Cabinet Office

epc

EPC BC Checklist

This document aims to provide the resilience community with an overview of key considerations for business continuity, referencing an array of key guidance including amongst others; the ISO22301, BS65000, BCI Good Practice Guidelines (GPG) and the Cabinet Office National Resilience Standards (NRS). Although the latter provides guidance for the multi-agency LRFs, they include universal principles that can assist practitioners.

RESILIENCE APPROACH

☑ Does your organisation take a resilience approach? Is business continuity effectively incorporated into the risk management, health and safety and facilities management processes to name a few examples as cited in **BS65000**? Is your organisation working collaboratively internally and externally?

ROLES AND RESPONSIBILITIES

☑ Have BC roles been identified? This could include strategic leads; BC advisor / coordinator; loggist; incident management team members; priority service leads; key workers? Are these groups aware of their roles and responsibilities and the command and control structures?

COMPETENCIES

☑ What skills and behaviours are required? Has your organisation got a competency framework identifying the different groups with a BC role and required skillset they need? Have they had sufficient training and experience? If not, what resources can be used to mitigate this gap and what is the leadership commitment from top management? (**ISO22301; ISO22330; BCI GPG**)

MONITORING & EVALUATION

☑ How is the impact of this incident is being monitored? Is your BC response tied into trusted and key guidance so that informed decisions can be made? Additionally, how is the effectiveness of solutions and strategies stated in your business continuity plans being measured? (**ISO22301: clause 9**)

COMMUNICATION

☑ Having procedures to communicate internally and externally to interested parties such as staff, customers, suppliers and the public, is a crucial part of BCM (**clause 8.4.3, ISO22301**). Do you already have a communications plan or have things been pulled together dynamically? If so, can a simple procedure be documented? How will your organisation work with the media?

DECISION MAKING

☑ Does your organisation have an agreed decision-making methodology and governance structure for BC? Are roles and authorities identified and awareness made?
JESIP provides a model (the **Joint Decision Model** or JDM) for making decisions that can be utilised for multi-agency response or at organisational level and incorporates considerations of legislation and obligations, find out more on JESIP https://www.jesip.org.uk/home

RECORD KEEPING

Is BC information documented including plans, procedures, roles and competencies? Are decisions, actions and rationale effectively recorded?
As per **ISO22301, clause 7.5**, documented information is a key aspect of business continuity management. This also links to the principles of **NRS for 'LRF Governance and Support Arrangements'**.

PEOPLE AND WELFARE

People support strategies and communication are continuous activities throughout a disruptive event – unlike many other aspects which are organised in line with the scale of the event (**ISO22330: People Aspects of Business Continuity'**). How is your organisation supporting the people it is formed from? Are these procedures incorporated into your BCMS documentation and committed to by top management? (**Clause 8.4.4, ISO22301**).

SUPPLY CHAIN

How are you assessing and mitigating supply chain risks or disruptions? Is business continuity effectively incorporated into contracting and procurement disciplines? This incident is supply chain focused, and a collaborative approach supported by top management (**ISO22318: Guidelines for supply chain continuity**) can ensure have the best approach to resilience.

INFORMATION MANAGEMENT AND SECURITY

If you have a large number of personnel working remotely, how is the organisation maintaining good information security and cyber risk awareness? Work collaboratively with your information security leads to ensure a sufficient approach. **NCSC** have released guidance to support home working: https://www.ncsc.gov.uk/guidance/home-working The **NRS for Cyber Incident Preparedness** also sites how resilience can be upheld via the LRF platform.

STAND DOWN

Do your plans include a process for standing the response down? Who makes this decision and what are the deciding factors? (**Clause 8.4.4.3, ISO22301**)

RECOVERY

Has your organisation considered recovery yet? Current decisions could undermine recovery so it is important consider it now even if the forward look isn't fully known. Effective consideration of recovery can even lead to innovation of current processes, organisations, communities and behaviours, which is in keeping with 'Continual Improvement' in **clause 10.2, ISO22301** and also 'Innovation' in **BS65000**. The **NRS for Local Recovery Management** includes under leading practice, a consideration of cultural complexities, vulnerabilities and local risks.

MAINTENANCE OF THE BCMS

How long will it be before we need to consider the upkeep of our BCMS as per the BCM Lifecycle (**BCI GPG**)? For example, consider whether the outcomes of your last BIA review are still accurate, or whether there were other priorities that should be incorporated? Robust arrangements for validation feature as part of **NRS for Business Continuity Management** under 'good practice' so how are the lessons learned from this incident going to be taken forward at organisational and LRF levels?