Official Journal
of the European Union

EN
C series

C/2026/3712

13.7.2026

COMMUNICATION FROM THE COMMISSION

Guidelines on the application of Article 13(5) of Directive (EU) 2022/2557 on the resilience of critical entities

(C/2026/3712)

I. INTRODUCTION

1. The purpose of Directive (EU) 2022/2557 on the resilience of critical entities ([1]) (the Directive) is to ensure that services essential for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market. The Directive is intended to enhance the resilience of the critical entities providing such services, creating an overarching framework for resilience to all hazards (natural and man-made, accidental or intentional).

2. In accordance with Article 6(1) of the Directive, Member States must identify their critical entities for the sectors and subsectors set out in the Annex to the Directive by 17 July 2026. To achieve a high level of resilience, such critical entities have obligations under the Directive, including the obligation laid down in Article 13 to take appropriate and proportionate technical, security and organisational measures to ensure their resilience. In this regard, Article 13(5) of the Directive mandated the Commission to adopt non-binding guidelines to further specify the technical, security and organisational measures that may be taken by critical entities.

3. In accordance with the provisions mentioned above, before the adoption of this Communication, Member States and stakeholders were consulted in a workshop held on 29 September 2025. The Critical Entities Resilience Group (CERG) was consulted on the outline of the Communication in its meetings of 10 April, 19 May and 30 September 2025. It was also consulted on the draft text of the Communication on 14 November 2025, and an updated version was shared with the CERG on 25 February 2026. A final consultation of the CERG on the draft guidelines took place on 6 March 2026.

4. This Communication is not legally binding and does not affect the interpretation of EU law by the Court of Justice of the European Union.

II. NON-BINDING GUIDELINES ON RESILIENCE-ENHANCING MEASURES

A. GENERAL CONSIDERATIONS

5. These non-binding guidelines aim to further specify the technical, security and organisational measures that may be taken by critical entities under Article 13(1)(a) to (f) of the Directive. The list of measures is non-exhaustive and may be complemented with additional measures.

6. Under Article 13(1), in implementing these measures critical entities must take the following into account.

   (a) Relevant information provided by Member States on the Member State risk assessment carried out under Article 5 of the Directive. Member States should send prompt, succinct and tailor-made information to their critical entities. Such information may include the reports referred to in Article 9(3) of the Directive, sent to the Commission using the common reporting template.

   (b) Relevant information on the outcomes of the critical entity risk assessment carried out under Article 12 of the Directive. Critical entities are encouraged to ensure a holistic approach by shifting from simply protecting critical infrastructure to ensuring the continuity of the essential service(s) they provide and linking the results of the risk assessment to their resilience-enhancing measures. In order to support resilience measures, critical entities should consider conducting comprehensive risk assessments that go beyond their direct dependencies, accounting for cross-border, sectoral and systemic interdependency aspects.

([1]) Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164).

7. According to Article 13(1) of the Directive, the measures to be taken by critical entities must be appropriate and proportionate. The appropriateness and proportionality of these measures should be assessed in relation to the results of the risk assessments mentioned above.

   (a) 'Appropriate' should be understood as risk-based or impact-based, effective and suitable measures that can make the critical entity fully resilient in the provision of essential services. The appropriateness of a measure may differ from one critical entity to another depending on their specificities.

   (b) 'Proportionate' should be understood as necessary and sufficient measures that are not excessive in terms of the level of risk and the severity of the disruptive incident. Measures should be tailored to the specificities of the critical entity in question and take into account aspects such as the nature of the essential service(s) provided, the supply chain and interdependencies, the cost effectiveness of the measures, the size of the entity and the geographical impact of the services provided.

8. The guidelines take into account all the sectors covered by Chapter III of the Directive ([2]). The non-exhaustive list of examples might not apply equally to all sectors and all types of critical infrastructure.

9. The measures to be taken will depend on the outcome of the Member State risk assessment and of the critical entities' risk assessments.

10. The resilience measures taken by critical entities under Article 13(1)(a) to (f) should be applied without prejudice to, and in coherence with, measures stemming from relevant sectoral legislation such as the legislation mentioned in recital 31 of the Directive, as well as the Network and Information Systems 2 (NIS2) Directive ([3]), the European Climate Law ([4]), the Regulation on risk-preparedness in the electricity sector ([5]), the Regulation concerning measures to safeguard the security of gas supply ([6]), the Directive on the safety of offshore oil and gas operations ([7]), the EU framework on maritime and port security ([8]), the General Data Protection Regulation (GDPR) ([9]), the Regulation for the implementation of the Single European Sky ([10]), the European Union Aviation Safety Agency Regulation ([11]), and the Implementing Regulation regarding air traffic management network functions ([12]).

([2]) Energy, transport, health, drinking water, waste water, public administration, space, production, processing and distribution of food.

([3]) 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 (OJ L 333, 27.12.2022, p. 80).

([4]) Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 (OJ L 243, 9.7.2021, p. 1), in particular as regards Article 5 referring to adaptation to climate change.

([5]) 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, p. 1), in particular as regards measures stemming from Articles 10 and 11.

([6]) 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), in particular as regards measures stemming from Article 8.

([7]) Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on the safety of offshore oil and gas operations and amending Directive 2004/35/EC (OJ L 178, 28.6.2013, p. 66), in particular as regards measures stemming from Article 3.

([8]) For example, Directive 2005/65/EC on enhancing port security and Directive 2002/59/EC on vessel traffic monitoring and information systems.

([9]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1).

([10]) Regulation (EU) 2024/2803 of the European Parliament and of the Council of 23 October 2024 on the implementation of the Single European Sky, in particular Article 22.2(b) (OJ L, 2024/2803, 11.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2803/oj).

([11]) Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency (OJ L 212, 22.8.2018, p. 1).

([12]) Commission Implementing Regulation (EU) 2019/123 of 24 January 2019 laying down detailed rules for the implementation of air traffic management (ATM) network functions (OJ L 28, 31.1.2019, p. 1).

11. When using artificial intelligence (AI) in their resilience measures (e.g. an AI system monitoring water pressure in a dam or controlling a power grid), critical entities must be aware that high-risk AI systems must comply with the safety requirements of the EU Artificial Intelligence Act ([13]). 'High-risk' means that they are intended to be used as safety components ([14]) in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity ([15]). Their failure or malfunctioning may put the life and health of people at risk on a large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities.

12. In conjunction with Article 13(2) of the Directive, recital 30 explains that *'[i]n the interests of effectiveness and accountability, critical entities should describe the measures they take, with a level of detail that sufficiently achieves the aims of effectiveness and accountability, having regard to the risks identified, in a resilience plan or in a document or documents that are equivalent to a resilience plan, and apply that plan in practice. Where a critical entity has already taken technical, security and organisational measures and drawn up documents pursuant to other legal acts that are relevant for resilience-enhancing measures under this Directive, it should be able, in order to avoid duplication, to use those measures and documents to meet the requirements as regards resilience measures under this Directive […]'.*

13. The role of the liaison officer designated by the critical entity in accordance with Article 13(3) of the Directive is crucial for the effective adoption and implementation of resilience-enhancing measures, since it ensures efficient and effective communication and coordination between the critical entity and the competent authorities regarding the obligations of the critical entity and the overall resilience framework.

14. In taking resilience-enhancing measures, critical entities are encouraged to identify all relevant assets, facilities and equipment and consider cross-border and interdependency aspects, given the highly interconnected nature of the sectors the Directive covers, including physical, environmental, cyber and supply chain aspects. A disruption in one area may have cascading effects on the entire internal market, thereby disrupting the provision of essential services.

15. The core mechanism for considering interdependencies is the critical entity risk assessment and the national risk assessment. Risk assessments should assess and take into account the extent to which other sectors depend on the essential service provided by the critical entity, and the extent to which that critical entity depends on essential services provided by other entities in other sectors, including, where relevant, in neighbouring Member States and third countries.

16. In taking resilience-enhancing measures, critical entities should consider taking relevant international and European standards into account.

17. The particularities of critical maritime infrastructure should be taken into account: such infrastructure is more difficult to monitor and protect; detection and localization of incidents, as well as repairs are more time-consuming and costly at sea.

B. PREVENTION MEASURES (Article 13(1)(a) of the Directive)

18. Critical entities are encouraged to take measures that enhance their resilience by improving their ability to prevent failures or disruptions. These measures should be integrated into the resilience plan mentioned in Article 13(2) of the Directive and be viewed as part of an integrated system rather than as isolated components. The effectiveness of any single measure depends on its interaction with other measures, including the physical protection of premises, response to, resistance to and recovery from disruptive incidents, and adequate employee security management.

([13]) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([14]) Safety components of critical infrastructure are systems used to directly protect the physical integrity of critical infrastructure or the health and safety of people and property, but they are not necessary for the system to function (Article 3(14) and recital 55 of the AI Act).

([15]) Annex III, point 2 of the AI Act.

19. Disaster risk reduction and climate adaptation measures should be based on plausible climate projections over the lifetime of the critical infrastructure. Critical entities are encouraged to avoid putting critical infrastructure (e.g. data centres or substations) in high-risk zones; take measures to structurally reinforce the infrastructure in question (e.g. fireproofing, flood, drought and blast resistance, liquid proofing), as well as non-structural measures (e.g. training and safety protocols) to prevent collisions, explosions, hazardous material spills or radiation; find nature-based solutions such as integrating green infrastructure (e.g. restored wetlands to absorb storm surges or urban forests to reduce the 'heat island' effect on electrical equipment); consider the immediate and long-term shifts in climate patterns that could degrade system integrity over time, such as extreme heat, flood and sea-level rise; plan for water scarcity; conduct stress tests to ensure the entity can function in a significantly more adverse environment (e.g. warmer, colder, wetter, drier, erratic or unseasonal conditions).

20. Critical entities are encouraged to consider creating an incident database, contributing to EU incident databases ([16]) and implementing a systematic incident-reporting system, which provides a history of events and enables not only incident prevention and risk reduction but also asset recovery.

21. To prevent human errors, critical entities are encouraged to identify error-prone tasks and implement appropriate countermeasures, including automation, continuous employee training, oversight and clear accountability, detailed process documentation, regular audits and inspections, and the development of a culture of resilience and responsibility.

22. To ensure that the resilience measures are applied in coherence with the NIS2 Directive, when applying their resilience measures, critical entities are encouraged to take into consideration measures relevant for the security of network and information systems as defined in the NIS2 Directive. The measures set out in Commission Implementing Regulation (EU) 2024/2690 ([17]) applicable to certain types of entities in the digital infrastructure, ICT service management (business-to-business) and digital providers sectors as defined in the NIS2 Directive ([18]), as well as the accompanying ENISA implementation guidance ([19]), may serve as further reference.

23. As regards operational technology, critical entities should incorporate manual overrides and human-in-the-loop provisions defining the specific conditions and requirements for human intervention and manual control in response to hazards.

C. PHYSICAL PROTECTION MEASURES (Article 13(1)(b) of the Directive)

24. Critical entities are encouraged to take physical measures against natural and man-made threats (e.g. hybrid threats, sabotage, terrorism, criminal acts, military/wartime targeting, espionage) and put in place procedural controls that serve to detect, deter, delay, deny, respond to and reduce the impact of disruptive incidents.

([16]) In aviation, relevant EU incident databases include the European Union Aviation Safety Agency incident reporting system, the network manager incident registers, and the aviation security occurrence system.

([17]) Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (OJ L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

([18]) As per Article 8 of the CER Directive, Member States shall ensure that certain provisions of the Directive, including Article 13, do not apply to critical entities that they have identified in certain sectors, including digital infrastructure. Member States may adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities, provided that those provisions are consistent with applicable Union law. ICT service management (business-to-business) and digital providers are not among the sectors defined in the Annex to the CER Directive.

([19]) https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

25. In planning appropriate and proportionate resilience-enhancing measures against man-made threats, critical entities should consider the relevance of specific threat scenarios. In particular, they are encouraged to:

(i) take into account the need for close public-private coordination protocols to support operational cooperation with competent authorities and ensure an appropriate and reciprocal flow of threat and incident information, in the interests of shared situational awareness;

(ii) in the case of potential hybrid threats from state actors which, in the case of critical entities are mainly sabotage attempts to disrupt assets and equipment, or preparations for such attempts (including espionage/surveillance), consider that state actors may sponsor and direct vulnerable or exploitable proxies (e.g. individuals or groups) to achieve their objectives, and that state actors may engage in coordinated attacks through multiple attack vectors in multiple domains and/or using multiple proxies;

(iii) take into account other potential threats, notably those stemming from terrorism and violent extremism, criminal activities, military targeting, insider threats, activism, etc.

26. Critical entities are encouraged to consider perimeter-hardening measures (deter and delay), such as high-security fencing (e.g. anti-climb/anti-cut), reinforced walls, gates, hostile vehicle mitigation, signage and lighting (e.g. high-visibility warnings to deter opportunistic intruders, and security lighting to eliminate dead zones for surveillance).

27. Access of vehicles, staff and goods to relevant premises should be channelled through a limited number of controllable checkpoints. Direct vehicle approach routes should be limited with a combination of physical barriers (e.g. fixed and retractable bollards, natural obstacles or other speed-control measures), and the prescribed maximum spacing between neighbouring barriers should be respected to prevent vehicle penetration.

28. External entry points (e.g. gates, doors) to relevant premises should be of robust construction or reinforced, and (retro)fitted with secure hinges and locking mechanisms. Facilities' frames (e.g. windows, skylights) should also be (retro)fitted with locking mechanisms and protective layering (e.g. bars, grilles, impact-resistant glass, protective membranes). Unconventional entry points (e.g. roof hatches, manholes and vents) to facilities or assets should equally be secured against unauthorised opening and tampering.

29. Critical entities are encouraged to consider perimeter monitoring and detection to identify breaches in real time (e.g. the installation of alarms or intrusion-detection systems, including interior and exterior sensors). These should maintain proper zonal coverage, be subject to consistent monitoring and response protocols, and undergo regular functional testing. Legitimate detections, system faults and false positives should be analysed and corrective measures implemented to maintain integrity.

30. Critical entities are encouraged to consider ensuring that video systems provide clear and environment-specific real-time and recorded coverage of relevant assets, facilities and equipment, as well as premises' approach routes and entry points. Surveillance time synchronisation, recording status and retention periods should be verified on a regular basis. Entities should conduct routine playback checks to confirm that faces, actions and events are identifiable for the intended forensic purposes following potential incidents. Spare critical components (e.g. storage media, power units) should be held commensurately.

31. Critical entities are encouraged to ensure that lighting arrangements provide even illumination of entrances, car parks, walkways and camera fields of view, avoiding glare and deep shadow that could impede detection or recording. Emergency and backup lighting should be tested on a regular basis. Remedial measures (e.g. lamp replacements, coverage adjustment, vegetation trimming) should be implemented on a regular basis.

32. Signage should clearly indicate security restrictions, monitoring and privacy notices, and routes for staff, visitors and deliveries.

33. Critical entities are encouraged to consider measures to control access (deny) using layered security zones, physical access management (e.g. badge readers, biometric scanners), mantraps and interlocking doors. The use of on-site security staff to patrol and manage access control to relevant facilities, entry points or equipment should be considered. Security staff should also serve an incident response function. They should maintain close and regular contact with relevant law enforcement authorities and defence actors.

34. Rooms and enclosures housing electricity, water, gas, heating, ventilation, air conditioning, telecommunications, security, network or other sensitive infrastructure or equipment should be locked and access-controlled, complemented by proportionate measures against unauthorised opening and tampering.

35. Mailrooms and delivery depots should be located away from relevant assets, facilities, equipment and high-occupancy areas, and equipped for segregation and the secure inspection of potentially suspicious items. Staff should be informed of clear procedures for suspicious items, including isolation, de-escalation, and notification of relevant internal and external stakeholders. Opening tools and personal protective equipment should be available if required. The chain of custody for valuable or controlled deliveries should be documented from receipt to recipient. Spot checks should be performed and recorded at regular intervals.

36. All external assets, facilities or equipment should equally be subject to proportionate protective measures. Any physical protective measures taken by critical entities require routine inspection and maintenance on a regular basis.

37. Measures relating to staff access controls and the physical information security of sensitive or classified information do not invalidate the cybersecurity risk management obligations laid out in the NIS2 Directive ([20]).

38. Further to the guidance under part F of these guidelines regarding employee security management, critical entities are encouraged to maintain a single authoritative register of physical keys and (electronic) credentials, including issuance, revocation and return dates. Lost or stolen keys or credentials should be revoked immediately and locks rekeyed or replaced where compromise is suspected.

39. Critical entities are encouraged to ensure that access rights follow the principle of 'least privilege' and are reviewed on a regular basis or upon role change. Relevant spaces should maintain a zonal architecture, controlled through corresponding measures for select individuals (e.g. distinguishing public, work, restricted and critical zones) and combining physical, technical and administrative controls. Access should be logged. Visitors should be channelled through a controlled point, registered, issued with visible identification, and escorted beyond reception unless otherwise authorised. Such means of identification should be immediately deactivated upon exit. The corresponding procedures should be simple, documented and communicated to all staff, in particular reception and security staff.

40. Any sensitive information assets should be positioned, protected and stored in a manner that reduces the risks to the integrity of those assets (e.g. unauthorised or accidental viewing, tampering, theft, environmental damage) and accessed on a need-to-know basis.

41. Critical entities are encouraged to establish and maintain an inventory and/or repository of sensitive information assets. Assets should be classified in accordance with the level of business or security sensitivity. Entities should then use a scheme to document information assets (e.g. restricted, internal, public or equivalent), and label and handle those assets accordingly. The rules and procedures for classification and handling should be communicated to all relevant staff and periodically reviewed. This includes rules for desk and screen access to information and the creation or copying of information.

([20]) Article 21.

42. As appropriate, critical entities should be mindful of the applicable national rules for the protection of classified information considered relevant for national security.

43. If external stakeholders require access to information assets, critical entities are encouraged to consider drawing up user guidance and non-disclosure agreements, or other relevant contractual mechanisms, as appropriate.

44. Any facilities housing sensitive information assets (e.g. archives, server rooms) or other areas from which sensitive information assets may potentially be extracted should be designated and supervised as secure zones, with particularly stringent access, viewing and removal controls.

45. Critical entities should ensure that access rights are regularly scrutinised and reviewed. Retention periods should be defined for sensitive information assets. Once these periods have been exceeded or other developments necessitate the reclassification of information assets, appropriate measures should be taken to sanitise or destroy those assets.

46. As regards the threats posed by unmanned systems ([21]) (drones), critical entities are encouraged to implement measures to facilitate the detection, tracking and identification of unmanned systems (e.g. radar, radiofrequency scanners, daylight/thermal cameras, acoustic sensors). Where possible, critical entities should also cooperate with telecommunication service providers to obtain access to data yielded by integrated sensing and communication (ISAC) technologies, with a view to detecting unauthorised drone activity within their security perimeter.

47. The threat of espionage/surveillance by non-cooperative unmanned systems should be mitigated by obscuring the visibility (aerial, maritime or terrestrial) of sensitive assets or equipment (e.g. concealment or repositioning) and, where appropriate, ensuring these are housed within closed facilities.

48. Critical entities should also mitigate the threat of sabotage by non-cooperative unmanned systems of facilities, assets or equipment. Examples of mitigation measures include counter-drone netting or canopies, and other structurally reinforcing measures such as blast-resistant windows, roof slab strengthening or full structural enclosures.

49. Critical entities may consider using geographical zones to manage and mitigate risks related to unauthorised or unsafe drone operations in the vicinity of their premises. Any decision to establish such zones should be subject to a risk and proportionality assessment done on a case-by-case basis, taking into account the potential sensitivity of information that could be revealed through the publication of geographical data related to critical entities. To do this, the entities would have to cooperate with the competent national authorities to ensure that relevant geographical zones are duly defined and digitally published in accordance with the applicable aviation framework. Such zones should, as a minimum, enable drone operators to benefit from geo-awareness functionalities. As technical capabilities evolve, and where supported by the regulatory framework, critical entities may also consider progressively using geo-fencing functionalities. Geo-fencing may serve as a preventive safeguard by reducing the likelihood of unintentional incursions by compliant drones into sensitive areas. Critical entities should maintain a direct operational link with the geographical zone manager. This would enable the timely visibility of authorised versus non-authorised drone activity in their vicinity and better support situational awareness and coordination with competent authorities.

50. It is essential to strengthen partnerships and communication with counter-drone operators in local law enforcement authorities and defence, or other actors legally mandated with mitigation capabilities (e.g. radiofrequency jamming, spoofing and other kinetic or non-kinetic measures). To this effect, critical entities are encouraged to facilitate the use of counter-drone systems to protect their perimeter, in accordance with the relevant legal framework.

([21]) Communication (COM)2026 81final of 11 February 2026 on an Action Plan on Drone and Counter-Drone Security.

D. RESPONSE, RESISTANCE AND MITIGATION MEASURES (Article 13(1)(c) of the Directive)

51. Critical entities are encouraged to consider the following measures to mitigate the consequences of incidents.

(a) Off-site crisis and disaster management: measures to mitigate the adverse off-site consequences of a severe disruptive incident and swiftly notify the relevant crisis- and disaster-management authorities to enable the implementation of off-site protective actions. This requires close coordination with relevant authorities, the establishment of tried and tested communication channels, as well as regular crisis- and disaster-management exercises.

(b) Off-site assistance: measures to effectively integrate off-site assistance into on-site response actions (including severe accident management, mitigatory actions and emergency response).

(c) Designing infrastructure to fail safely by ensuring that any disruption does not affect people's safety (including the safety of staff) and that cascading impacts on other assets are mitigated. Safe-to-fail features enable infrastructure to maintain essential functions during failure or support controlled shutdown procedures that prevent equipment damage and ensure restart capability once conditions permit that. Maintaining critical life-support conditions or passive survivability can be achieved through adequate storage capacity, control over thermal capacity, appropriate backup supply, and the security of hazardous materials.

52. In designing safe-to-fail infrastructure, critical entities are encouraged to consider the following elements: the storage capacity needed in worst-case failure scenarios to maintain critical life-support conditions; the backup supply required to maintain critical operations and support the controlled switch-off of infrastructure operations; the security of all hazardous materials stored or present in critical infrastructure, ensuring they are included in hazardous material coding and management plans and secured appropriately in the event of infrastructure failure; and thermal safety measures for critical infrastructure assets housing staff or temperature-sensitive equipment. Such measures may include both heating and cooling capacity to prevent casualties from extreme temperatures during extended disruptions.

53. Critical entities are encouraged to take measures to ensure availability, maintenance and repair capacities and define their supply needs clearly, diversify supply sources through alternative providers and routes, implement infrastructure reinforcement and redundancies, and establish backup systems with specifications for function, duration and restoration priority.

54. Critical entities are encouraged to take appropriate measures to ensure the integrity of IT networks and systems and software used in equipment, in particular in relation to reliance on high-risk suppliers, and protection against interference from radio frequency signals and cyber-attacks.

55. Alternative power systems may include generators and uninterruptible power supply (UPS) batteries. Backup systems should be periodically tested; power fuel autonomy should be maintained for at least 72 hours, and vendor contracts activated for emergency support (supply, interventions and repairs).

56. For water supply resilience, critical entities may limit water use to critical functions during disruptions and use alternative sources including backup wells, storage tanks, portable treatment units and flexible storage options. Critical entities in the drinking water sector are encouraged to identify priority points of delivery, in order to ensure an adequate response in contingency situations or during supply interruption. In taking resilience measures, critical entities must ensure that water intended for human consumption meets the quality standards set out in Directive (EU) 2020/2184 ([22]).

([22]) Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (recast) (OJ L 435, 23.12.2020, p. 1).

57. For other sector-specific utilities (e.g. hot water, chilled water, steam boiler) and supplies (e.g. chemicals, raw materials, spare parts), contingency planning in supply chains should consider shifting from just-in-time to just-in-case inventory models, where appropriate. Alternative systems should include prearranged back-up resources and supplies (buffer and safety/contingency stockpiles).

58. Critical entities are encouraged to develop comprehensive maintenance programmes based on manufacturer recommendations, operational experience and risk assessments. Predictive maintenance can be implemented using advanced monitoring technologies with integrated sensor networks. Regular and predictive performance-based maintenance, which uses data analytics and AI tools to monitor ageing and forecast failures might be appropriate to optimise the timing of any interventions required. Clear protocols should be established for responding to monitoring system alerts, including verifying alerts, assessing urgency and mobilising maintenance resources. These protocols should define escalation procedures for situations requiring immediate attention. Regular infrastructure inspections complement automated monitoring.

59. With regard to governance, critical entities should consider resilience as having to be embedded from the highest to the lowest levels of the governance structure. They should establish resilience objectives and adopt a strategy, policy and planning for resilience, communicate these to relevant stakeholders on a need-to-know basis, and conduct reviews on a regular basis. Account should be taken of existing vulnerabilities and how to better prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from an incident.

60. Critical entities are encouraged to establish clear decision-making hierarchies. Adequate competence on resilience should be consolidated at board level and in resilience or risk-management functions to ensure an adequate strategy, adequate policy and adequate operational planning for resilience. Critical entities are encouraged to consider appointing a resilience officer and ensure the clear delineation of coordinating roles and responsibilities for the implementation of resilience objectives.

61. Establishing and formalising cooperation with relevant public authorities, including policymakers, law enforcement authorities, emergency services and defence actors is also relevant in this context. Critical entities are encouraged to clarify of roles and procedures for information sharing, the notification and coordination of incidents, and mutual expectations.

62. Establishing and formalising cooperation with relevant private sector actors in the entity's own sector, other sectors and other Member States may also be considered.

63. Crisis communication protocols should be established to ensure timely and accurate information flow to internal and external stakeholders (including customers and the public) during incidents. Critical entities should maintain pre-approved communication templates, stakeholder notification routines and multi-channel communication capabilities, including redundant systems. Communications should be adapted to different audiences, including consideration of multiple languages and accessibility requirements.

64. Multi-scale redundancy design ensures services can be delivered at cross-border, national, regional and local levels with effective interoperability.

65. Critical entities are encouraged to ensure that emergency response procedures encompass multi-channel alert systems with geo-targeting capabilities, such as the space-based Emergency Warning Satellite Service of the Galileo Programme, clear communication chains of command, including designated spokespersons, and hazard-specific standard operating procedures (SOPs) tailored to site-specific risks. Critical entities should maintain emergency equipment, designate and train emergency response teams, and ensure evacuation procedures are accessible and regularly practiced.

E. RECOVERY MEASURES (Article 13(1)(d) of the Directive)

66. To ensure the continuity of operations, critical entities are encouraged to consider redundancy measures ensuring that essential services continue to be provided when primary systems fail. Such measures may include identifying which specific sub-services are most critical so that they are the first to be restored (service prioritisation), maintaining the ability to operate hardware manually if the automated or AI-driven systems fail or are tampered with, and workforce recovery in case of a disruptive incident.

67. Alternative sites for disaster recovery can be hot sites (fully equipped for immediate use), warm sites (partially equipped), or cold sites (requiring post-disruption setup). Backup locations should be sufficiently distant from primary facilities while remaining accessible. Where possible, mobile facilities (e.g. command centres) should be considered. Backups should be stored in physically separate or logistically isolated locations.

68. Without prejudice to the NIS2 Directive ([23]), critical entities should develop and maintain comprehensive business continuity plans (BCPs) based on business impact assessments (BIA) that identify critical functions, establish recovery priorities and define recovery time objectives (RTO) and recovery point objectives (RPO), including the establishment of service level agreements (SLAs). BCPs should specify clear activation criteria, resource allocation, roles and coordination mechanisms for response, recovery, resumption and restoration phases. They should be tested, reviewed and updated at planned intervals and following any significant incident or change to operations.

69. Crisis-management procedures should include incident command structures (ICS) with clearly defined decision-making authority and documented incident action plans. Critical entities should consider establishing crisis teams with predefined roles, escalation protocols, appropriate training, communication channels (primary and alternative) to ensure rapid and coordinated responses to disruptive incidents.

70. Workforce planning should address surge capacity requirements by maintaining a surge roster, training programmes and pre-established mutual aid agreements with partner organisations. Critical entities should develop competency frameworks and succession planning to ensure adequate depth in critical roles and maintain operational capability during extended disruptions or staff shortages.

71. To ensure effective recovery from incidents, critical entities should implement phased restart protocols that prioritise the restoration of critical functions based on risk assessment or BIA findings. These protocols should include systematic validation procedures for critical systems, comprehensive testing of data integrity and functionality, quality control measures, and controlled transition from emergency to normal operations through gradual capacity increases and performance monitoring.

72. Post-incident investigations should use structured methodologies such as root cause analysis to identify systemic causes rather than immediate symptoms. After-action reviews (AARs) should be conducted following all exercises and actual incidents to capture lessons learnt, with findings systematically captured and integrated into updated procedures, training programmes and risk assessments to prevent recurrence and strengthen organisational resilience.

73. In terms of supply chains, resilience is essential in the context of recovery from disruptive incidents. In line with their risk assessments, critical entities should consider mapping the supply chain for the provision of their essential services, develop long-term supply chain resilience strategies and regularly review and update the supply chain contingency plan. They are encouraged to identify alternative supply chains in case of disruptive incidents affecting their key supplier(s).

([23]) In particular, Article 21(2)(c) of the NIS2 Directive.

74. Critical entities should consider strategic stockpiling including buffer stocks, quick resupply mechanisms and off-site storage protected from common threats so that if the supply chain is disrupted, essential services are not interrupted.

75. Setting up formal contracts with other entities in the same sector to share resources, equipment or staff during a large-scale recovery effort is also worth considering.

F. EMPLOYEE SECURITY MANAGEMENT MEASURES (Article 13(1)(e) of the Directive)

76. Staff-related threats should be assessed and addressed so that the risk of human error, sabotage, insider threats and the risk of absence due to illness, emergency or external threats are mitigated. Critical entities are encouraged to identify and set up lists of categories of staff who exercise critical functions, including staff from external service providers (contractors and subcontractors).

77. When setting up these lists, critical entities should take into account the particularities of the essential services provided and link those services to the staff involved in their provision. To this end, critical entities should keep clear, comprehensive and up-to-date documentation of these categories of staff.

78. In addition to the considerations related to access rights above, critical entities are encouraged to establish to whom and under which conditions access to premises, critical infrastructure and sensitive information is given. Effective processes for granting and immediately revoking physical and system access should be in place and access rights should be strictly enforced.

79. Critical entities are encouraged to grant permission only on a need-to-know/need-to-access basis; only the minimum level of access necessary for staff to perform their role should be granted. Implementation strategies such as role-based access control (RBAC) ([24]), strong authentication and identity management ([25]), the separation of duties ([26]), time-based restrictions and just-in-time access ([27]) should be put in place, together with regular auditing and reviews.

80. In terms of background checks, in order to ensure a high level of employee security, it is important to implement robust internal procedures for requesting background checks in accordance with Article 14 of the Directive and to designate the categories of people required to undergo such background checks. Procedures for dealing with employees whose security clearance is withdrawn should also be put in place.

81. Critical entities are encouraged to define the background check policy, outlining which roles are sensitive, which roles have direct or remote access to premises, information or control systems, and the types of checks to be performed for each sensitive role, such as identity verification, criminal and employment records and education.

82. Where applicable, the measures should be coherent with the activities for background checks pursuant to the Commission Implementing Regulation (EU) 2024/2690 ([28]). Coherence with the human resources security measures taken by the entity in question pursuant to Article 21(2)(i) of the NIS2 Directive should also be ensured.

([24]) This could mean defining specific roles such as 'physical security guard', assigning a pre-defined set of access rights, and assigning staff to the relevant roles.

([25]) This could mean multi-factor authentication and unique identifiers.

([26]) This could mean designing access controls to ensure that no single individual has sufficient access to complete a critical, high-risk process on their own. For example, the person who approves a system change should not be the same as the person who implements the change.

([27]) Staff should only be granted access temporarily when they actively need it for specific tasks. Access should then be revoked immediately. There should be a policy restricting access rights outside specific working hours, where appropriate.

([28]) Point 10.2 of the Annex.

83. Requiring staff to have adequate qualifications and training, and providing such training, are part of ensuring appropriate employee security management, raising staff awareness of resilience measures and supporting the resilience measures taken by the critical entity in question. The critical entity risk assessment, the type of essential services it provides, and the measures planned or taken should determine the type and scope of training needed for its staff, to ensure that staff are not only generally aware of resilience measures but also technically and procedurally competent to execute their duties in a resilient way.

84. Training and qualification requirements relate to, among other things, risk assessment (e.g. for management/risk compliance staff), business continuity and crisis management (e.g. for business continuity staff), physical security (e.g. for security staff and those with access rights), incident response and mitigation (e.g. for operations staff, designated incident responders), access control and vetting (HR, security staff and managers of critical functions) and general awareness of resilience measures (of all employees).

85. Qualification requirements depend on the specificities of the critical entity in question and the essential services it provides. The objective of such requirements should be to ensure that staff are competent to execute the tasks outlined in the risk assessment and the resilience plan and in the business continuity and incident response protocols embedded in the resilience plan, within the scope of the resilience measures that critical entities take. Qualification requirements relate to operational and technical, organisational and management, or security and vetting tasks. The qualifications required should be defined in the internal resilience and HR policies of the critical entity in question.

G. AWARENESS-RAISING MEASURES (Article 13(1)(f))

86. A good programme to make staff aware of the resilience measures adopted by the critical entity and instilling a security culture are essential; staff are a vital element at every stage of the resilience cycle, from preventing disruptive incidents and mitigating insider threats to responding to them by activating the relevant procedures, reporting incidents and ensuring business continuity, as well as restoring operations to their pre-incident state. Without knowledgeable staff, even the best technical, security and organisational measures could fail.

87. Subject to sensitive information and on a need-to-know basis, raising awareness of resilience measures ensures an optimal resilience culture that makes resilience a shared value among the staff of a critical entity and reduces the risk of insider threats or social engineering.

88. Awareness-raising measures should be taken in conjunction with the measures for basic cyber hygiene practices and cybersecurity training pursuant to the NIS2 Directive ([29]).

89. Training organised by a critical entity is to be linked to the training requirements of the critical entity mentioned in points 82 and 83 above.. Training courses should cover the resilience measures taken by the entity in accordance with Article 13(1)(a) to (e) of the Directive, thereby covering the entire resilience lifecycle. This means understanding the threat landscape, the role of the critical entity in maintaining vital societal functions and the severe consequences of service disruption, recognising and reporting suspicious activities, vulnerabilities or unusual incidents promptly, and responding to and mitigating incidents. Function-specific training for staff with critical functions should be ensured.

90. Critical entities are also encouraged to consider training on gender-sensitive approaches, which, together with monitoring relevant indicators, may strengthen resilience, accountability and long-term sustainability.

([29]) Article 21(2)(g) of the NIS2 Directive.

91. Information materials shared with staff should be directly connected to the entity's risk assessment and the resilience measures taken. Such information materials should be clear and easy to digest and should explain the critical role of the entity and the impact of disruptions on society and the economy, all-hazards coverage, core security principles such as 'see something, say something', and the 'least privilege' principle for access to sensitive information.

92. Information materials could include visual materials for quick reference about e.g. physical security breaches, a loss of power/connectivity, the discovery of suspicious parcels, incident notification flowcharts and business continuity reminders extracted from the business continuity plan, physical protection guidelines and access control policies. To maximise awareness, these materials should be delivered in multiple formats such as digital ([30]) and physical ([31]), and be interactive ([32]).

93. Exercises are crucial for validating a critical entity's resilience plan and ensuring that its staff can perform their roles effectively during a real incident. In an all-hazards approach, entities could organise discussion-based exercises such as tabletop ([33]) simulations, and operations-based exercises such as drills ([34]).

94. In organising exercises, critical entities should focus on the outcome of their risk assessment, test the full cycle of resilience, and ensure good cross-sectoral coordination with other critical entities, where appropriate, to test cross-sectoral dependencies. They should ensure cooperation with relevant public authorities such as law enforcement, fire fighters, other emergency services and first responders in general in case of disruptive incidents and involve these public authorities in the exercises.

([30]) For example, intranet, mandatory e-learning modules with quizzes, short videos, screensavers with key safety reminders.
([31]) For example, posters, leaflets, quick-reference cards.
([32]) For example, frequently asked questions.
([33]) Testing the coordination, decision-making and communication processes during a simulated incident (e.g. major infrastructure failure, prolonged power outage, internal security breach).
([34]) Testing a specific, time-critical procedure such as activating the emergency generator, evacuating a critical area or isolating a compromised control panel.