Digital resilience

Introduction to workshop session

Localis

- Independent local government think tank
- Evidence-led, cross-party, place-focused
- Convening policy & practice
- Embracing complexity to apply insights and solutions to current English local governance context

Today’s session

- A short scene-setter: what it is, why it matters, what we’ll explore
- Focus: governing for ‘digital resilience’ and the continuity of services through change and crisis
- These slides are descriptive, not prescriptive
  - We’ll tease out actions and insights together

What do we mean by ‘digital resilience’?

- Digital resilience = keeping essential services **dependable** and sustaining **data + public trust** when:
  - *technology fails, suppliers change, or cyber incidents occur*
- It includes: **prevention → detection → recovery → learning**
- Three useful distinctions:
  - **Cyber security** (reduce likelihood of harm)
  - **Cyber resilience** (keep key functions going *despite* cyber events)
  - **Operational resilience** (people, routines, decision-making under pressure)

Why it matters now

- Public services are more digitally intertwined than even just a few years ago
- Four notable shifts are making digital resilience an increasingly live governance issue:
  - **Digitisation of core services** + higher availability expectations
  - **More disruptive threat landscape** (e.g., ransomware)
  - **AI and data-driven tools** → dependence on data governance + assurance
  - **Market volatility + legacy debt** constraining change and increasing risks

Continuity through change + crisis

- Disruption is rarely just ‘one thing’, it is usually off the back of cascading issues + confusion
- Common stress points (non-exhaustive):
  - **Identity & access** (who can do what, quickly and safely?)
  - **Data flows** (what is correct, what is current, what is shareable?)
  - **Supplier dependency** (support, pricing, exit feasibility)
  - **Operational handoffs** (who’s responsible during incidents?)
- The practical question: ‘**What is our minimum viable continuity?’**

Governance choices

- Resilience therefore depends on choices:
  - **Risk ownership** (who holds the risk, who can accept it?)
  - **Risk appetite** (what downtime/data loss is tolerable, if any?)
  - **Assurance** (how leaders gain confidence things will work)
  - **Decision-making rights** (who decides *fast* during an incident?)
- For this workshop: Taking digital resilience from just an IT issue to one of **accountability**, **decision-making** and **services**

LGR as a digital resilience ‘stress test’

- LGR compresses change across people, contracts, systems, governance
- Why it’s a stress test:
  - **Estate transition while services stay live**
  - **Supplier/contract changes** become operationally critical
  - **Data alignment** affects continuity (and future analytics/AI)
  - **Restructured governance** can disrupt incident response(s)

Hand-off to tables

- So today we're looking for examples, experiences, worries, trade-offs, actionable insights, etc. not 'perfect answers'. **Considerations & questions for you all to take back to your orgs**.
- On each table there should be a briefing note for a little more contextual information for you all.
- The first half will be on LGR and the second will be on digital resilience during times of cyber incidents/crisis
- Thank you for listening and we hope you enjoy the session today!