

(as submitted online by nima to MHCLG on 20 March 2026)

Nima response to The Single Construction Regulator Prospectus - Consultation Document (December 2025). CP 1464

11 Where do each of the proposed outcomes for the system sit on a scale from very useful to not useful at all?

Useful

2 What role would you and/or your organisation play in achieving these outcomes?

Nima is a UK-based not-for-profit, virtual, volunteer-led organisation committed to better information and data management. It supports digital transformation across the built and managed environment.

Established as the UK BIM Alliance in 2016 to continue some of the work of the UK BIM Task Group, nima incorporates bSUKI, the UK and Ireland chapter of buildingSMART International.

With the British Standards Institution, nima maintains the IMI Framework (formerly the UK BIM Framework), the overarching approach to implementing BIM in the UK and a repository of guidance on data and information management best practices.

Nima leads the Information Management Initiative (IMI), launched in partnership with the Construction Leadership Council in November 2024.

In this context, nima acts as a convening body that can help government and the regulator bridge policy, standards, practice, education, and implementation. It can help align standards, market guidance, competence development and industry adoption around practical information management expectations.

3 What will be the most important factors to achieving the proposed outcomes?

A single construction regulator will only be effective if it can rely on structured, assured, accessible and interoperable information across the whole building lifecycle. Without that, the regulator risks inheriting fragmented submissions, inconsistent terminology, duplicated reporting, weak audit trails, and poor transfer of knowledge between design, construction, occupation, refurbishment, and enforcement. To state matters plainly, information failure becomes regulatory failure.

4 What are the most important barriers that could prevent the proposed outcomes from being met?

If information standards are inconsistent, if systems do not interoperate, or if data cannot be trusted over time, then safety assurance becomes weaker, slower and more expensive. In practice, it also becomes a) harder to evidence, and b) more reliant on interpretation rather than verifiable data.

In short: interoperable, assured information is a precondition for effective building safety regulation across the asset's whole life-cycle.

Chapter 2: Integrating the regulatory system (2.4 Digital, Data and Efficient Regulatory Delivery)

6 Have you experienced any challenges with providing information via government digital services when complying with current regulatory requirements across products, professions and buildings?

Yes.

Common industry challenges include inconsistent data structures, repeated manual entry, poor interoperability between systems, uncertainty about required formats, and weak alignment between regulatory requests and how information is generated and managed in projects and asset operations.

7 How should the new regulator promote consistent digital standards and interoperability across the lifecycle of a building (including products, professions and buildings)?

1.1 Nima notes the consultation document's discussion (p.28) regarding the competence, capacity and conduct of professionals working in the built environment. The Information Management Initiative (IMI) is relevant here.

1.2 When the IMI was launched in November 2024, nima and the Construction Leadership Council pointed out that existing 'mandates' regarding information management (in the *Construction Playbook* and in Annex B of *Transforming Infrastructure Performance: Roadmap to 2030*, published in 2022) were:

- a) never formally mandated
- b) focused on 'information' not 'data and information'
- c) did not cover all lifecycle phases of the built and managed environment
- d) did not clearly articulate the value and benefits
- e) gave little practical guidance to individual users, and
- f) ineffective while much of industry was still in the early phases of digital adoption.

1.3 The IMI is intended to address these shortcomings. Its mission is:

To enable the digital integration of data and information across the whole lifecycle of the built and managed environment, enhancing collaboration, efficiency, safety and sustainability to meet the evolving needs of society, business, and the environment.

1.4 The IMI approach:

- a) builds off developments to date - notably, the UK's world-leading efforts to create BIM standards and guidance, now being broadened to embrace other areas of digital working
- b) sets an industry directive (ie: a direction of travel) that will help galvanise organisations (individually and collectively) to build their information management competences and capacities, which might then ultimately be Government-supported through procurement, regulation and legislation
- c) is supported through an evolving ecosystem of standards, guidance, tools, case studies and training (building on the UK BIM Framework – now the IMI Framework), and
- d) is founded on principles (see 1.5 below) and rules, tailored to groups across industry, that will provide clear guard rails to fulfil the outcomes and obligations.

- 1.5 The IMI sets out four key principles relating to purpose, people, process, and data and information:
- a) **Recognise the whole life purpose of information and data:** Identify the relevance and purposes of data and information to improve organisational and project outcomes, and consider an asset as both the physical structure and the data and information held to manage it (see also 1.16-1.18).
 - b) **Upskill people in information management:** Establish basic digital literacy as an organisational minimum requirement, make relevant data and information management skills part of individuals' continual professional development, and recognise and empower 'IM leadership'.
 - c) **Take a common, consistent and data-centric approach:** Converge on a common framework to define, procure, deliver, store and use interoperable data and information, and incorporate a data and information architecture relevant to the organisation and its collaborators.
 - d) **Establish clear data and information governance principles:** Adopt clear approaches on stewardship, ethics, quality, security, interoperability, longevity, openness and integrity of data and information; enable sharing and easy use of the right data and information at the right time and in the right structure by considering data and information independently from technology (see ss.1.8-12 for more detailed comments regarding interoperability).

1.6 The potential IMI outcomes include:

- a) adoption of consistent, standards-based information practices (e.g. ISO 19650)
- b) upskilling of teams in digital and data capabilities
- c) strong governance regarding trustworthy, secure and interoperable data
- d) alignment with national strategies for net zero, safety, productivity, etc

1.7 Nima is also developing its education and upskilling strategy, and has begun a detailed review of the competences needed by those working in the built and managed environment, consulting on potential updates to the sector's Learning Outcomes Framework (LoF) regarding information management.

1.8 In 2023, nima's 'think-tank', the GIIG, published *Delivering valuable data: An interoperability code of practice for technologies in the built and managed environment*. The code of practice was intended to help organisations achieve 'greater sharing of better data' and deliver better whole life outcomes in line with UK construction strategy.

1.9 The core focus was **interoperability**:

Information created or stored on a technology should be capable of secure exchange with other systems so that it can be used and managed. It should not be dependent on the technologies or services used to produce or process it.

1.10 The code of practice recommended five underpinning principles be applied:

- a) **longevity** – enabling long-term findability, access, reuse and exploitation, and continued value, of information
- b) **security** – maintaining security, confidentiality and privacy protections, while allowing sharing of non-sensitive information for the public good
- c) **information value** – enhancing the value of information created, managed and shared by technology-using professionals

- d) **information ownership** – ensuring enduring ownership and control by asset owner-operators of valuable data about the assets they own
- e) **competition** – promoting fair competition between technology providers (and indirectly among supply chain users of technologies)

1.11 For interoperability and the five underpinning principles, the Code of Practice recommended obligations for technology providers:

- a) **Interoperability** – ... ensure that their products or services support the exchange of non-proprietary information without loss, amendment, mis-interpretation or additional work for users, so that the integrity and value of information is not compromised.
- b) **Longevity** – ... ensure that their products or services support the continued findability, accessibility, interoperability and reusability of information – including for audit trail, provenance or regulatory purposes – throughout the lifecycle(s) of the asset(s) to which it relates.
- c) **Security** – ... support a risk-based holistic approach addressing people, process, physical and technical security aspects in response to a documented risk assessment; and adhere to advice from the National Cyber Security Centre and the National Protective Security Authority
- d) **Information value** – ... ensure they are able to help contracting authorities and their suppliers to maximise the value of the information deliverables that users create and exchange, and, particularly when providing long-term information management ‘stewardship’ services to an asset owner-operator, support users in maintaining the value of that information
- e) **Information ownership** – ... ensure that their products or services help asset owner-operators to assert and secure unrestricted ownership and control of their asset-related information.
- f) **Competition** – ... ensure that their products or services support non-proprietary exchanges of information between contracting authorities and their suppliers, and between suppliers.

Information management principles and the regulator

1.12 Nima feels the principles in the IMI and in the Code of Practice should be embedded in the construction regulator’s digital operating model guidance, procurement expectations, and interface requirements.

1.13 Existing government guidance (for example, in the GDS/CDDO Technology Code of Practice) on open, interoperable information requirements should be reinforced to avoid proprietary platform dependence. For regulated activity, government should be cautious about creating de facto dependency on closed vendor ecosystems.

1.14 Regardless of the software platform used to create it, regulated information must remain usable, portable, auditable, and intelligible over time. This is critical not only for competition and market fairness, but for regulatory resilience, enforcement, future investigations and long-term asset stewardship.

1.15 A single construction regulator will only be effective if it can rely on structured, assured, accessible and interoperable information across the whole building lifecycle. Without that, the regulator risks inheriting fragmented submissions, inconsistent terminology, duplicated reporting, weak audit trails, and poor transfer of knowledge between design, construction,

occupation, refurbishment, and enforcement. To state matters plainly, **information failure becomes regulatory failure.**

Interoperability, building safety and lifecycle assurance

1.16 There is a very direct relationship between the quality of information and the ability to manage safety risks in higher-risk buildings and other complex assets. The regulator will need to deal not only with design intent, but with design change, construction evidence, product traceability, commissioning records, operations data, maintenance history and ongoing safety case information.

1.17 If information standards are inconsistent, if systems do not interoperate, or if data cannot be trusted over time, then safety assurance becomes weaker, slower and more expensive. In practice, it also becomes a) harder to evidence, and b) more reliant on interpretation rather than verifiable data. In short: **interoperable, assured information is a precondition for effective building safety regulation across the asset's whole life-cycle.**

1.18 The focus on the whole life-cycle is something that is incorporated into proposed revisions to ISO 19650 Parts 1-3 (public consultation on parts 1 and 2 is currently [March 2026] in progress).

Consistent information and data requirements

1.19 This consultation is timely insofar as it can build on recent progress. The 'golden thread' principles — accurate, accessible, up-to-date and understandable information — demonstrate alignment with existing regulatory expectations. However, the industry is currently dealing with fragmentation between regulatory requirements, client requirements, asset management systems and supply chain tools.

1.20 Developers, asset owners, and clients need clarity on what information is required, when, in what format, to what standard and for what purpose. They also need confidence that information produced at gateway, handover and occupation/operational stages can be reused rather than recreated. A single regulator should therefore drive consistency in data requirements. Dutyholders should not be forced to respond to multiple overlapping or contradictory requests.

1.21 This is important commercially as well as operationally. Poorly coordinated information requirements increase transaction costs, delay decisions, increase disputes and weaken accountability across the supply chain. This will resonate strongly with both clients and delivery teams.

Standard information approach

1.22 To help reinforce requirements-led processes, the ongoing IMI is developing a standard information approach, working closely with the Manufacturers Information Hub to develop one joined-up approach. This (together with the organisational support that the IMI provides and the LoF) connects all three of the areas (building, products, professionals) that the Government wants to combine. It would also mean they are working in the same information system as other stakeholders such as insurers.

1.23 A standard information approach can also encompass automated checking and AI. The UK has already invested in this area, exploring, for example, how machine-readable building

regulations can be deployed to help meet regulatory requirements and provide constraints. Having verified, consistent manufacturers' product information is a key part of the puzzle.

Good IM practice adoption and proportionality

1.24 The regulator will need to bring industry with it. Many organisations are still at a relatively early stage in digital maturity, and many SMEs will be wary of a model that appears to create additional compliance burdens.

1.25 The regulator should promote a phased, principles-based and outcomes-led approach, supported by common standards, guidance, exemplars, and education. The emphasis should be on better information, better structure, better governance, and better interoperability, rather than more bureaucracy.

8 What digital tools and platforms do you find most effective for ensuring you meet regulatory compliance and why?

The most effective tools are those that support structured information, version control, auditability, secure sharing, open exchange, traceability of decisions and integration across disciplines and lifecycle stages without referencing specific vendors.

9 What are the opportunities and risks associated with automating regulatory compliance checking (e.g. AI-driven assessment), and how should oversight, accountability and human review be retained within automated systems?

Automation has real potential in completeness checks, consistency validation, classification, and identification of missing or conflicting information. Automation of compliance checking is already implemented in several European countries and cities. Automation can use rules (symbolic AI) or large language models (LLMs) (neural AI). However, such automation must not displace accountable human judgment, particularly in safety-critical contexts. Any use of automation should be transparent, auditable, and explainable, with clear lines of accountability.

Nima has produced a position paper on AI, aiming to provide clear, relevant, objective guidance on the use of AI, and to encourage appropriate habits and behaviours. Intended for information managers, asset managers, technologists and product specifiers in the built environment. It outlines key factors relating to use of AI in decision-making and information management processes.

The paper's advice ranges across 15 areas, including the need to establish a clear business case for using AI. It then explores some of the key criteria in assessing the suitability and viability of applying AI to a decision-making process (levels of complexity, uncertainty, novelty, criticality, and ethical and security risks all need to be considered).

Legislative and regulatory requirements are also a key factor: the automation of legislation, regulation and standards should be allowed or licenced so as to empower both applicants and regulators to benefit from automation. The UK Government InnovateUK DCOM initiative has demonstrated that automation of compliance checking is feasible given sufficient data quality. Skills and knowledge needs are also covered, exploring the extent to which AI might, for example, reduce or blunt the skills of staff, and the need to understand how AI tools are trained.

The paper also thinks long-term: information managers need to think about the resilience of tools, the organisational systems / processes to use them, and the governance required over asset life cycles often measured in decades. The accelerating pace of change in technology and tools and the need to identify emergent learning are also covered, alongside the commercial and security risks of using AI.

Chapter 3: Roles and responsibilities in an integrated regulatory system

15 Do you agree with the principles set out in this chapter, and the proposed roles and responsibilities for government, regulatory bodies and industry?

Yes

16 What are your views on how the new regulator can work with industry to support culture change, towards a quality and safety-led culture? What sort of incentives or sanctions do you feel would be effective in supporting this change?

A single regulator will not succeed through structural change alone; it will need to influence behaviours, competence, and market norms. Culture change requires consistent expectations, visible leadership, clear client demand, competence development, and practical support for implementation which should include automation to manage the burden in the time and effort on both sides.

A balanced approach is needed. Incentives could include clearer procurement expectations, standardised requirements, recognition of good practice and reduced friction for organisations that provide structured, assured, and reusable information. Over-reliance on sanctions risks driving defensive compliance rather than meaningful improvement.

17 What are your views on how industry can best drive the culture change and respond effectively to the changes proposed in this prospectus? In your view, how prepared are individuals and businesses for these changes? What would support industry to be more prepared?

Industry capability is uneven. Some organisations are progressing well, but many are not. Businesses would be better prepared through clearer definitions, simpler common requirements, aligned standards, training pathways, practical guidance, exemplar data requirements and targeted support for SMEs. Equally, Government has been uneven in its commitment to making regulatory resources accessible.

- Ends -