

EUROPEAN
COMMISSION

COMMISSION RECOMMENDATION

on operational continuity and stress testing guidelines for national contact points within the Union Civil Protection Mechanism

COMMISSION RECOMMENDATION

on operational continuity and stress testing guidelines for national contact points within the Union Civil Protection Mechanism

THE EUROPEAN COMMISSION,

Having regard to Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism, and in particular Article 7 thereof,

Whereas:

(1) Under Article 196(1), point (b), of the Treaty on the Functioning of the European Union (TFEU), the Union is to promote swift, effective operational cooperation within the Union between national civil protection services.

(2) The Union has a supporting competence in the field of civil protection, as stipulated in point (f) of Article 6 of TFEU.

(3) The Union Civil Protection Mechanism (UCPM), established by Decision No 1313/2013/EU of the European Parliament and of the Council[1], aims to strengthen cooperation between the Union and the Member States and facilitate coordination in the field of civil protection in order to improve the effectiveness of systems for preventing, preparing for and responding to natural and man-made disasters.

(4) The Union has witnessed several highly disruptive events in recent years, notably the consequences of the COVID-19 pandemic, Russia's war of aggression against Ukraine, the major IT disruption in 2024, Storm Éowyn in Ireland in January 2025, and the 2025 blackout in the Iberian Peninsula. Disruptive events may prevent or delay the functioning of civil protection systems, which should remain operational 24 hours a day and 7 days a week ('24/7').

(5) Article 7 of Decision No 1313/2013/EU stipulates that the Emergency Response Coordination Centre (ERCC) shall ensure a 24/7 operational capacity and serve the Member States and the Commission in pursuit of the objectives of the UCPM. Article 3 of Commission Implementing Decision (EU) 2025/704[2] further specifies that each Member State is to designate a national contact point (NCP) for the ERCC that is available 24/7.

(6) Commission Recommendation of 8 February 2023 on Union disaster resilience goals[3] calls upon the ERCC and civil protection authorities in the Member States and UCPM participating States, within their respective mandates, to reinforce their business

---

[1] Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

[2] Commission Implementing Decision (EU) 2025/704 of 10 April 2025 laying down rules for the implementation of Decision No 1313/2013/EU of the European Parliament and of the Council on a Union Civil Protection Mechanism and repealing Commission Implementing Decisions 2014/762/EU and (EU) 2019/1310 (OJ L, 2025/704, 15.4.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/704/oj).

[3] OJ C 56, 15.2.2023, pp. 1–11

continuity planning capabilities. It also specifies that the UCPM "should support the conduct of stress tests to test business continuity of emergency operations centres and work with Member States on the follow-up of lessons learned and recommendations". The stress testing of the emergency operation centres across Europe served as the flagship initiative of Goal number 5, titled *"*Ensuring a robust civil protection system", as outlined in the Commission Communication on the European Union Disaster Resilience Goals[4].

(7) Those efforts align with other frameworks that aim to strengthen resilience, including the European Preparedness Union Strategy[5] and NATO's baseline requirements for national resilience[6]. Specifically, Action 51 of the Strategy calls for the adoption of "guidelines for the 'stress testing' of emergency response and crisis centres across the EU".

(8) In that context, it is necessary to focus on the operational continuity of the UCPM NCPs and to increase their resilience, so that they can remain operational during disruptive events, by reinforcing their operational continuity plans and practices through systematic evaluation and stress testing.

(9) Moreover, response capacities that could be made available for intervention upon request through the UCPM may not belong to the NCP's authority. Securing communication with the entities managing those capacities during disruptions is essential for the operational continuity of the UCPM.

(10) Arrangements for ensuring continuity can easily go unnoticed until a disruption occurs. Such disruptions do not necessarily stem from major crisis or emergencies, but may result from minor incidents or from neglected or suboptimal conditions. To ensure informed decision-making on preventive and mitigation measures, the operational continuity planning for the NCP requires the identification of potential causes of disruptions affecting the NCP's essential functions[7]. Additionally, staff working in 24/7 shifts face unique psychosocial and wellbeing challenges, including health problems resulting from night shifts, work-related stress, and separation from family. If unaddressed, these issues can contribute to burnout, high turnover and potential staff shortages.

(11) Operational continuity arrangements should remain effective regardless of the nature or cause of the disruption, whether resulting from natural hazards, accidents, technical failures, human error, infrastructure or utility outages, large-scale staff unavailability, intentional or malicious actions, including cyber incidents and hybrid activities, or any other cause.

(12) By preparing for potential disruptions, NCPs increase their ability to respond swiftly and effectively, minimising the duration and impact of disruptive events. That preparation not only ensures that operations can restart within an acceptable timeframe

---

4 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'European Union Disaster Resilience Goals: Acting together to deal with future emergencies', 8.2.2023, COM(2023) 61 final.

5 Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Preparedness Union Strategy, 26.3.2025, JOIN(2025) 130 final.

6 Commitment to enhance resilience, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016.

7 Examples include software updates, uncommunicated changes to the corporate email domain, uncommunicated updates of contact details, persistent staff shortages, or the simultaneous retirement of a large portion of essential staff, whose replacement cannot begin until the retirement date.

but also limits negative consequences for stakeholders and external actors that depend on the NCP's activity and safeguards the organisation's mission and reputation.

(13) Disruptions originating from cyber incidents have distinctive characteristics that deserve special attention; unlike other threats to operational continuity, they may be intentional, can propagate across interconnected systems, and may compromise the integrity or confidentiality of data and communications, not just their availability.

(14) Regular training, exercises and updates are fundamental to an effective operational continuity programme. The more frequently an operational continuity plan is practiced, the better prepared the organisation becomes, as exercises help identify gaps and familiarise staff with procedures. Well-trained personnel, with a clear understanding of their roles and responsibilities, perform more effectively during disruptions. Similarly, involving stakeholders in exercises ensures that they understand communication protocols and know what to expect during real disruptive events.

(15) Exercises, stress tests and real incidents provide valuable lessons. To ensure that the operational continuity plan remains valid, it should be regularly updated to incorporate lessons learned from training, exercises, stress tests, real events, and technological advancements.

(16) Where the NCP is part of an entity that falls within the scope of applicable provisions of Directive (EU) 2022/2555[8], the lessons learned from the stress test should be taken into account when implementing cybersecurity risk-management measures, in particular with regard to business continuity, backup management, disaster recovery, and crisis management.

(17) Ensuring the operational continuity of the civil protection national competent authority goes beyond the functioning of its NCP. Therefore, this Recommendation may also serve as a valuable reference for the development of operational continuity within national organisations and civil protection systems, in accordance with recital 7 of Decision No 1313/2013/EU.

(18) This Recommendation should be comprehensive, reflecting the diversity of NCP structures and functions across Member States and UCPM participating States. It should be applied flexibly and adapted to each NCP's mandate, context, circumstances, and operational framework, given that each NCP has distinct characteristics, operates within a different legal framework, and faces different challenges, which may require tailored approaches to ensure operational continuity.

(19) This Recommendation is based on the outcome of consultations with the Commission Expert Group on 24/7 Operational Continuity in Disruptive Events, established by the Commission in 2025, and should be complementary to existing well-established standards and guidelines related to business continuity[9].

---

[8] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, pp. 80–152

[9] International standards: ISO 22301:2019 (Business Continuity Management Systems); FEMA's Federal Continuity Directive 1 (2017), Federal Continuity Directive 2 (2017), Continuity Guidance Circular (2018, 2024 update), Business Process Analysis and Business Impact Analysis User Guide (2019); and the Good Practice Guidelines (2018) from the Business Continuity Institute

HAS ADOPTED THIS RECOMMENDATION:

1. ADDRESSEES

This Recommendation is addressed to national competent authorities of the Member States and UCPM participating States.

Member States may find it relevant for other national crisis centres and entities managing UCPM capacities.

2. DEFINITIONS

For the purposes of this Recommendation, the following definitions apply:

(a) **'national competent authority'** means an authority appointed by a Member State or a UCPM participating State[10] within the framework of the UCPM, as referred to in Article 29 of Decision No 1313/2013/EU;

(b) **'national contact point' (NCP)** means a contact point for the ERCC in a Member State or in a UCPM participating State that is available 24 hours a day and 7 days a week, designated in accordance with Article 9(7) of Decision No 1313/2013/EU and Article 3(1) of Implementing Decision (EU) 2025/704;

(c) **'essential functions'** means the activities, operations or services of the NCP that are fundamental to the fulfilment of its mandate and mission and either cannot be interrupted or must be resumed within a short, predefined timeframe. For the purposes of these guidelines, whether a function is classified as essential shall be determined by the urgency with which it must be restored following disruption, and not solely by its strategic, operational or institutional importance. Accordingly, functions of strategic, operational or institutional importance that can withstand disruption or extended delay without unacceptable impact shall not be regarded as essential functions;

(d) **'essential staff'** means personnel working in the NCP who carry out or support essential functions, personnel who are part of the team responsible for managing or responding to a disruptive event, or personnel who fulfil both roles;

(e) **'scarce essential staff'** means essential staff whose small number constitutes a vulnerability to operational continuity in the event of their absence or unavailability to work, because they possess the certifications, security clearance, authority, decision-making responsibility, access rights, knowledge, expertise or language skills required to carry out specific activities necessary to ensure the continuity of an essential function;

(f) **'staff bottleneck'** means a situation in which the continuity of an essential function depends on the availability of one or more staff members of scarce essential staff;

(g) **'operational continuity'** means the capacity of a NCP to maintain its essential functions working – encompassing activities, operations or services – when the resources necessary to those functions, such as essential staff, incoming information, services, products, supplies, budgetary provisions, equipment,

[10] On participating States, see Article 28 of Decision 1313/2013/EU.

information and communications technology (ICT) systems or location requirements, become unavailable, damaged, unusable or interrupted;

(h) '**operational continuity plan**' or '**plan**' means either a single document or a collection of procedures for the operational continuity of the NCP;

(i) **'disruptive event'** means an incident or circumstance that prevents or substantially delays the execution of an essential function of the NCP.

(j) '**recovery'** refers to the restoration of the NCP's operational capabilities, facilities, systems and resources following a disruption.

3. RECOMMENDATIONS FOR OPERATIONAL CONTINUITY OF NCPS

3.1. Key recommendations

1. The NCP should develop a coherent and comprehensive operational continuity plan or a documented set of procedures covering all elements of operational continuity. Section 3. 2 contains further recommendations on the operational continuity plan.

2. The objective of operational continuity planning is to ensure that the NCP can fulfil its essential functions under degraded conditions when disruptive events occur. As such, operational continuity planning should assume that disruptive events will occur and that normal operating conditions may not be restored immediately or, in some cases, may not be restored at all. The NCP should be capable of maintaining essential functions under degraded conditions by using alternative procedures, alternative facilities, alternative communication channels and reduced resources until full capability is restored.

3. During disruptive events, resources should be prioritised towards sustaining the essential functions of the NCP. This may imply that non-essential functions may not be maintained.

4. Operational continuity arrangements should ensure the uninterrupted collection, analysis, validation and dissemination of the operational information necessary to maintain the NCP's situational awareness and support decision-making throughout the disruption.

5. Trained personnel are the main resource for ensuring operational continuity. While the operational continuity plan, associated arrangements and backup measures support continuity, it ultimately depends on staff being able to make decisions and apply these measures under pressure.

6. Operational continuity planning should be based on a thorough understanding of the administrative and operational arrangements of the organisation to which the NCP belongs. To achieve this, collaboration across departments should be actively promoted and facilitated.

7. The NCP should assess potential sources of disruptions to its activities. The focus of the assessment should be on their disruptive potential for the NCP's activities and on developing a response plan to ensure continuity of essential functions.

8. When assessing threats to operational continuity, special attention should be given to time-sensitive processes and bottlenecks, including:

   (a) single sources of information or information known only by a limited group of people, including classified information;

(b) unique equipment or unique service providers on which essential functions depend;

(c) single communication channels, contact persons or decision-makers;

(d) availability of scarce essential staff.

9. Bottlenecks in staff, facilities, communications, ICT systems, logistics and decision-making should be identified and removed. Where unavoidable, appropriate prevention and mitigation measures should be established and tested, including those suggested in Section 3.9.

10. Every disruption, exercise and stress test should identify lessons and lead to improvements in operational continuity arrangements, strengthening resilience over time.

11. For the purpose of operational continuity and stress testing for NCPs within the UCPM, the following non-exhaustive categories of disruptive events should be considered. Annex I provides a description of each category.

(a) unavailability of premises;

(b) disruption of electricity supply;

(c) disruption or failure of ICT systems;

(d) large scale staff absence or absence of scarce essential staff.

12. The NCP should ensure its ability to continue operating in the event of one or more of the continuity triggers listed in paragraph 11 above.

3.2. Operational continuity plan of the NCP

13. Each NCP should develop a coherent, comprehensive and written operational continuity plan, or an equivalent documented set of procedures, covering all elements of operational continuity and integrating and systematising the response to disruptions, including mitigation measures and agreements for immediate intervention.

14. The operational continuity plan should provide alternative arrangements for all essential processes, especially time-sensitive ones, ensuring that they can continue if primary resources fail. Backup and alternative arrangements should be fully independent. They should not rely on the same resources, such as the same building, power source, communication route, ICT platform or service provider. They should also not create new dependencies that could introduce further risks of disruption.

15. The operational continuity plan should be exercised regularly under realistic conditions. Plans that have not been validated through training, exercises or stress tests should not be considered operational. The operational continuity programme should include regular mandatory training for essential staff; regular testing and exercises involving the activation of the plan, and its systematic review and update, ensuring that all concerned staff and stakeholders are aware of and trained on the updates.

16. Depending on the organisation's structure, the NCP should involve in the development of the operational continuity plan personnel who are not directly involved in essential functions but who have the expertise or knowledge needed to support an overall understanding of the organisation's functions.

17. NCPs should consider designating, within their organisation, a continuity coordination function dedicated to the operational continuity plan. Depending on the size and structure of the NCP, the continuity coordination function should be exercised by a single coordinator, by a dedicated team bringing together representatives of the relevant operational areas, or through other arrangements adapted to the national context. Where a group is constituted, it should include members with expertise in the operational areas relevant to the implementation of the plan, such as ICT systems, alternative premises, human resources or logistics. The role of the continuity coordination function should be to ensure the consistent implementation, periodic review and updating of the operational continuity plan, including the verification of resources and arrangements on which the plan relies.

3.3. Identification of essential functions

18. The NCP should identify its essential functions and establish and maintain an inventory of them. In addition to the UCPM-related functions, such as managing requests for assistance and offering and deploying UCPM response capacities, the NCP may also need to ensure continuity of other essential functions for the organisation. Examples include coordinating with national or regional authorities, liaising with other international organisations, issuing public warnings, and supporting higher-level decision-making.

    For each essential function, the NCP should establish operational performance objectives defining the maximum acceptable degradation of services during disruptive events. Such objectives should include, where appropriate, the maximum tolerable period of disruption, recovery time objectives, acceptable loss of operational information, minimum staffing levels, communication availability and decision-making capability. These objectives should guide the design of the operational continuity plan and form the basis for evaluating stress tests performance. Annex II contains examples of operational performance objectives.

19. It is advisable to rank essential functions according to their priority or the urgency with which they must be resumed.

3.4. Business Process Analysis and backup resources

20. Based on the inventory of essential functions, the NCP should conduct a Business Process Analysis (BPA) and develop backup solutions to ensure continuity of its essential functions. The BPA should include a comprehensive understanding of how functions operate, by determining, for each function:

    (a) the tasks that compose the function;

    (b) the timing and sequence of tasks, including duration, and time-sensitive steps;

    (c) who performs what task, including the required profile, expertise or training;

    (d) the flow of information, including how data, requests, and outputs move between actors and systems;

    (e) who validates or authorises the process(es);

    (f) what resources are employed and what inputs from external actors are necessary, including information, datasets, services, products, supplies, budgetary provisions, equipment, ICT systems and location requirements, such as private companies supplying energy or providing security services. Special

attention should be paid to the classification level of the information, as well as the rooms and devices used to manage it;

(g) what outputs result from the function, including information, specific products or services, or coordination, validation or authorisation actions;

(h) which external organisation(s) or stakeholder groups receive the output(s);

(i) what dependencies and interdependencies exist that are essential for operations, including relationships and agreements with external actors – other Member States' and UCPM participating States' authorities, civil protection partners, essential infrastructure operators, service providers, suppliers, etc. – specifying the expected input or output;

(j) what backup resources and alternative arrangements are available.

21. When conducting their Business Process Analysis, NCPs are invited to take into account the table in Annex III.

3.5. Recommended practices for alternative facilities and equipment

22. The NCP should ensure its capacity to continue operating when its premises become temporarily inaccessible or unusable, including ensuring the availability of key equipment.

23. Primary and alternative facilities and temporary solutions should be secure and have an appropriate classification level. This should be proportionate to the nature of the crises addressed and the sensitivity or classification of the information being handled.

3.6. Recommended practices for electricity supply

24. The NCP should ensure its capacity to continue operating in the event of local outages or widespread blackouts.

25. Primary and alternative facilities, including temporary facilities, should have electricity supply arrangements that are resilient and have backup systems, so that the NCP can continue to operate and provide its essential functions during long power outages.

26. The measures set out for NCPs should be implemented, where relevant, in a manner that is consistent with national electricity risk-preparedness plans established under Regulation (EU) 2019/941[11] and national preventive action plans and emergency plans established under the Security of Gas Supply Regulation (EU) 2017/1938[12], as well as with existing national crisis-management arrangements.

3.7. Recommended practices for ICT systems

27. The NCP should ensure that the ICT systems supporting its essential functions are reliable and resilient. Special attention should be placed on:

(a) continuity of access to databases, documents, and emails, including the availability of updated contacts lists, continuity of communication with the

[11] Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, OJ L 158, 14.6.2019, pp. 1–21

[12] Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010, OJ L 280 28.10.2017, p. 1

ERCC and Member States and UCPM participating States, and continuity of processing and management systems for information collection and monitoring and the recording of actions taken;

(b) technology integration, by ensuring the compatibility and interoperability of essential systems with remote set-ups and alternative locations, including the capability of those locations to connect to the Common Emergency Communication and Information System (CECIS) and to handle classified information when operating remotely; such arrangements should be verified through appropriate testing;

(c) security of information and communications, including the possibility of establishing classified connections and exchanging classified communications both at national and international level.

(d) records of all third-party suppliers of the devices and software used in the NCP.

28. Particular attention should be given to cyber incidents as a distinct category of ICT disruption. The NCP should consider establishing coordination protocols with the national cybersecurity authority, as part of its broader operational continuity arrangements. Such measures should include early warning channels, joint incident response protocols, and the clarification of roles during a cyber incident affecting the NCP.

3.8. Recommended practices for human resources

29. The NCP should ensure that it has sufficient personnel to remain operational in situations of reduced staff availability and that its personnel have the necessary profiles and skills.

30. The NCP should consider the following:

(a) ensuring the availability of staff with the appropriate skills and background, including crisis management experience and, where applicable, the security clearance required to handle classified information. It should develop and implement mechanisms for verifying professional competencies and provide comprehensive onboarding and continuous training programmes to maintain and strengthen staff skills, ensuring that staff are fully prepared to respond effectively to UCPM activations. Training should also cover the prevention of disruptions caused by human error or malicious action, including essential cybersecurity and information security awareness, such as the risk posed by social engineering.

(b) providing regular training to keep staff updated on operational continuity arrangements and on the use of equipment and ICT systems in main and alternative locations. It should explore additional training for NCP staff in managing long-term disasters and crises and in UCPM operations.

(c) developing plans to ensure staff rotation during long-lasting emergencies, including the management of surge capacity. It should set up working groups with clear roles and succession plans to improve coordination during crises.

(d) establishing transport arrangements so as to ensure that essential staff are able to reach the location at which they are required to carry out their duties, where relevant, whether at the primary site, an alternative site or a mobile unit.

(e) putting in place appropriate safeguards to ensure the protection of personnel's health and safety.

(f) developing staff welfare plans covering food, water, lodging, access to NCP facilities and psychological support to help staff handle stress and fatigue. Such plans should provide for prolonged operations in confined environments and take into account the individual or personal circumstances of essential staff, including family-related needs where relevant.

(g) establishing data protection and privacy policies to ensure that continuity planning complies with the protection of personal data during and after incidents.

31. Essential functions should be supported by appropriate operational continuity arrangements, structured and systematic cross-training, and regular exercises, so that they can be carried out by several trained personnel avoiding staff bottlenecks.. No single essential function should depend exclusively on the availability of one staff member.

3.9. Prevention and mitigation measures for each category of disruptive event

32. The following section provides an indicative list of recommended prevention and mitigation measures for each category of disruptive event. While these can be implemented in parallel, each Member State should select the most appropriate and effective options based on its NCP's mandate, context, circumstances, capacity, the structure of its operational and legal framework, and the potential causes of disruptions that could affect its NCP's essential functions. The list is not meant to be applied in full simultaneously, as, in some cases, the implementation of one measure could conflict with the application of another measure or require excessive investment.

33. Recommended prevention and mitigation measures to address unavailability of premises:

(a) geographical distribution of the NCP into two or more geographically separate centres that operate simultaneously, providing mutual backup and overflow support for one another.

(b) relocation to alternative premises managed by the NCP's authority

(c) pre-arranged transport for essential staff to alternative premises (including in adverse weather conditions)

(d) remote work (involving flexibility of tasks that might be performed outside the physical location of the NCP).

(e) mobile command and control units that could temporarily host the essential staff from the NCP.

(f) activation of administrative arrangements with other authorities to use their premises

(g) devolution

34. Recommended prevention and mitigation measures to address disruption of electricity supply:

(a) activation of generators and Uninterruptible Power Supplies (UPSs).

(b) priority fuel supply arrangements and agreements with providers.

(c) energy autonomy and alternative energy sources for essential functions.

(d) maximising available power capacity.

(e) relocation to alternative premises managed by the NCP's authority with guaranteed electricity supply

(f) remote work from a building with guaranteed electricity supply

(g) mobile command and control units that are self-sufficient in terms of electricity

(h) activation of administrative arrangements with other authorities to use their premises with guaranteed electricity supply

(i) devolution

35. Recommended prevention and mitigation measures to address disruption or failure of ICT systems:

(a) redundancy

(b) regular and secure data backups, including off-site and offline copies

(c) alternative ICT systems, platforms and communication channels

(d) emergency ICT support teams or on-call technical response units

(e) cyber incident response procedures coordinated with the national cybersecurity authority.

(f) offline copies of essential contact lists, key procedures and operational documents

(g) mobile command and control units with access to primary and backup ICT systems

(h) relocation to alternative premises managed by the NCP's authority with access to primary and backup ICT systems

(i) activation of administrative arrangements with other authorities to use their premises with access to ICT systems

36. Recommended prevention and mitigation measures to address large-scale staff absence and absence of scarce essential staff:

(a) overtime management (short-term solution)

(b) reassigning tasks to available staff

(c) a pre-identified pool of trained personnel from within the institution, available on short notice

(d) prioritising staff recruitment

(e) investing in essential staff retention

(f) supporting the families of essential staff

(g) preventing staff bottlenecks by delegating authority and promoting shared leadership

37. Annex IV provides technical guidance for the implementation of each of the measures listed.

3.10. Continuity of operations in the case of UCPM activations

38. To enhance UCPM operations and ensure continuity, the following actions are recommended:

(a) Where the country has access to the Trans European Services for Telematics between Administrations (TESTA) or TESTA-EIRIS (TESTA successor), identify the country's national TESTA Coordinator. Ensure that the country's CECIS Contact Point has the contact details of the country's national TESTA Coordinator and that such details stay updated. Ensure that the country's CECIS Contact Point understands the operational continuity plan of its local/national access to the in-country TESTA gateway.

(b) Develop protocols to distinguish between failures in the TESTA connectivity and failures in the CECIS platform when requesting assistance through the UCPM, and to enable requests for assistance in the event of a TESTA disruption in the NCP's country.

(c) Where appropriate, explore arrangements for mutual operational support with other national authorities to ensure that the NCP can continue performing its essential functions if a disruption significantly degrades the NCP's operational continuity capacity. In particular, such arrangements should involve authorities with access to TESTA, so that the NCP can access CECIS from alternative premises.

(d) Where appropriate, explore the possibility of establishing bilateral administrative arrangements for mutual operational support with neighbouring countries that are Member States or participating States in the UCPM, in situations where a disruption significantly degrades the NCP's operational continuity capacity and the arrangements referred to in point (b) are not possible. Such arrangements should allow the NCP to use those countries' premises and access the TESTA network.

(e) Provide training on CECIS to new staff and schedule regular exercises for personnel.

(f) Based on the national civil protection structure, the continuity plan should include arrangements to ensure seamless communications between the NCP and other relevant authorities which, if necessary, are authorised to request the activation of the UCPM.

(g) The operational continuity plan should consider those national stakeholders that own and manage UCPM resources that do not belong to the NCP's authority but could be made available for intervention upon request through the UCPM.

39. The operational continuity plan should be aligned with the Commission Recommendation of 29 November 2024 on EU Host Nation Support Guidelines[13], specifically regarding UCPM activations by the NCP and its role in Host Nation Support[14].

---

13 C(2024) 8339.

14 Host nation support is defined in Article 4, point (9), of Decision No 1313/2013/EU as any action undertaken in the preparedness and response phases by the country receiving or sending assistance, or by the Commission, to remove foreseeable obstacles to international assistance offered through the

3.11. Activation of the operational continuity plan

40. Depending on the nature and scale of the disruption, the NCP operational continuity plan should define different activation levels, including a partial activation, where the NCP continues operating from its main premises under adapted procedures, and a full activation, which requires relocation to alternative premises or other alternative arrangements.

41. The criteria, activation levels and triggers, as well as the authority empowered to authorise activation, should be defined at national level, in line with each NCP's structure and operational framework. An illustrative example of an activation flow is provided in Annex V.

42. Activation procedures should enable the timely activation of continuity arrangements in response to both actual and anticipated disruptions, including events occurring outside normal working hours and events for which advance warning is available.

43. In the event that an incident disrupts the operational continuity of the NCP, triggering the activation of its operational continuity plan, the NCP should consider notifying the ERCC.

3.12. Training, exercises and regular testing

44. Operational continuity plans should be regularly trained, exercised and tested. It is recommended to schedule regular awareness and information sessions as well as training sessions and exercises related to continuity plans. Other regular training, such as onboarding training for new personnel, should also incorporate the necessary elements of the operational continuity plan. The participation of external stakeholders who could be affected by a disruption in the NCP's activities should also be considered in regular targeted awareness and information sessions, as well as in exercises.

45. At a minimum, the operational continuity plan should be tested annually. More frequent testing should be considered where justified by the NCP's structure, operational context or risk profile.

3.13. Recovery

46. Once the negative effects of the disruptive event have been mitigated, the NCP should treat the gradual return to normal operations as a distinct phase of operational continuity: recovery is the phase in which the NCP transitions from the operational continuity arrangements back to normal operations, including the resumption of important (but non- essential) functions that may have been temporarily suspended.

47. The operational continuity plan should define the conditions for initiating recovery, identify the authority empowered to authorise the transition, and specify the steps required to return safely to normal operations.

48. The following points should be considered in the recovery phase:

(a) *Verification of conditions for recovery*. Before transitioning, the NCP should consider whether the underlying disruptive event has been resolved or sufficiently mitigated; whether the primary premises, ICT systems and communication channels are fully operational again; and whether the integrity of databases and documents has been verified. Particular attention should be

---

Union Mechanism. It includes support from Member States to facilitate the transit of this assistance through their territory.

paid to data replicated during the disruption, to avoid losing information generated while operational continuity arrangements were in place.

(b) *Phased transition of essential functions*. Essential functions should not be transferred back at once. The NCP should consider transferring them in reverse order of priority, starting with those for which a brief interruption during the transition is most tolerable, while maintaining top-priority functions under the continuity arrangements until the normal environment is confirmed to be stable. Parallel operation should be used during the transition to reduce the risk of cascading failure.

(c) *Resumption of important functions*. Non-essential functions that were temporarily suspended during the disruption should be resumed only once essential functions are confirmed stable under normal arrangements. The order and pace of resumption should be adjusted to staff availability, recognising that operational continuity arrangements often increase workload and staff fatigue.

(d) *Check for additional vulnerabilities*. The NCP should check that operational continuity arrangements have not introduced additional vulnerabilities before returning to normal operations.

49. NCPs should also carry out the following activities:

(a) *Post-event debriefing.* To help identify what worked and what did not, the NCP should schedule a debriefing involving all staff categories that participated in the response.

(b) *After-action documentation.* The NCP should produce a structured after-action document that summarises the sequence of events, the activation of operational continuity arrangements, the performance of essential functions, the gaps observed, and the lessons identified.

(c) *Integration of lessons identified into the operational continuity plan.* After each disruptive event that triggers activation of the operational continuity plan, the NCP should set a defined timeframe for updating the plan, so that identified lessons are incorporated before they fade from operational memory. The NCP should therefore establish a process for tracking identified deficiencies and corrective actions, and for re-testing the updated measures as appropriate. Where relevant, lessons identified should also be translated into improvements to the NCP's normal activities.

3.14. Communication strategy

50. Efficient management of disruptive events involves communication, and each NCP should develop a solid communication strategy that acknowledges the NCP's responsibilities for general communication and for crisis communication. This strategy should guide the NCP's decisions and actions on information sharing during disruptions, ensuring that all involved or affected parties receive the necessary information and, where applicable, are able to act accordingly, thereby helping to protect the organisation's reputation and maintain trust. Annex VI contains suggested points to be considered by the NCP when developing a solid communication strategy.

4. RECOMMENDATIONS FOR ORGANISING AND CONDUCTING A STRESS TEST

51. The Commission recommends stress testing of NCPs in the UCPM. This section provides guidance on how to design and evaluate a stress test.

4.1. Purpose and objectives

52. The purpose of the stress test should be to assess the capacity of the NCP to continue performing its essential functions under disruptive conditions. To that end, the stress test should take the form of a limited-scale exercise designed to evaluate existing arrangements for operational continuity and the performance of targeted essential functions of the NCP under disruptive conditions, including by testing both primary and alternative resources.

53. The stress test should pursue the following general objectives:

(a) reviewing, updating and validating the operational continuity plan, as well as assessing operational continuity-related expertise, equipment and arrangements of the NCP;

(b) improving understanding of priorities and constraints and changing perceptions in relation to operational continuity of the NCP;

(c) identifying weaknesses, gaps, bottlenecks and dependencies as well as opportunities for improvement in the operational continuity plan, and in resources sustaining essential functions, related training, equipment and arrangements of the NCP;

(d) assessing the ability of NCP essential staff at various levels, including management, to perform their roles and responsibilities;

(e) assessing co-ordination and communication within the organisation and with external partners under disruptive conditions;

54. When planning the stress test, it is recommended to formulate specific objectives for the stress test that are measurable and aligned with the essential functions to be tested.

55. The stress test should not aim to identify threats that could trigger incidents capable of disrupting the normal functioning of the NCP.

4.2. Scope

56. The scope of the stress test should identify the following:

(a) the specific objectives of the stress test;

(b) the essential functions to be evaluated;

(c) the nature and duration of the disruption affecting continuity of operations;

(d) the resources involved, including staff members and their roles, premises, equipment and ICT systems;

(e) the degree of involvement of external stakeholders.

4.3. Scenario

57. A scenario-based approach should cover the consequences of incidents (triggers) that may cause disruption of operations and therefore activate the operational continuity plan of the NCP. It is recommended to exercise different scenarios and vary their

complexity, thereby preparing the organisation for a range of possible outcomes. It should be ensured that the scenarios are challenging but realistic, so as to provide meaningful insights into the effectiveness of the operational continuity plan. Annex VII provides two examples of scenarios.

58. NCPs are recommended to use the following non-exhaustive list of triggers for the activation of the NCP operational continuity plan: unavailability of premises (1), disruption of electricity supply (2), disruption or failure of ICT systems (3) and large-scale staff absence and absence of scarce essential staff (4).

(a) *Trigger 1: Unavailability of premises*. The building housing the NCP has suffered physical damage, is unreachable or has been evacuated. These circumstances render it unusable for an indefinite period of time.

(b) *Trigger 2: Disruption of electricity supply*. A failure in the electricity network leaves the building where the NCP operates without electricity. This power disruption persists beyond the operational duration of the NCP's backup generator before it requires refuelling. If the precise duration of the generator's fuel capacity is unknown, the disruption should be treated as indefinite.

(c) *Trigger 3: Disruption or failure of ICT systems*. As a result of a failure in the ICT system, the software or application(s) of the NCP are unable to operate effectively. This failure also prevents access to essential databases, leaving the ICT systems down for an undetermined period.

(d) *Trigger 4: Large-scale staff absence and absence of scarce essential staff*. A significant portion of staff is suddenly unable to fulfil its duties. This shortage could include the absence of scarce essential staff members and result in delays or disruption of operations. The duration of this unavailability is expected to last long enough to exceed the capacity for overwork among the remaining personnel.

59. Stress tests should progressively combine several disruptive events to assess the NCP's ability to maintain essential functions during cascading or compound disruptions that affect multiple resources at the same time.

4.4. Participants

60. It is recommended to identify participants in accordance with the defined objectives, essential functions and scenario of the stress test.

4.5. Evaluation, lessons identification and implementing improvements

61. When planning the stress test, it is advisable to establish an evaluation system. This helps identify gaps and areas for improvement in the operational continuity plan while assessing the overall success of the exercise. It also provides a basis for future planning and training on operational continuity of the NCP.

62. It is recommended to systematise the evaluation format, after both real events and exercises or training activities, including stress tests. For the purpose of the stress test, NCPs are recommended to use the evaluation grid provided in Annex VIII. This evaluation grid suggests evaluating operational continuity from two complementary angles:

(a) *Compliance with the operational continuity plan*, and

(b) *Maintenance of essential functions and fulfilment of predefined performance objectives*.

63. In addition, the table contained in Annex IX is intended to support NCPs in compiling the evaluation, identifying lessons and proposed improvements. Annex X contains a questionnaire template designed to gather feedback from participants.

64. Member States and UCPM participating States are invited to share non-sensitive lessons learned and proposed improvements with the ERCC after conducting a stress test of their NCP.

Done at Brussels,

For the Commission
Hadja LAHBIB
Member of the Commission

EUROPEAN
COMMISSION

ANNEXES 1 to 10

ANNEXES

to the

Commission Recommendation

on operational continuity and stress testing guidelines for National Contact Points within the Union Civil Protection Mechanism

ANNEX I
Categories of disruptive events

Four different categories of disruptive events can be identified for the purpose of operational continuity and stress testing for NCPs within the UCPM:

- *Unavailability of premises:* The premises of the NCP can no longer be used due to a physical or operational incident that prevents or severely limits access to the building or its use, either temporarily or permanently. Examples also include blocked key access routes, physical damage to nearby buildings, and failures or problems affecting utilities and installations, such as water, heating, ventilation or security systems[1]. Such incidents may also disrupt the normal activity of the NCP by forcing evacuation of the premises, preventing access to them, or rendering them unusable.
- *Disruption of electricity supply*: A power failure that affects the NCP's premises. A long-lasting failure of power supply may lead to a fuel-supply incident for backup generators. It may also have an impact on electricity-dependent systems, including ICT systems.
- *Disruption or failure of ICT systems:* the software or applications of the NCP are unable to operate effectively. Such a failure may take various forms, such as loss of access due to authentication issues, severe performance degradation, data corruption or unavailability, failure of interfaces with external systems, or disruption following updates or a cybersecurity incident, including cases such as illegitimate personification of a NCP main system, leading to the dissemination of manipulated information by the NCP.
- *Large scale staff absence or absence of scarce essential staff*: a significant number of essential staff are unable to reach the premises or are otherwise unable to work. The situation is aggravated when essential functions depend on a single individual or a small group of scarce essential staff, whose unplanned absence or unavailability causes disruption.

These four categories provide a framework for understanding the measures required to mitigate disruptions. However, disruptive events can also be triggered by other incidents, such as a sudden influx of information that exceeds the NCP's capacity to manage it, or the spread of false information that requires NCP resources for verification and dissemination of accurate information.

Furthermore, disruptive incidents can be interconnected, and a single event may affect several areas at the same time. For example, a fire may render the premises inaccessible while also causing a power outage and damaging ICT systems and data. They may also result from intentional or malicious actions, including cyber incidents and hybrid activities, and from several concurrent incidents, intensifying their overall impact. As a result, NCPs need to develop a comprehensive response plan that addresses each category individually, considers their combined effects, and prepares for the possibility of simultaneous disruptions to ensure the continuity of their operations.

[1] Disruption of electricity supply and disruption or failure of ICT systems are considered different categories.

ANNEX II
Examples of operational performance objectives

Capability	**Indicative operational objective** (to be assessed and adapted to national requirements)
Initial situational awareness	within 15 minutes
Activation of continuity arrangements	within 30 minutes
Alternative communications established	within 30 minutes
Alternative command location operational	within 2 hours
Decision support capability	uninterrupted whenever possible
Fuel autonomy	minimum 72 hours
Food and water autonomy	minimum 72 hours
CECIS operational	within 60 minutes
First operational situation report to the ERCC	within the first operational reporting cycle

ANNEX III
Table to support the Business Process Analysis

Essential function 1	*Name of this function.*
Description	*Include a description of this function, including the tasks it comprises.*
Inputs	*List the inputs (information, datasets, services, products, supplies, budgetary provisions, equipment, ICT systems and location requirements) necessary to complete this function and the external entities providing them, when applicable.*
Output	*List the information, product(s), service(s), or action(s) that result from this function and identify the (external) organisation(s), entity(ies) or concerned group(s) that receive them.*
Leadership (validation or authorisation)	*List the positions with a validation or authorisation role necessary to complete this function, if applicable.*
Essential staff	*List the positions of essential staff, and their profile, expertise and training, if applicable, such as security clearance.*
Facility	*List the physical location(s) or premises from which the essential function is performed.*
Equipment and systems	*List the equipment, systems and provisions necessary to complete this function. These could include secure premises, computers for encrypted communications, videowalls, high-level meeting rooms, equipment for videoconferencing, and computers with access to the Trans European Services for Telematics between Administrations (TESTA), etc.*
Essential records	*List the data and information needed to accomplish the function.*
Dependencies and interdependencies	*List the relationships or arrangements among the items identified above and specify, where relevant, the nature of the relationship or arrangement, the essential services needed (e.g. power supply, ICT, etc.), the impact in case of service or supply disruption, and the agreements with the entities that provide these services or supplies. The assessment should also describe interdependencies, including cascading effects where disruption of one service (for example electricity or ICT) affects other services and thereby amplifies the operational impact.*
Backups	*List the alternative resources or arrangements that would be activated to continue operating if the main resources or arrangements were affected by the disruptive event.*

ANNEX IV
Guidance for the application of mitigation and prevention measures

This section provides guidance for the application of mitigation and prevention measures, arranged by category of disruptive event. To avoid repetition, measures that are applicable to several different disruptive event categories are detailed only once in the first applicable category.

– Unavailability of premises:

- *Geographical distribution of the NCP into two or more geographically separate centres that operate simultaneously, providing mutual backup and overflow support for one another.* Each location should operate around the clock and be fully equipped to manage the entire workload if the other site(s) become(s) temporarily non-operational. Additionally, sites should be chosen based on a risk analysis of different risk zones and accessibility, with primary and alternative sites in different risk zones and access available through different transport routes. For example, in earthquake-prone areas, sites should be on different tectonic plates; in flood-prone areas, they should be at significantly different elevations or in different river basins.
- *Relocation to alternative premises managed by the NCP's authority*. Consider establishing at least two alternative locations. One should be near to the main premises to facilitate quick relocation and rapid resumption of essential functions. The other should be far enough away to ensure that major disruptive events, such as floods or snowstorms, do not impact both sites simultaneously. Ensure the security of information and communications and compatibility of essential ICT equipment and systems – such as CECIS or equipment necessary for classified communications- both in main and alternative premises.
- *Pre-arranged transport for essential staff to alternative premises (including in adverse weather conditions).* To ensure adequate staffing, establish arrangements to transport essential staff in the event of an activation of the operational continuity plan involving the use of alternative premises or remote mobile units. Consider the potential impact on transport routes such as traffic congestion and blockage from adverse weather conditions, infrastructure failure, civil unrest, or other causes.
- *Remote work (involving flexibility of tasks that might be performed outside the physical location of the NCP).* Identify which essential functions or steps that are part of the essential functions can be performed remotely. This could be possible because these functions/steps do not rely on equipment or systems exclusive to the main physical premises. Consider establishing a contingency plan or system to restructure staff's responsibilities, enabling some personnel to work from home while others are relocated to the alternative premises.
- *Mobile command and control units that could temporarily host the essential staff from the NCP.* These units should support the execution of essential functions from a mobile environment, including access to operational information systems and CECIS. Their required equipment and level of self-sufficiency should be defined to ensure operational readiness. They should be designed to sustain operations as a temporary backup for support to the main premises for a predefined period.

- *Activation of administrative arrangements with other authorities to use their premises*. Establish agreements with other national or subnational authorities for temporary shared use of their premises. Assess the layout, systems, equipment and security measures needed to perform the essential functions effectively. Ensure that these agreements include regular drills and test to validate the readiness and suitability of these alternative facilities.
- *Devolution:* Ensure that arrangements are in place and establish a system to delegate functions to other national authorities.

– Disruption of electricity supply:

- *Activation of generators and UPS.* Provide generators and UPS systems sized to ensure continuity of essential NCP functions for a defined minimum period. Their capacity should be sufficient to support operational requirements under prolonged power outages. Generators and UPS systems should be regularly tested to ensure operational readiness.
- *Priority fuel supply arrangements and agreements with providers.* Fuel supply arrangements should ensure sustained operations and be based on on-site fuel storage capacity and expected fuel consumption. Additional measures may include the availability of mobile fuel containers with pumping systems and/or priority supply agreements with nearby fuel providers.
- *Energy autonomy and alternative energy sources for essential functions.* The NCP should, where possible, be able to operate independently of the national power grid. If the grid fails for several days, as can happen during major disasters, continuity could be maintained through diversified power sources and a self-sufficient microgrid: for example, a wind or solar microgrid. Consider installing alternative energy sources, such as photovoltaic panels with battery storage, sized to supply the essential functions of the NCP.
- *Maximising available power capacity.* Establish internal protocols to maximise available power capacity by restricting the use of non-essential equipment and progressively disconnecting loads not required to support essential functions, thereby extending backup power autonomy without additional investment.
- *Relocation to alternative premises managed by the NCP's authority with electricity supply* (the relevant recommendations are set out under "Unavailability of premises")
- *Remote work from a building with guaranteed electricity supply* (the relevant recommendations are set out under "Unavailability of premises")
- *Mobile command and control units that are self-sufficient in terms of electricity* (the relevant recommendations are set out under "Unavailability of premises")
- *Activation of administrative arrangements with other authorities to use their premises with guaranteed electricity supply* (the relevant recommendations are set out under "Unavailability of premises")
- *Devolution* (the relevant recommendations are set out under "Unavailability of premises")

– Disruption or failure of ICT systems:

- *Redundancy*. Redundancy ensures that the failure of one component does not interrupt the function it sustains. The NCP should implement redundancy at complementary levels: (i) equipment (duplicate essential components), (ii) connectivity (multiple providers and diverse access paths, and (iii) applications and data (replication of essential databases and documents to a secondary site). Redundancy arrangements should have sufficient capacity to sustain operations if the main ICT environment fails, and should be tested periodically to ensure readiness and seamless failover in case of disruption. They must avoid shared dependencies with the primary system, such as the same power source, provider or physical infrastructure, that could fail simultaneously.

  Fibre lines are highly vulnerable to ground displacement, which can cause signal attenuation or loss and service interruptions. To mitigate this risk, satellite-based failover is recommended as a standard redundancy measure, enabling the backup network to maintain the same situational awareness as the primary network. Geographic data mirroring should be active-active, with primary and backup environments kept synchronised so that both can take over seamlessly. This redundancy and mirroring approach supports high availability and performance in fibre optic networks.

- *Regular and secure data backups, including off-site and offline copies.* Establish and maintain a structured backup policy for all data and configurations that are essential for NCP operations. This should define what is backed up, how frequently, where the backups are stored (including off-site or offline copies) and who is responsible for managing them. Backups should be encrypted and protected against unauthorised access.

- *Alternative ICT systems and communication channels. S*et up alternative tools and channels that can be used if primary ICT systems or networks fail. These may include satellite communications, high frequency (HF), very high frequency (VHF) or ultra-high frequency (UHF) mobile radio units, analogue phone lines, secure messaging applications or web-based platforms hosted outside the main infrastructure. Staff should be aware of when and how to switch to these alternatives.

- *Emergency ICT support teams / on-call technical response units.* Arrange quick access to ICT support, whether delivered internally (within the organisation) or by an external provider, by defining clear availability and response arrangements so that technical assistance can be mobilised quickly when needed to ensure prompt recovery of ICT systems.

- *Cyber incident response procedures coordinated with the national cybersecurity authority.* Establish coordination protocols with the national cybersecurity authority, including early warning channels, joint incident response procedures, and clearly defined roles and responsibilities during a cyber incident affecting the NCP.

- *Offline copies of essential contact lists, key procedures and operational documents.* Information such as contact lists, incident procedures and key templates should be available in formats that can be used without access to the main ICT systems.

- *Mobile command and control units with access to primary and backup ICT systems* (the relevant recommendations are set out under "Unavailability of premises")
- *Relocation to alternative premises managed by the NCP's authority with access to primary and backup ICT systems* (the relevant recommendations are set out under "Unavailability of premises")
- *Activation of administrative arrangements with other authorities to use their premises with access to ICT systems* (the relevant recommendations are set out under "Unavailability of premises")

– Large-scale staff absence and absence of scarce essential staff:

- *Overtime management (short-term solution).* Establish an overtime protocol that defines: clear triggers for when overtime may be used; who can authorise it; defined limits (maximum shift length, maximum weekly hours, and maximum consecutive days); minimum rest periods between shifts and after reaching the maximum weekly hours or maximum consecutive days; a fair rotation system so that the same staff are not repeatedly asked; a record-keeping system of overtime hours; pre-established additional remuneration; and practical support during extended hours (e.g. meals, rest areas, and transport home where needed).
- *Reassigning essential functions to available staff.* Prepare contingency arrangements specifying how essential functions will be redistributed in the absence of key staff. This includes identifying substitute personnel for each essential role and simplifying procedures where possible.
- *A pre-identified pool of trained personnel from within the institution, available on short notice*. Establish a system to mobilise backup staff from a pre-identified pool, defining clear rules covering who can mobilise backup staff and how, including activation criteria, communication channel(s) for mobilisation, personnel requirements (such as security clearance, training or expertise) and how time off or overtime is handled, with regular reviews to ensure that the system works well. Ensure that these rules are well known among personnel in the pool.

  This pool can be built through: (i) cross-training staff from other units—implement cross-training programmes so that multiple staff members can perform the same essential functions, focusing on roles identified as bottlenecks; and (ii) a "dormant pool" of former NCP essential staff—rotate staff out of NCP duties into other departments after a set period to create a dormant pool of backup personnel. Maintaining this dormant pool provides surge staffing capacity and enables swift activation, bypassing the months of training and security vetting typically required for such sensitive roles. In either case, arrangements should be formalised to ensure that staff belonging to the pool remain current through periodic refresher training and can be rapidly mobilised in a major crisis.
- *Prioritising staff recruitment.* Sustained 24/7 operation of NCPs requires stable staffing levels. The NCP may consider prioritising recruitment for roles supporting essential functions and anticipating predictable staff shortages (e.g.

simultaneous retirements or expiring fixed-term contracts), to start recruitment sufficiently in advance. Measures may include developing expedited hiring processes; in addition, continuous training of existing staff can further support staffing stability, by enabling internal mobility, skill development and succession across essential functions.

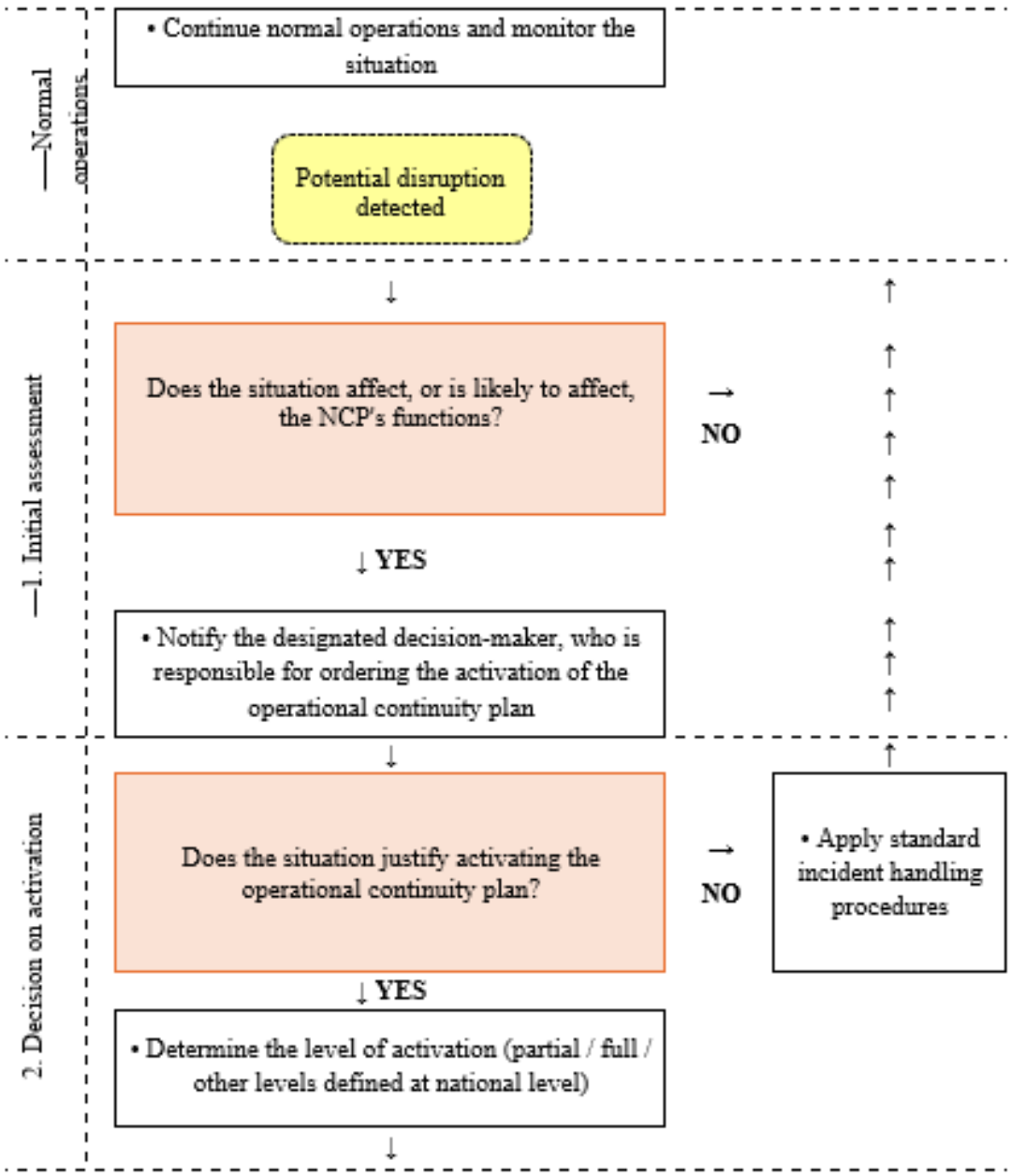
- *Investing in essential staff retention.* To retain personnel working in NCPs, motivation should be supported through a combination of benefits and incentives. Non-monetary incentives may include extended leave after a certain period of service, flexible rostering arrangements subject to minimum service coverage requirements, on-site rest areas, family support measures (e.g. childcare access), and access to discounted or free services such as public transport, healthcare, and cultural or sports facilities.
- *Supporting the families of essential staff.* Essential staff availability may depend on their families, in particular if they are at risk or left unattended. Consider putting arrangements in place, when relevant, to safeguard the families of NCP essential personnel, prioritising their safety so that staff can remain operational.
- *Preventing staff bottlenecks by delegating authority and promoting shared responsibility.* Ensure clear responsibilities and tasks. Establish protocols for delegating authority. Identify the successors with their respective positions, who would step in should the decision-makers responsible for essential functions be unavailable. Specify the circumstances and the sequence under which they would assume these roles. Where decision and responsibilities allow, ensure capacity building and regular training to take over authority in case of disruption. Consider whether distributing or sharing responsibilities among multiple staff members with a rotation system is feasible and helpful to avoid bottlenecks. Consider maintaining an updated handbook for new staff, designed to enable less experienced colleagues to independently manage a wide range of tasks while ensuring compliance with established standards and protocols.

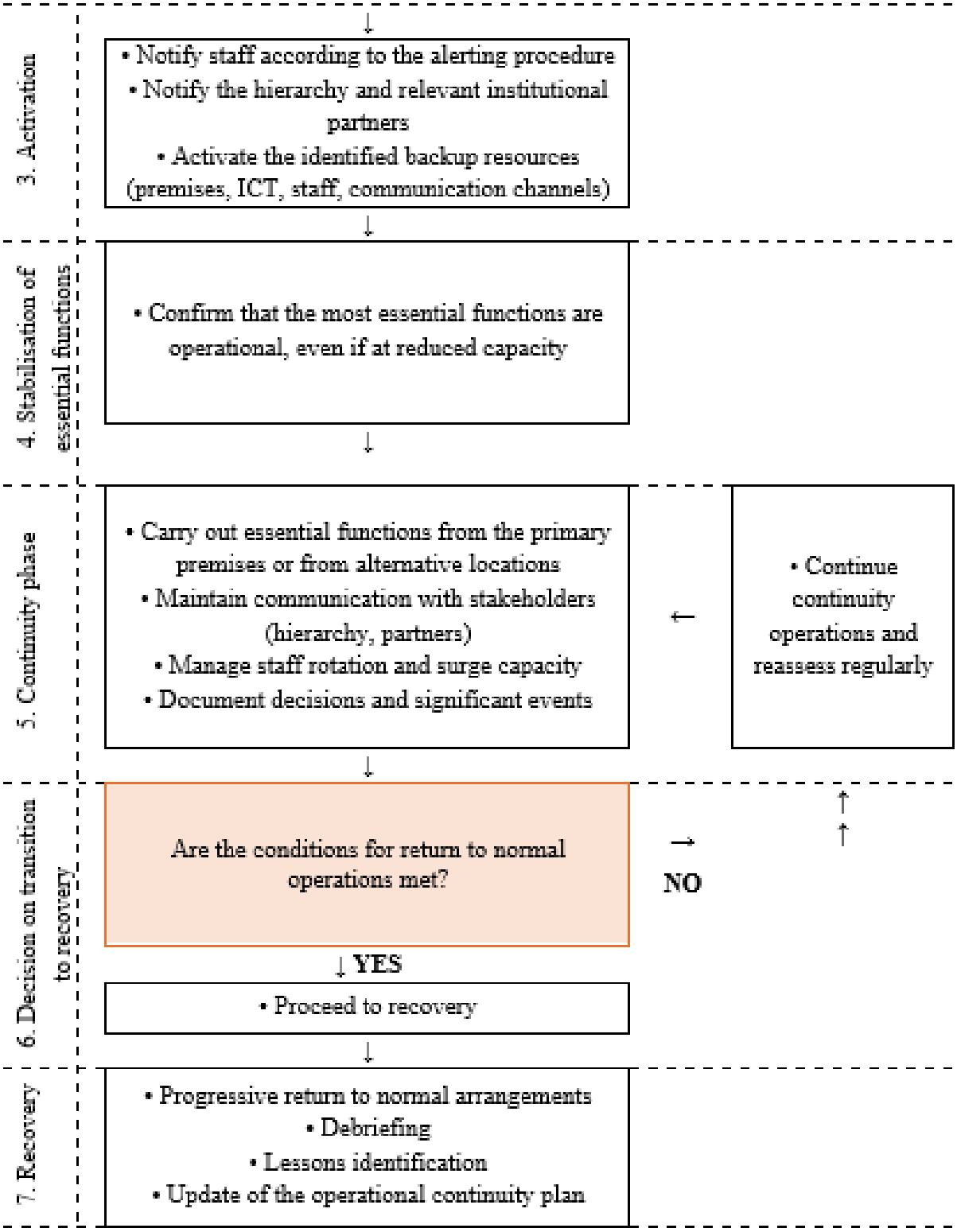
ANNEX V
Operational reference tools

This Annex provides an operational reference tool that NCPs should consider using when developing or reviewing their operational continuity plan.

Illustrative activation flow

The flow below is an example of how the activation of an operational continuity plan can be organised, from the moment a potential disruption is detected until the NCP enters a stable continuity phase. It is structured around decision points, not prescribed timeframes.




3. Activation
• Notify staff according to the alerting procedure
• Notify the hierarchy and relevant institutional partners
• Activate the identified backup resources (premises, ICT, staff, communication channels)
4. Stabilisation of essential functions
• Confirm that the most essential functions are operational, even if at reduced capacity
5. Continuity phase
• Carry out essential functions from the primary premises or from alternative locations
• Maintain communication with stakeholders (hierarchy, partners)
• Manage staff rotation and surge capacity
• Document decisions and significant events
• Continue continuity operations and reassess regularly
6. Decision on transition to recovery
Are the conditions for return to normal operations met?
NO
YES
• Proceed to recovery
7. Recovery
• Progressive return to normal arrangements
• Debriefing
• Lessons identification
• Update of the operational continuity plan

ANNEX VI
Key points to address when drafting a communication strategy[2]

– Identify the different audience groups, under the organisation's communication responsibility, that could potentially be impacted by the disruption of the NCP's operations or would need to be informed in case the organisation suffers a disruptive event, including:

  (a) the higher levels of the organisation, including the decision-making level;

  (b) the organisation's staff;

  (c) the stakeholders that provide input for the organisation's essential functions;

  (d) the stakeholders that receive the output of the organisation's essential functions;

  (e) the media;

  (f) the general public.

– For each audience group, define the purpose of the communication in the event of a disruptive event. Each group could require a different type, format, and content of information. The communication channel(s) used could also differ.

– Draft pre-established messages that are clear, concise and consistent across recipients, channels and over time. Ensure that they are tailored to the audience group they target, addressing their specific information needs.

– Identify alternative communication channels for each audience group to ensure effective communication if the disruption impacts standard channels.

– Consider proactive information as a better approach to reactive information.

– Where the communication strategy includes the possibility of disseminating messages through public TV and radio, coordinate the timing of these messages with news broadcasts to ensure effective integration and wide distribution among the population.

– Within the communication strategy, consider pre-assigning the role of information manager to a certain position, specifying its tasks before, during and after a disruptive event.

[2] These suggested items for the drafting of a communication strategy do not take into account the management of mis- or disinformation.

ANNEX VII
Examples of scenarios

Example of scenario 1

What: *power failure followed by data loss.*

Where: *the power failure affects the area where the NCP's main premises are located.*

Duration: *24 hours.*

Description: *repair works in the vicinity of the premises of the NCP have caused damage to the electricity distribution system. The sudden loss of power has caused damage to the NCP's computer systems, resulting in data loss. Power restoration works are expected to last 24 hours. The ICT failure lasts for 24 hours.*

Example of scenario 2

What: *inaccessibility of premises due to long-lasting snow.*

Where: *the whole area where the premises are located is affected.*

Duration: *over a week.*

Description: *A major snowstorm has hit the area where the NCP premises are located, leaving them inaccessible by road and public transport. The snowfall is so extensive that snowploughs are not sufficient to clear all main roads during the first 24 hours, with priority given to hospital access. The population has been requested to stay off the streets. For at least 48 hours, access by public transport or private vehicle to the NCP facilities is not possible. The cold wave continues in the area for over a week and snow on smaller roads persists for one week. As a result, one third of the staff scheduled to work in the following days cannot make it into work for one week because their place of residence is remote and smaller roads are the last to be cleared.*

Additionally, essential staff on duty on the day of the snowfall are stranded in the premises for the first 48 hours. Around one third have already reached the maximum number of hours they are permitted to work that week, and a further third will reach that limit within 24 hours. Consequently, they are legally entitled to adequate rest. They also require support for basic needs (food, personal hygiene), and, in some cases, measures to support their families, and/or evacuation.

ANNEX VIII
Stress test proposed evaluation framework

The outcome of the stress test should be assessed against two separate but complementary dimensions:

- *Compliance with the operational continuity plan*. This dimension should assess the extent to which the NCP implemented the applicable operational continuity arrangements during the stress test, including decision-making structures for activation, escalation, and recovery, internal and external coordination and communication, relocation arrangements and use of backup resources.
- *Maintenance of essential functions and fulfilment of predefined measurable operational performance objectives*. This dimension should assess whether the NCP essential functions were maintained or restarted within acceptable predefined limits, whether there were negative effects on other non-essential functions of the NCP, and whether the stress test achieved the predefined measurable performance objectives. Examples of operational performance objectives are provided in Annex II.

The two dimensions should be assessed separately in order to identify more precisely which improvements are needed. This distinction helps to ensure that compliance with the operational continuity plan is assessed separately from the effectiveness of the operational outcome. The evaluation report should present the result as two complementary scores: one reflecting compliance with the operational continuity plan, and the other reflecting the maintenance of essential functions and the fulfilment of predefined measurable operational performance objectives.

Evaluation grid for assessing compliance with the operational continuity plan.

Rating (0-3)	*Description*
0: Non-compliance.	*The exercise showed little or no alignment with the operational continuity arrangements. Core procedures were absent, incorrectly executed, or ignored.*
1: Partial compliance.	*Some points of the continuity arrangements were applied, but other important points were not followed correctly, were applied too late, or proved inadequate in practice. The test revealed substantial weaknesses and important opportunities for improvement in the plan.*
2: Overall compliance, with only minor deviations.	*The stress test was implemented broadly in accordance with the operational continuity plan. Deviations from the plan were limited. The test revealed some weaknesses and opportunities for improvement in the plan.*
3: Full compliance.	*The operational continuity plan was followed in full during*

	the stress test.

Evaluation grid for assessing maintenance of essential functions and fulfilment of predefined measurable operational performance objectives.

Rating (0-3)	*Description*
0: Not achieved.	*The NCP essential functions were suspended or delayed beyond acceptable predefined limits. Other non-essential functions of the NCP were significantly and negatively affected. The predefined measurable performance objectives were not achieved.*
1: Achieved with major challenges.	*One or more essential functions were restored only after a substantial delay exceeding acceptable limits. The stress test may also have caused relevant disruption or negatively affected other functions of the NCP. The predefined measurable performance objectives were achieved only partially or with major challenges.*
2: Achieved with minor deviations.	*Essential functions were maintained or restored within acceptable tolerance margins (with predefined acceptable limits exceeded by a limited time) without significant impact on other NCP functions. The predefined measurable performance objectives were largely achieved, and only minor deviations from the established limits were observed.*
3: Fully achieved.	*The essential functions covered by the stress test were maintained or restored without delays exceeding the predefined acceptable limits and without negative impact on other NCP functions. The predefined measurable performance objectives were fully achieved.*

ANNEX IX
Stress Test's evaluation, lesson identification and proposed improvements[3]

In the evaluation process, it is advisable to identify strategies for improving the areas that were inadequately addressed during the stress test exercise. Additionally, NCPs should consider incorporating successful items that emerged during the exercise but are not included in the current operational continuity plan.

The following table is meant to facilitate the compilation and alignment of the evaluation, the identification of lessons and proposed improvements after conducting a stress test.

Compliance with the operational continuity plan.	*Rating (0-3): ...* *Description...*
Maintenance of essential functions and fulfilment of predefined measurable operational performance objectives.	*Rating (0-3): ...* *Description...*
Findings and comments	...
Gaps and lessons identified	...
Proposed improvements	...
Actions needed for implementation	...

[3] This evaluation table is based on the Continuity Resource Toolkit developed by US Federal Emergency Management Agency (FEMA) to support communities and local authorities/organisations in developing operational continuity programmes and has been adapted to the stress test exercise.

ANNEX X
Participant's feedback form

The following questionnaire is recommended as a template for gathering feedback from stress test participants. The questions should be tailored to the specific scope and focus of the stress test. Collecting responses to these or similar questions from stress test participants, observers or personnel involved in real disruptive events can help identify lessons and gaps, which can then be used to update the NCP's operational continuity plan.

Activation of the operational continuity plan:

- Were established protocols followed?
- If not, what were the reasons for the deviation, and was it due to an error/problem or a positive/optimising adjustment?
- How efficiently were the protocols executed?
- What challenges were encountered?
- Was communication clear and effective during the activation?
- Were all essential personnel notified and mobilised in a timely manner?

Operational resumption, continuity and essential function performance:

- What was the time taken to resume the essential functions you are responsible for?
- Were all essential functions delivered efficiently and within expected timeframes? Assess the quality of outputs delivered under test conditions.
- Were there any noted delays or inefficiencies in performing these functions?
- Was prioritisation of any essential functions necessary during the exercise?
- How was prioritisation decided and communicated?
- Was the prioritisation effective in ensuring continuity and effectiveness?

Equipment and ICT Systems:

- Was all necessary backup equipment available and fully operational?
- Were electricity supply backup systems tested and fully functional?
- Were backup communication tools and channels tested and fully functional?
- Were other essential services and supplies available, tested and fully operational?
- Were any delays or inefficiencies caused by ICT systems identified?
- How effectively were issues solved?

Alternative facilities:

- Is the alternative location adequate in size, layout and equipment to allow you to work for a long time (several days)? If not, why and what could be done to improve it?

Communication and coordination:

- Were all participants, including the hierarchy and relevant teams or colleagues, adequately informed?
- Were internal communication and coordination effectively maintained throughout the exercise, including with hierarchy?
- Were communication and coordination with the ERCC effectively maintained throughout the exercise?
- If applicable, how effective was communication with the ERCC from the backup location?
- How was information exchanged and documented during the relocation or disruption?

Staff training and well-being:

- Do you think that you were well-prepared for the exercise based on pre-exercise operational continuity training?
- Were you well informed about the exercise once it began?
- Was there clarity in roles during the exercise?
- Was the exercise useful for staff training purposes?
- Were your personal and family needs considered, for example your need for transportation, rest, water or food?

Other general observations:

- What aspects of the exercise were most successful?
- What were the main challenges encountered?
- Did the exercise meet its objectives?
- Based on the experience during the exercise, how do you assess the capacity of the NCP to continue operating under the conditions of this exercise for 1 week?
- Identify possible additional resources or support needed for a similar disruptive event lasting longer than the exercise.
- Identify improvements for future training and exercises.