Department for Levelling Up, Housing & Communities

Setting a cyber security baseline for local authorities

Insights from the Cyber Assessment Framework for Local Government pilot

September to December 2022

LOCAL DIGITAL Cyber

Foreword from Local Digital

Local Digital is a dedicated team within the UK **Department for Levelling Up, Housing and Communities** (DLUHC).

Our **mission** is to support a national ‘Local Digital movement’ that brings together everyone required to make excellent local public services for users and taxpayers.

The Local Digital movement is a growing community of organisations working together with a shared vision: to deliver **more user-centred, cost-effective local public services through open, collaborative and reusable work**.

The community was drawn together around the Local Digital Declaration, a shared ambition for the future of local public services. The Local Digital Declaration includes a commitment to the **continuous improvement of cyber security practice**, to support the security, resilience and integrity of our digital services and systems.

LOCAL DIGITAL Cyber

Foreword from Local Digital

Our previous research highlighted that English local authorities are lacking a clear baseline standard when it comes to cyber security.

In line with the aims of the Government Cyber Security Strategy, we're exploring how the Cyber Assessment Framework (CAF) devised by the National Cyber Security Centre (NCSC) could be used across the sector in England to meet this need and help drive cyber resilience.

In the long-term, we think the CAF could be a central part of the post-Public Services Network (PSN) cyber landscape, and a routine part of good risk-management at local authority level. Following a common framework will also help grow our understanding of sector-level risks and vulnerabilities, and help DLUHC and other organisations to target support where it's needed most.

Our Cyber Assessment Framework for Local Government pilot, which ran between September and December 2022, was the first step in testing how some of this might work. This report outlines how we conducted the pilot, what we've learned so far, and the next steps.

Thank you to all our pilot council IT leads for their time and feedback, and to the many partners across Government who have offered input and advice, including the Local Government Association, Cabinet Office, DHSC, Home Office, the Devolved Administrations and the National Cyber Security Centre.

LOCAL DIGITAL Cyber

Contents

LOCAL DIGITAL Cyber

Executive summary

In late 2022 we conducted a 4-month pilot with 10 councils to explore how the NCSC's Cyber Assessment Framework (CAF) could be used to help assess and manage cyber risks across local government in England.

Pilot participants completed a self-assessment against the CAF in several stages. After each stage they participated in workshops to discuss their experience with the Local Digital team of cyber specialists.

The pilot demonstrated that the CAF and an associated profile for local government **has the potential to act as a benchmark and tool to improve cybersecurity in local government.**

Key findings:

- Using the CAF adds value for councils, such as helping them to identify new ways to improve cybersecurity, providing guidance on which areas to prioritise, and supporting communication with senior leadership.
- Council IT leads see potential for this value to increase through services like third-party audits and alignment with government compliance requirements
- The draft profile, which sets a benchmark for councils to aim for, is challenging but not disproportionate to the risk councils feel they face
- We need to do more to define how councils should apply the assessment across their organisation, and what 'essential functions' means in a local government context, as this may impact how achievable completing the CAF is for a council
- We need to do more to increase confidence in assessments, for councils to feel like they are taking the 'right steps', and to provide evidence to other organisations about their cyber security maturity

LOCAL DIGITAL Cyber

How did we get here?

Background and context to the pilot.

LOCAL DIGITAL Cyber

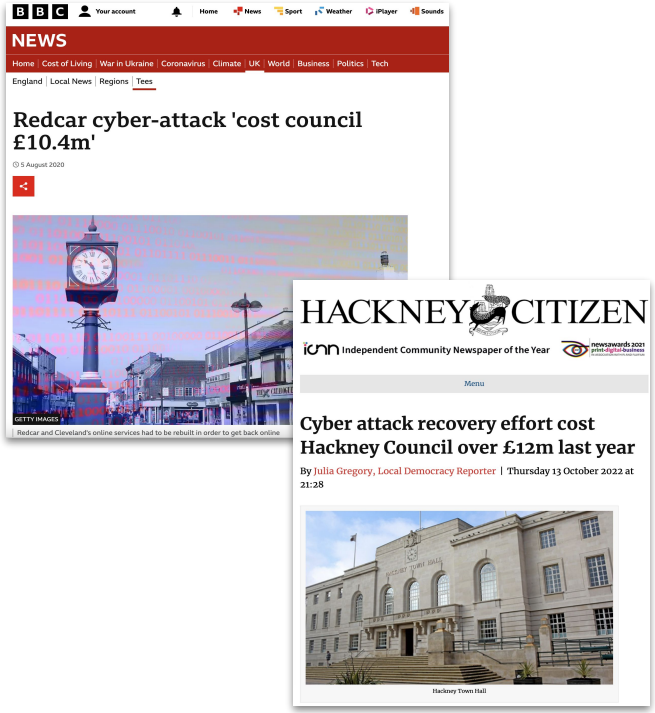
Understanding the local government context

There are 343 councils and combined authorities in England, each with different services, leadership, budget and population sizes, and ways of working. Councils are sovereign organisations that are responsible to their communities, and responsible for their own organisation risk levels. DLUHC acts as the steward for the local government sector.

Councils are responsible for critical services like benefits payments, social care and elections. They interact and share data with other government departments. If one council's system is compromised in a cyber attack, there is a risk that it would allow access to other state networks, or attract further attacks against the public sector if it is perceived as vulnerable.

The 2020 cyber attacks against Redcar and Cleveland and Hackney councils highlighted the catastrophic impact and far-reaching implications of such attacks. This includes threat-to-life if data on vulnerable people is lost, and significant financial costs for both the council and central government.

These cyber attacks highlighted a need to understand how central government can reduce cyber risk and optimise spending in support of, and collaboration with, local authorities.



LOCAL DIGITAL Cyber

2020-2021: Background to the pilot

In February 2020 the NCSC and DLUHC issued a survey to understand the mitigations councils have in place to reduce the risk and impact of malware and ransomware attacks.

By analysing the survey responses and findings from subsequent user research, we discovered that:

- there are many cyber standards, but no clear baseline
- an effective cyber baseline must encompass culture, leadership and ‘cyber first’ processes
- leaders need a better understanding of cyber risk to inform their decisions
- some councils held a misconception that PSN is an accreditation, and equates to being ‘cyber secure’

This research led us to consider what a baseline for cyber security in local councils should look like, including developing some initial prototypes.

We have also delivered a cyber support programme that has supplied over £19 million in grant funding to deliver specific technical remedial activities to 186 authorities.

The nine interrelated cyber security themes uncovered during the discovery phase in 2020.

LOCAL DIGITAL Cyber

2022: A new strategic direction

In January 2022, the Government Cyber Security Strategy set out the UK Government's approach to building a cyber resilient public sector. Its long-term aim is for the whole public sector to be resilient to known vulnerabilities and attack methods no later than 2030.

The strategy is underpinned by the adoption of the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) across government. Lead government departments are required to adapt this in a way that is most appropriate for the public sector organisations within their scope.

The role of DLUHC

While councils are responsible for their own IT networks and managing the associated risks, DLUHC is responsible for cyber policy and assurance relating to local authorities in England. As such, it's up to DLUHC to determine how best to implement the Government Cyber Security Strategy.

LOCAL DIGITAL Cyber

2022 onwards: setting a cyber security baseline for local government

This new strategic direction and the increasing cyber threats is why DLUHC is developing a baseline for local government to assist councils to identify and address cyber risks, in a proportionate way, that's rooted in the Cyber Assessment Framework.

We want to work with the sector to implement an approach that will bring genuine change. An approach that is focused on improvements, not paperwork, and that helps DLUHC understand risks to the sector at large.

We want to ensure this approach establishes trust between central government departments and local government, and enables information sharing.

LOCAL DIGITAL Cyber

A clear baseline for councils, rooted in the Cyber Assessment Framework

LOCAL DIGITAL Cyber

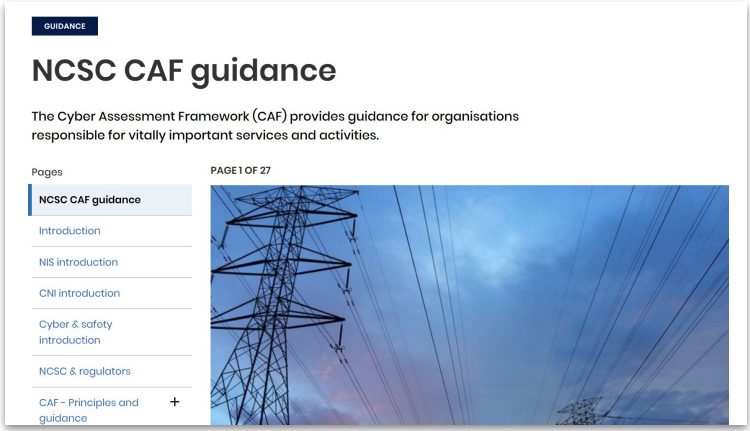
About the Cyber Assessment Framework (CAF)

The Cyber Assessment Framework (CAF) is an outcomes-based risk management framework. It was developed in 2016 by the National Cyber Security Centre, the UK's technical lead for cyber security.

It serves as guidance for those responsible for vitally important services and activities.

As well as central government, it is aimed at organisations that are:

- within the UK Critical National Infrastructure (CNI)
- subject to Network and Information Systems (NIS) Regulations
- managing cyber-related risks to public safety

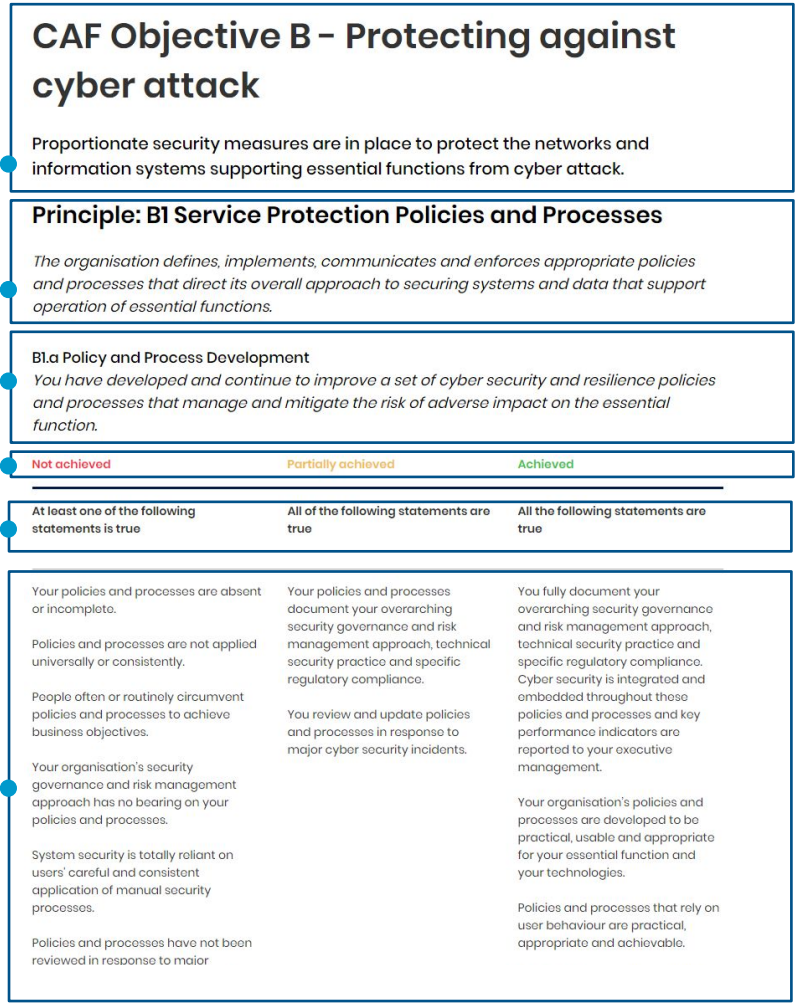


LOCAL DIGITAL Cyber

Overview of the CAF

The CAF is made up of principle and contributing outcomes, which focus on what needs to be achieved rather than a checklist of what needs to be done.

Sets of Indicators of Good Practice (IGPs) provide additional detail for each outcome.



Making the CAF sector-specific

The common core of the CAF (which consists of principles, contributing outcomes and indicators of good practice) is sector-agnostic. It's designed to be generally applicable to all organisations responsible for essential functions across all key sectors.

It is possible that there will be a need for some sector-specific aspects of the CAF, which could include the following:

Sector-specific CAF profiles

It will be a decision for the relevant regulator to put a regulatory interpretation on CAF results (such as which outcomes must be met). Some target profiles may well be sector-specific.

Sector-specific interpretations of contributing outcomes/IGPs

It may be necessary in some cases for a sector-specific interpretation of contributing outcomes and/or IGPs to better clarify meaning within the sector.

Sector-specific additional contributing outcomes/IGPs

The NCSC will be continuing to work with the full range of CAF stakeholders to determine if sector-specific aspects of the CAF are required, and to assist in introducing changes as necessary.

As part of the pilot, we hoped to identify which areas of the CAF may need to be adapted for local government.

LOCAL DIGITAL Cyber

Developing a CAF profile for local government

The CAF has been adapted for sectors like aviation and energy, and the NCSC and Cabinet Office have developed and are trialling a profile for central government. For the pilot, we tested if the central government profile was a proportionate target for the local government sector to aim for.

This profile sets out a baseline target for each of the 39 outcomes as either ‘Achieved’, ‘Partially Achieved’ or ‘Not Achieved’. If a council is meeting this baseline, they should have resilience to common attacks, low level threats and known vulnerabilities, but may have less to sophisticated attacks. The profile also represents appropriate security measures in place for the level of information assets a council typically holds.

For example, if the profile for outcome ‘B2.b Secure Configuration’ is ‘Partially Achieved’, then a council should aim to meet all the indicators of good practice in this section. They should also ensure that none of the indicators in ‘Not Achieved’ apply to the organisation. If just one ‘Not Achieved’ indicator is true, then the overall outcome is not achieved.

B4.b Secure Configuration

You securely configure the network and information systems that support the operation of essential functions.

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You haven't identified the assets that need to be carefully configured to maintain the security of the essential function. Policies relating to the security of operating system builds or configuration are not applied consistently across your network and information systems relating to your essential function. Configuration details are not recorded or lack enough information to be able to rebuild the system or device. The recording of security changes or adjustments that effect your essential function is lacking or inconsistent.	You have identified and documented the assets that need to be carefully configured to maintain the security of the essential function. Secure platform and device builds are used across the estate. Consistent, secure and minimal system and device configurations are applied across the same types of environment. Changes and adjustments to security configuration at security boundaries with the networks and information systems supporting your essential function are approved and documented. You verify software before installation is permitted.	You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of the essential function. All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment. You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented. You regularly review and validate that your network and information systems have the expected, secure settings and configuration. Only permitted software can be installed and standard users cannot change settings that would impact security or the business operation. If automated decision-making technologies are in use, their operation is well understood, and decisions can be replicated.

How we ran the pilot

LOCAL DIGITAL Cyber

Through the pilot, we wanted to…

Test the CAF for Local Government profile and content

- ❏ Do councils find the profile proportionate?
- ❏ Is it suitable for all different types of councils?
- ❏ How should assessment scope be defined?
- ❏ Is a single assessment per council realistic and meaningful?
- ❏ Are the IGPs relevant to the sector?

Understand the user experience

- ❏ Do councils find self-assessment useful?
- ❏ What are the challenges for councils?
- ❏ What skills, time and resources are needed?
- ❏ What additional guidance is needed?
- ❏ Where are there opportunities to add value?

Identify areas for further research

- ❏ How can we increase trust in assessments?
- ❏ Where is there potential to join up across other sectors and with other requirements?
- ❏ What support might councils need to assess and meet the standard?

LOCAL DIGITAL Cyber

Working with the pilot councils

From our experience delivering the cyber support programme, we know the importance and effectiveness of taking a collaborative approach with councils. By working with councils we can develop solutions to improve their cyber security that reflect their specific challenges and contexts.

The 10 pilot councils – while a small sample – represent a range of council types, sizes, geographies, IT setups (such as in-house and shared services), and cyber maturity across England.

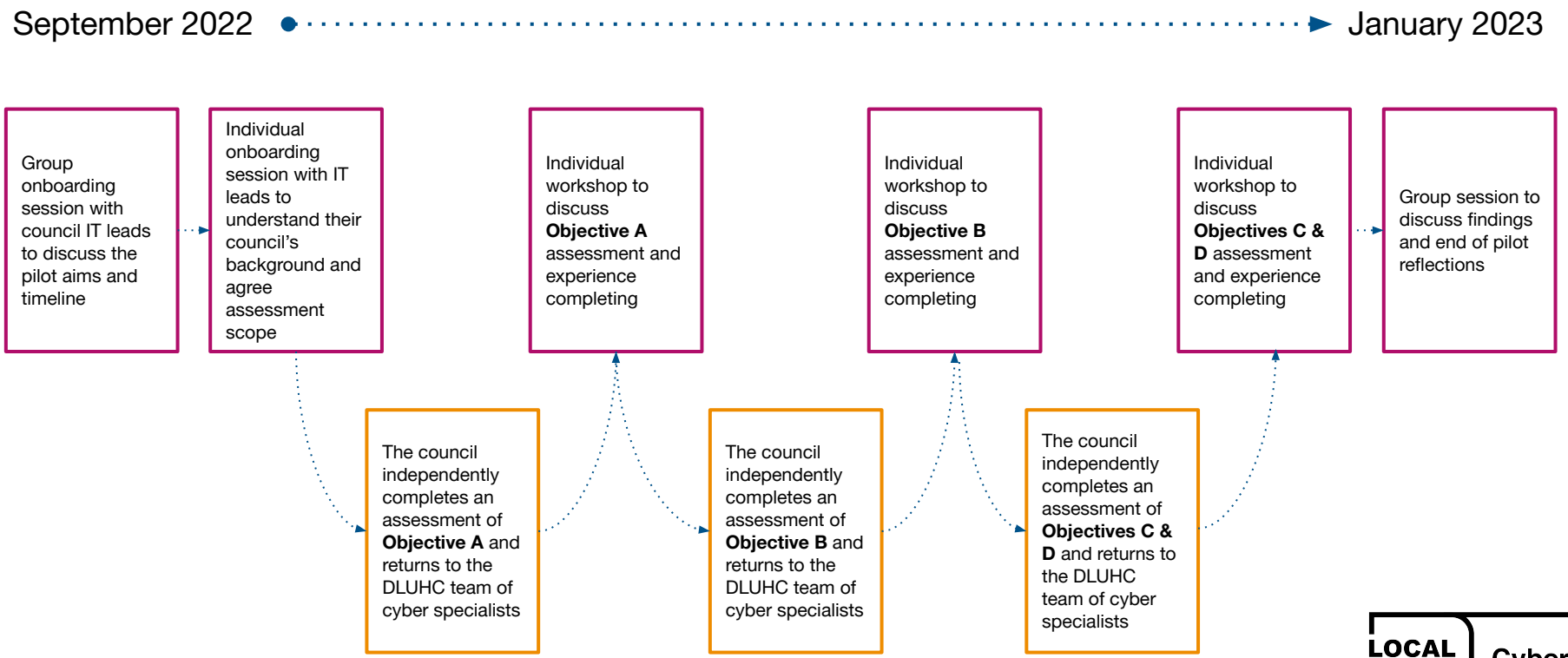
Council IT leads completed a self-assessment in stages. After each stage they participated in workshops to discuss the experience with the Local Digital team of cyber specialists.

While this staged approach is unlikely to reflect a council's experience of using the CAF outside of the pilot, having councils conduct a self-assessment ensured more in-depth insights than a traditional consultation exercise.

Pilot participants: Durham County Council, Copeland Council, Salford City Council, Norfolk County Council, Sandwell Metropolitan Borough Council, Brent Council (IT Shared Service), Southend Borough Council, Hart District Council (IT Shared Service), Dorset Council, Torbay Council

LOCAL DIGITAL Cyber

Pilot council user journey



LOCAL DIGITAL Cyber

Pilot materials

OBJECTIVE A: MANAGING SECURITY RISK

Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.

			DLUHC 2022 LG PROFILE	PLEASE COMPLETE THIS SELF ASSESSMENT			PLEASE ANSWER THESE RESEARCH QUESTIONS		
				Local Authority Self-Assessment	Date reviewed	Summary narrative in support of self-assessment rating *Please describe how you came to this assessment. How helpful were the Indicators of Good Practice? Are there any particular challenges related to this outcome?*	How confident are you in your assessment	Do you feel able to evidence your assessment?	Any other notes, comments, reflections *How achievable is the target DLUHC 2022 LG profile? If you're not currently meeting the profile, what actions or resources are needed?*
Principle	A1	Governance	The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems						
Contributing Outcome	A1.a	Board Direction	You have effective organisational security management led at board level and articulated clearly in corresponding policies.	Achieved					

Indicators of Good Practice and Improvement Actions

Indicators of Good Practice	Not Achieved At least one of the following is true	TRUE	Notes	Achieved All of the following are true	TRUE	Notes
	The security of network and information systems related to the operation of essential functions is not discussed or reported on regularly at board-level.			Your organisation's approach and policy relating to the security of networks and information systems supporting the operation of essential functions are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.		
	Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance.			Regular board discussions on the security of network and information systems supporting the operation of your essential function take place, based on timely and accurate information and informed by expert guidance.		
	The security of networks and information systems supporting your essential functions are not driven effectively by the direction set at board level.			There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level.		
	Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.			Direction set at board level is translated into effective organisational practices that direct and control the security of the networks and information systems supporting your essential function.		

OPTIONAL: are there any other indicators / sector specific considerations missing, that should be noted when assessing against this outcome?	

Actions	Ref	Actions identified: priority steps to meet LG Profile	DLUHC Comments

We created some bespoke materials, taking the [NCSC CAF v3.1] and translating it into an Excel workbook.

The CAF is not intended as a tick-box exercise. We included fields for pilot participants to include their personal views, rate their confidence, comment on challenges and record actions.

We also compiled an initial guide with suggestions for who in the council might need to be engaged throughout the exercise and where to look for evidence against particular outcomes.

[Find out how to access resources from the pilot.]

The CAF for Local Government pilot in numbers

10 councils
from across England took part in the pilot

70 hours
of workshops with pilot councils

220
attendees at our January end-of-pilot Show and Tell

16 weeks
in duration

13
Government departments and agencies engaged

1000+
data points

LOCAL DIGITAL Cyber

What we've learned so far

Key insights and themes

LOCAL DIGITAL Cyber

Using the CAF provides value to councils

- **All participants** identified actions to improve cybersecurity at their council based on the self-assessment. This included new actions not already identified through other standards or compliance processes, and prioritisation of existing planned actions.
- **Most participants** felt that the CAF helped them to consider new questions and areas, particularly across data storage and governance.
- **Some participants** expressed that the CAF would be a helpful tool to facilitate discussions about cyber risk across the business, and to engage with senior leadership.
- **Some participants** described the CAF as providing reassurance that they were on the right path to improving their cyber resilience.

We’re used to doing technical assessments, but this is more than that, and already it’s made us look at an area we had been ignoring.

IT lead, pilot council

LOCAL DIGITAL Cyber

However, the majority wanted more from the CAF than a self-assessment

- Some participants felt that **some form of assurance**, such as an audit by a third-party, **would increase the value of the CAF** in order to:
  - validate their self-assessment and highlight any gaps
  - act as an incentive for senior leadership to invest in cyber
- Some participants told us that **the value of completing the CAF was directly tied to how it might be used to reduce other compliance requests**, such as the NHS Data Security and Protection Toolkit.

These are both linked to the amount of time and resource the CAF profile requires to assess and meet, with IT leads facing tight budgets and challenges hiring and retaining cybersecurity staff.

Without significant investment we are not going to meet [the profile]... if it is a mandatory requirement, this will force SLT to take a different approach.

IT lead, pilot council

It's always an issue that central government or NCSC can't tell us to do something, because there's no legal right to make us follow it… Sometimes we don't follow central government guidance because there's no mandate, even though we would love to follow it. New duties require new funding, so it would be a lot easier and simpler in the long run.

IT lead, pilot council

Even though I can see the benefits of the CAF, we have incredibly tight budgets, so what SLT will say is "why do I need to complete this CAF?" For example, we need to have that certificate to stay connected to the PSN network. At the moment, it's fine not to meet [the CAF profile], as there isn't a tangible impact.

IT lead, pilot council

The draft profile is challenging, but proportionate

The pilot did not reveal any strong reasons why a single profile would not fit all types of council, but:

- ‘Good’ will not look the same for everyone – different councils are at different levels of maturity, and have different budgets and resources available
- some parts of the profile (supply chain, monitoring, response and recovery capability, root cause analysis) will require greater time, money and effort to meet – however, this was not regarded by councils as a good reason to lower the bar
- councils would value a way to demonstrate progress against outcomes where they are not yet meeting the profile, but where improvements have been made

Snapshot

A1.a Board Direction: the majority of councils on the pilot self-assessed as not meeting the profile for this outcome

B3.b Data in Transit: the majority of councils on the pilot self-assessed as exceeding the profile for this outcome

As expected, no council is meeting the profile yet, and there was a divergence in how councils self-assessed.

LOCAL DIGITAL Cyber

There were one or two sections that raised a couple of eyebrows... But we're confident that once work in progress is complete, they will be met. There's nothing in [the profile] that we couldn't or shouldn't do.

IT lead, pilot council

Participants found some areas particularly challenging to meet the profile

Areas that participants found particularly challenging included:

- **Risk management:** several councils highlighted a lack of cyber risk management processes.
- **Supply chain:** participants cited issues with supplier management, including a lack of visibility due to not auditing suppliers and a difficulty to get information from suppliers, and perceptions that suppliers do not stick to contracts.
- **Information security and data governance:** some participants expressed concerns that a move to the cloud might mean a loss of control over data, and others lacked oversight about what data was stored where across the council.
- **Lack of skills and resources:** where councils felt a lack of the right personnel or resources blocked their ability to meet an outcome.

Challenging does not necessarily mean that an area of the profile is not proportionate, however. Building on participant feedback, we also considered insights from the cyber support programme, and the professional experience of the DLUHC cyber security specialists to analyse the draft CAF profile with achievability and proportionality in mind.

Challenges - example responses from participants

"If it's a legacy system, there's no patches available. But we can't turn the system off because it's vital to a specific department. That unfortunately does happen quite a lot.. anything that is vulnerable, we move into like a walled garden or put it in a DMZ so it can't be accessed hopefully."

"We don't have a director member or anyone on the board that has responsibility or really takes ownership of cyber. It would be hard to engage them as they would probably just push back onto the ICT Strategic Lead saying that's his area and he is the expert, not them."

"I've not been on holiday once when I haven't been on standby, because there isn't anybody to really cover me in that sense. It's not from a lack of support though. It's just a reflection of the size of our organisation."

"We have hundreds of suppliers that we've never assessed. We don't have a process in place to manage those suppliers. There are third party solutions that have council managed or hosted elements and external elements… we've never really explored the risks of around those legacy systems."

"Policies and procedures are still being written and rolled out, so it's hard to audit if it is being followed. The question states 'most' policies, so I've had to again answer 'not achieved'."

Understanding what is achievable

In our analysis, we considered:

- Is the cost to meet the profile, the sustainability of a remediation, and the likely return of investment proportionate?
- Is the terminology used easy to understand and follow?
- Does it focus on essential functions?

We consider **97% of IGPs in the CAF to be achievable for councils**, either in the short or long-term future.

Understanding what is proportionate

The CAF was designed with critical national infrastructure in mind. The risk appetite of organisations within that category may differ from councils when defining and protecting their essential functions.

We identified the following outcomes that that may not be proportionate for councils as they are currently written or without additional guidance:

- **B2.b Device Management -** “Only corporately owned and managed devices can access your essential function's networks and information systems” may present an operational and financial challenge if a council has implemented bring-your-own-device (BYOD)
- **B5.b Design for Resilience -** this requires a clearer definition of 'operational systems' within a council context
- **D1.b Response and Recovery Capability -** the requirement for key roles to be duplicated may present a challenge regarding cost, affordability and return on investment

Achievability on an individual vs sector-wide basis

Some IGPs may be challenging for an individual council to achieve in isolation, and require a sector-wide approach.

For example, **B2.b Device Management** would be ‘not achieved’ if “you are not pursuing replacement for unsupported systems or software”.

We recognise the size of the challenge councils face for legacy systems and in some cases, viable replacements or alternatives do not currently exist in the market, making this contributing outcome difficult to achieve.

We believe there is opportunity for a sector-wide approach to identifying alternatives and working with the market to support councils in partially or fully achieving this contributing outcome over time.

“We have some legacy systems. We wish we didn't, but we do. You can't replace some of those systems, even when you want to, because there's no alternative systems in the marketplace. So we have to answer honestly.”

Keeping the CAF achievable for councils

We'll continue to review this area, as the resources and capabilities of the sector likely evolve, along with the threat landscape.

There are several possible methods to address IGPs or contributing outcomes that may currently be deemed not achievable, including:

- **Additional guidance** – addressing where any wording is unclear or providing guidance on how the IGP should be applied
- **Risk acceptance** – understanding the extent of the risk exposure if the target profile is lowered, to inform decisions around risk acceptance or alternative mitigations / compensating controls
- **IGP amendments** – if a risk exposure is deemed to be acceptable
- **Collaboration, funding and shared capabilities** – additional investment through centrally driven strategic work programmes, or establishing a shared capability to address a sector level problem

We need to do more to ensure a consistent approach to scope

Participants initially agreed with our starting assumptions that:

- the assessment should cover the entire council IT network and governance structures
- one assessment per council (rather than per function) is the right goal
- it should not be entirely left to councils to decide

This was because:

- they agreed that there needs to be consistency and shared understanding to make the draft profile meaningful
- it reflects the structure of the IT network and is therefore more straightforward
- this aligned with how they approach other cyber security assessments
- they had concerns that without this scope, certain vulnerabilities might be missed

But in practice:

- it's still difficult to define the boundaries of a 'whole organisation' – for example, what about third parties that hold council data? Or when councils host Fire and Rescue services, or Connected Places technology?
- it was challenging to have confidence that the assessment was representative of the council's whole network
- sometimes the written self-assessments did not align with the discussion in workshops – for example, a council with hundreds of systems might miss one by accident, or purposefully omit a piece of legacy software that was not 'representative' of the council's overall cybersecurity posture to allow an IGP to be met

I felt the scope was representative. Yes, it gave me problems, but I would have expected it to. Problems are not a bad thing when it comes to scope.

IT lead, pilot council

LOCAL DIGITAL Cyber

‘Essential functions’ is hard to define

NCSC designed the CAF for the use of organisations that play a vital role in the day-to-day life of the UK, such as those that form the Critical National Infrastructure (CNI), or are subject to certain types of cyber regulation, including the Security of Networks & Information Systems (NIS) regulations. The CAF has a particular focus on ‘essential functions’, which “if compromised could potentially cause significant damage to the economy, society, the environment, and individuals’ welfare, including loss of life”.

While councils play a vital role in day-to-day life in the UK, they do not currently fall under regulations like CNI or NIS. We wanted to understand how ‘essential functions’ might be defined in the context of local government. We found it was difficult because:

- in some cases, participants had not yet prioritised their services or faced challenges balancing the demands of different teams
- the term is intentionally subjective – what it means may differ across councils
- the definition may fluctuate depending on external circumstances – for example, if elections are imminent, voter registration will be a higher priority
- statutory services is not an adequate definition as their criticality may vary - for example, children's safeguarding and social care compared to library services
- a lack of network segmentation meant essential functions could not be assessed separately

We will continue to work with the sector to identify best practice and provide additional guidance on this.

I can't see how you would only select certain systems to define as ‘essential systems’, as they’re all integrated into your corporate functions… you could interpret that as just what [services] councils have to legally deliver. But a lot are discretionary, though in reality you have to do them.

IT lead, pilot council

Confidence in responses varied for councils

The pilot assessments were led by IT leads, who reported varying levels of confidence in their ability to self-assess.

The participants felt more confident when:

- dealing in areas where they had hands-on experience, or that fell under their technical purview, like Identity and Access Management (IDAM), Monitoring Coverage and Equipment Sanitisation
- they had been working on cyber strategy, and were already putting in place policies and procedures
- senior leadership were engaged in cyber issues

Participants felt less confident when:

- they were not sure they were accurately interpreting the language of the CAF
- considering areas that were harder to audit, such as around processes managed by third parties
- knowledge was held by other members of staff, especially where this was undocumented
- they felt you needed outside input, such as an expert audit
- nothing had gone wrong, yet – but they felt they had not been tested by a real-life incident

Confidence - example responses from participants

I've got a good handle on this topic because I'm actively looking at it. If it was a topic I hadn't looked at for 6 months, even if I'd written it, I'd have to go back.

I look at it as an auditor might - if we don't meet it to the letter, I'm not going to say "oh we're nearly there". But is everyone looking at it that way? You don't want to put everything achieved and then suddenly be asked to provide evidence and come up way short and lose your credibility within your organisation…

There's very little I feel we don't meet, or we're a long way off from. As we have done the ISO27001, I feel confidence in knowing we could provide evidence to prove our compliance.

In order to meet this IGP with high confidence, the entire organisation needs to become more educated and experienced in risk and also the CAF submission itself will need a lot more guidance for people to complete it accurately.

With security guidance, initially I was very high confidence – "of course we do that". But when I looked at the detail, I started to question, actually do we have all these things? It made me rethink our approach.

LOCAL DIGITAL Cyber

We need to build trust and confidence in assessments

The aim of the pilot was not to audit participant responses, so the DLUHC research team had limited time to review documentation, investigate systems, or speak to key members of the organisation outside of the IT team to validate the information provided.

As such, it was hard for the research team to feel confident in the self-assessment.

A key area that we will explore next is how to build trust and confidence into a CAF assessment.

Mindsets

We saw councils fall into one of two mindsets when completing the self assessment, which influenced how they self-assessed against the profile, where they saw value in the CAF, and confidence levels in their responses.

1. The CAF is a way to show my progress

Participants are looking for ways to track progress and view the CAF as similar to a maturity model. This may be driven by a motivation to share favourable reports with senior leadership that highlights their team's hard work.

With this mindset, participants might feel that the CAF is not a 'fair' reflection of their organisation's cyber security practices. For example if they are 'not met' against an outcome where they have done a lot of work to improve because of one IGP.

2. The CAF is a way to highlight our risk

Participants see the CAF as a tool to communicate the risk the organisation is facing. This may be driven by a belief that highlighting the risk will unlock more investment from senior leadership (rather than the organisation having a high risk tolerance per se).

With this mindset, participants will assume the worst in areas where they may have doubt on how to assess, and so may tend to record harsher self-assessments.

For future guidance, products and services DLUHC may develop around the CAF, it's important to consider how these mindsets may affect user behaviour.

What we've learned from running the pilot

LOCAL DIGITAL Cyber

What went well

Gaining in-depth insights

Working with the pilot councils was a fantastic experience, and a successful way to get in-depth insights.

Positive feedback from participants

We received positive feedback from several participants about this collaborative approach and effort to engage the sector - both about the pilot, and our wider cyber programme.

Engagement with the sector

By working in the open and sharing regular updates on our progress, we ensured the pilot acted as an effective springboard for engaging the sector and relevant stakeholders.

Councils outside of the pilot contacted us for information and attended events, and other government departments reached out to understand how to align our projects and avoid duplication of work or conflicting advice.

> *This has been the best department I've seen in all my twenty plus years of working at the council, I want that voice [on cybersecurity] to continue.*

LOCAL DIGITAL Cyber

What we can improve

Test in sections

Testing the entire CAF content in a short time frame was challenging - both for the participants to complete a detailed self-assessment, and for the DLUHC team to analyse the volume of data and ensure data quality. In future, we should consider breaking it down to focus on certain sections at a time.

Speak to more people outside IT teams

We did not speak to as many people outside of IT teams as we wanted, including senior leadership and third party suppliers. Doing so would have helped to validate some of the insights we heard secondhand.

Invest more time

We underestimated the time needed to ensure adequate and representative input from all parties, particularly in a shared service environment.

It also would have been helpful to invest more time on ensuring the alignment of expectations around what the pilot was aiming to do. This would help participants and the research team feel confident in their roles, and help manage expectations.

LOCAL DIGITAL Cyber

Next steps

LOCAL DIGITAL Cyber

Insights and implications

Insights from this phase of the pilot	Implications for the next phase
The CAF has the potential to be valuable to councils but is challenging within the context of council skills and resources	We need to research and test what kind of interventions will encourage uptake and ensure return on investment for councils
The CAF for Local Government profile is challenging but broadly proportionate	We need to continue to iterate certain sections of the CAF for Local Government profile to ensure it's proportionate for the sector
There is uncertainty around how to set the scope and define 'essential functions'	We need to ensure councils have access to guidance in these areas
Participant councils and DLUHC cyber experts lacked confidence in self-assessments	We need to research and test ways to build trust in the CAF for Local Government assessments

LOCAL DIGITAL Cyber

Creating organisation-wide change

In Spring 2023 we launched the Future Councils pilot, a new programme that will fund councils to make digital and cyber improvements across their organisations, reform key services, and influence organisation-wide factors that can unblock change.

The 8 councils involved in the pilot will each address three common challenges Local Digital has identified through its work and conversations with councils across England. One of these challenges is **how to make cyber improvements across the whole organisation**, rather than just one team or area.

Through the pilot, we will work with the councils to make these changes across their organisation, and understand what further support they need to do this. If successful, our goal will be to create replicable pathways that other councils might follow by 2025.

The pilot councils will be asked to assess their organisation's cyber security posture using the CAF. They will be provided with tools and guidance to complete the CAF assessment, and their participation in user research activities will help us continue to refine the content, scope and support for the wider local government sector.

Councils that are part of Future Councils will be expected to share learning openly. Any replicable pathways and reusable artefacts will be made freely available to enable other councils in the sector to apply in their own setting.

What happens now

While we feel confident that the CAF and the local government profile is the right approach for the sector, we plan to continue working closely with the local government sector in England to design and develop cyber security policy.

During the next phase of this work, we will be doing further research on:

- assessment scope and defining essential functions
- reporting and assurance models
- cross-government alignment
- how to engage with teams in councils outside of IT

Start using the CAF at your council

We're encouraging councils to familiarise themselves with the CAF and start thinking about how they would apply it within their organisation.

If you're interested in receiving an introduction to the CAF, the workbook template, and guidance from DLUHC, please email caf@localdigital.gov.uk.

To follow our progress, including the outcomes of further testing with the Future Councils pilot councils, subscribe to the Local Digital newsletter or follow us on Twitter or LinkedIn.

LOCAL DIGITAL Cyber

Department for Levelling Up,
Housing & Communities

Thank you

Contact us at caf@localdigital.gov.uk

@LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing