PFCC
POLICE, FIRE AND CRIME COMMISSIONER FOR ESSEX

PFCC Decision Report

Report reference number: 006-23 **Classification:** OFFICIAL
Title of report: IT Technical Refresh 2023/24
Area of county / stakeholders affected: Force-wide
Report by: Steph Gill (Head of IT Service Delivery) and Philip Bartholomew (Head of IT SACS) **Chief Officer:** Jules Donald (Director of Support Services) **Date of report:** 26/2/2023 **Enquiries to:** Steph Gill (Head of IT Service Delivery)

1. Executive Summary

To seek approval of the Stage D Technical Refresh Business Case (appendix A) for Essex with revenue recurring costs of £0.251m; one off revenue set up costs of £0.126m and capital costs of £3.052m in 2023/24.

2022/23 has seen the investment in and migration to third party data centres for both forces. Essex now has a primary third-party data centre with resilience provided by links and fail over processes between it and a secondary third-party data centre. This led to the fast-track replacement and rationalisation of a higher percentage of the infrastructure than would normally be undertaken in a single year. Funding for this was provided via the approval of the Data Centre migration programme full business case. Consequently, the capital requirement for technical refresh in 2023/24 has reduced by 28% compared to predicted costs pre-migration (2021/22) in line with the benefits of the Data Centre Migration Programme (DCMP).

The annual cycle of Technical Refresh across IT infrastructure and computers is essential to maintaining secure, resilient access to IT systems for all police officers and support staff.

In 2023/24, technical refresh covers the following areas:

ARC Data Centres	On-Premise Infrastructure	End User Devices
Isilon storage servers	DFU storage servers	Desktops
Load balancers	Backup servers	Laptops
Secure internet gateway	Checkpoint security	Printers
	Network switches	Monitors
	Network firewalls	Smartphones
	WIFI	Body Worn Video
	Structured cabling	IP telephones
	Video conferencing	Video conferencing
	Milestone (CCTV)	

2. Recommendations

This proposal requests continued investment in server, storage and network infrastructure after the move of both forces' data centres to Crown Hosting / Ark Data Centres, and also includes the remaining Essex estate IT infrastructure that is required to maintain internal force network connectivity and security. This proposal also includes the end user device replacement, which for 2023/24 consists of laptops, desktops, monitors, smart phones, printers, body worn video, Digital Forensics Unit devices, IP telephones, and video conferencing equipment.

It is therefore recommended that approval of £3.429m comprised of £3.052m capital, £0.126m one-off revenue and £0.251m recurring revenue funding, outlined in the Stage D Business Case, is agreed for the IT Technical Refresh programme to continue in the 2023/24 financial year.

3. Background to the Proposal

The annual cycle of technical refresh across IT infrastructure and end user devices is essential to maintaining resilient access to IT systems for all police officers and support staff, which remediates the risk seen in previous years where the IT infrastructure was unstable. The technology refresh process is the cycle of regularly updating key elements of an IT infrastructure to maximise system performance. Instead of using systems until they can no longer function, it is good practice proactively to upgrade or replace components of an infrastructure on a regular schedule. Maintaining IT infrastructure is costly and can be more so for legacy systems and services. Legacy technology that has not been updated can lead to poor performance and service delivery, inefficiencies in energy and space consumption, and bloated administrative and maintenance overheads. Alongside this, there are increased risks of maintaining ageing IT assets where a failure is likely rather than just possible. This will add to corporate concerns and budget challenges.

A technical refresh programme relates to more than just infrastructure, which is by and large made up of servers, storage, network devices and all the services these require to function. Technical refresh also extends to the majority of IT services that are consumed, from applications to services that are used by everyone in the organisation to a single user requirement. All users have a need to use laptops, desktops and mobile devices. By having a technical refresh programme, critical infrastructure and continued investment in the IT infrastructure will address current in-year capacity limitations, return the wider IT infrastructure to a position where it is fit for purpose and more able to meet in-year growth. The technical infrastructure refresh programme will improve performance and functionality and continue to improve our security position by eliminating security issues identified by IT health checks. Significant growth in data storage requirements will be subject to stand alone business cases submitted by the relevant organisational department.

This work will support the wider IT Programme of Work, the Data Centre Migration Project, and estates transformation and will have a major positive impact on our IT security by removing old unsupported IT systems. The move to more ‘agile’ devices from conventional desktops will support a more agile work force which is an enabler for proposed estate changes and will enable new working practices and maximise the use of valuable office space.

4. Proposal and Associated Benefits

Due to the nature of a business-as-usual technical refresh programme such as this, that requires investment in technology, there are no cashable savings. This proposal presents non-cashable benefits as follows:

Cost avoidance via continued improvement of highly available networking between police devices, sites and third-party services which form a large part of both operational and non-operational policing. The avoidance of downtime due to failing infrastructure or that which is not suitable for the ever-increasing size of digital media will undoubtedly improve policing efficiency and outcomes (for example, back record conversion (BRC) costs for one week of downtime for Storm would be around £17,500).

Avoidance of risk of out-of-support hardware which falls below national standards for connection to the PSN (Police Services Network), risking disconnection from this network and inherent vulnerability to cyber threats. PSN is the pan-government network that all central and local government departments use to connect to each other.

Increased compliance with national standards relating to both policing and the General Data Protection Regulation (GDPR); maintaining accreditation and avoiding risk of data breach and resulting fines from the Information Commissioner’s Office (ICO).

Avoidance of retrospective logging cost should ill-maintained or aging systems be unavailable. e.g., by maintaining systems on better designed new storage infrastructure within Ark Datacentres, de-duplication and more efficient archiving will reduce the amount of data being stored and therefore the costs associated with that storage.

Increased compatibility with future technology enabled by national programmes such as National Identity & Access Management (NIAM) and the National Law Enforcement Data Programme (NLEDS).

Reduction in potential costs incurred when third parties are required to assist with recovery of failed systems and data from ill-maintained infrastructure.

Maintenance of improved Wi-Fi provision will be an enabler to maximise the capability of mobile devices and increase the value provided by an increasingly agile workforce. Wi-Fi provision is also critical to ensure that Kent and Essex are able to comply with GDPR guidelines by central filtering of attempts to access malicious sites. Partnership working on police premises will be enabled by an adequately maintained Wi-Fi provision.

Replacement of aging end user devices is an enabler for full exploitation of agile working and the latest operational system upgrades required. It is increasingly important to stay on-track with hardware compatible with in-support Microsoft Operating Systems to reduce the likelihood of vulnerability to cyber threat by adhering to minimum national standards. As our IT programme of work introduces new services we must ensure all our devices support new software and application technology and security standards.

There is a detailed plan for the technical refresh that follows a large number of different technology platforms and devices and, as such, the procurement activity relating to these will be requested throughout the financial year. As with previous years, we will have a dedicated programme to track progress and spend which in turn updates Corporate Finance.

End user devices are tracked via a rolling replacement schedule, based on when the device will become end of life, usually replaced every three or four years depending on the device type. We then associate an estimated unit cost to those devices based on previous purchases and market trends / inflation to give us the estimated cost per device. End user devices form £2,470.5k of the overall capital spend. There is the possibility of further Chief Officer and Commissioner sign off where contracts fall into certain commercial spend categories (>£250k, >£1m etc).

5. Options Analysis

Unfortunately, the options are limited when it comes to refreshing infrastructure and end-user hardware. In years gone by the replacement of such hardware could be delayed purely at the risk of increased likelihood of failure. Now however the risk is much greater over time from increased vulnerability to cyber threat. Where previously vendors would support hardware and its firmware for five to 10 years, it is more common now for them to cease updates / support between three and five years after release. Therefore the resulting options are:

1. Continue to use hardware past vendor supported date, risking failure, cyber vulnerability and Police Network accreditation due to falling below minimum standards set by the national SIRO (Senior Information Risk Officer).
2. Stop using the hardware. This option would reduce the force's technical capability and / or resilience, ultimately affecting its capability to meet the Force Plan.
3. Refresh the hardware in line with guidance set by the original vendor and standards set by the national SIRO.

4. Move to cloud-based infrastructure, effectively renting the service from a third-party vendor. This option removes some periodic capital replacement, replacing it with re-occurring revenue and passes the cost and risk to the third-party.

This business case recommends option 3 due to the high likelihood of unacceptable risk / loss of service resulting from options 1 and 2 identified above, whilst considering a gradual move to Option 4 on a case-by-case basis. IT Services already have a ‘cloud first’ strategy where it is not prohibited by cost or risk, and there is now very little infrastructure residing within the police estate over that which is required to maintain connectivity at and between sites with the majority either in third-party Ark Datacentres or cloud based.

6. Consultation and Engagement

The following parties have been consulted, internal to Essex Police:
Information Security
7 Force Procurement
Corporate Finance
Strategic Change
Estates

7. Strategic Links

The Essex PFCC’s, Police and Crime Plan 2021 – 2024 states the intent to:

- *“Use technology more to help Essex Police be visible in their communities including developing mobile applications and enabling better connectivity”.*
- *“Invest in Body Worn Video and Tasers to help keep public, officers and staff safe and be effective in their roles”.*
- *“Continue to maximise the benefits of collaboration between Essex and Kent Police”.*
- *“Identify drivers who need remedial education by investing in technology to enable the police to process the increasing volume of video evidence supplied from dash-cams…”.*

Technical infrastructure refresh will support all the above statements. Over the next 12 months work will continue to upgrade, consolidate, and migrate IT systems away from on-premise server rooms to state of the art third-party Ark Datacentres, removing reliance on force estate and associated costs. Upgrade of local networking infrastructure will support the increasing volumes of network traffic uploaded from body-worn, digital interview and dashcam footage, whilst moving towards a ‘zero-trust’ model to reduce the likelihood of cyber attack.

8. Police operational implications

The technical infrastructure refresh programme has been planned in line with the Essex Chief Officer Group’s requirement to have a secure, stable and resilient platform on which all technical operational policing activity can take place, focusing on capacity and continuity of service.

9. Financial implications

The Stage B business case was approved during the 2022/23 budget setting process and funding has been set aside within the Subject to Approval Capital Programme.

This Stage D Technical Refresh Business Case is seeking approval for funding in 2023/24 only. The budget requirement to deliver the IT Technical Refresh programme for Essex is £3.429m comprised of £3.052m capital, £0.126m one off revenue and £0.251m recurring revenue funding.

The funding requirement for 2023/24 reflects a reduction of £0.341m in total and comprises of a reduction of £0.096m recurring revenue costs, one off revenue costs of £0.120m and reduction in capital funding requirement of £0.125m when compared to the Stage B Strategic Outline Case. These reductions have been made after reviewing the programme of work within IT for 2022/23, 2023/24 and 2024/25, as well as taking the opportunity to align skills and workload in the IT Target Operating Model (TOM) which will come into effect in November 2023. The TOM has allowed us to remove costs for cloud management and operation by creating dedicated roles within IT.

We have been able to bring forward further O365 developments around device management into 2022/23 and have removed costs associated with the CISCO phone system as we will address the future of this as part of the Microsoft Enterprise Agreement renewal in 2024/25.

The above figures exclude the costs associated with borrowing in respect of this project however it should be noted that this will lead to an increase in the force's capital financing requirement (CFR). This will result in charges to the revenue account relating to minimum revenue provision (MRP) and interest payable. For this project in year one, these costs will equate to the capital investment value of £3.052m being charged as MRP in instalments over the useful economic life of the related asset. In respect of interest payable for external borrowing it is assumed that the force will incur financing costs of approximately 4.5% for a period of seven years. On the assumption the principal is not repaid in full until the end of the borrowing term this will result in total charges to the revenue account of proceeding with this project of £4.014m, incorporating both the MRP and interest elements. It should be noted that the above financing costs are already budgeted in the MTFS 23/24 to 27/28 as part of the "subject to approval" capital projects, and these are being provided for information only in respect of understanding the cost implications to the force of proceeding with this project.

FUNDING SUMMARY – CORPORATE FINANCE USE ONLY

	Year 1 2023/24	Year 2 2024/25	Year 3 2025/26	Year 4 2026/27	Year 5 2027/28	Total
CAPITAL COSTS	£000'	£000'	£000'	£000'	£000'	£000'
(ESSEX ONLY)						
Stage B - budget setting	3177.2	4181.0	4283.5	2780.1	5988.5	20410.3
Stage D	3052.1	4181.0	4283.5	2780.1	5988.5	20285.2
Variance: Stage D compared to budget setting provision (if applicable)	(125.1)	0.0	0.0	0.0	0.0	(125.1)
REVENUE SET-UP COSTS SUMMARY						
(ESSEX ONLY)						
Stage B - budget setting	246.4	70.0	29.6	20.0	10.0	376.0
Stage D	126.4	70.0	29.6	20.0	10.0	256.0
Variance: Stage D compared to budget setting provision (if applicable)	(120.0)	0.0	0.0	0.0	0.0	(120.0)
REVENUE RECURRING COST SUMMARY						
(ESSEX ONLY)						
Stage B - budget setting	347.0	241.9	266.8	242.1	235.5	1333.3
Stage D	251.0	241.9	266.8	242.1	235.5	1237.3
Variance: Stage D compared to budget setting provision (if applicable)	(96.0)	0.0	0.0	0.0	0.0	(96.0)
TOTAL PROJECT COSTS						
STAGE B - BUDGET SETTING	3770.6	4492.9	4579.9	3042.2	6234.0	22119.6
STAGE D	3429.5	4492.9	4579.9	3042.2	6234.0	21778.5
NET IMPACT ON CAPITAL PROGRAMME-(SURPLUS)/DEFICIT	(341.1)	0.0	0.0	0.0	0.0	(341.1)

The table below provides a summary of the expected costs of technical infrastructure refresh from 2023 to 2028. We are asking for approval of spend in Year 1 (2023/24) only as part of this decision report. Costs for Years 2 – 5 are best estimates on what we know now. Each year we review and adjust the costs in-line with technical requirements and market value for items. This is why only Year 1 is showing a saving (£341.2) as we have been able to adjust workload in year and reduce costs as part of the wider IT target operating model.

1. DETAIL OF COSTS						
	Year 1	Year 2	Year 3	Year 4	Year 5	TOTAL
	2023/24	2024/25	2025/26	2026/27	2027/28	
	£'000	£'000	£'000	£'000	£'000	£'000
	Essex	Essex	Essex	Essex	Essex	Essex
Capital cost						
Infrastructure	**581.60**	**750.00**	**526.10**	**1,147.10**	**2,289.90**	5,294.70
End User Devices	**2,470.50**	**3,431.00**	**3,757.40**	**1,633.00**	**3,698.60**	14,990.50
Total Capital cost	**3,052.10**	**4,181.00**	**4,283.50**	**2,780.10**	**5,988.50**	**20,285.20**
Revenue set up cost						
Infrastructure	**126.40**	**70.00**	**29.60**	**20.00**	**10.00**	256.00
End User Devices	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	0.00
Total Revenue set up cost	**126.40**	**70.00**	**29.60**	**20.00**	**10.00**	**256.00**
Revenue recurring cost						
Infrastructure	**251.00**	**241.90**	**266.80**	**242.10**	**235.50**	1,237.30
End User Devices	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	0.00
Total Revenue recurring cost	**251.00**	**241.90**	**266.80**	**242.10**	**235.50**	**1,237.30**
Total Costs	**3,429.50**	**4,492.90**	**4,579.90**	**3,042.20**	**6,234.00**	**21,778.50**

10. Legal implications

The Essex server and network support and maintenance are covered under a contracted agreement with a supplier. We are contractually bound to maintain the hardware and its supporting infrastructure as part of this support and maintenance. Future contracts will be required for the data centre migration which will carry a dependency that Essex Police has adequate infrastructure in place to perform service and data migration from on premise to a hosted data centre.

11. Staffing implications

No staffing implications have been identified in the report.

12. Equality, Diversity and Inclusion implications

A secure, resilient, stable infrastructure allows services such as M365 (Teams, Yammer, SharePoint etc) to support officers and staff with technical reasonable adjustments as well as providing force wide platforms to share, engage and present equality, diversity and inclusion awareness and training.

13. Risks and Mitigations

An infrastructure that has the latest security developments and is running the latest versions of operating system software etc will greatly help address the cyber security risk of a robust infrastructure to protect the confidentiality, integrity and availability of our technology services and data (Identify, Protect, Detect, Respond, and Recover). The risk of cyber-attack is relevant to both forces.

Remediation work of the IT infrastructure continues to be undertaken to upgrade and replace systems and solutions where required to deliver a stable, resilient and performant infrastructure. Much of the work planned within this business case will help mitigate this risk.

14. Governance Boards

The stage D Technical Infrastructure Refresh business case has been through the following governance boards:

08/02/2023	Chief Officer Group, Essex Police
01/03/2023	Strategic Board, Essex Police

15. Links to Future Plans

The ongoing refresh of our technical infrastructure is pivotal to IT providing a full catalogue of services to Essex Police.

Growth in officers and staff increases the capacity requirements on all elements of server, network and end user device services.

An ongoing refresh programme supported by appropriate funding allows IT Services to ensure the Police and Crime Plan promises to “Deliver over 300 more officers” and “Use technology more to help Essex Police to be visible in their communities…” are fulfilled by ensuring the supporting services and infrastructure that are needed to deliver those promises are secure, resilient, and sustainable.

As Essex looks at its physical estate, including the headquarters site where much of the server and infrastructure service is based, IT needs to ensure we keep ahead of the requirement for relocation of services (data centre migration). This is only possible if the technical infrastructure is up to date and performing securely, efficiently, and resiliently, only achieved with a robust refresh programme.

16. Background Papers and Appendices

[redacted]

[redacted]

[redacted]

Report Approval

The report will be signed off by the PFCC's Chief Executive and Chief Finance Officer prior to review and sign off by the PFCC / DPFCC.

Chief Executive / M.O.   Sign:

Print: P. Brent-Isherwood

Date: 24 February 2023

Chief Financial Officer   Sign:

Print: Janet Perry

Date: 13 April 2023

Publication

Is the report for publication?   **YES** ☒

NO □

If 'NO', please give reasons for non-publication *(Where relevant, cite the security classification of the document(s). State 'None' if applicable)*

None

If the report is not for publication, the Chief Executive will decide if and how the public can be informed of the decision.

Redaction

If the report is for publication, is redaction required:

1. Of Decision Sheet? **YES** □ ☒   **2. Of Appendix?** **YES** ☒ □

NO	**NO**

If 'YES', please provide details of required redaction:
Appendix A and B – Commercially sensitive data relating to aging technology and services that should not be available commercially.

Date redaction carried out: 20th April 2023……………..

Chief Finance Officer / Chief Executive Sign Off – for Redactions only

If redaction is required, the Treasurer or Chief Executive is to sign off that redaction has been completed.

Sign: ……………………………………………………..........

Print: Janet Perry……………………………………

~~Chief Executive~~ / Chief Finance Officer

Decision and Final Sign Off

I agree the recommendations to this report:

Sign:

Print: ROGER HIRST

PFCC

Date signed: 19th April 2023

I do not agree the recommendations to this report because:

……………………………………..

....

....

Sign:

Print: