Ipsos MORI

Ipsos MORI Advice Note for Clients on Business Continuity as a result of the Coronavirus

Ipsos MORI has a formal Business Continuity Planning Policy and procedures in place to ensure the continued operation of its business in the event of a major business disruption or adverse event. Our planning and management of business continuity is externally assessed annually as part of our certification to the international standard for information security, ISO 27001 to which we have been certified since 2005.

Ipsos MORI's Senior Management Team are meeting regularly to assess the situation and will continue to monitor the situation closely. Business continuity plans and contact details have also been reviewed to ensure we are ready. The majority of staff are able to work securely from home using company issued IT equipment with remote access to company systems. Regular updates are going out to all staff in line with the Department of Health and Social Care and Public Health England's advice.

For now, it is very much "business as usual", but we will continue to plan for all eventualities and will update business continuity as we need to. Should there be any significant changes to "business as usual", we will update our clients through their usual contacts.

Please find a copy of Ipsos MORI's Business Continuity Planning Policy below for more details on our company approach. If you have any additional questions, please address these to your usual contact(s) at Ipsos MORI.

Version 2, 12th March 2020

Business Continuity Planning Policy

Our policy:

Our clients expect us to be able to deliver the level of service we have promised in all but the most extreme of circumstances. Ipsos MORI also has legal, regulatory and contractual obligations to ensure the appropriate standards of confidentiality, availability and integrity for the information we own, or process on behalf of others.

In order to meet those legal obligations and safeguard our corporate reputation, it's essential that we take appropriate steps to plan for major failures of our information systems, or any other reasonably foreseeable event that could interrupt our business activities.

Our planning and management of business continuity is externally assessed during external audits required to maintain our certification to the international standard for information security, ISO 27001. Whilst we have not certified to the international standard for business continuity, we have incorporated best practices set out in that standard within our business continuity management.

How we define a Business Continuity incident:

A "Business Continuity" incident is any major disruptive event affecting one or more of Ipsos MORI's offices to the extent that we are unable to carry out business as normal from the affected office(s). For example: the building may have been damaged or destroyed; power may be lost for an extended period of time; or there may be an off-site incident that results in the building having to be evacuated and/or people being unable to gain access to it for an extended period of time.

Our definition of an incident also applies to any major disruptive event affecting Ipsos MORI's IT infrastructure or systems that are critical to either providing services to our clients or in managing our business.

Governance of Business Continuity within Ipsos MORI:

The UK Management Board has established a sub-committee, our "Information Governance Forum", to provide senior management leadership and oversight of Ipsos MORI's integrated quality, compliance and information security management system, our "Business Excellence System", on its behalf. One of the key objectives of the Information Governance Forum is to provide assurance that Ipsos MORI is able to maintain continuity of service in the event of an incident; that any such incident is effectively managed with the safety of staff and visitors as the first priority; and that normal service is resumed as soon as possible.

The Information Governance Forum will achieve this by:

- Providing senior management input into, and oversight of, business continuity planning
- Assuring the effectiveness of the plans by having in place a rolling programme of business continuity testing, with the results of the tests reviewed by the Information Governance Forum
- Providing assurance that action points and recommendations made during testing are addressed when business continuity plans are updated
- In the event of an incident, to ensure, as far as possible, that root causes are identified and the effectiveness of Ipsos MORI's response is assessed and plans updated to address any lessons learned resulting from that assessment

Operational management of Business Continuity planning and testing is the responsibility of the Head of Compliance and resourced by Ipsos MORI's London Facilities Manager and assisted by the business continuity planning team for our major London offices

The Facilities Manager at each of our major offices is responsible for drafting and maintaining the Business Continuity Plan for their site using our standard templates.

The Office Manager in each of our small regional offices is responsible for documenting and maintaining the business continuity plan for their office.

Facilities and office managers being the "Site Manager" for their respective site in relation to business continuity planning for their site.

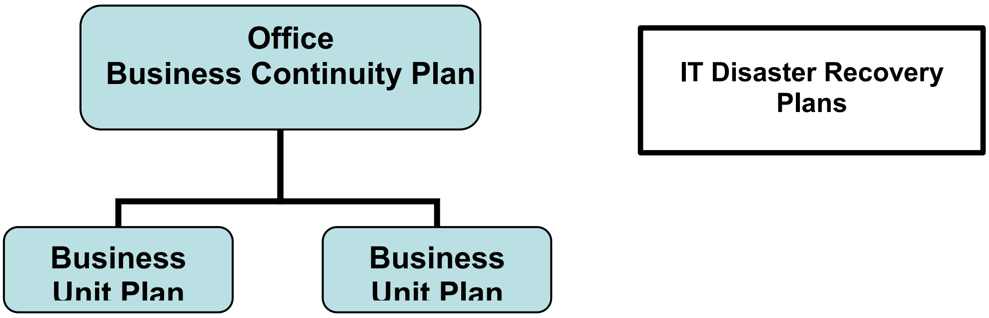
Business Impact Risk Assessments:
Business impact of threats to the continuity of our offices, infrastructure and systems are carried out as part of the information security site level risk assessments. Those risk assessments are reviewed at regular intervals in accordance with the schedule set out in Ipsos MORI's Approach to Risk document.

Our approach to business continuity planning:
Ipsos MORI uses a layered approach to planning for business continuity events in order to keep plans as simple and flexible as possible.

Planning for business continuity starts with our systems. Business critical systems are designed with failure in mind. Mitigation against any disruption to services resulting from any IT failure has been built into these systems in the following ways: Use of industry standard data centres having redundant power sources; dual WAN and internet connections at each of our major offices and data centres; Clustered production platforms, with warm stand-by systems available for our most critical systems such as email; and virtualised servers and systems that facilitate ease of recovery.

Continuity of business is also facilitated by our major business units not all being located in a single building. This makes relocation of key staff in the event of an office being lost a relatively quick and seamless process.

Our planning naturally includes formal Business Continuity Plans for each of our sites, which are supported by IT recovery plans. Our plans consist of the following coherent set of documents:



"Site Business Continuity Plan": A top level plan for each Ipsos MORI office/site. The plan provides details of the Site Incident Management Team led by a senior manager nominated to act as Incident Director, and the Incident Response Team. This document, together with the individual "Business Unit/Departmental

Business Continuity plans" for each Unit/Department at that site, forms the overall Business Continuity plan for each site. "Site managers" are responsible for ensuring the site plan is kept up to date.

"Business Unit/Departmental Business Continuity plan": For large offices with multiple business units, each business unit will develop its own plan with its own nominated Business Unit Lead that will be included as an appendix in the main Site Business Continuity Plan. The Business Unit lead will coordinate with the site Incident Management Team and may also be a member of the site's Incident Response Team.

The Business Unit plans will also outline the following:

- A prioritised list of information assets the Team/Department use, together with a realistic estimate of when they will require access to those assets to be restored
- What action Team/Departmental staff will take if the incident results in the site being unavailable as a result of the incident
- Key suppliers to be notified
- Key clients to be notified

The heads of each Business Unit/Department at the relevant site are responsible for ensuring the Unit/Departmental plan is maintained and kept up to date, and that all staff within Business Unit/Department has an up-to-date copy of the plan.

"IT Disaster Recovery Plans": These documents set out the detailed plans for the recovery of all IT and business information systems. They use the prioritised list of information assets detailed in each Site Business Continuity plan", together with information security risk assessment findings to establish priorities and recovery objectives for each system.

Business Continuity Incident Management:

Each site has an "Incident Management Team" whose primary objective is to provide leadership and direction with the aim of ensuring the safety of staff, visitors and the public, minimising the impact of any incident on the business and restoring normal business service as soon as possible. The Incident Management Team is responsible for:

- Invoking the Business Continuity Plan for the site in the event of an incident.
- Providing leadership and guidance to ensure all necessary tasks required to restore the ability of staff located at the site to provide on-going services to clients (internal and external), staff and other stakeholders according to the agreed recovery timetable.
- Keeping a record of actions taken and decisions made
- Ensuring the health and safety of all users of the site and any other affected individuals is treated as a priority throughout the management of, and recovery from, the Business Continuity Incident.
- Effective communications with staff, other Ipsos MORI and Ipsos Group sites, clients, suppliers and other stakeholders.

The Incident Management Team is made up of the following roles:

- Incident Director
- Facilities Manager
- Duty HR Lead
- Duty IT Lead
- Duty Communications Lead

The Incident Management Team is supported by an "Incident Response Team". The Response Team provides additional dedicated resources required to deal with the immediate impact of any incident; provide support to staff affected by the incident and to actively carry out tasks required to restore normal business services as soon as its safe and practicable to do so. This ensures the Incident Management Team can concentrate on the effective management of the incident.

Business Continuity and IT DR testing:

The effectiveness of Ipsos MORI's business continuity plans will be assessed by a rolling programme of site level Business Continuity Test exercises. These are scenario-based desktop exercises designed to simulate an incident, led by a facilitator, with records kept by another observer. These exercises are designed to provide the Site Incident Management and Response Teams with experience of managing an incident in a safe, controlled environment, whilst also assessing the effectiveness of the site's business continuity plans. The exercises may also involve practical tests of contact details out of hours, re-location of the incident management team to an alternate site, and may also be scheduled to coincide with drills testing evacuation procedures for the site.

The results of these tests are fed back to all staff involved in the test exercise, and are reviewed by the Information Governance Forum at its next meeting.

IT Disaster Recovery plans are also tested regularly. Testing activities will include:

- Use of Disaster Recovery plans as part of planned maintenance of our systems
- Planned tests aimed at recovering data stored for a project; part of, or an entire server or system.

Records of IT recovery tests are checked during internal and external audits, and reviewed annually by the Information Governance Forum.

Business Continuity Planning Assurance:

In addition to the senior management oversight provided by the Information Governance Forum, Business Continuity planning is formally reviewed and assessed during internal audits carried out twice a year. They are also externally audited by the external auditor leading on Information Security from our certification body as part of the annual external audits carried out to maintain our certification to the international standards for information security (ISO 27001), market research services (ISO 20252) and quality (ISO 9001).

In addition to the senior management oversight provided by the Information Governance Forum, Business Continuity planning is formally reviewed and assessed during internal audits carried out twice a year. They are also externally audited by the external auditor leading on Information Security from our certification body as part of the annual external audits carried out to maintain our certification to the international standards for information security (ISO 27001), market research services (ISO 20252) and quality (ISO 9001).

Document Control

Version	Date	Summary of changes	Authors	Approved by
V3	April 2019	Addition of document control & review panel. Minor tweak to Head of Compliance	Catherine Bolton	Tony Harper,UK Board Member of Business Excellence System

Document Review	
Version and Review Date	V3 May 2020
Reviewed Version	
Proposed changes (list chapter no and short description of changes)	
Review Committee	
Approval authority/Committee	
Next Review Due Date	
Note: Records within this table will not generate a change in the version number	