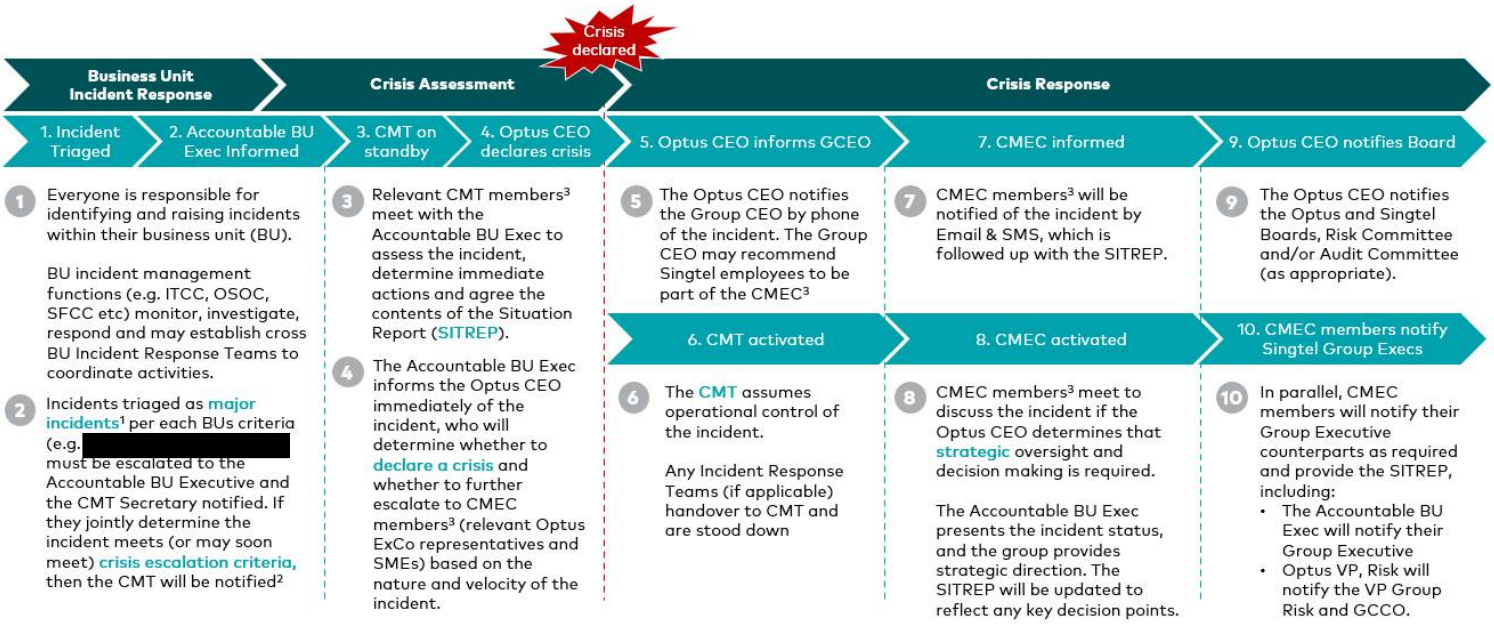
Stand Down CMT/CMEC

Once the situation is stable, there is low risk of recurrence and activity has slowed the business can return to BAU and the CMT, CMEC and supporting working groups can be stood down. A post incident review should be conducted to capture lessons learnt.

Plan Corrective Actions

Following the crisis, root causes should be thoroughly investigated with corrective actions planned and implemented to prevent future crises.

Crisis Notification and Escalation Process



[1] Major incidents will be notified retrospectively to Singtel in operational reports and via automated SMS or e-mail notifications where subscribed
[2] In addition to the criteria, any member of the CMT or CMEC may also refer an incident to the CMT Secretary for consideration to escalate as a potential crisis
[3] CMEC and CMT members are selected based on the required skills and authority for the crisis while maintaining a manageable size (ideally <12 members)

Crisis Criteria

Preservation of life is always the priority. Incidents where lives are at risk immediately trigger crisis management. Incidents involving the possibility of significant reputational harm or financial loss also trigger crisis management.

	FINANCIAL	BUSINESS INTERRUPTION	PUBLIC CONFIDENCE & REPUTATION	REGULATORY AND LEGAL	PEOPLE
Actual or Potential Impact[1]	• Cash loss [redacted]	• Loss of key services resulting in severe impact to customers • Full-service disruption to one or more enterprise customers or government agencies	• Widespread negative national, international or viral social media coverage • High number of internal or external customer or stakeholder complaints	• Allegation or violation of law or regulation subject to remediation costs or fines [redacted] or prison	• Fatality • Multiple serious injuries • Widespread illness
Optus Guidance (Example Events)[2]	• Significant internal or external fraud event, including theft • Property or assets lost, damaged or threatened • Revenue loss due to billing/ processing errors	• Extended ([redacted] network outage that impacts [redacted] of the customer base for a product offering, affects a high-profile location or affects a VIP enterprise or government customer • Extended mission critical IT system outage (i.e. unable to recover within time objective) • Extended ([redacted]) inability for the majority of customers to reach Optus to get connected or maintain their service[3] • Unavailability of a key facility for [redacted] (e.g. due to flood, fire, gas leak, industrial action etc.) • Cyber-attack (e.g. denial of service, ransomware) impacting availability of customer facing services	• High volume ([redacted]) of negative social media posts • Leak or unauthorised disclosure of large volumes of sensitive or personal data • Credible extortion or ransom request • Publicly visible cyber security incident (e.g. defacement of public web sites) • Incident likely to require a reactive national press release and/or market disclosure • Independent external enquiry likely to receive national interest	• Serious breach of critical telco or corporate regulatory requirements • Publicly disclosable investigation, enquiry or unfavourable regulatory action • Allegation, conviction or arrest of a member of the Board, Executive or Senior Management for illegal or fraudulent conduct	• Workspace safety incident affecting staff, contractors, customers or the public • Credible terrorist or bomb threat • Infectious disease and/or pandemic outbreak at orange alert level (WHO phase 5) • Hazardous levels of air quality (AQI >300)

[1] An incident or event need only satisfy one threshold to trigger escalation. For example, a minor network outage with widespread national media coverage shall qualify for escalation.
[2] In addition to the criteria, any member of the CMT or CMEC may also refer an incident to the CMT Secretary for consideration to escalate as a potential crisis
[3] Refers to the majority of the customer base for a given service offering and includes consideration of the timing of the interruption (i.e. if it is during business hours or a peak period)

1. Introduction

This document assists Optus to manage any crisis event that has the potential to impact the organisation's people as well as its operational and strategic objectives. This includes guidance on the:

- Initial assessment of incident severity
- Activation of crisis management teams
- Assessment of business impacts
- Implementation of crisis management strategies

1.1 Document Scope

The document is to be utilised by Optus management to coordinate the implementation of crisis management response and recovery strategies across the organisation including all departments, business units, data centres, exchanges and other sites. It sets out responsibilities and provides guidance for matters to be considered in a crisis.

This plan does not address Singtel group level crises. For the group level crisis procedures refer to the Singtel Crisis Management Plan.

1.2 Objectives

The objective of the Optus Crisis Management Procedure ('CMP') is to mitigate the effects of a crisis, minimise disruption to operations and recover operations by ensuring the right structures, roles and responsibilities are in place to manage a crisis.

1.3 Priorities

In the event of a crisis, the overall priorities are as follows:

- Ensuring the safety of personnel
- Minimising environmental damage
- Protecting and restoring critical business assets, processes and systems
- Minimising escalation of business interruption
- Maintaining control over potential impacts to the reputation of Singtel Group / Optus
- Fulfilling regulatory escalation requirements
- Maintaining media relations and internal/external communications
- Ensuring customer relations are maintained

1.4 Definitions

Refer to **Annex A**.

1.5 References

This document takes reference from Singtel Group Risk Management Framework, Singtel Group Business Continuity Management Policy and the Singtel Group Crisis Management Plan.

This document must be read in conjunction with all other relevant Singtel Group policies, procedures and guidelines, Optus Business Continuity Plans (BCP) and Incident Response Procedures (IRPs) such as bomb threat, fire evacuation procedures, cyberattacks, etc.

1.6 Incident Response, Crisis Management and Business Continuity

The Singtel Group Business Continuity Management (BCM) framework encompasses three inter-related responses to disruptions: Incident Response, Crisis Management and Business Continuity.

An incident is an occurrence by or due to a combination of unforeseen circumstances which, if not handled appropriately, can escalate into a major incident or crisis. Incident Response aims to provide a structure to manage, support response capability and coordinate activities, facilities and resources to deal with an incident.

A crisis is a critical event that may impact the Group's profitability, reputation, or ability to operate. Crisis Management is the overall coordination of the response to a crisis, in an effective, timely manner, to contain or minimise impact to the organisation's assets, personnel, operation and reputation.

Business continuity encompasses planning and preparation to ensure that Optus can swiftly recover to an operational state after an incident or crisis, meeting the business' predetermined recovery time objectives. It seeks to minimise the impact of business interruption through clear plans to aid and expedite the recovery and resumption of critical business functions.

Optus has a systematic approach for crisis management. Where possible, incidents will be handled within normal departmental procedures. However, any unexpected event or major incident will be assessed against the criteria for a crisis and may lead to the declaration of crisis if / when the crisis declaration criteria are met. Such declarations are made when the situation is or, is likely to become, a company-wide event requiring the coordination and authority of the Crisis Management Team (CMT) and, in some cases, the Crisis Management Executive Committee (CMEC).

When a crisis is declared, the CMT and the CMEC (if required) assembles at a designated Crisis Management Centre (CMC) or virtually as necessary, which is the central point of control for the company wide response.

The stages of an incident across incident response, crisis management and business continuity are represented below.

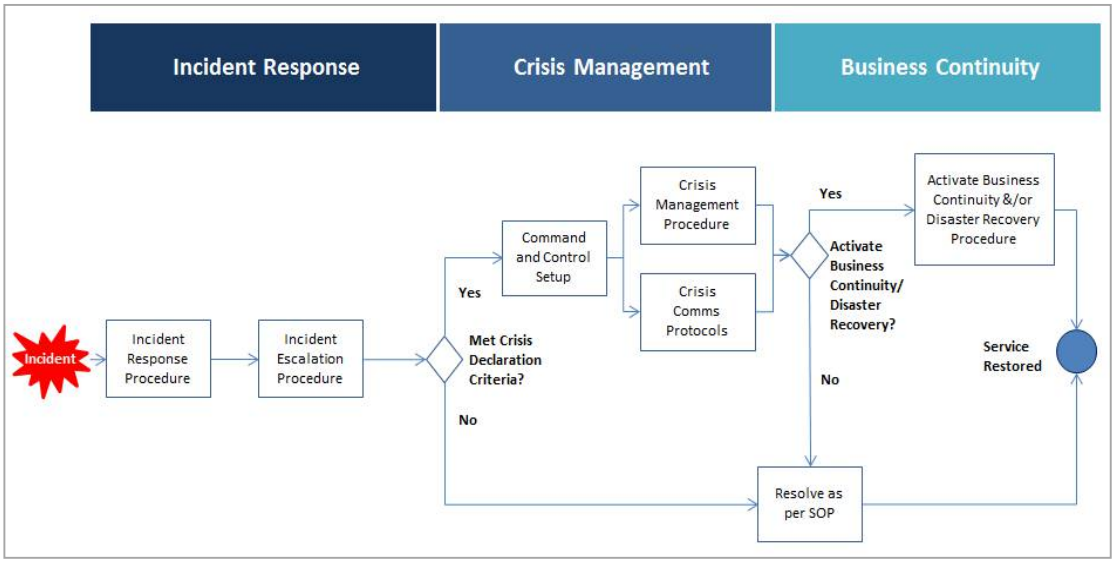


Fig 1. Incident Response, Crisis Management and Business Continuity

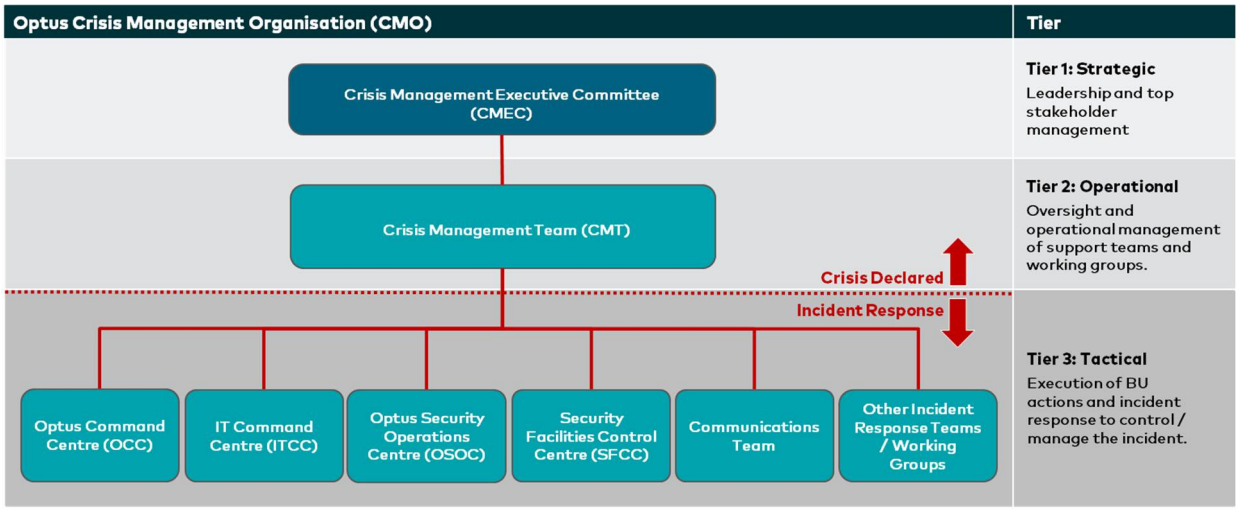
2. Crisis Management Framework

2.1 Crisis Management Organisation

The Optus Crisis Management Organisation (CMO) has a three-tiered structure in place. This includes:

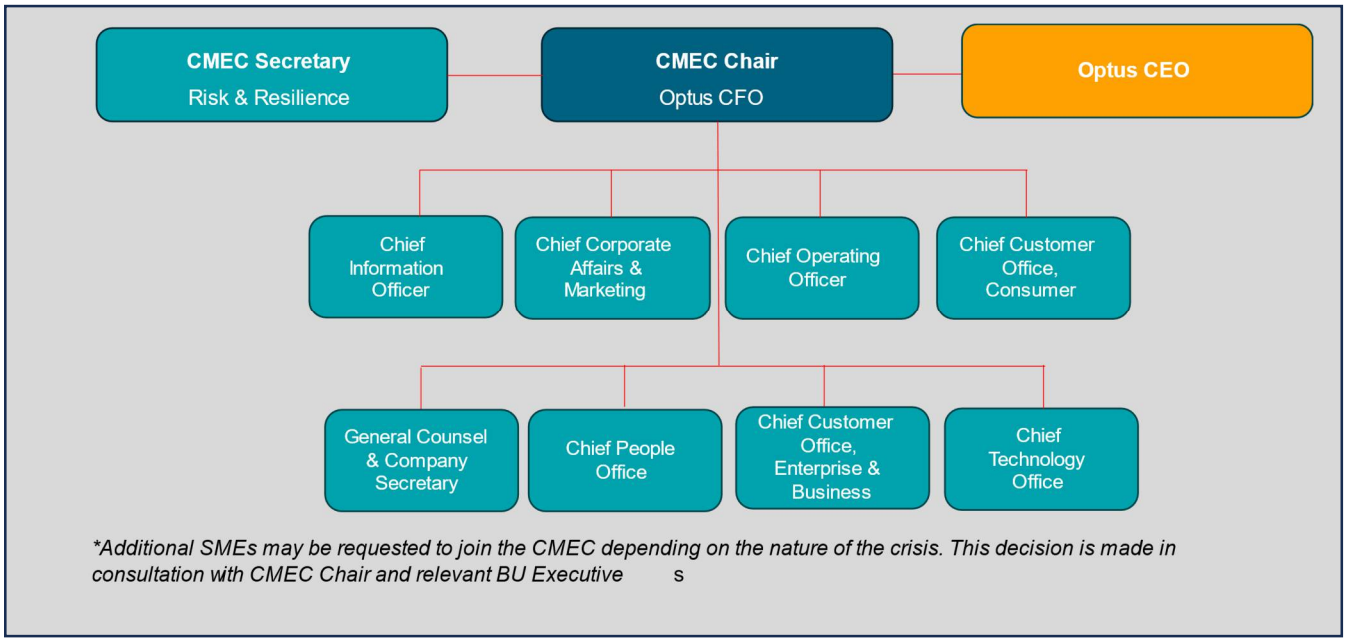
- Crisis Management Executive Committee (CMEC)
- Crisis Management Team (CMT); and
- Incident Response Teams / Working Groups (e.g. Optus Command Centre, IT Command Centre etc).

This tiering structure provides separation of roles and delineation between strategic, operational and tactical responses. It also enables Optus to manage resource allocation to address a crisis.



2.1.1 Crisis Management Executive Committee (CMEC)

The CMEC's role is to focus on strategic leadership and stakeholder management during a crisis.



CMEC's key responsibilities:

- Set crisis management objectives and priorities and provide direction on changes or updates to response and recovery efforts.
- Provide strategic oversight and guidance to the CMT.
- Provide updates to Singtel Executives (MC) and the Singtel Board where required.
- Appoint the media spokesperson for the company and approve the communications strategy to external agencies, media and shareholders.
- Maintain communication and liaison at an executive level with Government and Ministries, Regulatory Authorities, Customers, Employees, Shareholders, Suppliers, Vendors and Partners, General Public
- Ensure the safety and wellbeing of employees, customers, and other impacted stakeholders.
- Monitor the crisis as the situation evolves including by reviewing SITREPs from the CMT and assessing ongoing impacts e.g. financial, legal, operational, reputational, and human.

In addition to the above, key points to note:

- The designated CMEC Chair is the Optus CEO. In the event that the Optus CEO is unavailable, they have the authority to nominate an alternative individual to act as the CMEC chair during their absence.
- The CMEC Chair may assign a deputy chair, determine membership of the team based on type of incident and co-opt other subject matter experts (SME) into the CMEC.
- Not all members within the CMEC need to be involved in managing a crisis. This will depend on the crisis situation and will be determined by the CMEC Chair.

Refer to the separate CMEC Call Tree for full details of the CMEC members, including contact information and delegates.

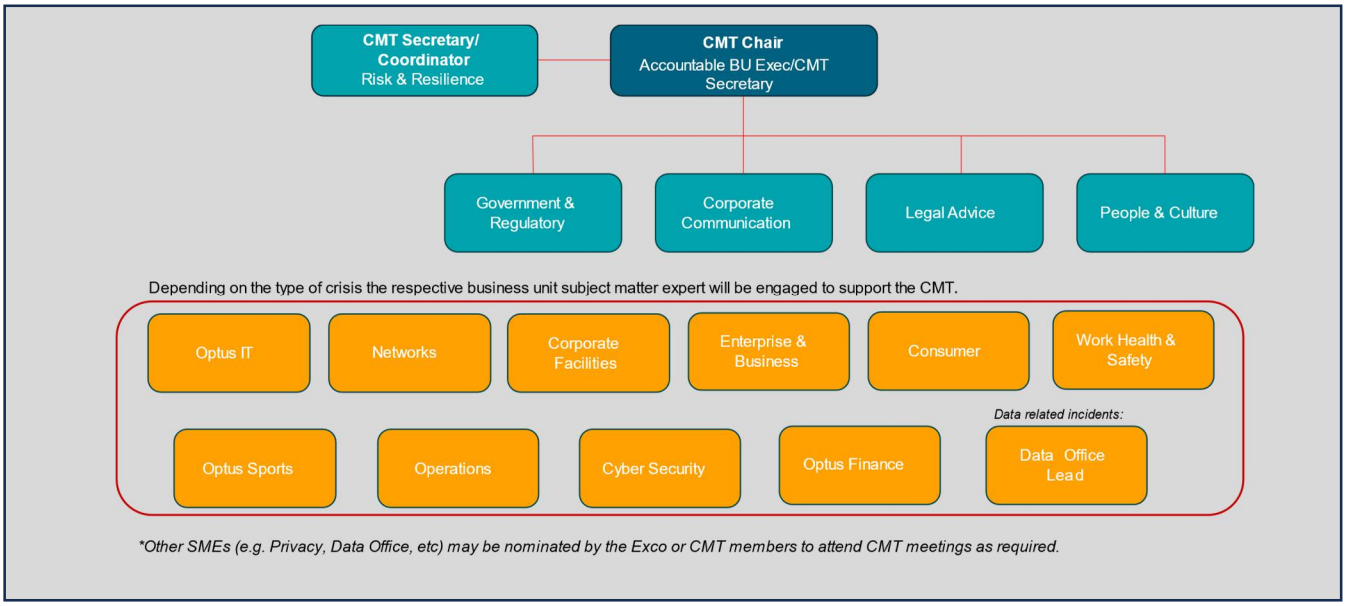
Responsibilities by CMEC Member

Role	Responsibilities
CMEC Chair / Co-Chairs	• Convene the CMEC. • Provide leadership to the CMEC throughout a crisis event. • Act as a key liaison between the CMEC and Singtel Group Executives. • Provide regular updates to Singtel MC and Singtel Board • Provide guidance and advice to CMT and other working groups on the strategic direction and priorities to be undertaken
People & Culture representative	• Confirm the safety and wellbeing of employees, customers and other impacted stakeholders. • Provide leadership and manage employee and people related issues. • Establish communications and on-going protocols with department representatives to obtain regular updates on people impacted by the event.
Comms & Regulatory representative	• Brief the CMEC Chair on reputational issues, whilst also managing all crisis-related internal and external communications. • Prepare and present a communications strategy for approval by the CMEC. • Advise the team on reputational impacts and messaging issues. • Coordinate the endorsement / approval of all key messages.
BU Executives and Subject Matter Experts	• Lead, guide and provide direction on issues impacting Optus within their area of responsibility. Other specialist personnel may be called upon as required depending on the nature of the incident.

Role	Responsibilities
	• Lead response and recovery activities for their BU area of responsibility, including overseeing activation of BU BCPs if critical business functions have been impacted.
CMEC Secretary	• Provide admin and logistical support to the CMEC Chair and other team members to enable effective team meetings, including activation of the Command Room, logistical support and provision of advice to team members. • Establish liaison with CMT to receive updates, including SITREPs, at designated intervals • Ensure all information, actions and decisions are recorded and visible. • Assist the CMEC to establish reporting schedules and requirements (i.e. update frequency, summary of impacts, changes to damage assessments, etc).

2.1.2 Crisis Management Team (CMT)

The CMT provides a central coordinating and operational management role during a crisis.



The purpose of the CMT is to provide operation control during a crisis in consultation with the Crisis Management Executive Committee (CMEC). The CMT can operate in conjunction with or independently of the CMEC.

CMT's key responsibilities:

- Manage organisation-wide response to a Crisis:
  - Evaluating the full extent and impact of a crisis
  - Co-ordinating immediate actions to stabilise the situation and prevent further escalation of the crisis
  - Determining priorities of restoration and recovery
  - Coordinating restoration and recovery
- Manage resources, including material, equipment, staff and funds
- Provide regular status update to CMEC
- Support CMEC communication and liaison with the relevant stakeholders
- Identify, assess and prioritise any issues resulting from the crisis.

- Verify that appropriate actions have been taken.
- Determine if BCP needs to be invoked and advise from impacted teams.
- Ensure consistent communications with all key internal and external stakeholders as required.

In addition to the above, key points to note:

- CMT Chair may be a CMEC member nominated by the CMEC Chair depending on the nature of the incident.
- CMT can operate in conjunction with or independently of the CMEC.
- Not all subject matter experts (SMEs) within the CMT need to be activated. This will be determined by the CMT Chair depending on the nature of the incident.
- SMEs may be required to lead support teams and/or working groups to enable completion of actions within their areas of responsibility.

Refer to the separate CMT Call Tree for full details of the CMT members, including contact information and delegates.

Responsibilities by CMT Member

Role	Responsibilities

CMT Chair (Accountable BU Executive)	• Provide leadership to the CMT throughout a crisis event.
	• Confirm membership of the team including roles and responsibilities of each member.
	• Receive brief from the Incident Manager of the escalating team/s.
	• Key liaison between the CMT and CMEC, including:
	  ○ Informing CMEC Chair when a CMEC may need to be invoked
	  ○ Establishing processes with the CMEC to approve crisis response and recovery actions, including the communications strategy
	  ○ Providing SITREPs and regular briefings to the CMEC
	• Establish reporting mechanisms to update the CMEC and all other relevant stakeholders of progress with crisis response strategies.
	• Implement management controls to minimise ongoing financial impacts associated with recovery efforts.
	• Agree protocols for on-going CMT meetings including welfare requirements for CMT members.

People & Culture representative	• Confirm the safety and wellbeing of employees and other impacted stakeholders. • Provide advice and manage employee and people related issues. • Establish internal protocols with department representatives to obtain regular updates on people impacted by the event.
Comms & Regulatory representative	• Brief the CMT on reputational issues and impacts. • Prepare and present a communications strategy for CMT approval. • Coordinate the endorsement / approval of all key messages. • Manage all crisis-related internal and external communications, including with the public, media, regulators, and others. • Monitor and manage Optus' reputation and public image.
Legal representative	• Provide advice to the CMT on any legal and regulatory compliance obligations and impacts, including the potential for breaches and mandatory notifications. • Refer matters for external legal counsel where advice is required. • Review any external communications prior to distribution.

Department representatives and Subject Matter Experts	• Contribute to CMT discussions on impacts, actions, next steps and resourcing relevant to their area of expertise.
	• Lead investigation, response and recovery activities for their business area including by:
	  o Allocating resources to the crisis response
	  o Directing the activities of any incident management functions within their business unit
	  o Establishing working groups and other communication channels to coordinate activities outside of the CMT
	  o Collecting and analysing supporting information
	• Notify department BCP reps to activate their BCPs if critical business functions need recovering.
	• Review and provide input to the consolidated SITREP.

CMT Secretary	• Provide administrative and logistical support to the CMT to enable effective team meetings, including:
	  o Activation of the Crisis Management Centre
	  o Logistical support, including notifying CMT members of scheduled meetings, maintaining CMT roster etc.
	  o Providing advice.
	• Ensure all information, actions and decisions are recorded and visible, including by:
	  o Compiling the consolidated SITREP based on updates from CMT members
	  o Circulating the SITREP to CMT and CMEC members
	  o Updating Action and Decision registers to provide team members with a rolling record
	• Identify requirements for specialist support to assist the CMT with Key decisions
	• Oversee CMT meeting protocols to ensure that a productive environment is maintained.

2.1.3 Business Unit Incident Management Functions

Business Unit Incident Management Functions, including those listed in the table below, are usually involved when there is a major incident as part of a business unit's incident escalation process. They may be relied upon to provide tactical support to the CMT before and during a crisis by:

- Executing CMEC/CMT strategies and implementing actions within departments or focus areas to minimise impacts, prevent escalation and facilitate restoration of products and services
- Providing information to the CMT to support impact assessments and decision-making.

Function	Responsibilities
Optus Command Centre (OCC) - Nokia GDC - Optus Retained Network Management - Broadcast Operations Centre (BOC) - Satellite Operations	• Escalation of any NETWORK INCIDENT, which adversely affects Network Operations or Customer Service. • Liaise with the CMT to coordinate Network restoration and recovery. • Recommend to stand-up an Incident Management Team or CMT for incidents requiring escalation. Includes events which causes or could result in a loss or major outage of a critical facility, e.g. exchanges, data centre, satellite earth station or business critical applications.

Function	Responsibilities
Optus Security Operations Centre (OSOC)	• Escalation of any CYBER INCIDENT including suspected intrusion or compromise of IT systems or networks • Initial assessment team in the early stages of an incident. • Provide cross-functional expertise to manage early-stage incidents before they escalate to crisis level • Provide threat intelligence and conduct investigations to determine extent and source of intrusions • Recommend to stand-up the Rapid Response Team (RRT) or CMT for incidents requiring escalation
IT Command Centre (ITCC)	• Escalation of any major IT INCIDENT, which impacts the availability or performance of IT systems. • Liaise with the CMT to coordinate IT restoration and recovery • Monitor IT system availability and performance to proactively identified incidents and outages • Triage and respond to IT incidents notified to the IT helpdesk
Security Facilities Control Centre (SFCC)	• Escalation of any life-threatening EMERGENCY or physical security incident, e.g. fire/bomb threat, terrorist threat • Advice to the Site Emergency Contact and Chief Warden.

Note: Other support teams and working groups (e.g. Communications team, WHS support, social media management etc) may also be established during an incident, which should report back to the CMT via an appropriate BU CMT member.

2.1.4 BU Incident Management Teams

In order to support incidents that require cross-functional support and/or a whole of company response, incident management teams may be established to co-ordinate activities. These groups are facilitated by business units as part of their incident management processes. For example, Networks will establish their own BU Incident Management team to co-ordinate the Optus wide response to major network incidents (SL1).

The responsibilities of IMTs are to:

- Assesses impact of the incident and whether escalation to a crisis is required
- Assess and manage internal and external impacts to ensure we are responding effectively to an incident.

IMT Transitioning Protocol in Crisis Scenarios

If an incident managed by the IMT escalates to a crisis and involves cross-functional team members from multiple business units, the IMT will stand down and operational control will be transferred to the CMT, which will manage the organisation-wide response. However, if the IMT is composed solely of individuals responsible for the technical response within a specific business unit, the team will continue operating, providing updates to their BU CMT representative and following directions from the CMT.

2.2 Crisis Management Process

There are three phases to identifying whether an incident needs to be escalated and declared as a crisis and managed through to recovery and closure. These are summarised in the table below and explained in more detail in the following section.

Phase	Phase Name	Description
Phase 1	Assessment and Activation	• Identifying a potential crisis • Assessing the potential crisis • Declaring a crisis • Activating the CMEC and CMT • Singtel Notification
Phase 2	Managing the Crisis Response	• CMEC meetings • CMT meetings • Recovery action plan • Crisis communications • Crisis monitoring
Phase 3	Managing Post-Crisis Actions	• Planning corrective actions • Standing-down the Crisis Management Organisation

The crisis management process is activated for events that meet defined crisis escalation criteria. **Refer to Annex C – Crisis Escalation Criteria**.

3. Phase 1: Assessment and Activation

This section outlines the activities to escalate an incident for consideration and declaration as a crisis, and to activate the crisis response. Escalation of an incident includes an assessment of whether it has the potential to cause significant impacts to Optus and its stakeholders. This section also outlines how the crisis management organisation is activated to provide leadership during the crisis.

3.1 Identifying a potential crisis

A crisis is a local, regional or global event that has the potential to cause personal harm or has a major financial, operational, reputational, regulatory and/or legal impact on Singtel Group and its stakeholders. It requires a distinct strategic, operational and tactical response that must take priority over normal business activity.

There are several ways a crisis may be identified for escalation. Refer to Annex B for a list of contact points to which major incidents and potential crises should be reported.

3.1.1 Identification within a Business Unit

The escalation of incidents at Optus occurs through established processes, policies and procedures within business units. Where possible, incidents are to be managed at the business unit level according to these policies and procedures to prevent the situation from escalating. Business units may have a dedicated Incident Management Function to co-ordinate these activities.

Whenever a BU has escalated an incident to a major incident status, **the Accountable BU Executive and CMT Secretary must be notified** so they can jointly assess whether to escalate the incident as a potential crisis.

Major incidents include:

- Network Incidents rated [redacted]
- IT Incidents rated [redacted]
- Cyber Security incidents rated [redacted]
- Any other incident with a moderate or greater impact as per the Risk Impact Rating Scale

3.1.2 Activation of Business Continuity Plans

The BCM Representative should notify the Accountable BU Executive and CMT Secretary if a BU plans to activate its Business Continuity Plan, so an assessment can be made on whether to escalate as a crisis. **Whenever more than one BU activates their Business Continuity Plan, this would ordinarily trigger escalation as a crisis to manage a coordinated response** across BUs.

3.1.3 Identification by Incident Management Teams

When an IMT is established to respond to an incident, it is critical that the team assesses the incident's actual and potential impacts to determine whether it qualifies as a potential crisis. This assessment should be done both initially and as an ongoing activity. It should also consider whether the incident requires strategic decision making or access to resources that are beyond the control of IMT participants.

If the IMT determines an incident may be a potential crisis, the Accountable BU Executive and CMT Secretary must be immediately notified to assess whether the incident meets the criteria to be escalated as a potential crisis.

3.1.4 Referral by CMT/CMEC Member

Any CMT or CMEC member may, at any time, refer an incident to the CMT Secretary for escalation as a crisis, in which case the CMT Secretary will convene the CMT.

3.2 Standby

Where events are developing and there is a threat of them escalating to a crisis, the CMT should be given advance notice to place them on standby. This is relevant in cases such as:

- Threat intelligence, such as weather forecasts, indicate the potential for a crisis or disaster to occur.
- A major incident, such as an IT outage, is likely to breach SLA's and escalate to a crisis.
- There are unverified reports about a potential crisis event.

Standby notice should be provided via SMS notification to relevant CMT members advising of the developing situation. Refer to the example below:

Example standby notification

Optus CMT Standby: <description event>. Further information to follow. Please be ready to join the CMT at short notice if required.

If an event is resolved before the CMT is activated, a follow up notification should be provided to inform them to stand down.

3.3 Assessing the potential crisis

When a potential crisis has been identified, there are two assessment steps that occur to enable the declaration of a crisis and activation of the crisis response activities.

3.3.1 Step 1 - Preliminary assessment

In the first instance, the Accountable BU Executive and the CMT Secretary are notified of a potential crisis and will make a joint assessment of whether to proceed with escalating the event and convening the CMT to conduct a full assessment. This assessment is made using the criteria outlined in Annex C – Crisis Escalation Criteria.

The Accountable BU Executive and CMT Secretary may be notified of a potential crisis via automated incident communications (e.g. SMS/e-mail) or by direct contact (e.g. call, instant message etc).

If the potential crisis is to be escalated, all relevant CMT members will be notified via SMS.

Example escalation notification

Optus CMT Escalation: The crisis process has been triggered to assess a potential crisis. <Describe event>. Please join the meeting at <time> at OCS <location> or online <conference details>.

3.3.2 Step 2 - CMT assessment

Following the preliminary assessment, the CMT Secretary will convene the relevant CMT members to perform a full assessment of the incident and compile the initial Situation Report (SITREP). This initial meeting may take place either virtually or at the Crisis Management Centre depending on the nature and context of the crisis.

Refer to Annex D for an initial CMT meeting agenda template.

3.4 Declaring a crisis

Following the preliminary and CMT assessment of the crisis, it is the responsibility of the Accountable BU Executive to inform the Optus CEO who will determine whether to declare a crisis. In deciding whether to declare a crisis, the CEO may refer to the SITREP prepared by the CMT.

Note: Only the Optus CEO or, in the event they are absent or unreachable, an authorised deputy, can declare a crisis on behalf of Optus.

The Optus CEO must inform the Group CEO of the declaration of a crisis as soon as possible after it is made. When the Group CEO is informed of the declaration of a crisis, the Group CEO may recommend Singtel employees to be part of the Optus CMEC.

If the Optus CEO determines that the crisis has Singtel group wide impacts and requires a co-ordinated Singtel group wide response, then it will be immediately escalated to the Group CEO for crisis declaration and activation of group wide crisis response protocols.

Factors that may be considered by the Optus CEO when declaring a crisis include:

- The extent to which the safety and wellbeing of people are at risk.
- The possibility of significant reputational, financial or operational impacts to Optus and its stakeholders that threaten the ongoing viability of the organisation.
- The magnitude of resources and funding required for investigation and response activities.
- The need for urgency, strategic decision making and an organisation-wide approach in responding to the event.

In declaring a crisis, the Optus CEO will also determine whether the CMEC should be convened as part of the crisis response. Typically, this will be required when:

- There is a need for strategic Executive level decision making, including decisions about resource allocation and prioritisation across multiple business units.
- The Executive team need to be intimately across the crisis in order to provide updates and manage the expectations of Singtel group counterparts and external stakeholders such as customers, regulators, authorities etc.
- There is a high likelihood for external media attention requiring aligned messaging and a media spokesperson to be appointed from amongst CMEC members.

Regardless of whether the CMEC is to be convened, relevant CMEC members will be immediately notified of the crisis by phone and provided a copy of the SITREP by email.

3.5 Activating the CMEC and CMT

If the Optus CEO determined that the CMEC is required following declaration of a crisis, then it will be activated and assume strategic control of the crisis. In parallel, the CMT will assume operational control of the crisis and any Incident Management Teams shall be stood down.

3.5.1 Activating the CMEC

The CMEC Secretary will convene the relevant CMEC members. Key outcomes of the initial CMEC meeting include:

- Shared understanding of the situation, facilitated by the Accountable BU Executive
- Potential impacts, risks and challenges associated with the crisis are understood
- Strategic response strategy is determined, incorporating communication strategies
- Roles and responsibilities are assigned, and CMEC membership agreed. This may require some members to be dismissed and additional subject matter experts assigned
- Logistics including crisis communication and collaboration protocols are agreed. This includes the responsibilities for which CMEC members will inform which Singtel Management Committee members.
- The SITREP is updated to reflect any outcomes and decisions of the CMEC.

Refer to Annex E for an initial CMEC meeting agenda template.

3.5.2 Activating the CMT

Although the CMT was already convened to perform an initial assessment of the crisis, it will be formally activated following the declaration of a crisis.

As part of activation, any IMT currently in place will hand over operational control of the incident to the CMT and be stood down. It is important that all IMT responsibilities and activities are handed over to the CMT.

The steps to be followed to perform handover from IMT to CMT are as follows:

- The IMT Chair will be invited to the CMT to present on the incident impacts, actions taken, current status and planned or recommended next steps
- The CMT Secretary will summarise in the SITREP, including any further actions required and ownership for those actions.
- The IMT Chair will share a list of the IMT members so their CMT counterpart can reach out to receive a more detailed handover including information such as stakeholder contact points, artefacts etc.
- For IMT members with no CMT counterpart, the CMT Chair and/or Secretary will determine whether to include them as a member of the CMT.

3.6 Singtel Notification

3.6.1 Group CEO Notification

The Optus CEO (or authorised deputy) is responsible for notifying the Singtel Group CEO as soon as practical following the declaration of a crisis. Depending on the context of the crisis, the Optus CEO may use their discretion to first convene the CMEC to ensure the relevant Optus Executives have properly assessed the crisis and agreed on the immediate crisis action plan before notifying the Group CEO. The Group CEO should be notified using a direct communication method (e.g. phone call) and provided a copy of the SITREP for full context of the crisis.

3.6.2 Singtel Management Committee Notification

CMEC members will inform relevant Singtel Management Committee members as agreed in the initial CMEC meeting. This will typically follow functional alignment. For example, in most cases the Optus CIO would inform the Group CIO, the Optus CFO would inform the Group CFO etc. Notifications should be made using a direct communication method (e.g. phone call) with a copy of the SITREP provided for full context of the crisis.

3.6.3 SOPL and Singtel Group Board Notification

The Optus CEO (or authorised deputy) is responsible for notifying the Singtel Group Board of Directors once the Group CEO and relevant Management Committee members have been informed. This would typically be via e-mail with the SITREP attached and depending on the nature of the crisis may also be followed up by phone call.

The Optus CEO is also responsible for informing any other Singtel Optus Pty Ltd Board members who are not part of the Singtel Management Committee or Board.

4. Phase 2: Managing the Crisis Response

This section provides guidance to CMEC and CMT teams during the response and recovery stages of the crisis. During this phase, the recovery action plan is developed and implemented to address the crisis and minimise its impact. In parallel, the crisis communication plan is enacted to ensure both internal and external stakeholders are informed.

4.1 CMEC Meetings

The purpose of the CMEC during the crisis response is to provide strategic leadership and stakeholder management. The CMEC will met on a regular cadence to receive information relayed from the CMT and make key strategic decisions as required.

Refer to Annex G for a suggested CMEC agenda.

4.2 CMT Meetings

Regular crisis management meetings must be organised and used as an opportunity to share situational information, confirm incident objectives, discuss response and recovery strategies and provide updates to the team.

Important notes for facilitating the regular CMT meetings:

- Use team timeouts, typically 20-30 minutes to directly engage stakeholders by telephone or meetings. Timeouts become longer when implementing crisis strategies.
- Use disciplined team updates, less than 5 minutes in duration to refocus the CMT when returning from a timeout outside the CMC.
- Once the team has assembled in person or via video / tele-conference, the CMT Chair should conduct the first meeting.
- Information should be collected as facts, assumptions or issues and recorded digitally or on visible boards within the CMC. All tasks should be recorded and delegated to an individual with a due time and date.

Refer to Annex F for a suggested CMT agenda.

4.3 Recovery Action Plan

In responding to the crisis, the CMT should develop a recovery action plan to document the actions to be taken, by whom and by when in order to minimise the impact of the crisis and recover to normal business operations.

The development of the plan is an iterative activity that is revisited at each CMT meeting. The CMT monitors the implementation of the plan and new actions are defined in a continual Plan-Do-Check-Act cycle.

In defining actions as part of the recovery action plan, the following should be considered:

- Emergency protocols that need to be activated, such as evacuating sites, distributing emergency notifications or contacting emergency services.
- Other containment actions that need to be taken to prevent the crisis from spreading, for example isolating or shutting down facilities or systems, suspending services, quarantining affected individuals etc.
- Investigative actions that need to be taken to gather information about what has (or is) taking place, including any steps to preserve evidence that might be required.
- External specialist advice or assistance that might be required to assist in managing the crisis, for example external legal counsel or forensic investigators.
- Upcoming business activities that need to be cancelled or deprioritised in response to the crisis, such as product launches, IT or network changes, marketing campaigns etc.
- IT Disaster Recovery Plans that need to be invoked to restore IT systems.

- Business Continuity Plans, including contingency strategies or manual workarounds, that need to be invoked to ensure critical operations and services can be maintained.
- Steps to develop and agree the communication plan.
- Legal and regulatory risks and requirements, including any government agencies and/or regulators that may need to be engaged.
- Financial, human and third-party resources required to implement recovery and corrective actions, and the steps necessary to secure these resources. That may include, for example, understanding the level of insurance cover available, possible compensation payments that may be required etc.

Refer to Annex H.

4.4 Crisis Communications

Corporate Affairs are responsible for maintaining a Crisis Communication Plan that provides a framework for developing, approving and distributing communications during a crisis. That includes both internal and external communication.

Refer to the Optus Crisis Communication Plan for details.

4.5 Crisis Monitoring

During and after implementation of the recovery action plan it is important that the CMT and CMEC continue to monitor the crisis. This includes:

- Monitoring the impacts of the crisis to determine whether the action plan is working effectively to contain the crisis.
- Identifying changes in the situation that might influence the need for a new or different action plan, for example availability of resources, number of people or assets affected, outcomes from investigation activities etc.
- Monitoring feedback or commentary from stakeholders both internally and externally, including media reports, social media activity and customer verbatims as appropriate.

As part of monitoring the crisis response, the SITREP and recovery action plan should be updated accordingly.

5. Phase 3: Managing Post Crisis Actions

This section will provide guidance to the CMEC/CMT in the post-crisis phase including implementing corrective actions to prevent future crises, returning to a Business-as-Usual state and conducting post-incident reviews. This phase will typically commence after the situation has been stabilised, impacts are being managed and minimal potential exists for further escalation.

5.1 Planning Corrective Actions

In responding to a crisis, it is important to identify corrective actions to address the root cause of why the crisis occurred in the first place to prevent it from happening again. Aside from being the right thing to do, it is also essential that these corrective actions are taken in order to protect Optus from legal and regulatory risks and restore public trust and confidence.

Before standing down the Crisis Management Organisation, it is important that corrective actions are identified by the CMT, and agreement is reached on how they will be governed and delivered outside of the crisis structure:

- It may be possible to implement some corrective actions as part of the crisis response.
- Most corrective actions will likely take time to implement will need to be transitioned to either a crisis recovery project or BAU to be implemented sustainably.
- Corrective actions should usually be captured as part of the Issue Management process.
- Owners should be identified for each corrective action, and a handover to these owners should take place prior to crisis closure.

Examples of corrective actions could include:

- New or updated policies, standards, procedures or plans.
- New or upgraded systems, facilities, equipment or other infrastructure.
- Implementation or remediation of controls.
- Audits or investigations to determine exposure in other areas of the business.
- Rolling out training or awareness activities.
- Organisational changes such as updating roles, responsibilities or resourcing.
- Customer remediation or compensation for affected individuals.

Depending on the nature of the crisis, it may be appropriate to communicate the plan for implementing corrective actions to key stakeholders internally and externally.

5.2 Triggers for Standing Down

The Crisis Management Organisation should be stood down once the CMT Chair and/or CMT Secretary assesses that:

- The situation has been stabilised and there are limited new developments or changes on a day-to-day basis.
- The source of the crisis has been mitigated and there is limited risk of it imminently reoccurring.
- There are few, if any, remaining decisions and actions required from the CMT and CMEC.
- Teams assisting with the crisis are no longer required to be actively working on it.
- Corrective actions (if required) have been defined and the focus of the CMT and CMEC has shifted towards primarily implementing them.

5.3 Stand Down Process

Stage	Details
Return to Business-as-Usual (BAU)	• The CMT Chair or Secretary, in conjunction with the CMEC (as appropriate) should determine the point in time that the crisis has been controlled sufficiently and the affected areas of Optus can return to BAU. At this point, a declaration should be made by the Optus CEO that the crisis is over. • Depending on the nature of the incident, it may be necessary to implement a temporary BAU state, which would differ to the pre-incident situation. • Any protocols which have been put in place should revert back to BAU processes and/or be handed over to an on-going recovery project team.
Stand-down team	• The CMT and any other activated response teams should formally disband. • The stand down needs to be communicated to all parties who have been interacting with these teams and a new point of contact established for necessary continued communications. • A series of debriefs should be scheduled to bring all team members together prior to formally standing down the respective teams.
Post Incident Review	• Post Incident Reviews should be conducted by the CMEC and CMT to fully debrief all team members and capture the successes, learnings and recommendations following an incident. Refer to Annex I.

6. Crisis Communication and Collaboration

6.1 Crisis Management Centre (CMC)

The CMC is the central point of control, providing a focus for the company wide response initiated by the declaration of an Optus Crisis. Normal management and operational functions, where possible, continue throughout the period of the crisis. The CMC provides organisation wide oversight as well as augmenting operational decision making where required.

Site Details	
Location:	[redacted]
Supporting rooms:	
Equipment:	• Detailed instruction manuals for the CMEC and CMT • Nominated break out rooms • Connectivity: data points, phone connections and back up landline connections to alternative carrier services
Initial Response Cabinet:	The CMC contains some equipment including telephone handsets and stationery, so that the Centre may be activated quickly in the first instance. The initial response cabinets are located in: [redacted]

Office Equipment

The CMC also requires office and display equipment - computers, stationary, white-boards and overhead projector - as well as ready access to a photocopier and a facsimile machine. Computers, electronic white-boards, an overhead projector and some additional equipment are readily available on [redacted]. Other equipment needs to be found and procured from within the building. Procuring such equipment takes **priority** over other operations and the CMEC and CMT can requisition needed resources as appropriate.

6.2 Situation Report (SITREP)

Each team member in the CMT will be required to contribute to a SITREP in the early stages of the incident. The SITREP is designed to provide a snapshot summary of the situation, actions and issues.

Key content includes:

Element	Description
Situation	A brief summary of the incident details - location, time, who / summary of situation to date
Issues	A brief description of issue(s) that are known/reasonably expected to arise before the next SITREP is issued
Actions Taken	A brief report of actions completed to date
Actions to be Taken	A brief report on planned / scheduled actions
Other Considerations	Anything else that may be relevant to current or future management of the incident

A SITREP should be completed as soon as possible after the incident has occurred and then repeated as key information changes.

The SITREP template is to be used to ensure the consistent provision of information across streams. Refer to Annex K– Template (SITREP)**Error! Reference source not found.**.

6.3 Crisis Communication Requirements

Following declaration of a crisis and activation of the CMT and/or CMEC, the following notification timeframes should be adhered to where possible for updates to key stakeholder groups:

Channel	Initial comms	Updates	Closure
[redacted]	Within [redacted] mins	Within [redacted] mins	Post-restoration
E-mail	Within [redacted] mins	Within [redacted] mins	Post-restoration

6.4 Record Keeping

It is critical to keep a record of key information, decisions, actions and situation updates during a crisis. The primary record of these items is the SITREP, however there are also a number of supporting logs and registers that should be maintained:

- Personal Log (**Annex L)** – to be maintained by all team members
- Action Register (**Annex M)** – central register to record all actions. To be maintained by the CMT and CMEC Secretary
- Decision Register (**Annex N)** - central register to record all key decisions. To be maintained by the CMT and CMEC Secretary

At a minimum, all decisions and actions made during the crisis **must** be documented to ensure there is a clear record of the response and to demonstrate due diligence in managing the crisis. The level of detail should be sufficient that someone new to the crisis response could take handover based on the crisis records.

6.5 Crisis Collaboration Tools

The designated primary and secondary crisis collaboration tools are summarised below.

As the regular BAU collaboration tool, [redacted] is the primary collaboration tool. [redacted]

Activity	Primary Tool	Secondary Tool
Host Meetings	[redacted]	[redacted]
Perform 1-1 Calls		
Message		
Track Actions & Tasks		
File Share		

Note: [redacted]

Annex A - Definitions

Term	Definition
Business Continuity Planning (BCP)	The preparation that enables Optus to resume business as quickly and efficiently as possible if an unplanned event occurs. It includes: • continuity planning before an event; • crisis management during an event; and • recovery management after an event.
Optus Crisis	The official declaration of a situation which is a companywide crisis requiring the coordination of activities, facilities and resources to restore the company to pre-crisis operational capacity.
Crisis	A crisis is a critical event that may impact the organisation's profitability, reputation, or ability to operate. It may not be time-dependent and usually does not deny access to facilities and infrastructure. Crisis Management is the overall coordination of an organisation's response to a crisis, in an effective, timely manner, to contain or minimise impact to the organisation's assets, personnel, operation and reputation. Early indications of a crisis include: • Internal incident notifications from Networks/EMDS/IT/affected BU • Significant increase in Customer complaints • Abnormally high online chatter • Query / report from media / regulators Examples of crisis are: • major fire/explosion; • loss of a major Exchange that is critical to operations, etc; • loss of a critical Exchange, Hub, or Satellite Earth Station; • loss of a Data Centre; • loss of a major facility, e.g. a major office or network management facility; • loss of a business-critical IT application; • loss of a Satellite; • cyber attack affecting our systems, infrastructure or data; • a natural disaster, requiring the implementation of Federal, State or Territory emergency/disaster plans. • Arrests involving any member of the Senior Leadership Team or any employee where criminal charges made could impact the brand.
Emergency	Any event which arises from internal or external sources which may adversely affect the safety of persons in an Optus building or facility, and which calls for an immediate response by the occupants. An emergency generally refers to a single untoward event which should be managed by either local management, the relevant Department or the local Site Emergency Contact (SEC).

Incident	An untoward event that results in or has the potential to cause: • injury to personnel, requiring medical treatment • damage to property or facilities, • disruption of systems or leakage of data, • disruption to operations and customer service. An incident generally refers to a single untoward event which should be managed by either local management, the relevant Department or the local Site Emergency Contact. It should be reported using the standard Incident Report and escalated if necessary. Examples are: • Workplace accident; • Damage to customer property; • Bomb threat.
Major Incident	An untoward event or series of events that threatens to escalate in intensity and/or magnitude beyond the framework of normal management expertise or resources. A major incident could meet one or more of the following criteria: • harm to people, which could result in hospitalisation or loss of life, • major damage to assets, systems or network, • significant business interruption, • significant impact on the company's ability to deliver products and maintain customer service; • adverse publicity. A major incident should be managed through the relevant Major Incident Management (MIM) processes. Examples are: • serious workplace accident; • partial disruption to services, • interoffice fibre (IOF) cuts, • switch/transmission outages, • cyber attack, • severe storm damage to overhead network.
Recovery Strategy	An overview of current plans and future requirements, to control risks and to minimise the impact of an unplanned event on one or more identified Risk Exposures.
Risk Exposure Assessment	A detailed, systematic examination of any activity, location or operational system to identify risks and their likelihood and potential consequences.
Risk Management	The set of ongoing management and engineering activities of a business to ensure that risks are effectively identified, understood, and minimised to a reasonably achievable and tolerable level.

Annex B – Incident Contact Points

Key incident contacts are summarised below. Refer also to the separate Crisis Call Tree for the contact details of each CMT and CMEC member.

Contact Point	Contact Details
CMT Secretary	[redacted]
CMEC Secretary	
CMT Conference Bridge	
CMEC Conference Bridge	
Backup Conference Bridge	
Emergency	
Network Incident	
Cyber Security Incident	
IT Incident	
Reputation Incident	

Annex C – Crisis Escalation Criteria

Preservation of life is always the priority. Incidents where lives are at risk immediately trigger crisis management. Incidents involving the possibility of significant reputational harm or financial loss also trigger crisis management.

	FINANCIAL	BUSINESS INTERRUPTION	PUBLIC CONFIDENCE & REPUTATION	REGULATORY AND LEGAL	PEOPLE
Actual or Potential Impact[1]	• Cash loss [redacted]	• Loss of key services resulting in severe impact to customers • Full service disruption to one or more enterprise customers or government agencies	• Widespread negative national, international or viral social media coverage • High number of internal or external customer or stakeholder complaints	• Allegation or violation of law or regulation subject to remediation costs or fines [redacted] or prison	• Fatality • Multiple serious injuries • Widespread illness
Optus Guidance *(Example Events)*[2]	• Significant internal or external fraud event, including theft • Property or assets lost, damaged or threatened • Revenue loss due to billing/ processing errors	• Extended [redacted]) network outage that impacts [redacted] of the customer base for a product offering, affects a high profile location or affects a VIP enterprise or government customer • Extended mission critical IT system outage (i.e. unable to recover within time objective) • Extended [redacted]) inability for the majority of customers to reach Optus to get connected or maintain their service[3] • Unavailability of a key facility for [redacted] (e.g. due to flood, fire, gas leak, industrial action etc.) • Cyber attack (e.g. denial of service, ransomware) impacting availability of customer facing services	• High volume ([redacted]) of negative social media posts • Leak or unauthorised disclosure of large volumes of sensitive or personal data • Credible extortion or ransom request • Publicly visible cyber security incident (e.g. defacement of public web sites) • Incident likely to require a reactive national press release and/or market disclosure • Independent external enquiry likely to receive national interest	• Serious breach of critical telco or corporate regulatory requirements • Publicly disclosable investigation, enquiry or unfavourable regulatory action • Allegation, conviction or arrest of a member of the Board, Executive or Senior Management for illegal or fraudulent conduct	• Workspace safety incident affecting staff, contractors, customers or the public • Credible terrorist or bomb threat • Infectious disease and/or pandemic outbreak at orange alert level (WHO phase 5) • Hazardous levels of air quality (AQI >300)

[1] *An incident or event need only satisfy one threshold to trigger escalation. For example, a minor network outage with widespread national media coverage shall qualify for escalation.*

[2] *In addition to the criteria, any member of the CMT or CMEC may also refer an incident to the CMT Secretary for consideration to escalate as a potential crisis*

[3] *Refers to the majority of the customer base for a given service offering and includes consideration of the timing of the interruption (i.e. if it is during business hours or a peak period)*

Annex D – CMT Agenda (Initial meeting)

#	Agenda Item	By whom	✓
-	Establish Log Keeping and Records	CMT Secretary	☐
1	Agree CMT Chair who will also be a CMEC member	All members	☐
2	Convene meeting and confirm welfare of all team Members. Ensure there are no conflicts of interest that may compromise management.	Chair	☐
3	Agree crisis team meeting protocols: • Purpose of meeting. • Duration.	Chair	☐
4	Confirm team roles and responsibilities. Determine need to dismiss team members and/or include subject matter experts, as required.	Chair	☐
5	Share information based on received SITREPs: • Health & Safety • Customer Impact • Network Impact (including any impact to 000 services) • IT Impact • Regulatory • Legal • External Media (including social media) • Additional information (all CMT Members).	All members	☐
6	Determine if any team members have previous experience in a similar event	Chair	☐
7	Conduct joint impact assessment for current situation.	All members	☐
8	Determine if any BCPs need to be invoked. If so, recommend to the BCM Representatives.	Chair	☐
9	Confirm what existing Incident Response Teams are in place and need to be stood done if a crisis is declared.	CMT Secretary	☐
10	Set objectives for response/recovery.	All members	☐
11	Provide overview of relevant legal obligations, including extent of record keeping required	Legal Representative	☐
12	Confirm data storage protocols for crisis event documentation.	CMT Secretary	☐
13	Allocate immediate tasks/actions from joint assessment to members of the team.	Chair	☐
14	Confirm time of follow-up meeting.	CMT Secretary	☐

Annex E – CMEC Agenda (Initial Meeting)

#	Agenda Item	By whom	✓
-	Establish Log Keeping and Records	CMEC Secretary	☐
1	Convene meeting and confirm welfare of all CMEC and CMT Members. Ensure there are no conflicts of interest that may compromise management.	Chair	☐
2	Agree crisis team meeting protocols: • Purpose of meeting. • Duration.	Chair	☐
3	Confirm CMEC member roles and responsibilities. Determine need to dismiss members and/or include subject matter experts, as required.	Chair	☐
4	Determine the membership of the CMEC. Appoint a deputy.	Chair	☐
5	Share information based on received SITREPs: • Health & Safety • Customer Impact • Network Impact (including any impact to 000 services) • IT Impact • Regulatory and Legal • External Media (including social media) • Additional information (all CMEC Members).	All members	☐
6	Determine if any members have previous experience in a similar event	Chair	☐
7	Share summary of CMT's impact assessment for current situation.	CMT Chair	☐
8	Set crisis management objectives and priorities.	All members	☐
9	Establish crisis communication protocols, including appointment of media spokesperson as required.	All members	☐
10	Confirm data storage protocols for crisis event documentation.	CMEC Secretary	☐
11	Allocate immediate tasks/actions from joint assessment to members of the team.	Chair	☐
12	Confirm time of follow-up meeting.	Chair	☐

Annex F – CMT Agenda (Follow-on Meeting)

#	Agenda Item	By whom	✓
1	Re-convene meeting and confirm welfare of all team members. Ensure there are no conflicts of interest that may compromise management.	Chair	☐
2	Provide update to crisis team: ▪ Summary of new information and response actions to date (all team members). ▪ Confirmation of staff safety, potential injuries & follow-on welfare (People). ▪ Communications and media (Communications). ▪ Disruption to services (all CMT members). ▪ Additional information from CMT Members.	All members	☐
3	Review of potential impacts.	All Members	☐
4	Confirm “problem ownership” and responsibility delegation between Optus and external parties (e.g. emergency services, government body, etc).	Chair	☐
5	Allocate subsequent tasks/actions from joint assessment to members of the crisis team.	Chair	☐
6	Agree time of regular meetings.	CMT Secretary	☐

Annex G – CMEC Agenda (Follow-on Meeting)

#	Agenda Item	By whom	✓
1	Re-convene meeting and confirm welfare of all team members. Ensure there are no conflicts of interest that may compromise management.	Chair	☐
2	Provide updates on current status of the crisis: ▪ Summary of any developments since initial meeting, including outcome of any investigation activities ▪ Discuss any changes to actual or potential impacts ▪ Provide update on action items and any other relevant actions taken since initial meeting	All members	☐
3	Confirm people impacts including staff safety and wellbeing considerations.	People & Culture	☐
4	Discuss the status of communications, including review of any communication plans and/or messages.	CMT Chair	☐
5	Provide update on status of stakeholder engagement activities including with Singtel, government, regulators, employees etc.	All members	☐
6	Identify and discuss additional actions or decisions required, including those escalated from the CMT.	All members	☐
7	Review and approve activation of relevant BCPs based on recommendation from CMT.	All members	
8	Agree time of regular meetings and any other logistics such as rosters, communication and collaboration protocols, etc.	CMEC Secretary	☐

Annex H – Template (Recovery Action Plan)

RECOVERY ACTION PLAN					
Time and Date:		**Author**:		**Version #:**	
Situation *(A brief summary of the incident details)*					

Actions to be taken *(Report on planned/scheduled actions)*	**Responsible Person**	**Time/Date for Completion**

Issues *(Present brief description of issue(s) that are known/reasonably expected to arise before the next plan release is issued)*
Next Plan due:
Produced by Optus | Commercial in Confidence | Not for public distribution under any circumstances

Annex I – Template (Post Incident Review)

POST INCIDENT REVIEW		
FACILITATOR:		
LOCATION:		
DATE:		
What occurred? Summary of facts: Sequence of events:		
Actions taken Describe key decisions made and actions taken:		
Emergency Response	**Questions:** Was an evacuation required? Were any staff injured or affected by the incident? Were any visitors or members of the public injured or affected by the incident? Was the building/site secured to prevent re-entry? Were emergency procedures followed correctly? Were incident details reported using the correct escalation processes in a prompt manner? <u>Additional Comments:</u>	Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐
Assessment of Impacts	**Questions:** Was an impact assessment conducted? If an impact assessment was conducted, how was this information used? Were the outcomes of the impact assessment reported to the CMT? <u>Additional Comments:</u>	Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐

POST INCIDENT REVIEW		
Team Activation and Escalation	**Questions:** Were teams activated in accordance with the agreed structure? Was the incident given an incident classification? Was the incident escalated to the appropriate team/s? Were formal CMT meetings held? Were incident command facilities activated? If teams were activated, were all key portfolios represented by appropriately qualified personnel? Were hand-over procedures implemented to ensure the sustained operation of the CMT? Additional Comments:	Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐
Communications	**Questions:** Were all key stakeholders notified? Were communications appropriate for the type, size and scale of the incident? Were communications undertaken in a timely manner? Was the media communicated with in an effective manner? Were communication templates used? Was an action and media log maintained throughout? Additional Comments:	Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐
People Management	**Questions:** Were appropriate actions and strategies identified to manage the welfare of people impacted by the incident? Was an action log maintained throughout? Additional Comments:	Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐
Business Recovery	**Questions:** Were operations disrupted as a result of the incident? Was a Recovery Action Plan developed to facilitate resumption of critical business functions? Was an action log maintained throughout? Additional Comments:	Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐ Yes ☐ No ☐ N/A ☐
What went well? Identify and examine actions that had positive results and why		

POST INCIDENT REVIEW	
What could be improved? Identify actions or areas that could benefit from improvement and why	
Actions arising Identify actions arising from this debrief and responsibilities for following up	
Acknowledge Ask for any additional questions from participant/s	
Sign-off	
Facilitator Name and Signature	
Date:	

Annex J – Out of hours site access

Security procedures to facilitate afterhours access to OCS are:

OCS Emergency Access

The access key for the Crisis Management Cabinets is held in the [redacted] for use during activation of the CMC. The Security Team and the SFCC have access to [redacted] and assist with issuance of this key when necessary.

At OCS the standing SOP for the onsite guard supervisor is upon notification of a declared crisis to ensure that the CMC is immediately opened and the CMC cabinets opened for access by CMT personnel.

Authority to draw the Master Key and Access Cards

The [redacted] may only be drawn by staff authorised by the CMT Chair. This authorisation is normally limited to Team Leaders and Deputy Team Leaders of the Business Recovery Support Teams and senior members of the CMT.

Subsequent Issue

Subsequent issue of the keys to members of the CMT or the Support Teams is controlled by the CMT Chair and Co-chairs. All keys must be signed for.

Annex K – Template (SITREP)

OPTUS SITUATION REPORT					
Time and Date:		**Author**:		**Report #:**	
Highlights					
Situation *(A brief summary of the incident details - location, time, who / summary of situation to date. On update, delete old information)*					
Issues *(A brief description of issue(s) that are known/reasonably expected to arise before the next SITREP is issued)*					
Actions taken (*Brief report of actions completed to date (New))*			**Actions to be taken** *(Report on planned/scheduled actions)*		
Other considerations *(Anything else that may be relevant to current or future management of the incident)*					
Next SITREP due:					
Produced by OPTUS | Commercial in Confidence | Not for public distribution under any circumstances					

Annex L – Template (Personal Log)

PERSONAL LOG			
Name:		**Role:**	
Date	**Time**	**Item** *e.g. phone call, meeting, decision*	**Notes**

Annex M – Template (Action Register)

ACTION REGISTER					
No.	**Date**	**Action**	**Responsible Person**	**Due Date**	**Status / Outcome**
1					
2					
3					
4					
5					
6					
7					
8					

Annex N – Template (Decision Register)

DECISION REGISTER					
Date	**Time**	**Issue**	**Decision**	**Authorised By**	**Comments**