NOTTINGHAMSHIRE
Fire & Rescue Service
Creating Safer Communities

Nottinghamshire and City of Nottingham
Fire and Rescue Authority
Finance and Resources Committee

ICT RESOURCE REVIEW

Report of the Chief Fire Officer

Date: 29 June 2018

Purpose of Report:

To provide Members with an update of demands for resources in delivering the ICT Strategy of the Fire Authority.

CONTACT OFFICER

Name :	Craig Parkin Assistant Chief Fire Officer
Tel :	0115 967 0880
Email :	craig.parkin@notts-fire.gov.uk
Media Enquiries Contact :	Therese Easom (0115) 967 0880 therese.easom@notts-fire.gov.uk

1. BACKGROUND

1.1 The overall aim of the Information and Communications Technology (ICT) Strategy for Nottinghamshire Fire and Rescue Service (NFRS) ICT Strategy was to achieve a balance of organisational efficiency and new innovations:

"To reduce organisational risk by creating a foundation of ***standardised***, ***resilient*** and ***integrated*** systems with ***simplified*** processes; delivered by cost-effective ICT services and solutions that are focussed on the needs and objectives of Nottinghamshire Fire and Rescue Service."

1.2 In April 2016, the Finance and Resources Committee report 'Information and Communications Technology Strategy 2016' provided Members with a report on the progress of the Information and Communications Technology (ICT) Strategy 2013. The report also outlined the Service's proposed approach to ensure that it continues to provide an effective ICT infrastructure, to meet its information management and IT security responsibilities until 2020.

1.3 Furthermore, in January 2018 the Finance and Resources Committee was provided with an update on the progress of the current ICT Strategy. This report highlighted that additional permanent skill requirements had arisen within the ICT Department because of the increased number of risks and responsibilities that need to be managed, both from internal and external factors.

1.4 The Assistant Chief Fire Officer and the Head of ICT were tasked by the Finance and Resources Committee to produce a further report detailing the outcomes of an assessment of future demands and the resources required to proportionality manage identified risk.

2. REPORT

2.1 Continued pressure on funding and resources means that the Service is required to focus on managing those areas of highest risk. Adopting a risk based approach at both a strategic and tactical level will ensure that resources are focused on areas that best deliver priority services.

2.2 The overall budget pressures of NFRS and study of future demands placed upon the delivery of ICT on the Service has highlighted the need for continued efficiencies. This means that the Service will need increased capacity to achieve further efficiencies and develop the infrastructure to deliver services.

2.3 To achieve this, it will require a shift in emphasis from how the Service currently operates and adopts new ways of working. This will effectively mean broadening the roles and responsibilities of the existing staff, along with increasing resources in areas of technical expertise, should this be supported by the Authority.

2.4 The current ICT Department has evolved since 2012, with the introduction of dedicated ICT strategies and the need to attain improved levels of security to manage risk. These changes address increasing workloads, expanding roles and responsibilities of the function and the overall strategic direction of ICT to support the delivery of services by NFRS.

2.5 At present, the ICT Department establishment consists of two sections:

- Information Technology – managed by the IT Manager
- Project Management – managed by the Service Project Manager

2.6 Since 2016, a temporary establishment has been in place to enable the ICT Strategy and specific ICT projects to be delivered, these are as follows:

- The ICT Service Improvement Section
- The ICT Service Transformation Section
- The ICT Service Operations Section
- The PSN Security Team

2.7 The ICT Department provide ICT technical support activities into NFRS through a combination of in-house expertise and maintenance from external specialist service providers.

2.8 The successful delivery of ICT services demands more than the implementation of technology by technical development staff; the traditional in-house development approach no longer meets the needs of NFRS. Therefore, to ensure a professional service is provided there should be greater focus on 'IT as a Service', rather than the delivery of technology:

> "IT as a service (ITaaS) is an operational model where the IT organisation of an enterprise is run much like business, acting and operating as an internal service provider. In this model, IT simplifies and encourages service consumption, provides improved financial transparency for IT services, and partners more closely with lines of business. This type of IT transformation is business focused rather than cost focused, leading directly to improved levels of business agility."

2.9 The transformation of the culture within the ICT will align with the principles of ITaaS needing to focus resources on the following key capabilities to address future demands:

- The effective management of ICT projects and ICT changes and the provision of project and programme management expertise to the Service;

- The proficient management of the delivery of ICT Operations through greater emphasis on IT Service Delivery Management;

- The provision of a professional and dedicated cyber-security capability to ensure the continued protection of the NFRS ICT Infrastructure and support the continued access to the Emergency Services Network;

- The effective administration of the electronic document and records management solution provided by Microsoft SharePoint, to support the compliance of NFRS with General Data Protection Regulations (GDPR);

- The effective management of the NFRS ICT Network Infrastructure, using in-house resources and capabilities;

- Undertaking Continual Service Improvement (CSI) and Business Analysis activities to drive efficiency throughout the Service;

- The long-term support of 'local' technical issues relating to the East Midlands Tri-Service Control solution, that are not supported within the Managed Service Agreement delivered by Systel;

- The provision of shared IT Service Delivery Management resource to represent the interests of the East Midlands Tri-Service Control partners.

2.10 The completed analysis, the requirement to enhance the cyber-security stance of NFRS and increase collaboration activities with Tri-Service partners and beyond has also provided a re-focus on the wider organisational environment of NFRS and its future.

2.11 This has emphasised that the Service will need to provide a larger scope of ICT activities to support the organisation, particularly around the management of information security and governance. Whilst seeking more efficient ways of working.

2.12 This report identifies how efficiencies and change can be implemented through the resources provided across ICT, recognising the need for increased investment to save measures to achieve a more effective and secure ICT infrastructure for the whole organisation.

2.13 Government expectation of public bodies for continual investment and development of their ICT is contained within the 2016-21 cyber security strategy. This is reflected locally within the Services protective security framework approach, coordinated by a Security Steering Group.

2.14 Numerous high profile cyber-attacks have been reported across the public sector, presenting increased risk to communities should critical services be unavailable. Whilst this is recorded within the corporate risk register and business continuity approach, it stills requires actions to be deployed to remove, reduce or tolerate arguably the most significant of identified risk.

2.15 The speed of growth and reliance upon technology is complicated for any organisation to keep track of, however, this is a key enabler for all

departments to support greater efficiencies as a collective, rather than within the ICT department in isolation.

2.16 Given the changing nature of technology it is now considered appropriate for the current ICT strategy and structure to be reviewed and amended to ensure this remains fit for purpose and facilitate continuous improvement.

3. FINANCIAL IMPLICATIONS

3.1 The annual pay budget including the temporary establishment of the ICT Department is currently £858,901 funded by an increase of £195,000 to the ICT salary budget for two years between 1 April 2017 to 31 March 2019 from an earmarked reserve.

3.2 To sustain the Service's ability to maintain a resilient and adaptive ICT function is highly likely to require budgets to meet the eight key capabilities detailed in within this report on a substantive basis potentially resulting in an annual pay budget increase in excess of £200k.

3.3 The increase to the pay budget would be offset by some revenue budget savings generated during FY 2018-19 and FY 2019-20 and should be viewed as a potential invest to save approach for the Service.

4. HUMAN RESOURCES AND LEARNING AND DEVELOPMENT IMPLICATIONS

4.1 The ICT Strategy, Tri-Service Control collaboration project and Emergency Services Mobile Communication Programme (delivering ESN) continues to place significant demands upon the Service, which has resulted in several fixed term arrangements being put in place.

4.2 These have all been delivered within the Service's existing policy framework, but this report highlights the need to build in further capacity on a permanent basis and plan to address future risk. This report presents a wide range of implications, potential new roles, regrading of existing roles and significant training of all post holders to maintain currency.

4.3 To further enhance the cost effectiveness, resilience and knowledge of the ICT Department, further investment will be required to improve the skills of the internal staff. This will reduce the current reliance upon external resource for the provision of technical expertise and further build resilience.

4.4 Given the increased reliance upon technology that drives internal demand across the Service, the use of IT Service Management (ITSM) principles, the change in culture towards ITaaS, the need for improved cyber-security and the requirement to achieve and maintain ESN code of connection, it is proposed that the current structure of the ICT Department be reviewed and amended as appropriate. This clearly has implications for the Services permanent

establishment and if supported will be dealt with via the Human Resources Committee.

4.5 The effective management of ICT change projects and the provision of project and programme management expertise to the Service, will require a range of changes. Including an expanded role for Service Project Manager and a new role of ICT Service Delivery Manager replacing the current Information Technology Manager role.

4.6 The establishment of a cyber-security capability both in terms of management and governance to ensure the continued protection of the NFRS ICT Infrastructure.

4.7 The effective administration of the electronic document and records management solution provided by the Service Microsoft SharePoint solution, to support the compliance of the NFRS to GDPR, will require the changes to the ICT establishment and increased levels of administration.

4.8 The effective management of the NFRS ICT Network Infrastructure, using in-house resources and capabilities would require changes to the duties of the role of IT Development Officer, these being expanded to the role of ICT Technical Analyst, with IT Infrastructure Development Officer incorporated into the role of ICT Technical Analyst.

4.9 Undertaking Continual Service Improvement (CSI) and Business Analysis activities to drive efficiency throughout the Service, would require the new role of Information Security and Governance Officer and role of ICT Business Analyst. An apprentice role could provide support of 'local' technical issues relating to the East Midlands Tri-Service Control solution.

5. EQUALITIES IMPLICATIONS

An equality impact assessment has not been undertaken as this report does not amend the current provision of services.

6. CRIME AND DISORDER IMPLICATIONS

There are no crime and disorder implications arising from this report.

7. LEGAL IMPLICATIONS

There are no legal implications arising from this report.

8. RISK MANAGEMENT IMPLICATIONS

8.1 Cyber security is currently itemised within the Service's risk register and seeks to reflect the national cyber security strategy 2016-2021, underpinned by a range of workstreams within the Service.

8.2 The reliance upon external supplier contract resource to supplement gaps in internal technical resource was identified as a risk within the current NFRS ICT Strategy. The over-reliance on external development resource to ensure project advancement and maintain internal service levels is resulting in increased expenditure to the ICT revenue budget and reduced levels of corporate knowledge being maintained.

8.3 The current level of resilience within the established ICT development resource impacts upon major development project areas, due to availability of skills due to external factors, unplanned absences and other unforeseen circumstances.

8.4 The increased focus on ITaaS would require a more dedicated IT Service Management to reactively and proactively maintain the continuous availability and reliability of all ICT services provided to NFRS and for the implementation of continuous improvement activities during the lifecycle of all ICT services.

8.5 The provision of business analysis and project delivery activities is essential to the success of current and future ICT projects; the ICT Service Transformation work stream must therefore be given adequate opportunity to develop without other competing demands.

8.6 The management of cybersecurity risk through the establishment and maintenance of an Information Security Management system is an essential requirement to enable NFRS to achieve Emergency Services Network (ESN) code of connection. The information security management role would be responsible for proactively monitoring and maintaining the security, integrity and availability of the ICT infrastructure, systems and information assets.

8.7 As the provision of ICT increases in its complexity it becomes necessary to implement systems to monitor the processes used within the ICT service delivery lifecycle. To manage this risk, a permanent continual service improvement activity should be established to ensure that the ICT service delivery lifecycle offers best value to the organisation.

8.8 The proposals detailed above will enable the Service to better deal with the risks that will result from the transformation and development of the organisation; in line with the current NFRS ICT Strategy and the NFRS organisation development strategy.

8.9 The current temporary funding of additional resources within ICT if not maintained present a significant challnege in the Services ability to deliver future strategies given increased levels of demand and therefore its choices in managing risk.

9. COLLABORATION IMPLICATIONS

9.1 The Service is currently engaged in a range of collaborations drawing upon the ICT function, including the Information Technology Manager into the Tri-Service Control project.

9.2 The Head of ICT represents the Service at the East Midlands Tri-Service Control executive board and acts as regional technical advisor to the East Midlands ESN strategic board and programme, including commitments at a national level.

9.3 The expansion of the role of 'Head of ICT' into the revised role of 'Head of Technology, Information Security and Projects' would ensure that collaborative opportunities are explored as part of the East Midlands Tri-Service Control Consortium and the Emergency Services Network.

9.4 The NFRS ICT Service Desk will provide a triage service for incidents raised by NFRS staff prior to being passed to the appropriate external support provider. This additional administration and first-line support function will improve the support of the Integrated Command and Control solution and thus benefit all parties concerned.

9.5 The monitoring of the performance of the network infrastructure that interconnects the East Midlands Tri-Service Control solution will become the joint responsibility of all three partner ICT Departments. This will significantly improve the management of the infrastructure which supports the Systel solution and enable the ICT Departments of the East Midlands Tri-Service Control Consortium partners to work more collaboratively.

9.6 An extranet capability is being developed in-house by the ICT Department to assist with future collaborative opportunities between partner organisations and reducing many barriers to closer working and sharing of information. Collaboration will have implications with a greater focus on information security and network monitoring.

10. RECOMMENDATIONS

It is recommended that Members:

10.1 Note the contents of this report.

10.2 Support a review of ICT structure to identify additional resources.

10.3 Receive further update reports on progress in delivering resources to manage future risk and review of the ICT strategy.

11. BACKGROUND PAPERS FOR INSPECTION (OTHER THAN PUBLISHED

DOCUMENTS)

None.

John Buckley
CHIEF FIRE OFFICER