

Notice of Non-key Executive Decision

Subject Heading:	Extension of Cyber Analyst Service – Block Hours
Cabinet Member:	Cllr Middleton
SLT Lead:	Simon Oliver Director of Technology and Innovation
Report Author and contact details:	Alexandra West, Acting Head of Information Assurance (DPO) alexandra.west@onesource.co.uk
Policy context:	The Council has a statutory duty under the Data Protection Act and the UK GDPR to protect the information it processes while delivering statutory and resident services. The Cyber Analyst Service - Block Hours provide specialist technical capability to act on threat intelligence, to advise on technical security issues and to assure that the delivery of services is as secure as possible so that the integrity of Council services remains intact to ensure continued delivery of all services.
Financial summary:	The financial commitment being asked for is £150,000 to provide 12 months of specialist cyber capability to the Information Assurance function.
Relevant OSC:	Overview & Scrutiny Committee
Is this decision exempt from being called-in?	Yes

Non-key Executive Decision

The subject matter of this report deals with the following Council Objectives

- People - Things that matter for residents [X]
- Place - A great place to live, work and enjoy [X]
- Resources - A well run Council that delivers for People and Place [X]

Part A – Report seeking decision

DETAIL OF THE DECISION REQUESTED AND RECOMMENDED ACTION

Following the successful trial of Cyber Analyst Service – Block hours, to extend the contract with Stripe OLT Consulting LTD (Company No. 08257141) by 12 months as defined in the original G-Cloud arrangement.

Please note that this report seeks to correct the following governance issues:

- The original officer decision was made using a Newham form but a Havering contract was issued.
- The original officer decision referred only to the 6-month trial and not the option to extend 2 x 12 months following a successful trial (the option to extend was included in the contract).

AUTHORITY UNDER WHICH DECISION IS MADE

3.4 Powers of Second Tier Managers

Financial responsibilities

- (a) To incur expenditure within the revenue and capital budgets for the relevant service as approved by the Council, subject to any variation permitted by the Council's contract and financial procedure rules.

STATEMENT OF THE REASONS FOR THE DECISION

Since September 2022, OneSource on behalf of LB Havering and LB Newham, has been trialling the Stripe OLT Cyber Analyst Service – Block Hours.

According to industry reports (CSOonline), a data breach costs UK companies an average of \$3.88m per breach and 33% of organisations report the loss of customers following such an incident. Service disruption at councils that have been hit by a cyber-attack runs to many months with associated costs to the organisation, staff, and residents/customers.

Non-key Executive Decision

The cost of a breach is not just measured in regulatory fines but also in staff time lost due to the inability to carry out their functions and core staff organising, fixing, and responding to the breach. It is therefore imperative that the Council does everything possible to prevent cyber-attacks with associated data loss, including appropriate oversight of third party suppliers and partners that process Council data.

Cyber security is not a fixed state, aspired to and then reached, but a constant and continuous effort to identify and fix gaps, to implement and monitor appropriate controls to ensure the continued confidentiality, integrity and availability (CIA) of the data that the Council is responsible for as data controller.

This service provides advice and guidance to both technical and business colleagues, identifies gaps in the cyber posture, as well as activities to remedy them, and supports the Boroughs in their continuous improvement efforts to strengthen and deepen their cyber security posture.

The service is providing much needed capacity and expertise and is supporting the Boroughs to treat their number one risk: the risk of falling victim to a cyber-attack.

While efforts were made to recruit an individual to the role of cyber analyst, this was unsuccessful due to the pressurised market.

In order to find the much needed capability and capacity, a decision was made to think about alternative solutions. A possible alternative delivery model was identified as working with an external security partner who could provide the required capability and capacity. A 6-month trial was planned and the G-Cloud Framework was identified as a safe procurement route that meets the Council's needs and enabled a partner to be selected in a timely manner. An assessment of suppliers was performed against search terms and a Partner identified.

The trial has been assessed as successful by key officers, including the Chief Information Officer, and permission is now being sought to extend the current contract with the supplier of the trial (Stripe OLT) to provide the same services for a further 12 months.

The service will continue to ensure that disruption from cyber-attacks will be kept to a minimum, that services will continue to deliver uninterrupted, and that business continuity plans will not have to be activated for serious and long term outages. The cost of this preventative service should not be deemed prohibitive, compared to the cost and service disruption of a Hackney-style ransomware attack. It must be emphasised that the success of this service is prevention and the absence of service disruption and is therefore to be classed as an invest to save measure. Furthermore, compared to the cost of building an in-house team, this solution is not just cost effective but provides a real reduction in cost (£150k vs c £470k).

Below is a list of activities that are included in the service:

- a. Monitor, triage, and respond to emails in cyber-security mailbox
- b. Run weekly and monthly vulnerability scans
- c. Respond to security alerts from SOC
- d. Advise CIO and Information Assurance Lead on emerging threats
- e. Review relevant configurations for security requirements (e.g. Firewalls, Endpoints)
- f. Advice on Access Permissions Management

Non-key Executive Decision

- g. Advise on controls for legacy software
- h. Attend meetings as directed by Information Assurance Lead
- i. Attendance of weekly CAB to provide security advice and guidance
- j. Support the Enterprise Architect by providing specialist security expertise
- k. Review of DPIAs and advice on security requirements/controls
- l. Review of and advice on security requirements/controls of suppliers (SCRM)
- m. Advice, review and testing of backups
- n. Develop security metrics for Information Governance Boards
- o. Provide technical advice on risks and controls to Infrastructure Programme
- p. Ensure patching is up to date by liaising with Ops team
- q. Organise PEN Tests (including scope and remediation work)
- r. Advise on security content of relevant policies, standards, and processes in IG Framework
- s. Provide technical advice on risks and controls of software (new and updates) and processes (new and existing)
- t. Support the councils' audit processes by contributing and advising on information and security focused audit programmes
- u. Support the development of security related training by providing

OTHER OPTIONS CONSIDERED AND REJECTED

The Cyber Analyst market is competitive and resource is both costly and difficult to engage.

Following several unsuccessful recruitment campaigns, other solutions were sought. Engaging with a partner allows access to a wide skill set, redundancy (i.e. continued cover even when individuals are away), at competitive pricing. Engaging with this service covers the skillset of 5 different levels of security personnel (availability of the skill sets combined is equivalent to 1 FTE which is deemed to be acceptable given current budgetary pressures).

Options considered:

1. **Do Nothing:** This option cannot be chosen as falling victim to a cyber-attack remains the Council's top corporate risk and the Council has a statutory duty to ensure all information is processed securely. "Do nothing" would mean implementing systems that are not checked for security controls, not being able to provide advice and guidance to operations and business colleagues on safe and secure methods of processing data (including not being able to process Data Protection Impact Assessments) to name but a few.
2. **Build an in-house function:** In order to provide the required capacity and skillset to ensure Council operations are legal, compliant and secure, a team of ca 5 x FTE would have to be employed. The total cost of such a team is estimated to be in excess of £350,000. It would include a Cyber Security Manager, a Senior Cyber Analyst, 3 x Cyber Analysts. The cost of a fully resourced function would be closer to £470,000.

Non-key Executive Decision

PRE-DECISION CONSULTATION

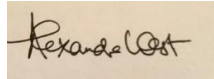
No consultation is required for this decision.

NAME AND JOB TITLE OF STAFF MEMBER ADVISING THE DECISION-MAKER

Name: Alexandra West

Designation: Acting Head of Information Assurance

Signature:



Date: 01/02/2023

Part B - Assessment of implications and risks

LEGAL IMPLICATIONS AND RISKS

This report seeks approval to extend the G-cloud contract with Stripe OLT Consulting LTD for a period of 12 months until March 2024.

The Council has the general power of competence under section 1 of the Localism Act 2011 to do anything an individual may generally do subject to any limitations. The recommendation in this report is in keeping with these powers.

The option to extend the term was contemplated at the time the contract was awarded and the contract includes a provision to extend the initial 6 month term for 2 periods of 12 months each until 2025.

Therefore, the proposed extension is in compliance with the limitations imposed by the Public Contracts Regulations 2015 and Regulation 72(1) (a) in particular.

In accordance with Contract Procedure Rule 19.8, the reasons and authority to extend the contract must be recorded in writing and loaded onto the Council's preferred e-tendering suite.

Officers have confirmed that the provider has performed the service to a satisfactory level under the current contract.

FINANCIAL IMPLICATIONS AND RISKS

The cost of the contract for 12 months is £150,000 (12 x £12,500). This cost will be paid for by Havering and split 50/50 with the London Borough of Newham. The costs will be funded from each authority's 'evergreening' budgets.

There will be an option to extend a further by a further 12 months at the end of the contract period.

HUMAN RESOURCES IMPLICATIONS AND RISKS (AND ACCOMMODATION IMPLICATIONS WHERE RELEVANT)

There are no Human Resources implication, nor risks, associated with this decision.

Non-key Executive Decision

EQUALITIES AND SOCIAL INCLUSION IMPLICATIONS AND RISKS

There is no requirement to conduct an EQIA as this decision has no impact on any vulnerable groups.

BACKGROUND PAPERS

None

Non-key Executive Decision

Part C – Record of decision

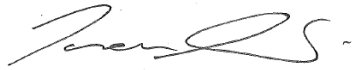
I have made this executive decision in accordance with authority delegated to me by the Leader of the Council and in compliance with the requirements of the Constitution.

Decision

Proposal agreed

Details of decision maker

Signed



Name: Simon Oliver

Head of Service title: Chief Information Officer

Date: 10/02/2023

Lodging this notice

The signed decision notice must be delivered to the proper officer, Debra Marlow, Principal Democratic Services Officer in Democratic Services, in the Town Hall.

For use by Committee Administration

This notice was lodged with me on _____

Signed _____