LGA – Cyber resilience funded programme 2019/20

Invitation to apply for funding to improve your council's cyber resilience.

The purpose of this programme is to support councils, either individually or in partnership, to strengthen their cyber resilience where gaps or weaknesses have been highlighted in the recent Cyber Security Stocktake.

Programme Background

With councils making more local services available digitally, getting more elected members and staff online and working in a more collaborative and integrated way with partner organisations – which requires the sharing of resident and business data – reviewing and reinforcing current cyber security arrangements to ensure these are fit for purpose is a key priority.

We know that councils have already taken a range of steps to protect themselves from cyber-attacks, including technical measures such as using firewalls and scanning services or carrying out penetration tests. Many have also adopted several recognised compliance regimes, such as cyber essentials or PSN or IG Toolkit. There are also non-technical measures councils have put in place, such as developing training for staff and councillors, ensuring governance arrangements are in place to enable regular reporting of cyber risks, and planning for the eventuality of an attack occurring.

However, as we have seen through recent cyber-attacks including the WannaCry ransomware attack which affected the NHS, and a significant number of high-profile attacks on private sector businesses, those with criminal or hostile intent will continue to try to breach our security to steal the data we hold and/or damage our systems. The ability and complexity of

attacks is increasing, and therefore so too are the measures we must take to remain resilient against them.

There are **case studies** available on the LGA website from councils who have experienced attack. The impact on a council can be extremely damaging: stopping vital services as well as adding costs to hard-pressed budgets to deal with the impact. It can be commensurate with other kinds of major incident.

This threat cannot be eliminated completely, but the risk can be greatly reduced to a level that allows us to continue to benefit from the huge opportunities that digital technology offers to public services.

With this context in mind, as part of the National Cyber Security Strategy (2016 – 2021), the LGA has been awarded funding from the Cabinet Office to ensure that, alongside other parts of the public sector, councils are as resilient against cyber-attacks as possible.

The first stage of this programme of work involved a "Stocktake" of the cyber security arrangements in the summer of 2019 of councils in England. All councils in England took part, and councils should use their assessment from the Stocktake to inform how they bid for funding.

The second stage of this programme involves direct grant funding to councils over a number of phases. Councils must submit a bid to apply for funding. The type of work being prioritised for funding at each stage is explained below.

Phase 1 - Closed - Fix
We prioritised: Quick fixes for councils to address urgent issues identified in the Stocktake.

Phase 2 – Open now until 29th May – Fix and Consolidate
We will prioritise: Bids to fix any issues identified and not yet addressed in Phase 1, as well as joint bids between councils or partners to consolidate and join up efforts and resources, and build joint sector capacity.

Phase 3 - 2019/20 and 2020/21 - Enhance
We will prioritise: Bids with a focus on the proactive capabilities of the sector which will build sustainability.

Please note: You can bid again in multiple phases. You are not limited to one bid.

Phase 2 Details

The aim of Phase 2 is to:

- Build upon the work in Phase 1 by fixing any issues identified in the Stocktake, but not yet addressed in Phase 1; and

- Focus on individual or joint bids between councils and partners to consolidate work across the sector by joining up efforts and resources and, in doing so, developing the sector's cyber resilience, and/or building sector capacity.

  In both cases we welcome individual and joint bids.

There are two types of bid, as follows:

Type A: 'Fixes' – Building upon Phase 1

We welcome bids from councils or groups of councils wishing to address those areas identified for improvement within their Stocktake assessment(s). We will prioritise 'red' and 'amber red' RAG rated councils.

In Phase 1 the type of bids we supported were:

- Staff awareness raising and training (funded for the first year only, more on this below).

- Funding for advice and consultancy to improve cyber security arrangements or gain compliance against a certain standard e.g. ISO270001 or Cyber Essentials+.

- Technical training courses for IT staff.

- Funding to run phishing exercises.

We will continue to consider bids in line with the above and also more broadly to support the following areas which may have been identified through the Stocktake exercise:

- Technology

    - Support to procure, implement or develop a particular security product/solution.

    - In phase 1 we did not fund high value tech items such as SIEMs, not because we do not see a value in these products, but because it would have overstretched our budget to fund all that asked and we could not commit to the ongoing licence costs.

    - This remains the current position for Phase 2, however we are working with NCSC to explore the best way we could meet this need for the sector.

- Governance

    - Support to review and revise board structures, roles and reporting.

    - Support to review and implement policies and procedures around cyber resilience, such as emergency and contingency plans, or risk registers.

- Leadership

    - Support to improve the understanding of the corporate team or political leadership.

- Training and awareness

    - Support to introduce more robust training and awareness raising around cyber security for all staff/and or councilors.

    - Support to introduce specific training for technical staff.

    - Support to embed cyber awareness more broadly across the council and its partners.

You may also bid for funding in areas not explicitly covered by a question in the Stocktake if you can explain why this supports efforts to improve your cyber resilience (and/or the cyber resilience of the councils you are working with).

Type B: Sector Development Project

We also welcome individual or joint bids between councils and partners to consolidate work across the sector by joining up efforts and resources and, in doing so, developing the sector's cyber resilience, and/or building sector capacity.

Bids under this category should be projects which aim to pilot/explore/develop a proof of concept which could potentially be scaled up and shared with all English local authorities.

Examples of this type of project might include:

- Training and Awareness: A project to explore sustainable solutions for staff training and awareness. This may include reviewing any existing training packages developed in house by a council / group of councils to see if these might be used more widely across the sector, or building on these to create an ongoing solution.

- Developing a technical training programme for IT staff throughout the country. This could include, for example, PEN testing, how to run phishing exercises, effective logging.

- Developing a sector led approach to disaster recovery and incident response. This could include a model of peer support to deal with incidents.

- Developing guidance on effective governance around cyber resilience. This might include advice on business continuity planning, effective risk registers, or board structures.

Where there are multiple bids looking to do similar work, we will bring colleagues together to avoid duplication. Therefore, we encourage collaborative bids and joint working across the sector when applying for funding under this category.

Bidding Process

Bidding for Phase 2 will be completed via a secure online form. A unique link will be sent to a named person in your council. This will be the person who led on completing the Stocktake on behalf of the council. If you are unsure who this is then please get in touch with us at *cybersecurity@local.gov.uk*.

This form is designed to help add clarity to the information and details we need from your bid, and streamline the bidding process.

A PDF of the full set of questions contained in the form can be found at the bottom of the page to help you prepare your submission, however we ask you to submit bids through this online form only and not through any other means.

If your proposal is part of a group of councils then a bid should only be submitted once for the group – by the lead council. An individual council who is part of a joint bid may also apply separately for funding for activities relating solely to the council.

The online form is designed so that it can be used to apply for Type A or Type B funding or both.

For "Fix" bids, we will assess each bid solely on the information submitted via this form. For 'Sector Development Project' bids, we will use the information in this form as the basis for further discussion.

We further advise that you:

- Discuss the specific area or areas identified in your council's Cyber Security Stocktake assessment (or the broad themes identified by a group of councils) which you are planning to address.
    - You may wish to prioritise both 'red' and 'amber' areas.
- Outline the activity, programme of work or product you are seeking support for, and how it addresses the particular area or areas identified (measurable, and practical).

    - Please consider on-going sustainability of the improvements sought.

- Cover all of the activities you would like funding for from this phase in one bid submission.
    - You do not need to submit a separate bid for each area or activity, multiple items may be detailed in one bid.

    - Bidding in this phase does not preclude you from bidding again in future phases, however when bidding again you must be able to provide evidence that prior funding is being used and actioned as agreed.

    - As well as submitting a bid for your own council, you may also concurrently take part in a joint bid with a group of councils where you are not the lead authority. Please make reference to this in your individual bid if known at the time of bidding (including the name of the lead council).

Indicative costing for bids

Whilst the form will ask you to put an estimated costing for the activity, this can be your best estimate.

If you have researched or obtained quotes for the cost of the measures you wish to implement, please include any supporting information in your bid.

We will not fund work that is 'business as usual', or activities a council would be expected to fund themselves. We will, however, fund necessary initial work to set in train a strong, sustainable and effective cyber security programme where immediate and pressing vulnerabilities have been identified.

How the LGA will review bids

The LGA will accept bids up until the closing date on 29th May. The assessment process will be carried out throughout June, funding will then be awarded to the successful bidders subject to funding having been transferred to the LGA by the Cabinet Office. LGA colleagues may contact the named lead contact to clarify any details in your bid.

Bids will be assessed together and not on a first come first served basis. The LGA will review all bids and allocate funding based on our review of the totality of the bids received.

The LGA will review bids with support from a trusted, expert panel of local government cyber security professionals, with representatives from each region. With their input, we will endeavor to allocate the funding fairly and proportionately, employing a strategy that will best meet the needs of the sector.

Where appropriate, council names will be anonymised throughout this process.

The LGA will issue grants to named individual councils. Where commonalities are identified across several bids, we may offer councils grants on the basis of a joint solution or approach where appropriate. We will discuss this with you if this is the case.

If successful, confirmation of agreed funding will be sent to the council or lead council.

Grants will likely be paid into council accounts in July, subject to the LGA receiving the funding from Cabinet Office and volume of bids received.

The role of suppliers

The LGA has not shared any council's information as disclosed in the Cyber Security Stocktake with any supplier, except where a council has given explicit consent to one the specialist advisors employed by the LGA. Your council's assessment remains strictly confidential to you.

The LGA will never promote one particular vendor or supplier to your council. It is up to your council to choose any supporting supplier, if relevant to the activity you have bid for.

However, we may support you to improve the service your existing supplier gives you, or help you work with other councils to raise common issues with a supplier.

Security of the bidding process

We recommend limiting the amount of sensitive information that is shared. If you deem any information too sensitive to share then please get in touch to arrange an appropriate alternative.

Questions

Email: Cybersecurity@local.gov.uk

Phone: If you would prefer to speak to an LGA colleague by phone, you can email the above address to arrange this.