Ministry of Justice

HM Prison & Probation Service

Policy Name: HMPPS Business Continuity and Resilience Policy Framework

Re-Issue Date: 06 March 2023 **Implementation Date**: 03 July 2019

Replaces the following documents (e.g., PSIs, PSOs, Custodial Service Specs) which are hereby cancelled: Business Continuity Policy Framework 2019

Introduces amendments to the following documents: N/A

Action required by:

☒	HMPPS HQ	☒	Governors
☒	Public Sector Prisons	☒	Heads of Group
☒	Contracted Prisons	☒	Youth Custody Estate
☒	Women's Estate	☒	Probation Service Delivery Units
☒	Approved Premises	☒	Probation Service Interventions
☒	Regional / HQ Probation Directorates	☒	

HMPPS Directors/Governors must ensure that any new local policies that they develop because of this Policy Framework are compliant with relevant legislation, including the Public-Sector Equality Duty (Equality Act, 2010).

Mandatory Actions: All groups referenced above must adhere to the requirements section of this Policy Framework, which contains all mandatory actions.

Audit/monitoring: Assurance by HMPPS National BC&R Team

Resource impact: *Given that this new framework does not introduce any significant additional duties for staff, we believe there will not be any appreciable impact in terms of demands on staff, and that it will not be necessary to fund any additional staff as a result.*

Contact: BC&R@justice.gov.uk

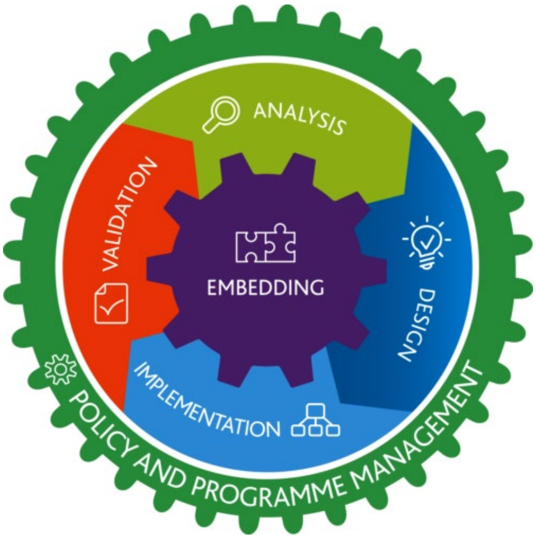
Deputy/Group Director sign-off: Andy Rogers, Deputy Director

Approved by OPS for publication: Sarah Coccia (Executive Director Prisons) and Ian Barrow (Executive Director Probation), Joint Chairs, Operational Policy Sub-board

Revisions

Date	Changes
March 2023	• We have simplified the process. • Created one national policy with several annexes but only one required for annual review and completion per site. • Included a guidance document for completion of the annual return. • Provided templates for incident reporting, exercises and lessons learnt logs. • Removed the need for a separate BC establishment risk register. • Removed the self-compliance return requirement. • Increased support visits. • Arranged Regional workshops to embed Business Continuity across HMPPS, raising awareness and understanding.

Contents



1. Purpose

1.1 Business continuity (BC) is about having a plan to deal with demanding situations, so HMPPS can
continue to function with as little disruption as possible to the delivery of our core business

1.2 The Business Continuity and Resilience Framework sets out a process and assured procedures that guide and prompt HMPPS to **respond, recover, resume, and restore** to a pre-defined level of operation following disruption. Business Continuity plans are the contingencies on which we depend to guide us through exposure to a range of threats to delivery of business as usual. We use this process to control and prepare our response to a range of potential triggers and to mitigate the impacts on our day-to-day delivery of critical activities.

1.3 This policy framework sets out the arrangements necessary to ensure Business Continuity Management (BCM) across our organisation is performed in accordance with the International Standard for Business Continuity Management (ISO) 22301 as required by Cabinet Office. All providers of HMPPS services, including privately operated establishments are required to produce and maintain Business Continuity Plans (BCPs). BCPs will ensure critical business activities and / or locations remain operational during major incidents/crisis. A prompt and efficient recovery of “business as usual” activities must take place in the event of an incident or other disruption affecting premises or resources, including staff and information.

1.4 The Business Continuity Management (BCM) lifecycle above shows the stages HMPPS will move through annually to improve organisational resilience. At the core of the lifecycle is the need to embed business continuity within the day to day practice of HMPPS.

1.5 This policy framework is designed to address the five-core business continuity (BC) risks to our organisation:

- Management of staff
- Building premises
- Data and information technology (IT) infrastructure
- Utilities
- Third-party suppliers

In addition to the five core risks, we must also analyse and prepare for the following:

- Seasonal Illness preparedness

- Fuel Shortage
- National Power Outage (NPO)

1.6 The HMPPS Business Continuity and Resilience Team actively horizon scan to anticipate future risks that could impact on the delivery of our core business. The team operate on behalf of OneHMPPS to recognise and control known risks and build capability to respond to unpredictable threats. The team also write national level continuity plans in conjunction with wider Government and ensure our organisation has the foundations in place to respond to nationally and internationally impacting events when necessary.

1.7 This policy framework provides guidance for HMPPS leaders to follow when preparing for a range of credible and incredible interruptions to business continuity. It sets standards that all leaders are expected adhere to and provides the playbook for all organisational preparedness and response work. In following this policy framework, leaders with responsibility for delivery across HMPPS will be supported to respond to and recover from unforeseen interruptions to our core business and return to a 'business as usual' state in a planned, controlled, and timely manner. This will be achieved through a combination of risk assessment activity, resilience planning, incident management and development of contingency arrangements.

2. Evidence

2.1 A simple test of an organisation's crisis management response is whether the narrative surrounding the crisis becomes focused on how the leadership has failed, rather than how well (or badly) the situation is being handled. Although it may be true that the outcome of an incident is outside the control of HMPPS, how the response is handled is certainly within our control.

2.2 The public's confidence in our ability to safely manage prisons is closely tied to our corporate image; this is equally true of other government departments and public organisations. One of the keyways HMPPS will be judged by the public is how long it takes until we are prepared to acknowledge that a crisis exists and how quickly we respond. Disruptive incidents are, by their very nature, infrequent and unpredictable events. There is the potential for a lack of experience in dealing with them, which introduces the risk that our staff lack confidence in what they should do in such a situation.

2.3 For this reason, HMPPS invests heavily in building resilience and preparedness for crisis, to ensure that the potential confusion and lack of information associated with interruptions to business continuity are overcome quickly and operational resilience is restored. It is important that our response techniques are well-understood and rehearsed. HMPPS response to situations is well developed and rehearsed, and we have effective systems and processes in place to ensure that interruptions to operational delivery are appropriately escalated, communicated, and managed. We are well practised at briefing senior stakeholders internally and across Government as individual situations evolve and there is a high degree of confidence in our ability to quickly restore business as usual.

2.4 Although each individual situation is unique, prior planning and adherence to the Business Continuity Framework, create a solid foundation for effective response and enable us to build back better and stronger defences to future situational threats.

2.5 The business continuity profession continues to evolve as its value is recognised by a wider audience. The world in 2022 continues to be challenged by socio-economic and geo-political change. Organizations must respond and adapt to familiar challenges such as the increasing dominance of technology and the internet, as well as new disruptive threats arising from the globalisation of terrorism and the rapid increase in cyber threats. In this demanding environment, the discipline of business continuity is increasingly relevant.

The ongoing demand for global guidance in the discipline is demonstrated by the adoption and wider acceptance of the international standard for business continuity management (ISO 22301:2012) by organizations worldwide, and the publication of related standards, for example, the Business Impact Analysis (BIA) ISO/TS 22317:2015. The increasing awareness of the importance of enhancing organizational resilience reinforces the value of building effective business continuity capabilities and is central to the purpose of the Business Continuity Institution.

2.6 Business continuity is the key discipline that sits at the heart of building and improving the resilience of organizations. It is a tried and tested methodology that an organisation should adopt as part of its overall approach to managing risks and threats. Business continuity management identifies an organisation's priorities and prepares solutions to address disruptive threats. This understanding supports the design and implementation of plans to protect and continue the value creating operations of an organization in the event of any disruption. An effective business continuity programme supports the strategic objectives of the organisation and pro-actively builds the capability to continue business operations in the event of disruption. The programme includes the identification of risks and threats, the creation of response structures and plans to address incidents and crises and promotes validation and continuous improvement. The programme is flexible to changes in the internal and external operating environment and delivers measurable value to the organisation. Business continuity is relevant and applicable to all industry sectors and organizations regardless of size, complexity, type, and location.

3. Definition

3.1 **Business Continuity** is the capability of an organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident

3.2 **Business Resilience** builds on the principles of business continuity but extends much further to help enhance our ability to tackle challenges, fend off potential risks and bounce back more quickly.

The state of business resilience has been described as the ability of an organisation to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper."

3.3 A Business continuity event can emerge as a threat to staff, safety, buildings, or the organisational structure of the business that requires a level of intervention to be taken to restore normal operations.

3.4 There are countless different threats and circumstances that could lead to a breakdown in business continuity. In HMPPS operating environment we have assessed that the impact on the business is likely to involve one of, or a combination of the following drivers, which will vary in their degree of impact.

- Damage to, or loss of access to parts of the physical estate that are essential to operations because of
  - Environmental threats: flooding, storm, or other severe weather conditions.
  - Acts of offender/civil disruption or terrorism either aimed directly at locations or occurring in the surrounding area.
  - Fire or contagion affecting the location or nearby buildings
- Staff shortages because of
  - Industrial action by staff
  - Severe transport disruption
  - Serious outbreak of a contagious illness
  - Inability of staff to attend workplace owing to environmental factors (flood/severe weather)
- Loss of utilities

  - Electricity, heating, cooling, gas for cooking or water supply
  - Limited power supply for electric vehicles
- Loss of communications
  - Failure of IT systems
  - Damage to, or unavailability of paper records
  - Failure of telephony
- Business Continuity incidents affecting third party suppliers
  - Financial or contractual difficulties
  - Supply chain disruption
- Seasonal illness preparedness
  - Outbreak control
- Fuel Shortages
  - Lack of supply for generator
  - Lack of fuel available for staff
  - Differing types of fuel for vehicles (petrol, diesel, red diesel, electric)

4. <u>Outcomes</u>

4.1 BCM processes will be embedded across HMPPS and demonstrated through evidenced and effective:

- Identification of potential local and national threats/risks to our core business
- Strategic and tactical level planning to deal with these eventualities should they materialise
- Completion of the Business Continuity Document by locations and business units. These must be reviewed annually and submitted via the BC & R functional mailbox, 'BC&R@justice.gov.uk'
- Building of local, regional, and national capability in ways of working strengthen Business Continuity and Resilience
- Exercising, maintenance, and review of plans at local and national level
- Aligned Business Continuity processes and delivery across OneHMPPS
- Compliance with this policy framework across HMPPS and privately operated establishments
- Development of national Business Continuity plans for critical risks impacting all core business across HMPPS
- Communication of emerging risks / threats to our core business
- Sharing of best practice and lessons learned

5. <u>Roles & Responsibilities</u>

5.1 <u>HMPPS Business Continuity and Resilience Team</u>

- Act as a national support for all business continuity matters and provide 24/7 business continuity support and guidance in the management of (BC) incidents via out of hours on-call processes

To provide support for Prison Gold Command for all serious Business Continuity incidents

- Act as a national resource for co-ordinating, mentoring and sharing of good practice to support HMPPS locations and business units in achieving compliance with this policy framework

- To undertake a qualitative and quantitative assurance programme to provide assurance via the Directorate of Security Management to HMPPS, MoJ and Cabinet Office
- Work with the MoJ Business Continuity team as a pivotal point of contact for HMPPS
- Work with the MoJ Departmental Operations Centre to ensure HMPPS are at the forefront of managing emerging risks via both risk analysis and exercising of national plans
- Maintain regular engagement with senior management across OneHMPPS, keeping them informed of emerging risks and the work being developed by the team to mitigate those risks
- Maintain OneHMPPS Agency level Business Continuity Risk Register
- Ensure accurate details of all Business Continuity leads across OneHMPPS is maintained
- Support OneHMPPS in the development of the Business Continuity document at local level – this includes all prison establishments, probation delivery units, approved premises, interventions, NTRG/NTDSG and all HQ functions
- Provide post- incident business continuity support across OneHMPPS
- To develop an extensive resource of Business Continuity desktop exercises to assure robust Business Continuity planning across OneHMPPS
- To develop national level Business Continuity plans for OneHMPPS for all critical risks to our core business
- To support Business Continuity leads across OneHMPPS with the delivery of Business Continuity exercises
- To develop and maintain an online resource for communication across OneHMPPS via the new Intranet
- Represent OneHMPPS at cross government working groups and business continuity related exercises
- To deliver a rolling programme of workshops across OneHMPPS to embed Business Continuity into the core business of OneHMPPS

5.2 **Role of HQ directorates**

- All HMPPS HQ teams are required to build their BC plans on the newly procured MoJ Business Continuity database which can be found by following the link https://mojbusinesscontinuity.continuity2.com
- This will be monitored by the MoJ and HMPPS National BCRT (Business Continuity and Resilience Team)
- Training and user log in details for Business Continuity leads across HMPPS HQ teams can be arranged by contacting the MoJ Business Continuity team at CorporateBusinessContinuityTeam@justice.gov.uk

5.3 **Role of the Prison Group Director's (PGD), Deputy Directors, and Heads of Corporate Services**

- To nominate a regional lead to have oversight of Business Continuity within their group and ensure they are aware of these responsibilities
- To act as a conduit between the HMPPS BC&R Team and the respective prison and probation regions
- To ensure HMPPS BC&R Team are informed of any staff movements amongst Business Continuity leads
- To develop Prison Group Directorate / Probation Regional BCPs where appropriate
- To ensure all BCPs across Prison Group Directorates and Probation regions are maintained and exercised as outlined in this framework

5.4 **HMPPS Governors/ Controllers and Regional Probation Directors**

- HMPPS Governors/ RPDs must ensure all staff are made aware of this framework
- Staff must be given the opportunity to contribute towards the business continuity process, and made aware of the relevant BCPs
- HMPPS Governor/ RPDs must ensure that all prison establishments (including privately operated establishments), PDUs (Probation Delivery Units), APs (Approved Premises), regional and HQ sites have a nominated Business Continuity Lead. The Business Continuity leads must ensure their Business Continuity documentation is agreed, published, and maintained in accordance with this policy framework
- For Business Continuity Plans to remain effective they must be regularly reviewed and tested. Staff with responsibility for maintaining BCPs must review and test their plans annually. At least one risk/scenario must be tested every 12 months as a minimum by means of a desktop exercise to ensure that they meet the requirements of this policy framework – the HMPPS BC&R Team can be utilised to facilitate exercises
- HMPPS Governors/ RPDs must ensure that completed Business Continuity documentation is returned annually to HMPPS BC&R team using the functional mailbox, BC&R@justice.gov.uk
- Functions that share building premises must ensure that their requirements are included in the Business Continuity documentation for their location
- Risks identified within Business Continuity documentation must be incorporated into local risk registers which should be regularly reviewed, and actions must be taken to minimise risks where possible. The national HMPPS BC&R team should be informed of identified risks

5.5 **Local Business Continuity leads**

- Complete the Business Continuity documentation for their HMPPS locations and business units and ensure they are reviewed least annually or following an incident or exercise
- Test at least one local BCP annually as a minimum
- Ensure the HMPPS BC&R Team have up-to-date contact details
- Submit copies of the completed Business Continuity documentation to the HMPPS BC&R Team annually to BC&R@justice.gov.uk
- All Business Continuity Leads must ensure that effective links are made with Local Resilience Forums (LRF) and the HMPPS BC&R Team
- Ensure lessons learned from local level tests or implemented plans are shared with the HMPPS BC&R Team
- Notify HMPPS BC&R team of any Business Continuity related issues that may affect HMPPS locations and business units and submit a detailed Incident Reporting Form (IRF) to the functional mailbox at BC&R@justice.gov.uk within 3 working days of the incident occurring
- Ensure identified local Business Continuity Risks are incorporated into local risk registers, are reviewed regularly, actions are taken to minimise the risk and the HMPPS BC&R team are informed of and updated on the status of identified risk

6. **Business Continuity Documentation to be completed by each site/regional/team SPOC (Single Point of Contact)**

Detailed supplementary guidance is available on the Intranet to support the development of business continuity documentation across OneHMPPS

The Business Continuity documentation consists of the following tabs:

6.1 Key Contacts and Locations/ Functions

Individuals to be contacted in the event of a Business Continuity incident must be identified for all locations and business units. Individual functions staffing requirements and all non-standard working arrangements must be included

6.2 Communication & Activation

This gives a flow chart of how the plan will be activated in response to an incident causing significant disruption to normal service/business particularly the delivery of critical functions/ activities. A member of the nominated Business Continuity team will normally activate and stand down the plans.

All those required to be contacted on activation of the plan(s) should be detailed. The nature of the communication will be dependent on the type of incident and the time of occurrence. It is necessary to differentiate between those who must always be informed of an incident, and those who will only need to be contacted dependant on type of incident.

6.3 Business Impact Assessment (BIA)

6.3.1 All HMPPS locations and business units must complete the BIA/BCP section of the document. This takes into consideration their critical functions/ activities that will need to continue during Business Continuity incidents or disruption. It is necessary for all locations and business units to assess their critical functions / activities and ensure these are stipulated in the document. The BIA is a risk assessment to analyse the impact specific Business Continuity risks may have on the delivery of critical functions/activities.

6.3.2 The 7 key Business Continuity risks to consider are:

- Loss of/ or loss of access to premises
- Staff shortages
- Loss of communications
- Loss of utilities
- Business Continuity incident affecting third-party suppliers
- Seasonal illness preparedness (pandemic)
- Fuel Shortages

6.3.3 A section for ‘Additional Risks’ is included on the document for specific risks that are not listed above but need to be considered for specific locations and business units i.e., flood risk.

6.3.4 The BIA considers both the products and services that an organisation delivers as well as the processes, activities and dependencies tat ensure the delivery of these products and services. The level of detail to which activities need to be analysed may depend on their complexity.

6.4 Business Continuity Plans (BCP)

The aim of a BCP is to ensure the location or business unit has in place documented plans that detail how they will manage a Business Continuity incident, maintain, and recover its critical functions/ activities to an acceptable level. The plans should be easily accessible and contain clear instructions to follow in the event of an incident.

Each plan must consider:

- Specific strategies or mitigations to ensure the critical functions or activities identified in the BIA are delivered to an acceptable level

- Details of actions and tasks that need to be performed
- Details of the resources required
- Details of Business Continuity arrangements for staff, prisoners, and people on probation with specific educational or physical requirements
- Prioritised objectives in terms of the critical functions/ activities to be recovered, the timescales in which they are to be recovered and the recovery levels needed for critical functions/ activities

6.5 Decision Log & Outcomes

All Business Continuity incidents must be recorded on the decision log with the date/type of the incident that occurred, details of decisions made, outcomes and lessons learnt from each incident.

7.0 BC Incident reporting

7.1 The HMPPS Business Continuity team must be notified of any Business Continuity related issues that may affect HMPPS locations and business units and submit a detailed Incident Reporting Form (IRF) to the functional mailbox at BC&R@justice.gov.uk within 3 working days of the incident occurring. This report can be found in Annex G of this policy

7.2 These incidents are monitored and reported to the MoJ Corporate Business Continuity team and Cabinet office by the HMPPS Business Continuity Team. The HMPPS Business Continuity Team will complete a quality assurance check and then forward to the MoJ Business Continuity team within 3 working days of receipt.

8.0 Validation & Assurance

8.1 At least one risk/scenario identified in each plan must be tested annually as a minimum through exercising. This process tests the completeness of the plans and enables an assessment of:

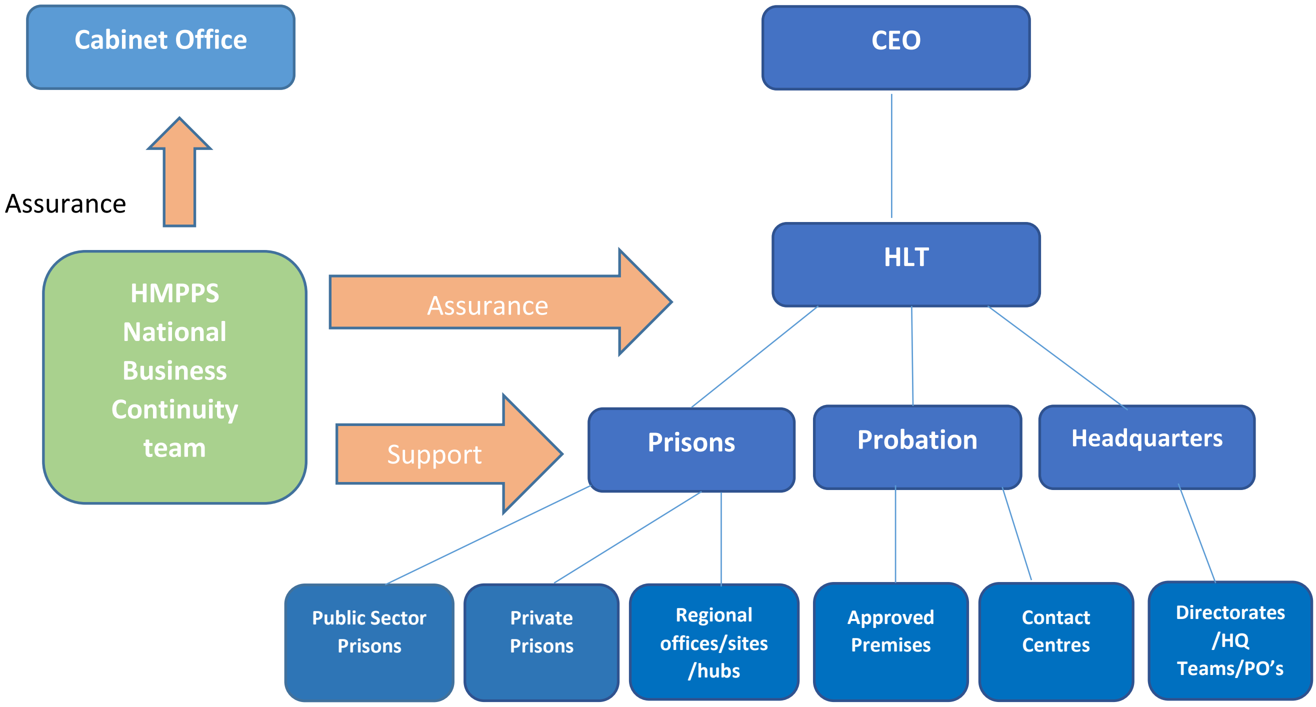
- Staff preparedness and awareness
- Awareness, responsiveness, and effectiveness of external parties
- Appropriate allocation of staff and key resources
- Plan effectiveness

8.2 Careful consideration should be given to ensure exercises are communicated to all those that may be affected or present. It is essential that any disruption caused by an exercise is minimal and anticipated.

8.3 The Business Continuity documentation must be reviewed annually, following an exercise and/or BC incident.

8.4 Debrief sessions must be held following an exercise and lessons learnt log completed. The log must provide an overview of the exercise with agreed actions and lessons learnt.

8.5 The log must be submitted to the HMPPS Business Continuity Team to facilitate the sharing of good practices across HMPPS. A copy of this information must be retained a locally.



8.6 To embed Business Continuity across the organisation, the HMPPS Business Continuity team will provide support across the organisation, including Headquarters functions, to ensure compliance against the Policy Framework.

8.7 **Assurance from Sites/Regions**

8.7.1 The HMPPS Business Continuity team will provide regional workshops to Business Continuity leads across the estate with the aim of embedding Business Continuity across the organisation and attaining quantitative assurance from the regional level.

8.7.2 The HMPPS Business Continuity team will obtain assurance through annual Business Continuity documentation returns and site visits. The team will visit sites/regions to offer support and guidance to obtain assurance of policy compliance. These visits will be conducted on a rolling cycle.

8.7.3 Assurance will be provided to the Directorate of Security SMT (Senior Management Team) by the HMPPS National Business Continuity Team as required.

8.8 **Qualitative Assurance**

8.8.1 The HMPPS National Business Continuity Team will develop a rolling validation programme to provide qualitative assurance. This will include support and assistance for sites/regions to conduct exercises to validate the quality and resilience of their plans.

8.8.2 The validation programme will also assist in raising awareness of Business Continuity throughout HMPPS via lessons learned communications.

9. Annexes

Annex A	BIA/BCP template to be used by Prison establishments https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1098962/Annex_A_-_BIA_-_BC_Template_-_Prisons.ods
Annex B	BIA/BCP template to be used by Probation Delivery Units https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1098964/Annex_B_-_BIA-BCP_Template_Probation_Delivery_Unit.ods
Annex C	BIA/BCP template to be used by Probation Approved Premises (AP) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1098967/Annex_C_-_BIA-BCP_Template_-_Approved_Premises_Template.ods
Annex D	BIA/BCP template to be used by Regional offices/sites/Hubs https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1098968/Annex_D_-_BIA-BC_Template_-_Regional_Offices_-Sites_-_Hubs.ods
Annex E	BIA/BCP Template – Probation - UPW /Programmes /other Functions https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1098969/Annex_E_BIA-BCP_Template_-_UPW_-_Programmes_-_Other_functions.ods
Annex F	Supplementary Guidance for completion of Annex A-D BC documentation https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1098970/Annex_F_-_Supplementary_Guidance_to_aide_completion_of_BIA-BCP_templates.odt
Annex G	Business Continuity Incident Reporting Form https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1098971/Annex_G_-_BC_Incident_Report_Form_.odt
Annex H	Exercise Plan template https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1098972/Annex_H_-_Exercise_Plan_template.odt
Annex I	Lessons Learnt Log template https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1098973/Annex_I_-_Lessons_Learnt_log_template.odt