Cyber resilience for local government reorganisation

You're reorganising.
The clock is running.

Your council is merging, consolidating services, or preparing for unitary status. Every system migration, data transfer and access change you make between now and Day One is a window of cyber risk. For CEOs, CDIOs and Directors of Digital in reorganising councils.



This isn’t a future problem.

Councils across England are going through structural reorganisation right now, making complex decisions about which systems to keep, which data to migrate and which contracts to renegotiate, all while maintaining statutory services and protecting sensitive citizen data. Timelines are set by central government. Budgets are already stretched.

The challenge isn't understanding what needs to change. It's doing it safely, at pace, without disrupting the services your communities depend on.

MHCLG (Ministry of Housing, Communities and Local Government) recognised the scale of this risk. In February 2026, Local Digital published a dedicated Digital and Cyber Playbook specifically to help councils manage cyber, data and service continuity risk during reorganisation. That tells you where the national conversation is.

This guide sets out where the cyber risks are highest during reform, what good practice looks like, and how SCC Digital Services supports councils through each phase of the journey.

Sources: Grant Thornton, 2025

1 in 5

Councils at risk of financial failure

This will rise to 41% within five years without structural change.



Where reorganisation creates cyber risk.

Structural change doesn't just reshape your organisation. It reshapes your attack surface. These are the four risk areas that matter most during reform.

System and data migration

Merging or separating council systems means moving data between environments that were never designed to work together. Every migration is an opportunity for misconfiguration, data loss or unauthorised access. Legacy systems running in parallel with new platforms create blind spots that are hard to monitor and easy to exploit.

The MHCLG Digital and Cyber Playbook was published specifically because these risks are real and immediate. It calls out the need for councils to plan cyber resilience into every stage of reorganisation, not bolt it on afterwards.

Identity and access sprawl

When two or more councils merge, you inherit overlapping user populations, inconsistent access rights and duplicated identities across systems that don't talk to each other. Staff from different organisations suddenly need access to shared platforms. Leavers from legacy structures may retain access longer than they should.

This isn't just a technical problem. It's a governance gap that creates risk at exactly the moment when leadership attention is focused elsewhere.

43% **of councils report integration issues with legacy systems.**

40% **cite skills and digital capability gaps.**

Sources: Government Transformation Magazine, 2025

"Reorganisation creates tight timelines, high risk and complex decisions across systems, data, contracts and people."

Local Government Reorganisation Digital and Cyber Playbook, Local Digital (MHCLG)

Ransomware and incident exposure

Ransomware is now the most serious cyber threat facing UK local government. Nationally significant attacks more than doubled in 2025. Individual council incidents have cost close to £1m to recover from. And the trend is accelerating.

Transition periods are when you're most exposed. Teams are stretched across two operating models. Governance is in flux. Legacy systems are still live but may not be actively monitored. Incident response plans written for the old structure may not apply to the new one.

Supply chain and third-party risk

When two or more councils merge, you inherit overlapping user populations, inconsistent access rights and duplicated identities across systems that don't talk to each other. Staff from different organisations suddenly need access to shared platforms. Leavers from legacy structures may retain access longer than they should.

This isn't just a technical problem. It's a governance gap that creates risk at exactly the moment when leadership attention is focused elsewhere.

2x

Nationally significant ransomware attacks on UK public bodies more than doubled in 2025.

£1m

Individual council recoveries have cost close to £1m.

Sources: NCSC Annual Review 2025

If you can see your council in any of those four areas, the risk is already live.

The next two pages cover the framework that makes reform defensible, and how SCC maps to each phase of your timeline.

THE FRAMEWORK

CAF: the framework that makes reform defensible

The Cyber Assessment Framework isn't a compliance exercise. For councils going through reorganisation, it's the most practical tool available for identifying where your gaps are before they become incidents.

CAF gives you a consistent, outcomes-driven approach to cyber resilience that aligns with national policy. It extends accountability beyond IT into leadership and governance, which matters when your entire organisational structure is changing. And it provides a common standard that makes sense to auditors, regulators and central government alike.

For councils in reorganisation, CAF is particularly valuable because it helps you:

- Baseline your current cyber posture before structural change begins.
- Identify which systems, data assets and governance structures are most vulnerable during transition.
- Prioritise investment against nationally recognised risk criteria, not guesswork.
- Demonstrate progress to leadership, members and central government in a consistent format.

200+

councils signed up to CAF readiness activity to identify gaps in critical systems, governance and capability.

Local Digital, CAF Service Design & Pilot Programme

SCC's assessments are aligned to CAF but focused on reform impact.

We don't deliver generic compliance reviews. We assess the areas most vulnerable during your specific reorganisation timeline.

Your reform timeline. Our services mapped to it.

Most MSPs will tell you they understand the public sector. We'd rather show you what we've done. SCC Digital Services works with councils to embed cyber resilience into each phase of reorganisation, not as an afterthought but as a core part of how you plan, execute and land structural change. Our approach is built around your reform timeline, not a generic service catalogue.

Reform timeline | pre-merger → Day One → steady state



PHASE 1
Pre-merger planning

- CAF-aligned maturity and risk assessments focused on reform impact, not generic compliance.
- Identify which systems, data and governance structures are most vulnerable during transition.
- Baseline your current cyber posture so you have a clear starting point.
- Map critical dependencies and third-party risks before contracts are renegotiated.



PHASE 2
Day One Readiness

- Managed cyber resilience: continuous monitoring, threat detection and incident response during transition.
- Secure data integration with embedded identity and access controls across merging environments.
- Protection of statutory services while migration is underway.
- Predictable costs that let you plan budgets against a fixed model, not reactive spend.



PHASE 3
Post-merger steady state

- Ongoing managed services with continuous improvement against CAF outcomes.
- Interoperable architecture that reduces supplier lock-in and supports future flexibility.
- Regular reporting that demonstrates measurable progress to leadership and central government.
- Knowledge transfer so your internal teams build capability, not just dependency.

*"We enable councils to strengthen cyber foundations before reform pressure peaks, ensuring **Day One** readiness and controlled progress."*

Kieron Holmshaw, Public Sector Cyber Specialist, SCC Digital Services

This isn't about selling you a product. It's about making sure your reform doesn't create the next headline.
Every capability is tied to a phase of your journey and measured against outcomes that matter to your leadership team.

THE PROOF

Borough of Broxbourne Council

The challenge

Broxbourne's cyber foundation had fallen behind the services it needed to protect. Infrastructure was ageing, patching was manual and inconsistent, and vulnerabilities went unseen because the team had no visibility of them. With essential public services and sensitive citizen data at stake, the risk was becoming impossible to ignore.

What SCC did

SCC started with a full scoping review that surfaced unsupported software, hidden vulnerabilities and the root causes of recurring issues. On that foundation, SCC deployed Managed Vulnerability Assessment and Managed Extended Detection and Response, delivering continuous vulnerability insight, real-time alerts and rapid response, with SCC specialists working as an extension of the council's team.

The outcome

Broxbourne now has a clearer security posture, a more stable environment and a marked reduction in vulnerabilities across the organisation. Compliance is smoother and more predictable, and threats are detected early rather than discovered by chance. The annual IT health check has shifted from a source of stress to a structured, proactive process.



"We're proactive, confident, and able to focus on what really matters."

Kirstie Morey
Digital Services Manager,
Borough of Broxbourne Council

Watch the full Broxbourne story
vimeo.com/1170635934

THE PROOF

Why councils choose SCC's Digital services



Over 50 years supporting UK public sector organisations.



CAF-aligned delivery designed for reform timelines, not generic compliance.



Managed services model with predictable costs, built for constrained budgets.



Named sector specialists who understand local government, not just technology.

CREST accredited Security Operations Centre incident response, delivered from our UK CDC.

Information Security Management System ISO 27001 Certified

Certified ISO 9001:2000 Company

Certified ISO 9001 Company

CREST

CYBER ESSENTIALS CERTIFIED

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection
Identity and Access Management
Information Protection and Governance

Member of Microsoft Intelligent Security Association
Microsoft Security

Microsoft Verified Managed XDR Solution

NEXT STEP

Start the conversation

You don't need another generic cyber assessment. You need someone who understands what reorganisation does to your risk profile and can help you plan around it.

Book a 30-minute reform readiness conversation.

We'll discuss where your council is in the reform timeline, your current cyber posture, and the practical next steps available to you before **Day One**.



Kieron Holmshaw

Public Sector Cyber Specialist,
SCC Digital Services

kieron.holmshaw@scc.com
07939597252

About SCC Digital Services

SCC is a strategic technology partner to the UK public sector with over 50 years' experience supporting local authorities, central government and regulated organisations. SCC Digital Services helps public bodies modernise securely, improve resilience, build sovereign solutions and deliver better outcomes through technology, aligning cyber capability with reform ambition.

Sources: Grant Thornton, 2025

Book your reform readiness conversation

Speak to your SCC account manager or scan to book

Book Now

Simplify the complex