Local Government Association

public·digital

Cyber incident grab bag 2.0: supporting your response

27 April 2026

www.local.gov.uk

What we will cover today

1. Welcome
2. The reality of recovering from a cyber incident
3. What the grab bag is (and isn't)
4. How to use the grab bag in practice
5. Key updated content on coordination with central government
6. Keeping the grab bag updated moving forwards

Local Government Association

public·digital

1. Welcome

Why a grab bag?

- A field guide for councils in a cyber incident
- Built from lessons learned from real incidents
- Designed to support decisions when:
  - systems are down
  - pressure is high
  - information is incomplete

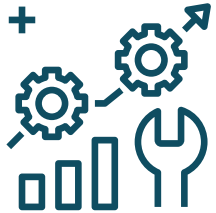
Local Government Association

public·digital

Who's it for?

INCIDENT RESPONSE

- Senior leaders coordinating the response
- Service leads maintaining critical services
- Digital/IT leads managing systems and recovery
- Communications teams managing messaging



PREPAREDNESS

- Leaders and officers testing readiness
- Service and digital teams running exercises
- Corporate teams identifying gaps and dependencies
- Teams building shared understanding across the organisation

Local Government Association

public·digital

> Like a friend who was alongside you during a very challenging time.

Local Government Association

The evolution of the Grab Bag

Then

- Focus on **whole-organisation response**
- Structured around stages of an incident (from initial response → recovery)
- Organised across 7 key themes, including:
  - Healthy teaming
  - Coordinating with government & law enforcement
  - Delivering services
  - Safely restoring systems
  - Protecting data

Now

- Added service-specific guidance for high-impact areas:
  - Adults' social care
  - Children's services
  - Finance
- New module on responding during complex organisational change
- Content updated based on real-world incidents and council feedback

Future

- Continue to expand service-specific modules
- Work with councils to co-develop and iterate content
- Evolve as a living resource based on emerging risks and needs

UX review

Light-touch review & enhancement of the current Grab Bag content, including learning from experience of real-life use

Adults'

NEW: Service specific content for adults' social care

Children's

NEW: Service specific content for children's social care

Finance

NEW: In-depth content for financial management after a cyber incident

Complex change

NEW: Guidance on responding to cyber impacts during a time of complex organisation change

Playbook

NEW: A playbook to support future enhancement of the Grab Bag and development of further new service modules

Local Government Association

public·digital

2. The reality of recovering from a cyber incident

Local Government Association

The incident itself is just the start

Initial hours and days

Emergency

Forensic analysis of the attack

Urgent continuity measures

Assessment of recovery options

Expect no access to systems

Weeks (and months) of business continuity

System recovery

Restoring systems and data

Working towards more sustainable continuity measures

Managing comms and reassurance

Expect to be using workaround systems

The months (and years) that follow as you recover

Restoring services

Rebuilding data and records

Clearing service backlogs

Rebuilding integrations with partners

Continuing to manage complex comms

Expect the return to normal to be slow & complex

Local Government Association

An example of a timeline

Local Government Association

public·digital

3. What the grab bag is (and isn’t)

What the grab bag is

- When a council is hit by a cyber incident
- Absolute priorities a council or service must consider
- Accessible
- Good practice, not ‘best’
- Community co-creation and evolvement
- Open resource

What the grab bag isn’t

- Comprehensive or overly descriptive
- Technical or for IT folk
- Doesn’t replace existing Business Continuity (BC) or Disaster Response (DR plans

What we did

Content design workshops

We ran **5 workshops** with attendance from a range of councils

Council engagement

42 council officers participated in the workshops

Partner review workshops

5 review workshops with partner organisations (central government, regulators, professional bodies)

Partner engagement

23 partner representatives participated in the workshops

Local Government Association

public·digital

4. How to use the grab bag in practice

Imagine you've identified a cyber incident…

Homepage – start here


Cyber incident grab bag for local authorities

A practical resource for responding to major cyber incidents.

Introduction

This is a tool designed to support councils through the early stages of responding to a serious cyber incident. The guidance helps councils to anticipate the likely challenges they will face, find support and authoritative information, and chart their course through to a sustainable recovery.

The grab bag does not replace your council's pre-existing Business Continuity Plans, Disaster Recovery Plans, or Emergency Plans. It should be used alongside those to guide you through the initial weeks of your cyber incident response. For further guidance and templates for these plans, visit the LGA's cybersecurity blueprint series.

The guidance is organised across eight themes which will apply across your response to a cyber incident. The grab bag also includes service specific guidance which provides more detailed advice for critical services.

- Healthy teaming: the steps you will take to ensure that you have the right people assigned to your response, effective coordination and a sustainable pace.
- Coordinating with central government and law enforcement: guidance on how to access support from central government, NCSC, NCA and other partners across government.
- Informing and supporting: advice to support your communications, engagement and work to build trust with residents, businesses, partners and colleagues.
- Delivering your services: guidance to support the deployment of your Business Continuity Plans and adapting them as the situation evolves.
- Safely restoring technology and systems: advice on how to ensure that your disaster recovery and system restoration work is safe, secure and helping you act strategically to enhance your overall cyber resilience.
- Protecting data: the measures needed to mitigate risks to personal and other sensitive data, and to ensure that you are complying with your responsibilities under the Data Protection Act.
- Working with elected members: coordination with elected members, including political leadership and other frontline councillors.
- How to make sure your incident plan reflects reality: guidance for managing a cyber incident when organisational complexity or change affects ownership, roles or decision making (for example, Local Government Reorganisation, political change, or shared services).
- Service specific guidance: guidance for specific services, where incidents create unique risks or challenges (for example, adult and children's social care).

Stages of your response

The grab bag is organised across four initial stages of your response to a cyber incident. These do not have exact timings, as the nature of any individual attack will vary, but they broadly reflect how a response evolves – from the initial hours, through the first days and weeks, and into longer term recovery.

The stages reflect the initial intensity and uncertainty that is typical following a cyber incident. They develop in line with the pace of your response, as more information becomes available and your plans progress.

The grab bag combines key strategic actions with learnings from other incidents to help you prioritise, coordinate and sustain your response.

Stage one: confirming the need to act (initial hours)

In the initial stages of a cyber incident there will be limited information, high pressure and a need to ensure that your first steps set you up for a successful response and recovery.

The guidance provided for this stage is designed to help you establish a clearer picture of the situation, take steps to alert relevant authorities and partners, connect with support, and prepare to mobilise your response.

Notification to government, law enforcement and partners

At this stage, you should notify the relevant authorities and partners as soon as possible.

- Report the incident to the NCSC, using their report a cyber incident tool
- MHCLG will be notified via the NSSC report but you can also contact them directly at: lgcybernotifications@communities.gov.uk
- If the incident involves a data breach (including unavailability of personal data), use the guidance provided by the information commissioner (ICO) to determine whether they need to be notified
- Report the incident to the police as a cyber crime using the Report Fraud service
- Consider contacting your local Warning, Advice and Reporting Point (WARP) for local security mutual support.

You can use the government's where to report a cyber incident tool to help identify the right organisations to contact.

Refer to the coordinating with central government and law enforcement agencies section for more information.

Stage two: taking your crucial first steps (days)

Cyber incident grab bag: Healthy teaming

Cyber incident grab bag: Coordinating with central government and law enforcement

Cyber incident grab bag: Informing and supporting

Cyber incident grab bag: Delivering your services

Cyber incident grab bag: Safely restoring technology and systems

Cyber incident grab bag: Protecting data

Cyber incident grab bag: Working with elected members

Cyber incident grab bag: Ensuring your incident response reflects reality

Cyber incident grab bag: Service and situational guidance

Introduction

Sections

Stages

hours
days
weeks
months

Sections

New!

Ensuring your incident response reflects reality

Service & Situational advice

www.local.gov.uk

Stages of your response

1	2	3	4
Notifications **(Summary + → coordinating with central government and law enforcement agencies)**			
Confirming the need to act	*taking your crucial first steps*	*building confidence through your response*	*designing your recovery path*
hours	**days**	**weeks**	**months**

www.local.gov.uk

From stages to sections

	1	2	3	4
Advice	*Confirming the need to act*	*taking your crucial first steps*	*building confidence through your response*	*designing your recovery path*
	hours	**days**	**weeks**	**months**
Advice	*Confirming the need to act*	*taking your crucial first steps*	*building confidence through your response*	*designing your recovery path*
	hours	**days**	**weeks**	**months**
Advice	*Confirming the need to act*	*taking your crucial first steps*	*building confidence through your response*	*designing your recovery path*
	hours	**days**	**weeks**	**months**

Seven sections covering the critical aspects of your response

www.local.gov.uk

Service and situational guidance

Cyber incident grab bag: Service and situational guidance

Detailed guidance to support specific council services and situations during a cyber incident.

Situational guidance

Use these modules where the nature of your incident or operating environment creates additional complexity.

Ensuring your incident response reflects reality

Use this module if your incident involves unclear ownership, or complex organisational arrangements. This often arises when councils operate across shared services, partners or suppliers, or where roles, leadership or governance arrangements are changing and not fully established.

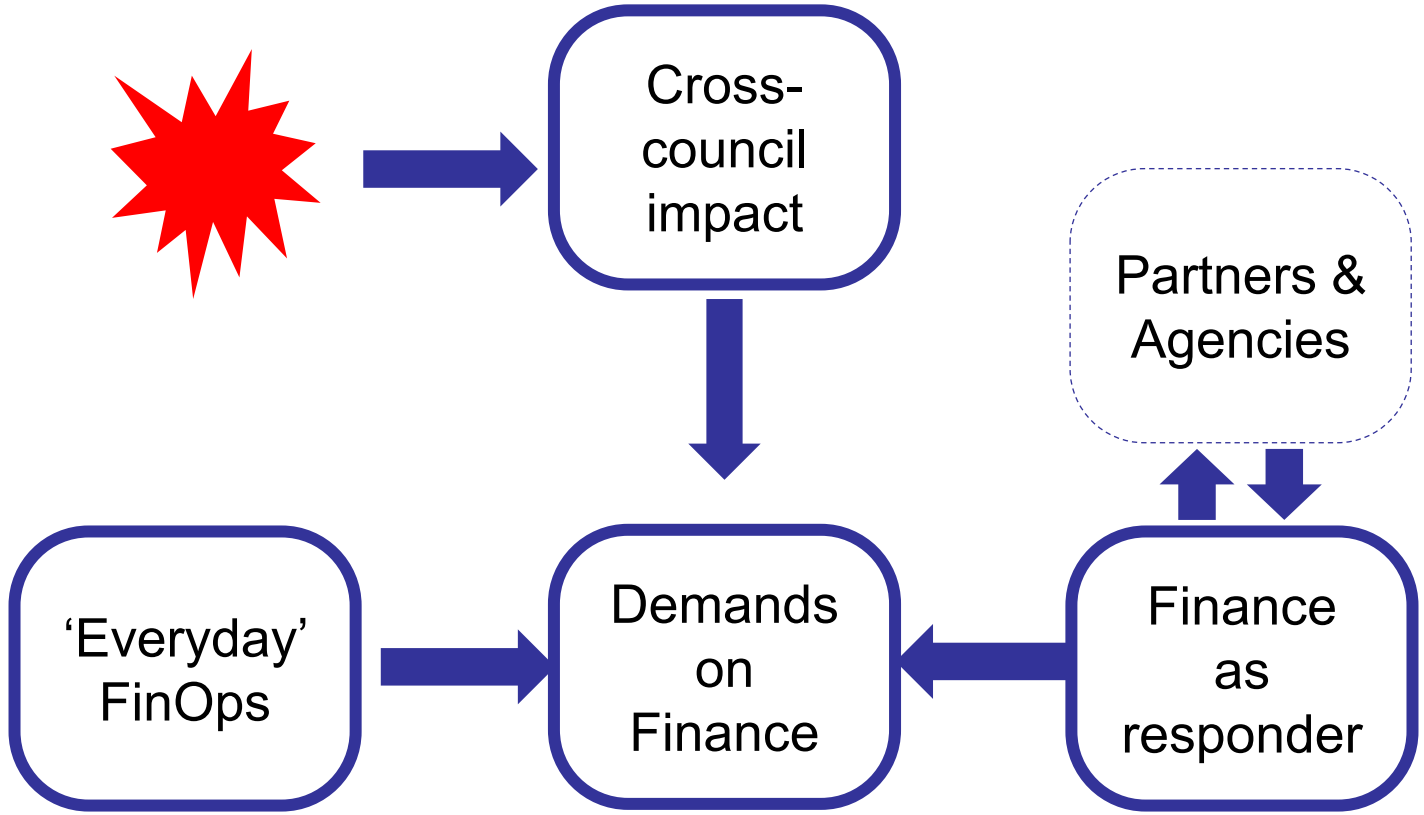
Finance

This module covers finance and treasury management, income collection, payments to residents and suppliers, and other finance functions. This includes management of risk of fraud while normal systems and controls are impacted, and engagement with external partners and suppliers.

Managing a cyber incident impacting children's services

www.local.gov.uk

How to use the service and situational guidance



www.local.gov.uk

Local Government Association

public·digital

5. Updated content on co-ordinating with Central Government & available support.

Ministry of Housing,
Communities &
Local Government

Local Digital Cyber Incident Response (CIR) service

@LocalDigital

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

Cyber Incident Response (CIR) service

What?

Local Digital have procured a CIR service for English councils, which will support them to respond to and recover from cyber incidents.

Why?

- Standardised approach
- Incentivise reporting to the National Cyber Security Centre (NCSC)
- Use of NCSC assured providers
- Financial support
- Remove access barriers
- Value for money
- Access to incident reports

LOCAL DIGITAL Cyber

CIR service overview

The contract will be delivered by KPMG and Accenture - both are NCSC assured Tier 1 response providers.

The NCSC assured CIR scheme provides confidence in companies which meet their rigorous standards for high quality cyber incident response.

CIR companies help organisations which have been the victim of a cyber attack.

Cyber attacks can take many forms such as denial of service, malware, ransomware or phishing attacks and is defined by the NCSC as:

- a breach of a system's security policy to affect its integrity or availability
- the unauthorised access or attempted access to a system

LOCAL DIGITAL Cyber

How to report a cyber security incident

If you think your council is subject to a cyber security incident, please it report to:

- the NCSC via their **incident reporting portal**. If the incident happens outside of normal business hours, please also call NCSC (please notify MHCLG Local Digital if you do not have this phone number and we can provide this directly).

You should also notify, where relevant:

- the Information Commissioner's Office (ICO), using their self-assessment tool to determine whether you need to report a breach
- the National Crime Agency (NCA) or call 0300 123 2040
- your regional Warning, Advice and Reporting Point (WARP) for threat intelligence sharing

When the NCSC receives a report, it shares details with MHCLG to assess whether the incident meets the CIR activation threshold. MHCLG monitors reports 24/7.

LOCAL DIGITAL Cyber

What is the service activation threshold?

Once we receive an incident report from NCSC, we will assess whether it meets the activation threshold for accessing our CIR service.

MHCLG will determine whether the incident appears to meet the criteria for a 'severe incident’.

We will use the information provided by NCSC from the council’s incident report. Relevant factors include the:

- significance of the service disruption and data loss
- impact on operational activities
- MHCLG’s remaining available budget for the service

Activation of the service is at MHCLG’s discretion, and MHCLG may alter the service activation criteria at any time without notice.

What is covered?

MHCLG will cover the costs of CIR support for the containment and eradication phases of an eligible incident.

Councils can choose to fund the recovery phase, with the same CIR provider, at their own cost.

Containment phase

Eradication phase

Recovery phase

LOCAL DIGITAL Cyber

What councils can expect from MHCLG during a cyber incident

- When experiencing a cyber incident, MHCLG will act as the central coordinating body across government to support the impacted council, including:
- Coordinate the cross-government response to ensure a joined-up approach.
- Supporting restoration of services by liaising with relevant government departments (e.g. HMLR and DWP).
- Facilitating information sharing between councils and government departments where required.
- Keep government stakeholders informed through regular updates to ensure the council is appropriately supported.

LOCAL DIGITAL Cyber

Ministry of Housing,
Communities &
Local Government

Questions?

@LocalDigital

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

Ministry of Housing,
Communities &
Local Government

Thank you!

DefendAsOne@communities.gov.uk

@LocalDigital

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

Local Government Association

public·digital

6. Keeping the grab bag updated moving forwards - Playbook

Preparation

- Initial desktop content review
- Recruitment of research participants/ stakeholders
- Workshop planning and preparation
- “Rough first draft” of module content / content updates

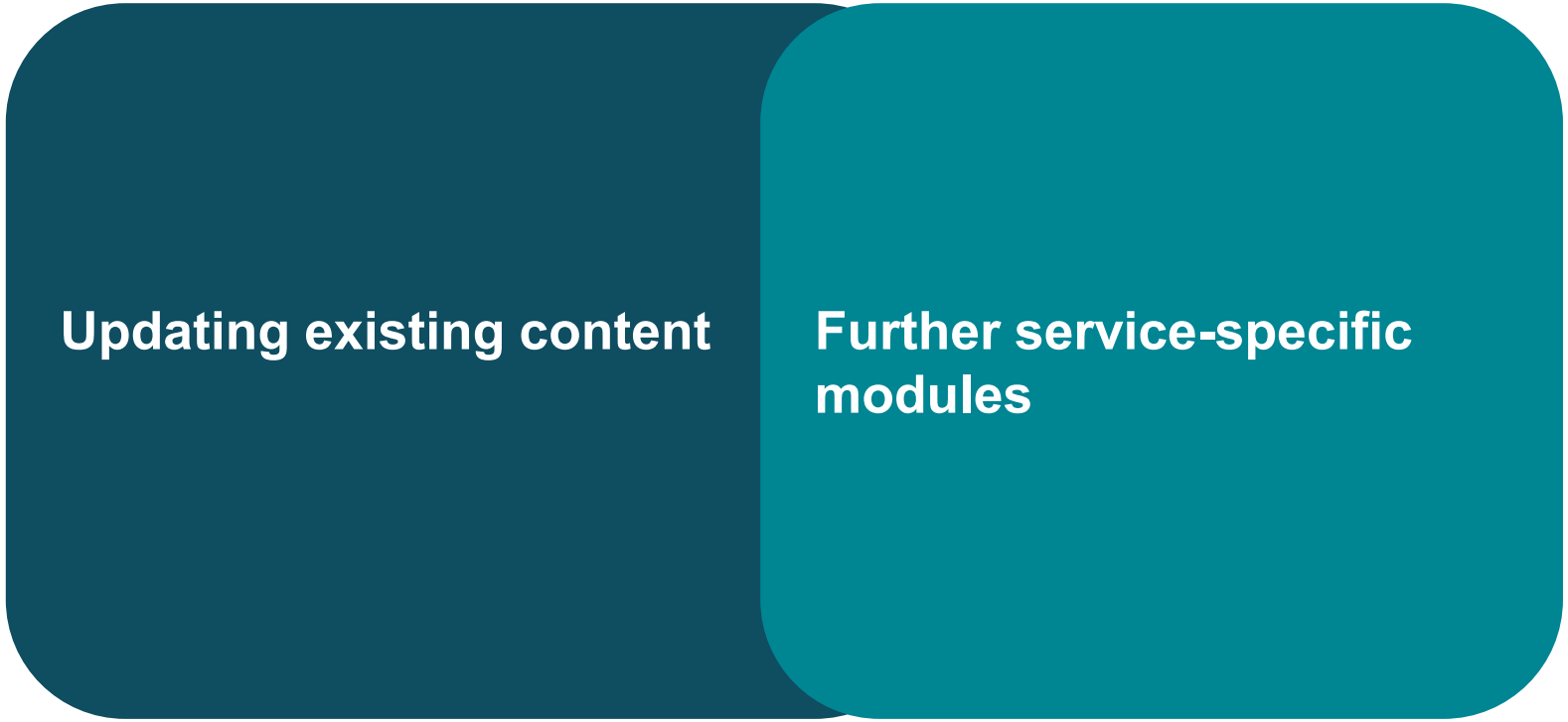
User research

- Interviews and workshops with ID’d stakeholders
- Feedback on ‘Rough first draft’
- ID of user needs and synthesis of feedback

Collaborative design

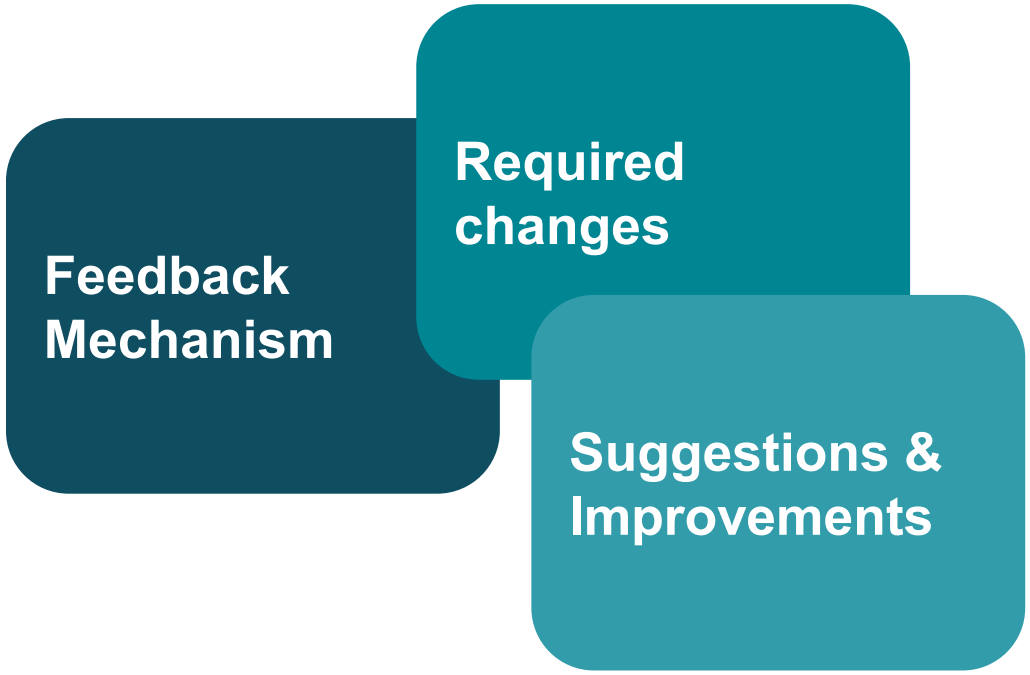
- Content revisions and updates based on research & feedback
- Workshops / co-editing of revised content & updates
- Preparation of final content for publication

Further iteration: Led by the sector to meet *its* needs.

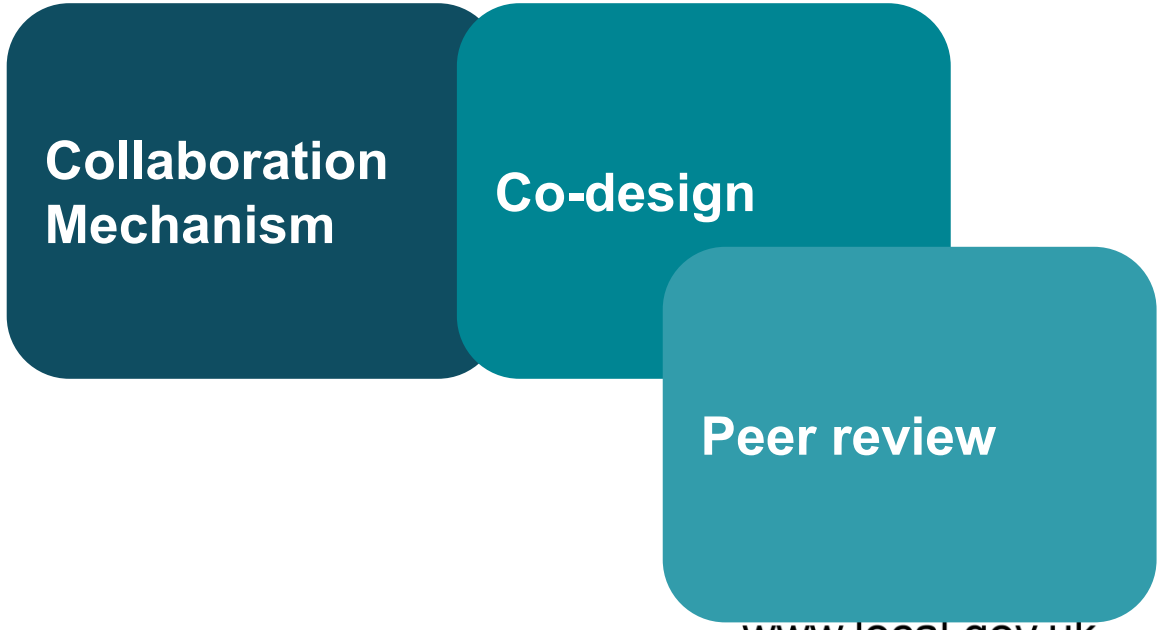


Online form coming!

Updating existing content



Further service-specific modules



Local Government Association

public·digital

Thank you!

cyberanddigital@local.gov.uk