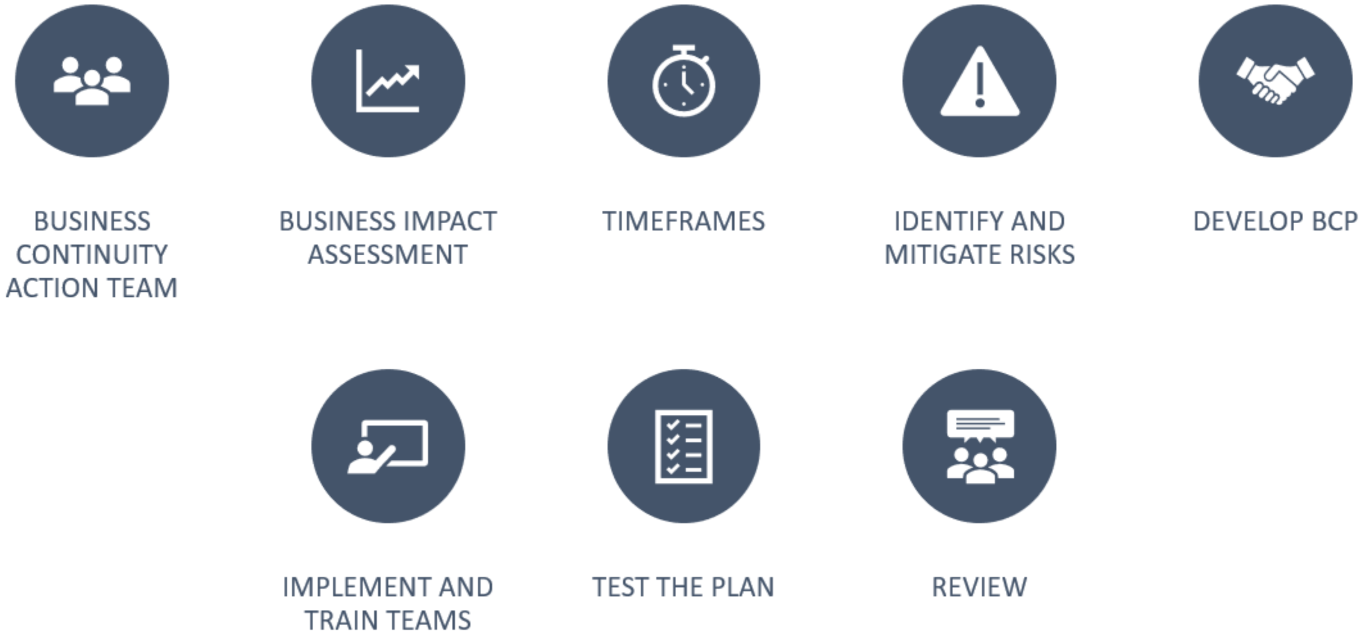


BUSINESS CONTINUITY ACTION TEAM

BUSINESS IMPACT ASSESSMENT

TIMEFRAMES

IDENTIFY AND MITIGATE RISKS

DEVELOP BCP

IMPLEMENT AND TRAIN TEAMS

TEST THE PLAN

REVIEW

# Business Continuity Planning Best Practice Examples & Lessons Learnt from Covid-19 –

# **Safe Working Environments for TEC**

TSA™

The voice of technology
enabled care

Business Continuity Planning Best Practice Examples and Lessons Learnt from the Covid-19 Pandemic
Version 1.0
7th May 2021

# Contents

# Section 1:

# Business Continuity Best Practice

## Introduction

Many organisations will have a Business Continuity Plan (BCP) in place and we have seen that this has been of vital importance during Covid-19. However, it is vital that these are reviewed and updated to ensure they remain relevant and have evolved as a result of lessons we have learnt during the pandemic.

Some organisations may have in-house experts on BCP, or utilise external consultants to advise them, but this short guide offers some suggestions on how to prepare your BCP and keep it agile and current.

## What is Business Continuity Planning?

Business continuity is about anticipating the crises that could affect an organisation and planning for likelihood of them happening, to make sure that the business can continue to function in the event of an emergency.

The BCP sets out clear roles and responsibilities, for example those assigned to manage all liaison with service users, employees, commissioners and the emergency services. It details a series of contingencies actions that enable key business activities to continue in the most difficult circumstances, such as when a vital computer system or other equipment is unavailable. Importantly, it also details clear emergency procedures to ensure that the safety of employees is a top priority. During pandemics such as Covid-19, these contingency plans have proven vital in keeping services operational.

While disaster recovery planning has traditionally focused on the initial recovery of the business operations and service provision, Business Continuity Planning addresses all the requirements essential to keeping the business running longer term and includes processes to keep disruption to users and employees to a minimum. In short, it is about ensuring that a crisis is managed effectively.

There are international standards for Business Continuity, such as ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements. However, this guide will help you with the fundamentals of continuity planning and demonstrate some of the lessons learnt during the Covid-19 pandemic.

## What Types of Disasters Should You Plan For?

It will depend on your business, the type of service, or equipment you provide, along with the locations in which you operate, but it is important to identify the possible challenges applicable to you. Whilst not an exhaustive list, the below are some of the types of incidents or crises that could occur:

Natural Disasters – as the title indicates, these are disasters that you have no control over: fires, floods, earthquakes, Pandemics etc.

Inclement Weather – there may be times when weather conditions are so severe, that staff may not be able to get to the workplace, or where travel in general is difficult, such as snowstorms, severe flooding, or even heatwaves. These conditions may also affect the working environment, or cause damage to equipment.

Malicious Attacks – malicious attacks are not limited to ransomware or hacking; vandalism, riots, terrorism and reputational threats, all mean your company harm and can lead to loss of service.

Technological disasters – these include computer network failures, communication systems, hardware failures or problems associated with using outdated equipment.

Denial of Access – It may be that your offices are functioning without issue, but circumstances around the site can lead to denial of access. For example, strike action, or environmental issues.

Human Error – disasters are not always natural or malicious and human error is as significant consideration. For example, employees can accidentally delete important data, bring in external devices that contain malicious software.

Political Events – Brexit for example, has seen a huge impact on how organisations operate. Sourcing equipment from Europe is now more challenging and the results may continue to have an impact on human resources.

Economic Situations – A significant financial crash, or problems with debtors.

Supply Chain Disruption – For many organisations, their service delivery, or supply will be dependent on partners in the chain. What will you do if key suppliers go out of business, or cannot guarantee an uninterrupted supply? Where would you seek to find alternatives?

## Main Components of a BCP

As many organisations are unique, you may wish to add to this list, but below are some of the fundamental elements of Business Continuity Planning:

1. Establish a Business Continuity Action Team. This should be formed from key personnel within your organisation and any stakeholders you believe can support the process. Members of the Action Team may drop in and out as required by the circumstances, but below is an example of what this Action Team could look like:

| Business Continuity Planning and Action Team | |
|---|---|
| **Key Business Activity** | **Responsible Person/People** |
| Business Continuity Planning and Action Team Lead | The person with overall responsibility for the Action Team. You may also wish to nominate a deputy |
| Facilities Management | Who will lead on any issues related to premises, remote location buildings and utilities? |
| Directorate | A nominated person who will represent the executive team and act as a link between the executive board and the action team and can assist with decision making. |
| Board Members | As above for any Non-Executive representative that may be appropriate. |
| ICT Operations Staff | Selected members of the IT team, who can deal with aspects of ICT continuity, website, email, |

| | |
|---|---|
| | communication systems and source IT equipment as needed. |
| Health and Safety | The person with company responsibility for Health and Safety, along with the staff representative, Business Risk Manager |
| Product and Sales | The person who can advise on any requirements regarding the products, or services provided. |
| External and Internal Comms | Company, or group marketing and communications staff, for both external and internal communications. |
| Human Resources | Company and staff representation with focus on staff welfare and any HR legal issues. |
| Finance | Finance Manager, or other finance officer, who can advise, should this be required |
| External Partners | Are there any external suppliers, or partners that need to be involved? Commissioners, critical equipment/systems suppliers. |

When starting off the process, try working through the following good practice tips:

1.1. Take time to fully understand your operational vulnerabilities. Be realistic and critically evaluate your processes and technology systems. What are your weaknesses and how can you make them more robust?

1.2. Understand the difference between Disaster Recovery (DR) Plan and Business Continuity Plan (BCP). DR is mainly centred on restoration of services, or systems after an incident. It is just one part of the whole BCP, which focuses on longer term sustainability of operations.

1.3. What are your critical business functions? Make a list of all business functions, both automated and manual and Identify the effects that the failure, delay, loss, or disruption of each function can result to. This will help you determine the prioritization of critical business functions.

1.4. Look at your equipment and systems for resilience. Whether these are cloud based, or housed on-site, identify equipment that you may want to prioritise in your business continuity plan such as servers, special equipment, and irreplaceable software.

1.5. Ensure all emergency contact information is both up to date and easily accessible to staff. This could be part of structured on-call process for out of hours working.

1.6. Consider third party risks as part of your BCP. This could be your communications partner, or monitoring platform provider, or vehicle service provider, but they play an integral part in your continuity of service. Review contracts and ensure they support your BCP.

1.7. Alternate site locations. Are there other offices, or premises you could use if you cannot access the main locations? These could be designated as primary and secondary sites etc., with a set location as a "rally" point for staff to meet.

1.8. Alternative communications. What will you do if internet connection, phone lines, and telecommunications systems are damaged or completely destroyed during a disaster?

1.9. Are there some services you can bring in-house, even if for the short term?

1.10. As you can see from the Action Team table above, include your staff. It helps to have buy in and have their suggestions for identification of risk.

1.11. During any incidents, how will you communicate with people. This may need different messaging and mediums, depending on who your message is for. Consider the Service

User and Customer needs. How will you keep them updated, especially during pandemics, when situations may change rapidly?

2. Conduct a Business Impact Assessment (BIA). This analysis supports the entire business continuity process. It is used to identify, quantify, and qualify the impact of a loss, interruption, or disruption of an event on the business. A BIA identifies mission-critical activities and the timeframes within which they must be recovered. It should consider both internal and external organisational risks.

Timeframes and Recovery Objectives are normally identified in terms of:

- Recovery Time Objective (RTO). The period a business' activities and resources must be recovered to an acceptable capability after a disruptive event.
- Recovery Point Objective (RPO). The point in time to which products, activities, or data in a known, valid, or integral state, can be restored from.

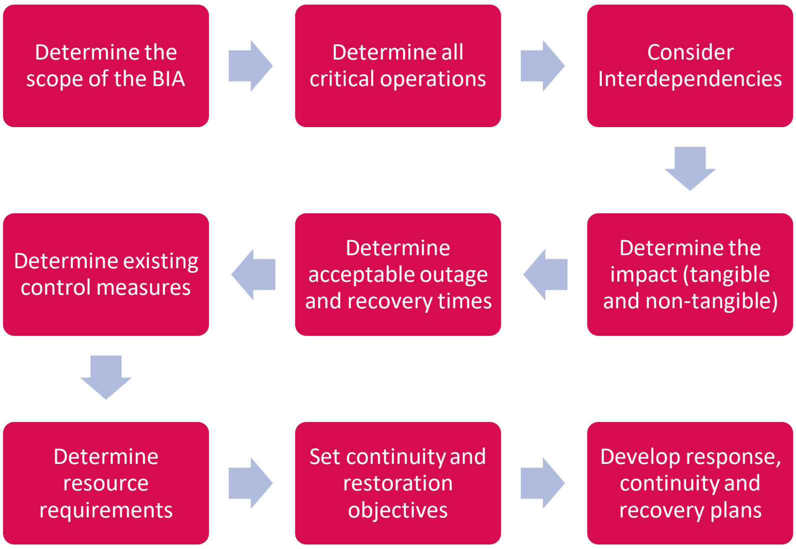
Explore all the risks that your organisation is exposed to and the possible major disruptions that could occur. This can include single points of failure of systems, power, communications and your supply chain.

You should also include the impact a disaster in the TEC department would have on the organisation, or business overall. Following a disaster, planning may also be extended to include consideration on:

- Is the organisation recovering effectively?
- What are the milestones for effective recovery?
- How will you know when you have recovered sufficiently?
- Consider the use of Recovery Planning Compliance Audits from an external source.

Organisations should always reference back to the Service User and Customer experience and the impact that any disaster would have on them.

2.1. A Business Impact Assessment could look like this:



Determine the scope of the BIA

Determine all critical operations

Consider Interdependencies

Determine the impact (tangible and non-tangible)

Determine acceptable outage and recovery times

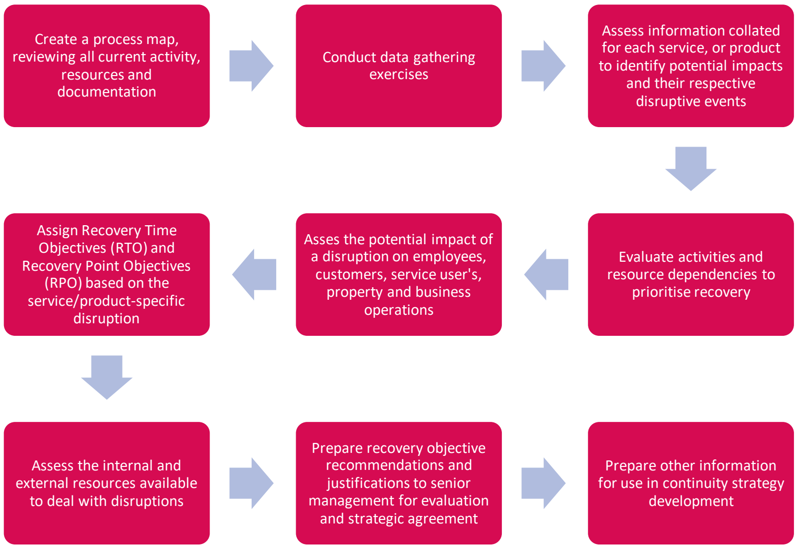
Determine existing control measures

Determine resource requirements

Set continuity and restoration objectives

Develop response, continuity and recovery plans

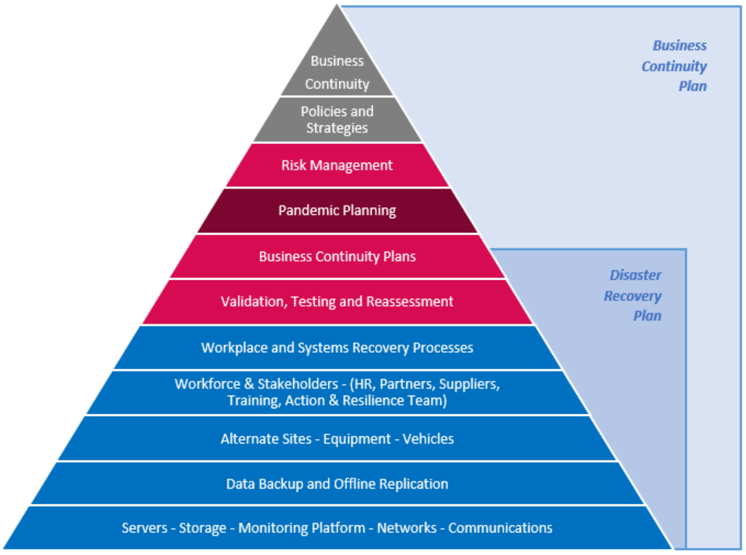
2.2. A Business Impact Methodology could be viewed as:


Create a process map, reviewing all current activity, resources and documentation
Conduct data gathering exercises
Assess information collated for each service, or product to identify potential impacts and their respective disruptive events
Evaluate activities and resource dependencies to prioritise recovery
Asses the potential impact of a disruption on employees, customers, service user's, property and business operations
Assign Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) based on the service/product-specific disruption
Assess the internal and external resources available to deal with disruptions
Prepare recovery objective recommendations and justifications to senior management for evaluation and strategic agreement
Prepare other information for use in continuity strategy development

3. Mitigate Identified Risks. After the BIA, an organisation should look to mitigate risks that have been identified and which threaten the health and safety of people, operations, service user's, company assets, or the environment by reducing the risk to an acceptable level. Strategies to help mitigate risk is shown in further sections

4. Develop your Business Continuity Plan. This will follow from everything you have recorded in the BIA process and should identify requirements for emergencies and disasters, such as the Covid-19 pandemic. A typical Business Continuity Planning model, adapted for the TEC Sector and for pandemics, is shown below:

Business Continuity Planning Model


Business Continuity
Policies and Strategies
Risk Management
Pandemic Planning
Business Continuity Plans
Validation, Testing and Reassessment
Workplace and Systems Recovery Processes
Workforce & Stakeholders - (HR, Partners, Suppliers, Training, Action & Resilience Team)
Alternate Sites - Equipment - Vehicles
Data Backup and Offline Replication
Servers - Storage - Monitoring Platform - Networks - Communications
Business Continuity Plan
Disaster Recovery Plan

5. Implement the plan and Train Teams. Conduct training for employees with key roles and assignments in the business continuity, disaster recovery, and incident response processes.

6. Distribution of the Plan – Consider who should be on the distribution list for your BCP. This may include internal staff, partner organisations and stakeholders. Who else in the wider organisation would benefit from being included in the distribution of the plan, especially your BCP feeds into a wider continuity plan?

7. Test the Plan. Testing is the generic term used to describe the critical process of exercising strategies and plans, rehearsing with co-workers, and testing systems (technology infrastructure and administrative) to demonstrate business continuity. If time allows, testing could be in the forms of:
   7.1. A table-top exercise. This usually occurs in a conference room with the team poring over the plan, looking for gaps and ensuring that all business units are represented therein.
   7.2. In a structured walk-through. each team member walks through his or her components of the plan in detail to identify weaknesses. Often, the team works through the test with a specific disaster in mind. Some organisations incorporate drills and disaster role-playing into the structured walk-through. Any weaknesses should be corrected and an updated plan distributed to all pertinent staff.
   7.3. A full emergency evacuation drill. This type of test lets you determine if you need to make special arrangements to evacuate staff members who have physical limitations. Disaster simulation testing can be quite involved and should be performed annually. For this test, create an environment that simulates an actual disaster, with all the equipment, supplies and personnel (including business partners and suppliers) who would be needed. The purpose of a simulation is to determine if you can carry out critical business functions during the event.

   During each phase of business continuity plan testing, include some new employees on the test team. "Fresh eyes" might detect gaps or lapses of information that experienced team members could overlook.

8. Review and improve your business continuity plan. Much effort goes into creating and initially testing a BC plan. Once that job is complete, some organisations let the plan sit while other, more critical tasks get attention. When this happens, plans go stale and are of no use when needed.

   During the Covid-19 pandemic, we have seen that circumstances change and evolve quickly. We also know that technology moves on, as do people, so the plan needs to be reviewed and updated, too. Bring key personnel together at least annually to review the plan (more frequently during the pandemic – as often as resources allow) and discuss any areas that must be modified to ensure effectiveness and to reflect changes in the operation and personnel. Keep up to date with developments on the TSA website, which will inform your BCP review.

## Templates

We have provided some basic sample templates for BCP planning and reporting, which you may find useful. These can be amended and added to as necessary for your organisation. They are a good starting point for those organisations embarking on or reviewing their processes.

These include:

- Business Continuity Planning Checklist - Appendix ‘A’
- A Basic Business Continuity Plan Template - Appendix ‘B’
- Simple Disaster Recovery Report Template - Appendix ‘C’

# Section 2:

# Lessons Learnt from the Covid-19 Pandemic – Safe Working Environments for TEC Services

## Introduction

The following guidance has been provided to help TEC Organisations to consider ways to help support their business continuity plans and to ensure that employees can work safely in the TEC sector.

It should give you confidence to know that if the correct safety measures are put in place, services can continue to operate safely, providing the valuable support that your service users need.

We understand that there have been technical challenges during the pandemic and that both physical and mental wellbeing of staff are vitally important. In many cases it has been challenging to maintain staff levels, due to some members of the team contracting the virus and with those who have needed to shield.

This practical guidance will help with reducing the concerns that members of the team may have in returning to the workplace.

The following links have been provided, to guide organisations to the current Government guidance on working safely.

### Guidance for England

Working Safely in Offices and Contact Centres
Working Safely in Other People's Homes

### Guidance for Scotland

Guidance in Scotland for Covid-19 Safe Working

### Guidance for Wales

Guidance in Wales for Covid-19 Safe Working

### Guidance for Northern Ireland

Guidance in Northern Ireland for Covid-19 Safe Working

### Health and Safety Executive

Covid-19 Risk Assessment

## The Importance of the Quality Standards Framework During Covid-19

Most organisations probably feel that there is never a good time for an audit, especially during a pandemic. However, during times of extreme pressure, like Covid-19, it is important that services work hard to maintain high levels of safety and quality. The best way to understand that standards are being maintained, is through the TSA audit programme, against the Quality Standards Framework (QSF). The contingencies that TEC Quality have put in place, as part of their own UKAS accreditation COVID-19 planning, ensure that services are staying safe, which provides wider confidence within the TEC sector.

Throughout the early part of the pandemic, TSA conducted a large-scale outreach programme to almost all TEC services across the UK. This work demonstrated that those organisations who are certified to the QSF, were better prepared for the pandemic, than those that were not certified. This is because the QSF continually challenges organisations on their operational readiness for disasters such as pandemics, but also promotes continued improvement and innovation.

Therefore, we recommend that services ensure that they continue with their certification if it has already been achieved, or if not already, start the journey to certification to ensure the challenging standards are being met.

Performance Measurement in line with the Quality Standards Framework is equally important, as this will help organisations to assess if contingency plans are working, or whether further modifications are needed.

More information on the standards and our audit scheme, can be found on our UKAS Accredited TEC Quality Website. TEC Quality is a subsidiary of TSA.

## Identifying Risk

In everyday life, employers have an obligation to protect employees from harm and during the Covid-19 pandemic, this responsibility is the same. As with other work-life risks, employers should conduct a risk assessment for Covid-19, which will help identify the associated risks and help protect your teams.

The Health and Safety Executive (HSE) stat that organisations must:

- identify what work activity or situations might cause transmission of the virus
- think about who could be at risk
- decide how likely it is that someone could be exposed
- act to remove the activity or situation, or if this isn't possible, control the risk

We already know some sections of the community are more at risk than others and this should be included in any risk assessments.

The HSE can provide more information on Managing Risk and what to include in a Covid-19 Risk Assessment. The risk assessments will help inform your decisions and what protective measures need to be put in place for staff and the results of the assessment should be shared with them.

It is also advisable to consult with Health and Safety representatives with organisation and include staff representatives in any discussions. In this way, a culture of collaboration is developed helping staff to feel included in the solutions you decide upon. It is usually the case, that those team members working in the environment, will understand what the best solutions could be. Therefore, consultation with all concerned parties will be key to success in eliminating risk.

You should also consider multiple risk management. For example, snowstorms during the pandemic, or lack of access to locations during a technical failure.

## Risk Management

As mentioned in the previous section, employers have an obligation to protect staff in the workplace.

Each of the home nations governments, have provided guidance on how to protect workers and to manage the risk of spreading the Coronavirus for business continuity and for when they return to the workplace. The general arrangements that employers are required to put in place, include:

- Completing a Covid-19 risk assessment and share it with staff. Please refer to the HSE information in the Links section of this section of the website.
- Ensure any local DR/BCP contingencies for TEC sections align with overall organisational BCP
- Conducting cleaning more frequently, especially those surfaces that are being touched a lot
- Instruct staff and visitors to use hand sanitiser frequently.
- Develop wellbeing action plans for staff, that can be easily accessed by managers and supervisors.
- Ensuring that where possible, those members of staff that can work from home, do work from home (TSA has provided separate guidance for home-working, which includes risk assessments for these workers).
- Providing an environment for effective social distancing and enforce this with clear signage
- Increasing ventilation in workspaces, by keeping doors and windows open if possible and always running ventilation systems, or consider the installation of air purification systems.
- Minimising the possibility of visitors to those attending for essential purposes.
- Use of “key fob” access systems, minimise entry to essential staff only.
- Keeping a register of those people who do visit the premises within the last three weeks, with full contact details.
- Conduct staff and visitor temperature checks prior to entry into work premises.
- Requiring that those people who do visit premises, wear a mask.
- Staff using the Test and Trace app for their country, which will track if they have been in contact with an infected person recently – please see further details below.
- Turning away anyone (staff member, or a member their household, or visitor) who attends with Coronavirus symptoms, such as:
    - Persistent cough
    - High temperature – *thermometers could be provided by the employer, to temperature screen staff and visitors prior to entering any work premises (One of the primary symptoms of COVID-19 is a temperature of above 38°C, or 100.4°F).*
    - Have lost their sense of taste, or smell

## Home Working

For most of 2020, the COVID-19 virus has proven to pose a health threat to TEC monitoring service staff, and the people they come into contact with. This Guide, which forms part of a series of documents for Safe Working Environments, aims to provide additional advice to help manage the risk.

During pandemics or outbreaks of disease, when infection can pass quickly between members of a call handling team who work near each other, the ability of staff to handle calls from home may be a practical step in managing a crisis

An increasing number of monitoring centre staff are likely to be carers, or they will have responsibilities that make it difficult for them to be away from home at work for most of the week; an opportunity to work at home on some days may be attractive to them. They may also be classed as vulnerable themselves and need to be "shielded", but this does not necessarily mean that they are unable to work.

Travel difficulties make home working a practical alternative to working from a set location, especially during holiday periods and at times of poor weather and road conditions are bad. Staff working from home can be more flexible in providing additional call handling capacity at times of peak demand.

Improvements in telecommunications infrastructure, virtual private networks and call handling platforms, have enabled home working to become a viable option for telecare monitoring centres. Some organisations are developing virtual call centres that allow home workers to handle all incoming calls. People with special counselling, clinical or language skills may increasingly work from home on an "on-call" basis.

Many responder and installation services already operate "on-call" functions by utilising home working, which can be extended to the normal working day, minimising the need to attend the office other than for specific reasons, such as to collect equipment.

Staff with physical disabilities may have excellent interpersonal skills enabling them to empathise with service users, but may be unable to travel to a monitoring centre on a daily basis, so home working becomes a convenient option for them.

Home workers may help service users to accept the use of national (or international) monitoring centres by providing some local knowledge and accents. The effects of working from home needs to be considered holistically, so that the home working environment does not adversely affect the health and well-being of staff, their families, or causes disruption for neighbours.

TSA has provided some specific guidance with regard to call handling services, which can be found below and has been revised, following learning from organisational experiences of offering TEC Services from home.

home_working_for_call_handlers_during_the_covid-19_crisis_v2.0_10th_november_2020.pdf
homeworking_checklist_template_13.11.20.docx

## Flexible Working

Flexible working is a way of working that suits employees needs and circumstances. It can be requested by any employee, not just disabled workers and carers and this is a legal entitlement, which is known as making a statutory application and is open to staff who have been in employment for more than 26 weeks.

Full details on the formal version of flexible working can be found here https://www.gov.uk/flexible-working but for the purposes of this document, we will discuss how flexible working can help organisations and teams during the Covid-19 pandemic, in an informal manner.

Home working is a type of flexible working, but others, some of which we are familiar with include:

- Job sharing – Where two people do one job and split the hours.
- Part time – Working less than full-time hours (usually by working fewer days).
- Compressed hours – Working full-time hours but over fewer days.
- Flexitime – The employee chooses when to start and end work (within agreed limits) but works certain 'core hours', for example 10am to 4pm every day.
- Annualised hours – The employee has to work a certain number of hours over the year but they have some flexibility about when they work. There are sometimes 'core hours' which the employee regularly works each week, and they work the rest of their hours flexibly or when there's extra demand at work.
- Staggered hours – The employee has different start, finish and break times from other workers.
- Phased retirement – Default retirement age has been phased out and older workers can choose when they want to retire. This means they can reduce their hours and work part time.
- Agency, or Bank Staff – A possible solution to finding additional resource, may be through establishing a relationship with an agency, or by creating a 'bank' of additional staff you can call upon at short notice.

Due to operational constraints, it is not always possible to provide flexible working and employers may still need to apply some levels of restriction, or control. For example, whilst flexible workers may be allowed to work whatever hours they choose, there may still be some core hours that require covering.

However, if you can achieve the right balance of operational requirements and worker preference, there are many potential benefits of flexible working. These can include:

- Reduction in staff turnover
- Increases productivity
- Can attract top talent
- Improved diversity
- Better employee engagement
- Reduce office-based cost's
- Can be an eco-friendly option

There are also challenges to flexible working, that need to be overcome. Employers need to consider and prepare for:

- Training requirements
- Supervision/management arrangements – it can be harder to keep track of what staff are doing
- Regular communication is vital
- ICT and data security implications
- Family member pressures

Covid-19 has changed the way we work and many organisations have stated that they will not go back to old, fully office based working practices. More flexible working options have proven to provide a balance for work and home life and have been very effective.

## Business Continuity and Safe Working – Good Practice Examples

We have seen that the establishment of an effective BCP is key to success in the current situation and the previous section will help with the preparation of this, but swift decisions with support from senior management, with buy-in from staff are essential.

Organisations have demonstrated they can act and react quickly and below are some examples that will support you in similar situations.

## TEC Monitoring Centres

We have already been informed by the Government, if staff can work from home, then they should. However, we understand that a lot of monitoring centres cannot provide home-working solutions and teams will need to attend the work location for this purpose.

In addition to the general guidance for staff working safely in work environment, TEC Monitoring Services may wish to consider taking the following additional precautions to help protect teams and assist with business continuity:

- Review call volumes and call flows and plan for the minimum number of staff required to be on site. It is possible that admin functions, or other non-call handling activities could be conducted from home.
- Where a partially replicated Disaster Recovery location is utilised, or where a reciprocal DR arrangement is in place, some organisations contracted with a second service, such as Tunstall, Eldercare, or others to provide an additional tier of DR, if the first layer could not be invoked.
- Obtain a personal computer keyboard and mouse for each member of staff. These can be easily exchanged as each member of staff finishes and takes over duty and is a low-cost safety measure.
- Where home working is employed for call handling, organisations will need to fully assess the technical requirements and licencing arrangements that will need to be put in place. Licences may be required for both monitoring platform and in-house ICT systems. Additional equipment, such as laptops and mobile phones will be required.
- Ensure the monitoring centre is cleaned more frequently (at the end of each shift) than other office spaces, due to the 24-hour nature of the call handling environment.
- Position Perspex screens between workstations, to limit the possibility of airborne virus contamination
- Where systems and premises allow, organisations may employ multiple site call handling. This may involve having the DR location active, at the same time as the main site, with both sites can have calls routed to them and can call handle simultaneously. This may be dependent on the monitoring platform and version currently in use.
- Identify areas where there is a likelihood of staff to congregate in groups and limit access to these areas.
- Identify situations where staff may pass things to each other, such as parcels, keys, equipment, or post an eliminate direct contact.
- Limit the access to the call handling area to operators only. Other members of staff, such as admin, managers and team leaders may be able to work from home, or separate parts of the building

- If the space and amount of equipment permits, rotate the use of computer workstations, so that some are left un-used on alternating shifts.
- Instruct staff to wear face masks over the nose and mouth when moving around the office.
- Call handling performance is an important aspect of Business Continuity. Whilst call volumes may increase and performance may drop below normal levels during a pandemic, continual monitoring of exception reports will help as part of you contingency planning and will help to identify if they are working, or need to be adjusted in some way.
- Where call volumes increase and where systems allow, it is useful to amend the customer reassurance message, to reflect the current wait information, to help manage customer expectations.
- Non-Emergency administrative calls (inbound and outbound), our outbound proactive calling that does not need to be completed from the Monitoring centre, could be redirected to other teams and offices.
- Ensure the correct Covid-19 Health and Safety signage is in place.
- Provide thermometers for personal temperature checks for staff prior to entering the Monitoring Centre
- You will need to make special arrangements for those you are classed a clinically vulnerable. Definitions of this can be found here.
- Consider splitting staff into dedicated teams where possible, to limit the cross flow of staff between operations.
- Create an Alarm Centre "bubble", which restricts staff entry to authorised personnel only
- Where possible, rotate home working and site working between staff. This will reduce the feeling of isolation for some home workers.
- Stagger shift start times, by 15, or 30 minutes, to limit the contact between operators at shift handover times.
- You may wish to consider more frequent "call quality checks" for home working, as supervision of call handling is more difficult.

## TEC Installation and Responder Services

Installation and Responder Services need special consideration during pandemics such as Covid-19, as they will have direct contact with service users, who will not only be vulnerable, but also likely to be more susceptible to the virus. In addition, the Installers and Responders themselves are likely to be at more risk of contracting the virus.

We saw in the early days of the pandemic, that quite a few services in this category were suspended because of the risk, but were later reinstated, as they can be conducted safely with the right protection methods put in place and the correct guidance is followed.

These services remain vital to many people and to partner organisations such as the Ambulance Service, where they realise the demand for ambulances would undoubtedly increase if responders were not in place.

Part of the TSA outreach programme has been to evaluate what additional measures organisations are putting in place, which enhance the disaster recovery and business continuity processes and also offer increased levels of protection.

Circumstances affecting installation and response teams are in the main quite similar to each other and some actions that organisations may be able to implement include:

- Introduce screening questions to check for Coronavirus, upon taking referral’s and before entry into properties to conduct installations.
- Responders conduct a Covid-19 assessment prior to entry into any properties
- Depending on risk level, it may be necessary to further assess installation and restrict installations to emergencies only.
- Where routine welfare visits are normally undertaken, it may be possible to change the process to conducting telephone check calls, or rotating the process over a period of days.
- Rotation of responder staff vehicles if possible. If the pool of vehicles is large enough, it may be possible to rotate the use of vehicles after cleaning, to further reduce the possible presence of the virus.
- It may be possible to utilise vehicles from other departments, such as the maintenance department, or hire additional vehicles to increase the overall numbers available
- As with office areas, more frequent deep cleaning and decontamination of vehicles is advised
- Can staff use their own personal vehicles to conduct their duties, rather than company vehicles? This would mean checking that the correct vehicle insurance is in place by the employee and would incur mileage costs.
- Segregate clean/contaminated equipment for delivery and collection – both at storage locations and in vehicles to avoid any cross contamination
- Provide secure, local outfield storage units – not at head office. These can be re-stocked as and when required, but would reduce the need for mobile staff to attend a central location.
- Implement, or increase the use of “self-installation” models. Details can be found on the TSA website on the link below. Where this has been employed, it may be prudent to do follow-up inspections of the installation, when the pandemic permits.
- Greater use of new, more easily deployed equipment. For example:
    - OwnFone – Footprint
    - Oysta – Mobile GPS device
    - MindMe – Mobile GPS device
    - Pebbell – Mobile GPS device
    - Chiptech – GO mobile and the EVA alarm unit with voice guided self-installation to minimise physical contact
    - Tunstall Healthcare – has developed the Tunstall+ app to support roll out of the Smart Hub and is also launching two apps, MyCareTrack and Carechat which enable client connections without the need for a standards compliant alarm hub in the home.
    - Legrand – Reach IP alarm units can be sent out pre-programmed to provide a “no contact” installation
- Organisations should follow the TSA and Government guidance on the use of the correct levels of PPE and Infection Prevention and Control
- Ask any non-essentials people on-site to leave the room when installing equipment, or responding to an incident
- If the above is not possible, try to maintain 2m distance between people
- Ensure supply chain of alarms and options for repairs of equipment is robust and that suppliers have sufficient stock levels
- Research alternative supplier options to widen the choice of equipment available – this may mean working with the procurement department to ensure that this is facilitated and that no internal procurement rules are breached within the organisation.

TSA has produced some additional resources that will help in this area. You will find the links below:

- Specialized Group Living, Installation & Maintenance of TEC
- Infection Control & TEC Equipment Decontamination during COVID-19
- Pandemic Escalation Guidance for Monitoring & Responder Services
- An Introductory Guide to Installing TEC Equipment
- A Guide to providing a self-Installation service
- An Introductory Guide to Responding

## Social Distancing

Social distancing means keeping people apart, both in the workplace, as well as in a social environment, to help reduce the spread of the Coronavirus. Wherever possible, you should keep metres apart from each other.

Although the social distancing rules put in place by the devolved Governments may differ, the following advice is provided by the Health and Safety Executive, who regulate in all of the home nations.

Some of the measures you can put in place include:

- Mark out work areas with highly coloured floor tape
- Provide signage to remind staff and visitors of the distancing rules
- Move work layouts, so that staff work side by side, rather than opposite each other
- Limit the movement of people around the work areas:
- If possible, rotate between jobs and equipment (if they do not have their own equipment for individual use)
- The use of vehicles and lift's
- In high people traffic areas, such as kitchens, reception areas, walkways, corridors, or office access turnstiles
- Prevent any non-essential trips within buildings, or between work sites
- Introduce an electronic booking systems for desks, or workstations to help manage their use and record staff movements.

As in all situations with Covid-19, you should check the public health guidance for the country you are in:

- Wales
- England
- Scotland
- Northern Ireland

If staff are unable to socially distance, you should consider the following:

- Can the activity be done from home?
- Can the activity be suspended for the time being, until alternative arrangements can be made?
- Reduce the numbers of staff working closely to the minimum
- Limit movement around the work area concerned
- Limit the amount of different equipment, or surfaces that workers need to touch
- Provide screens between staff, to create a physical barrier, which should be cleaned regularly

Detailed guidance for most situations can be found on the HSE website.

## Government Test and Trace Systems

The Government has introduced this service to help return life more to normal, in a way that is safe and protects our health and social care. The service allows them to trace the spread of the virus and isolate new infections and play a vital role in giving an early warning if the virus is increasing again, locally, or nationally.

Details of the Test and Trace services for each country and how to get the app can be found here:

- England – Test and Trace
- Scotland – Test and Protect
- Wales – Test, Trace, Protect
- Northern Ireland – Stop Covid NI

(*Note: There are some specific workplace scenarios when you should pause the contact tracing feature. These are:*

1. *when you are working behind a Perspex (or equivalent) screen*
2. if you are putting your phone in storage, such as in a work locker, and it will not be on your person
3. if you are a health or care worker practising infection prevention and control (IPC) working in a clinical setting.)

For further workplace advice about the government test and trace services, please see the following links:

- in England, see NHS Test and Trace workplace guidance on GOV.UK
- in Scotland, see Test and Protect advice for employers on GOV.SCOT
- in Wales, see Test, trace, protect advice for employers on GOV.WALES

## Post pandemic Playbook

So, what are organisations thinking about now that we are starting to see the full operational impact of the pandemic on services. We have seen successful rapid implantation of new working practices and technologies, but how do stabilise this process?

It is important that the hard lessons we have learnt during Covid-19 are not lost and that organisations continue to plan.

A post-pandemic playbook is a return-to-business plan for how your business will function once the COVID-19 lockdowns are lifted. A good playbook considers:

- Employee needs (leaders, communication, HR),
- Your workplace (health and safety in the office),
- The new landscape of the TEC industry

Those forward-thinking organisations are already planning to/for:

- Capitalise on the lessons learnt – new marketing strategies, use of digital marketing and the use of new technology
- Make remote working a longer-term success. This will mean revisiting essential areas such as technology provision, home working risk assessments, supervision and training etc.
- New leadership models. We need to shift to dynamic, effective leadership models that may require retraining at the management level.

- Reinforce Business Continuity Plans
- Think about organisational structures, roles and staffing profiles
- Move toward more automated services if possible
- With a higher dependence on technology, reinforcement of cyber security
- Re-cast ICT into a new cost profile
- Re-think digital transformation plans
- Cloud based ICT services
- New and additional technologies need to be budgeted for.
- Inflation is likely to increase in 2021 and we *may* see an increase in other forms taxation.
- Consider service redesign for LEAN operations
- Introduce new models of service – a move to Proactive and Preventive service offerings
- Reinforce, or restructure the supply chain
- Understand what will we now demand from our technology?
- Explore new models of engagement with customers and staff
- Reskilling of existing staff, or new talent acquisition
- Become a learning organisation
- Plan for future pandemics

Essentially, a post-pandemic plan is needed now. If your organisation has not begun planning, you should consider taking the first steps as soon as possible.

The following five guidelines are essential for a successful post-pandemic playbook. Consider each carefully as you construct your plan.

1. Set people as your priority. The health and safety of your employees, service users and customers should come first.
2. Define your business destination. Build a guideline and vision for a successful recovery. Without clear objectives, it is hard to plan ahead.
3. Outline realistic outcomes. Consider who are your stakeholders in this process.
4. Safely test your approaches. Perhaps look for evolution, rather than revolution.
5. Look what your peers are doing. Learn from the successes and failures of others in the sector and create a flexible plan.

All organisations have an opportunity to reshape and rebuild for the future. Many are already re-writing their processes and procedures in preparation.

## Appendix 'A' – Business Continuity Planning Checklist

| Planning Activity | | Outcome | By Whom? | Status |
|---|---|---|---|---|
| **1.** | **General Activities** | | | |
| **1.1.** | Assign responsible person for planning and preparation at senior executive Level | | | |
| **1.2.** | Appoint planning team members, with defined roles from a range of organisational stakeholders | | | |
| **1.3.** | Identify the scope of responsibility and critical activities to be undertaken by the group | | | |
| **1.4.** | Plan for review of Government and TSA guidance, along with receipt of pandemic alerts and develop a dissemination plan | | | |
| **1.5.** | Consult with the workforce, via staff, or staff representatives if in place | | | |
| **1.6.** | Conduct consultation with key suppliers on their contingency plans to ensure continuity of supply chain | | | |
| **1.7.** | Identify and consult with key systems providers | | | |
| **1.8.** | Conduct Business Impact Assessment | | | |
| **1.9.** | Adapt the Business Continuity Plan | | | |
| **1.10.** | Adopt a process to implement the changes identified to the BCP | | | |
| **1.11.** | Test the BCP if time permits through desktop, or simulated exercises | | | |
| **1.12.** | Amend the BCP resulting from any weaknesses identified during tests | | | |
| **1.13.** | Share best practice with other, similar organisations if possible | | | |
| **1.14.** | Review the BCP routinely during the pandemic | | | |
| **1.15.** | Establish trigger points, or alerts that my lead to invocation of the company's response plan | | | |
| **1.16.** | Understand what you will need to do, should a member of staff become infected and who has been within the workplace. | | | |

| 2. | Operational Activities | | | |
|---|---|---|---|---|
| 2.1. | Conduct a process mapping exercise, to identify all the critical operational activities, which includes the employees required to fulfil them | | | |
| 2.2. | Plan for the possible impact of employee absence | | | |
| 2.3. | Identify all key service and equipment providers | | | |
| 2.4. | Assess and plan for the impact of disruption to the supply chain, both in the UK and abroad if applicable | | | |
| 2.5. | Examine the impact of the pandemic on your service users and customer's requirements | | | |
| 2.6. | Assess the business need for any face-to-face meetings and plan for remote working, if not already in place | | | |
| 2.7. | Plan for limited travel arrangements | | | |
| 2.8. | Consider any financial arrangements necessary during the pandemic. This could include: Invoicing, payments, authorised signatories, overdraft arrangements, spending limits etc. | | | |
| 2.9. | Assess the extent to which other customers will be dependent on your services, or products and make necessary arrangements | | | |
| 2.10. | Agree the circumstances under which you may decide to suspend, or scale back your services, or product supply. | | | |

| 3. | Additional Measures to Support Continuity | | | |
|---|---|---|---|---|
| 3.1. | Identify business critical personnel and appoint deputies | | | |
| 3.2. | Identify and plan for special requirements for staff with specific health needs, or other vulnerabilities | | | |
| 3.3. | Identify alternative workforce resources | | | |
| 3.4. | Establish rapid training plans for extended workforce | | | |
| 3.5. | Establish a communication plan and provide regular communication updates to Service User's, Customer's and staff, in a manner appropriate to the current state of the pandemic | | | |

| | | | | |
|---|---|---|---|---|
| 3.6. | Ensure that communication is culturally and linguistically appropriate to the current situation | | | |
| 3.7. | Ensure that staff are informed of your pandemic preparedness and response plan | | | |
| 3.8. | Prepare an emergency communication plan and revise periodically throughout the pandemic | | | |
| 3.9. | Plan for increased uptake of staff welfare, or counselling services | | | |
| 3.10. | Appoint a specific officer that staff members can talk to about any concerns they have | | | |
| 3.11. | Review policies for sickness absence, compassionate leave and associated remuneration levels. Review the information provided by the Government in this area regularly. | | | |
| 3.12. | Review and implement amended travel policies | | | |
| 3.13. | Implement Home Working Policies and Practices, which should include the sourcing of additional equipment, such as laptops etc. | | | |
| 3.14. | Plan for changes to interaction with your service users, commissioners, or customers | | | |
| 3.15. | Review business Indemnity Insurance requirements. This could include suitability and indemnity levels. | | | |
| 3.16. | Research pandemic planning in your regions and localities of operation, for example via regional resilience teams and local resilience forums. | | | |

| 4. | Workplace and Workforce Risks | | | |
|---|---|---|---|---|
| 4.1. | Refer to Government and TSA Guidance on Infection Prevention and Control | | | |
| 4.2. | Prepare policies on hygienic behaviour of staff and workforce teams | | | |

|  |  |  |  |  |
|---|---|---|---|---|
| **4.3.** | Plan for frequent and effective cleaning of equipment, company vehicles and workplace locations as guided by national recommendations |  |  |  |
| **4.4.** | Provide sufficient and accessible means for reducing the spread of infection, through hand washing and office sanitisation |  |  |  |
| **4.5.** | Consider creating a policy on access to medical treatment for staff |  |  |  |
| **4.6.** | Disseminate regular updates on the pandemic to staff |  |  |  |
| **4.7.** | Create environments that limit face-to-face contact with service users, customers, or suppliers |  |  |  |
| **4.8.** | Where possible, introduce methodologies for home-working and flexible working practices. See TSA Guidance |  |  |  |
|  |  |  |  |  |
|  | *Organisations can add their own checklist items as necessary.* |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix ‘B’ – A Basic Business Continuity Plan Template

| | |
|---|---|
| Organisation Name | |
| Address | |
| Version Number | |
| Responsible Person | |

## Table of Contents

## Glossary of Terms

| | |
|---|---|
| | |
| | |
| Note: Continue table as necessary | |

## Scope of the BCP

Define the scope and aim of your business continuity plan.

| |
|---|
| |
| |
| |

## Goals, Objective's and Outcomes

List the goals, objective's and desired outcomes of the plan.

| |
|---|
| |
| |
| |

## Key Operational Functions

Information listed here is used to recover essential business process. Information should include key process, IT systems, and data backups.

| |
|---|
| |
| |
| |

## BCP Planning and Action Team

List the roles and names of the action team members.

| Role | Name/Title |
|---|---|
| Planning & Action Team Leader | TBA |
| Etc. | |
| Etc. | |

## Business Impact Analysis

| |
|---|
| |
| |
| |

## Recovery Priorities

Define and list your business recovery priorities.

| |
|---|
| |
| |
| |

## Recovery Teams

| Team Roles: | Team Responsibilities: | Team Contact Details: |
|---|---|---|
| | | |

## Recovery Plan

Define the activities needed to allow your business to continue.  Include a list of recovery tasks.

## IT & Communication Systems and Resources

List the IT and communication systems and resources needed for your recovery plan.

## Maintenance Protocols

## Indemnity and Insurance Information

## Employee Contact List

| Name | Telephone Numbers |
|---|---|
| | |

## Supplier Contact List

| Name | Contact Details |
|---|---|

## Partner/Stakeholder Contact List

| Name | Contact Details |
|---|---|

## Alternative Operating Locations

| Addresses | Facilities Available |
|---|---|
| | |
| | |

## Appendix ‘C’ – Simple Disaster Recovery Report Template

| | |
|---|---|
| Organisation Name | |
| Address of Incident | |
| Date of Incident | |
| Time of Incident | |
| Time Incident Resolved | |

| |
|---|
| Description of Incident |
| |
| Activities Undertaken by Staff Involved to |
| |
| Outcome of the Incident |
| |
| Recommendations for Further Action |
| |
| Changes Required to BCP |
| |

| | |
|---|---|
| Date Senior Management Informed | |
| Improvement Plan Approved Date | |
| Date Improvement Plan Completed | |