



**Cabinet Office**  
70 Whitehall London SW1A 2AS

Dame Meg Hillier MP  
Chair, Public Accounts Committee  
House of Commons  
London  
SW1A OAA

By email to: [pubaccom@parliament.uk](mailto:pubaccom@parliament.uk)

28 February 2024

Dear Chair,

Following last week's PAC hearing on Preparedness for Extreme Weather, I agreed to write to you to set out how the Cabinet Office Resilience Directorate is taking forward the commitment in the Resilience Framework to:

**By 2030:**

***Introduce standards on resilience across the private sector, where these do not already exist, adjusted to take into account the current landscape, priorities and needs across and between sectors. Build upon existing resilience standards for CNI to create common but flexible resilience standards across CNI, and do more on the assurance of CNI preparedness. Review existing regulatory regimes on resilience to ensure they are fit for purpose. In the highest priority sectors that are not already regulated, and for the highest priority risks, consider enforcing standards through regulation.***

The Framework further says "*Partnerships with the private sector and experts will be strengthened to deliver and inform vital work on resilience. To support a new way of partnership working with the private sector, the UK Government will provide guidance on risk in order to help the private sector to meet new standards on resilience. These standards will be enforced through regulation only in the highest priority cases. The UK Government will build on existing structures to draw in external expertise and challenge to ensure that our approach is based on wide ranging knowledge and experience.*"<sup>1</sup>

As I said at the Public Accounts Committee meeting, before we look to direct any new measures from the centre of government, which may otherwise conflict or duplicate duties or incur disproportionate regulatory burdens or costs on businesses and consumers, it is important that we understand the existing extensive landscape of standards and regulation

---

<sup>1</sup> Page 6,  
[https://assets.publishing.service.gov.uk/media/63cff056e90e071ba7b41d54/UKG\\_Resilience\\_Framework\\_FINAL\\_v2.pdf](https://assets.publishing.service.gov.uk/media/63cff056e90e071ba7b41d54/UKG_Resilience_Framework_FINAL_v2.pdf)

across sectors, and what is in development already and how far they deliver the desired outcomes.

It is a longstanding principle, endorsed by successive governments, that resilience responsibilities should flow from business-as-usual activities. Resilience is a collective task that is part of the mainstream of organisational activity, and holding it separately diminishes its impact and effectiveness. This organising principle means that resilience responsibilities sit within wider economic, social and safety regulatory frameworks, and are balanced carefully against other priorities such as taxpayer and customer costs. Where we have cross-cutting expectations, such as those found in the Civil Contingencies Act, we are ensuring proper connection between those frameworks.

For example, there are sector specific standards and licence conditions overseen by regulators including Ogem,<sup>2</sup> OfCom,<sup>3</sup> Ofwat and the Environment Agency,<sup>4</sup> the Health and Safety Executive (HSE),<sup>5</sup> and the Office for Nuclear Regulation (ONR)<sup>6</sup> - both in terms of general resilience of operations and supply, and also specifically in terms of the continuity of provision of essential services, and requirements for when services are interrupted including time taken to recover. There are also sectors that do not have regulators, but are still subject to regulation, legislation and standards.<sup>7</sup>

Nevertheless, and as reflected in the ambition set out in the Resilience Framework, the Government believes that we can and should tighten up this system. Our review shows that some of the existing regulations are sector specific (vertical) while others are thematic and cross several sectors (horizontal). Further, some standards are inspected and enforced by regulators, such as those included in footnotes 2-6, while others are common organisational standards on a voluntary or accredited basis, e.g. British Standard 65000 on organisational resilience, ISO22316 on enhancing organisational resilience, or ISO22301 on international

---

<sup>2</sup> The Energy sector is a highly regulated industry, with regulation and standards built into licensing conditions, enabling enforcement action to be taken where owners and operators are in breach. There are numerous industry codes covering physical, cyber and hazard vectors; Licence Conditions (including those to protect and make infrastructure more resilient, but also to adequately respond to incidents that occur, such as the Electricity System Restoration Standard) and the Gas Act 1986 and Electricity Act 1989.

<sup>3</sup> For the Telecommunications sector, there are several standards and conditions, including the General Conditions of Entitlement, which relates to network functioning requirements; and the Network and Information Systems Regulations 2018, which are General legal duties providers must adhere to manage the risks to those network and information systems that underpin the provision of those essential services.

<sup>4</sup> For the Water sector, examples include the Network and Information Systems Directive; Water Supply (Water Quality) Regulations 2016; and Security and Emergency Measures Direction (SEMD) 2022. SEMD requires water companies to meet 33 outcomes spanning contingency planning, emergency preparedness, security, testing and exercising, and implementation of response plans. Further, HMT's National Infrastructure Strategy sets a requirement for the water industry to plan to deliver resilience to a one in 500-year drought.

<sup>5</sup> HSE monitors regulation on safe shutdown of Chemical sites. They also have an inspection regime related to the cyber security of the safe storage of Toxic Gases.

<sup>6</sup> The ONR has extensive powers to inspect and enforce regulation and statutory guidance, including the Security Assessment Principles (SyAPs) for cyber, physical and personnel security.

<sup>7</sup> The Defence sector is not regulated in the same way, but is subject to the same legislation and regulations as other sectors, such as JSP 440 and 503 on defence security and resilience. In a limited number of areas there are Defence exemptions in place, which have their own regulatory structures in place, such as the Defence Safety Authority.

standard for Business Continuity Management. Therefore, we will need to design carefully the interaction between standards and the right means to oversee them for assurance purposes.

For example, as Mr Hargreaves and I said at the hearing, if standards are self-reported, independently assessed and verified, inspected, and enforced by regulators and/or underpinned in legislation, we must be cautious of putting in place horizontal adaptation standards that apply across all sectors. Such actions might resolve the cross-sector consistency problem, but could instead create other problems, such as clashes across vertical sector-specific regulations. This could potentially lead to an extremely complex set of challenges in navigating and applying the measures.

Another factor to consider, as outlined at the Committee, is that standards and regulations that lead to general and broad improvements come at a cost to the businesses, and it is important to consider where those costs flow to. For example, they can sometimes be passed on to consumers through their utility bills, where the overall burden and customer affordability will be a key consideration. Furthermore, relevant regulatory multi-year cost control periods will need to be understood and factored into infrastructure improvement plans and target dates for implementation of the standards.<sup>8</sup>

Finally, the Resilience Directorate is responsible for overseeing resilience in a holistic, all-threats-and-hazards approach across the 89 National Risk Register risks. Therefore, while appropriate standards across the extreme weather and climate adaptation risks are a priority for us, we also need to act on other urgent threats, and for example we are already putting in place and extending across wider sectors standards for cyber security, through the Network Information Systems (NIS) regulations.

Mapping the standards and regulatory landscape is therefore a large and complex task, which is why 2030 was set as the implementation date for this Resilience Framework commitment. But as I also said at the Committee, 2030 is not a target date and we will deliver the commitment sooner if possible, particularly where there is an urgent need. Equally important to note is that we are not holding back other parties putting in place standards sooner. Our interest is in ensuring that the priority risks are addressed and the landscape is efficient and coherent and delivers the desired outcomes overall.

In order to make rapid progress, we have been building the requisite data and engaging across the private sector and their sponsoring departments in government to understand the current standards and regulatory landscape and where further measures may be required. This will allow us to take forward this programme in a structured way. Our activities include:

- (1) Assessing what is already in place in terms of standards and regulation (and associated targets and metrics);
- (2) Understanding what is in development across sectors in terms of vertical and horizontal standards, as well as voluntary measures by companies or sectors and those underpinned by regulatory policy or interventions;

---

<sup>8</sup> For example on the energy sector

<https://www.ofgem.gov.uk/energy-policy-and-regulation/policy-and-regulatory-programmes/network-price-controls-2021-2028-riio-2/electricity-distribution-price-control-2023-2028-riio-ed2> and in the water sector <https://www.ofwat.gov.uk/regulated-companies/price-review/2024-price-review/>

- (3) Assessing how far these activities take us in terms of the outcomes needed, in order to mitigate priority risks;
- (4) Using the integrated data we are developing on vulnerabilities and gaps, and assessing which of the above measures would best deliver the outcomes we are seeking for the defined priority risks;
- (5) Advising Ministers where and how we should act, including taking account of better regulation principles, costs to the Exchequer and the private sector, and how costs may impact consumers and taxpayers. This would also include consideration of the timing of any interventions in order to maximise impact, whether by the Cabinet Office or by individual Departments for their sectors.

In line with (1) to (5), activities to date and planned events to inform the approach include:

- Carrying out a cross-departmental review, to map the landscape of current powers and duties across critical sectors, via the Government Legal Department;
- Meeting with the British Standards Institution on the standards framework and our different options in terms of setting and embedding standards;
- Carrying out a cross-cutting self-assessment exercise across all departments that sponsor CNI. This detailed survey, comprising 93 questions across risks and preparedness information categories, has allowed us to identify strengths and areas for improvement across departments, sectors and thematic risk areas captured in the National Security Risk Assessment (NSRA);
- Mapping CNI assets across the country in the Knowledge Base database. This allows us to identify interdependencies across critical infrastructure and systems, including where there may be a case for strengthening arrangements;
- As part of the Third National Adaptation Programme examining the Climate Change Committee's Climate Change Risk Assessment (CCRA3) risks, we are facilitating a series of workshops to assess impacts across sectors of extreme heat impacts over time. We also plan to take a similar approach for droughts, wildfires and flooding;
- Attending workshops with the UK Regulators Network, the Institute of Regulation, essential service providers and consultants to understand measures and resilience activities in place, and how we can most effectively develop this framework in future;
- Integrating the data we hold from the NSRA, Department and Sector Capabilities Assessments and exercises to inform our focus on any priority vulnerabilities;
- A series of workshops with the National Infrastructure Commission and sector-sponsoring departments to inform the relevant climate adaptation standards that should be developed;
- Attending a conference workshop and planning an exercise to test the interactions between the financial sector and electricity and communications sectors, again to inform where improvements may be needed;
- Examining a potential option for a future unifying 'umbrella' HMG Resilience Functional Standard that clearly articulates the desired practices, guidelines and systems for continual resilience improvement. This will support collaboration across organisational boundaries, and support efficient and effective delivery of public services across sectors. We envisage this standard may be helpful to shaping the UK Resilience Academy's syllabus for assuring continuity and consistency across training and preparedness, and mandating the recording and implementation of lessons identified into future planning and doctrine;

- Engaging with HM Treasury and departments that oversee the economic regulated sectors to understand the timing and nature of the cost control periods, and how the infrastructure investments are costed and recovered, and within these, our opportunities for interventions;
- Engaging internationally on standards and regulation in other jurisdictions in order to learn from approaches elsewhere. This includes attending meetings with senior officials from Australia, Canada, New Zealand and the USA in our 'C5' CNI group, as well as with the OECD and NATO and their members;
- Assessing the needs of vulnerable people and the support they need, as well as defining those vulnerabilities for different scenarios, again to support any regulatory requirements or standards then we may need to embed further to what is already in place. This is also informing the approach to economic regulation announced in the 2023 Autumn Statement;
- The Government further announced in the Autumn Statement up to £10 million of funding over 2024-25 and 2025-26 to finance research on risks to the economy and public finances, including the understanding of risk impacts, their potential mitigations and response preparations. This research will help to ensure the stability of the macro-economic environment and support the sustainability of the public finances, and we are currently working with HMT to develop the approach for utilising this fund; and
- Placing the Resilience Standards<sup>9</sup> on a statutory footing for Category 1 and 2 responders<sup>10</sup>, requiring they have due regard to the standards whilst fulfilling their duties under the Civil Contingencies Act. The standards are already frequently used by the Local Resilience Forum community, but this change would raise their profile with the aim to increase consistency in their usage.

The aim of the above activities is to provide a firm evidence base and business case for advice to Ministers on options for further standards related work, where they are not already in place elsewhere, as well as regulations across the relevant sectors where needed.

This year we expect to bring proposals to the Director-level cross-government Resilience Steering Board, or the Climate Resilience Steering Board specifically in relation to extreme weather and adaptation. The Ministerial National Security Council (Resilience) will also consider these matters.

I hope the above makes clear the extensive work we have been taking forward, and will continue across the course of this year and beyond toward the implementation of the Resilience Framework commitment.

---

9

[https://assets.publishing.service.gov.uk/media/5f4e1107e90e071c6c7d940c/NRS\\_for\\_LRFs\\_V3.0\\_Aug2020.pdf](https://assets.publishing.service.gov.uk/media/5f4e1107e90e071c6c7d940c/NRS_for_LRFs_V3.0_Aug2020.pdf)

<sup>10</sup> The Civil Contingencies Act 2004 divides local responders into two categories, imposing duties on each category. Category 1 responders are those organisations involved in most emergencies (emergency services, local authorities), Category 2 organisations are less likely to be involved in the heart of planning work but will be heavily involved in incidents that affect their own sector (utilities, transport operators).

**Yours sincerely,**

*M. Clarke*

**Matthew Clarke**

**Resilience Director and Head of Resilience, Cabinet Office**