STAFFORDSHIRE FIRE AND RESCUE SERVICE

Item 5 (iii)

IT STRATEGY ADVISORY AUDIT

Internal audit report 2.21/22

Final

3 February 2022

1. EXECUTIVE SUMMARY

With the use of secure portals for the transfer of information, and through electronic communication means, remote working has meant that we have been able to complete our audit and provide you with the assurances you require. It is these exceptional circumstances which mean that 100 per cent of our audit has been conducted remotely. Based on the information provided by you, we have been able to sample test and review systems and documentation to inform our conclusions.

Why we completed this audit

The Staffordshire Fire and Rescue Service (SFRS) Safety Plan 2020-2024 - which sets out the priorities for protecting Staffordshire residents - explicitly outlines the following in its introduction to the key strategic aims *'consideration of new technologies, equipment and training will allow us to explore alternative approaches to how we deliver an effective and efficient service.'*

Coupled to the impact caused by the global pandemic, there has been a concerted effort to change existing working practices to facilitate remote working and collaboration. In addition, SFRS is striving to achieve cost efficiencies by rationalising its software estate and identifying potential areas of duplication i.e. disparate systems which all perform the same functionality. This has led to SFRS undertaking some large projects; including the roll out of Office 365 across their IT estate.

It has been recognised that investment in modernising and developing ICT will be the key enabler to deliver strategic aims, but there is a risk that without sufficient oversight of the various workstreams in progress at SFRS, the output from this work will not deliver the intended outcome.

The key objective of this review is to confirm that appropriate controls are in place for the effective operation and governance of the IT Strategy. This work is advisory in nature therefore we have not provided a formal assurance opinion.

Conclusion

Our review identified that the work to deliver the objectives outlined in the Digital Strategy was underway, but the processes for ensuring that this work was adequately planned, governed, reported and aligned to the broader SFRS was not in place. This has been exacerbated by some changes within the key staff at SFRS and periods of absences within the ICT team which has constrained resources. Whilst it was evident from discussions with the key contacts during this review, that there was an understanding of some key issues such as the requirement to deliver Office 365 to deliver better opportunities for remote working, collaborating and resilience – this work did not seem aligned with broader initiatives to address strategic objectives. Consequently, there is a risk that the work underway is a series of disparate projects which are not necessarily aligned to the broader strategic objectives of SFRS.

Consequently, this review has identified a number of key areas of weakness that management need to focus on, to formalise and enhance their current processes to demonstrate how ICT – and at a broader level SFRS – ensure that they meet the strategic objectives of SFRS.

Key findings

We identified the following weaknesses resulting in the agreement of two high and four medium priority management actions:

There is no clear demonstrable link between the Staffordshire Fire and Rescue Service Strategy (as articulated in the SFRS Safety-Plan-2020-V1) and the Digital Strategy. In addition, it is not clear if the objectives outlined in the Digital Strategy have been formally agreed and have the necessary 'buy in' from Management. There is a risk that key objectives have been determined without the engagement of all stakeholders across SFRS. This could lead to changes which are short term reactions from the organisation and may not reflect the direction of travel of the Authority. Consequently, valuable resources may be wasted on activities which do little to help SFRS achieve their broader strategic objectives. ***(High - Management Action 1)***

Whilst some key strategic objectives have been identified in the Digital Strategy, there is no formal project management methodology, roadmap or programme of work to support the achievement of these objectives. This increases the risk that this work is not effectively planned, resourced and delivered. ***(High – Management Action 2)***

Following discussions with the Director of Community Safety we were advised there was no defined process for ensuring that all external influences were fully considered before developing the Digital Strategy. Whilst there was evidence that some budgetary influences had fed into ICT projects, such as the Service 2025 project (which sought to look at future ways of working and the rationalising of IT systems), it was not evident that this was driven by the Digital Strategy, it was largely a result of pressures to cut costs. Therefore, there is an increased risk that the decisions are not being made based upon their strategic importance. ***(Medium – Management Action 3)***

There are no formal IT working groups or projects tasked with identifying strategic objectives and delivering them. Inquiry of the Project Co-ordinator confirmed that there is a planned meeting structure and Terms of Reference (ToR) for a number of new IT groups, but these had yet to be agreed and implemented. The absence of any working groups inhibits the ability to deliver on the objectives of the Digital Strategy and could lead to the resulting work not being sufficiently discussed, challenged or agreed with stakeholders. ***(Medium – Management Action 4)***

SFRS has not formally agreed any SLAs or KPIs in relation to ICT. This increases the risk that the performance is not measured against the strategic objectives. This also limits the accountability of ICT's performance and delivery against any agreed objectives. ***(Medium – Management Action 5)***

Through inspection of the 'Service Digital Strategy V1' we confirmed that there are no references to any review cycles of the Digital Strategy. This increases the risk that the document is not subject to review and revisions to ensure that it remains aligned to the broader SFRS Strategy. ***(Medium – Management Action 6)***

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Strategy Alignment	
Control	Missing Control - There is no clearly demonstrable link between the Staffordshire Fire and Rescue Service Strategy and the Digital Strategy.
Findings / Implications	We obtained and inspected the SFRS Safety-Plan-2020-V1 which outlines the key strategic priorities. There are mentions of technology within sections 1, 2 and 4 of the Strategy document. In particular, there is the following comment within section 4: *'The service needs to continually improve, adapt and evolve to be able to thrive in a time of unprecedented change and financial challenge. Our people are at the heart of that. We encourage our people to explore new ways of working and embrace new technology.'* In addition, there were a few references to Cyber Security within the document, specifically in the introduction section of the Strategy: *'As well as aiming to cause physical harm, terrorist attacks now seek to disrupt services by preventing access to buildings or damaging computer systems. We have measures in place involving physical and cyber security, but we must continue to be vigilant and develop our buildings, systems and staff knowledge to keep pace with the threat.'* We obtained and inspected the Service Digital Strategy V1 and sought to confirm if there was any reference to how new technology and cyber security issues were going to be addressed. The Digital Strategy outlines the following key objectives • Enable anytime, anyplace working • Provide the right information to the right people at the right time • Allow collaborative and connected working • Provide resilience and security • Rationalise all the systems and applications Whilst there is a link between some of the high-level objectives in the SFRS Strategy and the Digital Strategy (such as the resilience and security objective which are aligned to the cyber security threat), not all of the links are so clear. In addition, it is not clear if the objectives outlined in the Digital Strategy have been formally agreed and has the necessary 'buy in' from Management. There is a risk that the key objectives have been determined without the engagement of all stakeholders across SFRS.

Strategy Alignment				
	This in turn increases the risk that the changes being made are short term reactions from the organisation and may not reflect the direction of travel of the Authority. Consequently, valuable resources may be wasted on activities which do little to help SFRS achieve their objectives.			
Management Action 1	Management will ensure that the Digital Strategy is clearly aligned to the broader SFRS strategic objectives. As part of this, Management may wish to consider the following strategic development checklist: 1. Understand the current position 2. Reflect on how you got there 3. Be clear about your corporate identity (mission, vision and values) 4. Analyse your strengths and weaknesses 5. Analyse the business environment 6. Identify and evaluate strategic options 7. Set objectives 8. Communicate the strategy 9. Implement the strategy 10. Review progress	**Responsible Owner:** Head of ICT	Date: April 2022	**Priority:** High

Strategy Implementation and governance arrangements	
Control	Some key strategic objectives have been identified in the Digital Strategy but there is no prescribed project management methodology, roadmap or programme of work to support the achievement of these objectives.
Findings / Implications	Inspection of the Service Digital Strategy confirmed that there were the following key strategic areas: • flexible working; • collaborative and connected working; • resilience and security; • rationalising systems and applications Inquiry of the Project Coordinator, who works closely with the Head of IT confirmed that these areas were being addressed by the ongoing project work. However, the work was not clearly defined as a broad programme of work with a cohesive set of aims and objectives. This increases the risk that the work being delivered by IT meet a series of short-term demands made by the business, but do not align with the broader direction of strategic travel. This could ultimately lead to scarce resources being inefficiently assigned.

	We obtained and inspected the 'SFRS ICT Roadmap 2021-2025' and confirmed that this contained work to upgrade systems, network infrastructure, disaster recovery (DR) capability and telephony. Whilst it is evident that developing the DR capability would have a direct effect on the strategic objective of improving resilience, it is not clear if this work is driven by the Digital Strategy. Further inquiry of the Project Coordinator confirmed the Office 365 project addressed some of the key Digital Strategic objectives: • Flexible working (cloud access makes remote working easier); • Collaborative/Connected Working (MS tools will help with collaborative working); and • Resilience/Security (implementation of Multi-Factor Authentication (MFA) tools provide additional security) However, we also noted that whilst there was project management documentation for the Office 365 work (such as deployment tasks, risk register and project plan), this was not evident for the other work such as Project 2025 and the work to develop the DR capability. Inquiry of the Office 365 Project Manager confirmed that there is no prescribed methodology for delivering project work. This increases the risk that this work is not effectively planned, resourced and delivered.			
Management Action 2	Management will introduce a programme of work to deliver the strategic objectives. This will be underpinned by clearly defined project roadmaps, workstreams and project plans which follow a prescribed project management methodology.	**Responsible Owner:** Head of ICT	**Date:** April 2022	**Priority:** High

External influences	
Control	As part of the 'Service 2025' project some of the external influences, primarily budgetary influences were considered and fed into the Digital Strategy. However, other external influences such as changes to regulations or technology had not been formally considered.
Findings / Implications	Following discussion with the Director of Community Safety we were advised there is no defined process for ensuring that all external influences were fully considered before developing the Digital Strategy. However, we were informed of the Service 2025 project, which sought to look at future ways of working – primarily through the cost lens. We confirmed that this project led to ICT rationalising some of the disparate IT systems in use across SFRS. We obtained and reviewed the 'Service 2025 Admin Workstream – ICT Systems Overview' document which outlined where there was potential to rationalise systems. However, as already noted, the Service 2025 project was not driven by the Digital Strategy, it was largely a result of pressures to cut costs. Therefore, there is an increased risk that the decisions were made for cost reasons instead of their strategic importance. Without a full consideration of all external influences, using a strategic analysis model such as PESTLE or SWOT, there is no demonstrable link to confirm that strategy has fully considered all external factors. This could lead to the strategy quickly becoming redundant as external factors render the assumptions and objectives redundant.

External influences				
Management Action 3	Management will consider the use of a strategic analysis model, such as SWOT or PESTLE to determine how the external factors feed into the Digital Strategy.	**Responsible Owner:** Head of ICT	**Date:** April 2022	**Priority:** Medium

User Requirements	
Control	Missing Control - There are no IT working groups or projects involved with planning future requirements.
Findings / Implications	From inquiry of the Project Co-ordinator, we confirmed that ICT only tend to liaise with business areas to discuss issues as required. We obtained and reviewed evidence to confirm that ICT are in regular contact with key stakeholders such as the Police (who are part of a shared service with SFRS). Recent examples of meetings regarding PSN, Wi-Fi, and telephony was provided. Following discussions with the Director of Community Safety we were advised that there was limited representation at a Directorate level from ICT. This is due to a combination of factors including the long-term absence of the IT Manager following a period of sickness. Consequently, there is an increased risk that the lack of ICT involvement at senior, strategic level meetings could lead to poorly informed decisions due to the lack of any support or challenge from a technology perspective. However, there are no formal IT working groups or projects tasked with identifying strategic objectives and delivering them. Inquiry of the Project coordinator confirmed that there is a planned meeting structure and Terms of Reference (ToR) for a number of new IT groups. These include: • ICT CAB and Systems Security Meetings • ICT Commercial Meetings • ICT Delivery Meetings • ICT Manager's Meetings • ICT Project Meetings Establishing a set of working groups with defined ToR's which are aligned to the Digital Strategy (and suitable stakeholders) would help facilitate the delivery of the objectives of the Digital Strategy. However, at the time of this review, these had not been agreed and implemented, increasing the risk that the strategic objectives and resulting work has not been sufficiently discussed, challenged or agreed with stakeholders.

Management Action 4	Management will establish formal engagement leads in each business area to liaise with ICT regarding current and future requirements. The work to identify IT working groups and Terms of Reference will be reviewed through the lens of an agreed Digital Strategy and approved.	**Responsible Owner:** Head of ICT	**Date:** July 2022	**Priority:** Medium

Monitoring and reporting processes				
Control	Missing Control - SFRS has not formally agreed any Key Performance Indicators (KPIs) or Service Level Agreements (SLAs) in relation to IT.			
Findings / Implications	We obtained and inspected evidence of some client feedback forms, reporting feedback on specific tickets raised with the Helpdesk function, however these responses are not mandated. Whilst we were able to obtain and review some evidence of reporting in relation to the progress of individual projects e.g. O365 reports, there is no defined reporting process which feeds Management Information (MI) back to a decision making level. This increases the risk that management do not have sufficient data or information to support their decision making processes. There are no formally agreed KPIs or SLAs in relation to the performance of ICT. This increases the risk that the performance is not measured against the strategic objectives. This also limits the accountability of ICT against any agreed objectives.			
Management Action 5	Once the Digital Strategy has been agreed and communicated, a set of clearly defined KPIs s and SLAs will be agreed to measure the performance of IT in delivering these objectives.	**Responsible Owner:** Head of ICT	**Date:** July 2022	**Priority:** Medium

Strategy review				
Control	Missing Control - There is no review process/cycle defined in the Digital Strategy.			
Findings / Implications	Inspection of the 'Service Digital Strategy V1' confirmed that there are no references to any review cycles of the Digital Strategy. This increases the risk that the document is not subject to review and revisions to ensure that it remains aligned to the broader SFRS Strategy.			
Management Action 6	Management will ensure that the Digital Strategy is regularly reviewed to ensure that it remains aligned to the broader SFRS Strategy.	**Responsible Owner:** Head of Strategy and Intelligence	**Date:** July 2022	**Priority:** Medium

APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

Objective of the review	Agreed actions		
	Low	Medium	High
To ensure that appropriate controls are in place for the effective operation and governance of the IT Strategy.	0	4	2
Total	**0**	**4**	**2**

APPENDIX B: SCOPE

Scope of the review

The internal audit assignment has been scoped to assess the controls that manage how the Staffordshire Fire and Rescue Service manages the following risk(s):

Objective of the area under review	Risks relevant to the scope of the review
To assess that appropriate controls are in place for the effective operation and governance of the IT Strategy.	The IT strategy is not aligned with the overall business strategy, meaning corporate business objectives are not achieved or supported. External factors are not considered during development and implementation of the IT strategy. The IT strategy is developed without user consultation. Strategy implementation and governance arrangements are in place and appropriate. Monitoring and reporting arrangements are not effective.

Scope of the review

The following areas will be considered as part of the review:

This advisory review will include a high-level overview of the controls in place for the development, management and implementation of the IT strategy at Staffordshire Fire and Rescue Service.

Our audit will review the following areas;

- Alignment of the IT strategy with broader Staffordshire Fire and Rescue Service strategic objectives
- Ensuring external influences feed into the strategy development process
- User Requirements are consulted on and represented appropriately
- Strategy Implementation and governance arrangements are in place and appropriate across the key strategic areas of:
  - flexible working;
  - collaborative and connected working;
  - resilience and security;
  - rationalising systems and applications
- Monitoring and reporting processes are adequate and effective.
- A regular review process is defined within the strategy

The following limitations apply to the scope of our work:

- We will provide an advisory audit report highlighting specific actions required by Management to address specific risks in relation to the ICT Function and ICT Strategic Planning.
- This review will be delivered on an advisory basis and a formal assurance opinion will not be provided.
- The results of our work are reliant on the quality and completeness of the information provided to us
- Our work does not provide any guarantee against errors, loss or fraud or provide an assurance that error, loss or fraud does not exist.

Please note that the full scope of the audit can only be completed within the audit budget if all the requested information is made available at the start of the audit, and the necessary key staff are available to assist the audit process during the audit. If the requested information and staff are not available, we may have to reduce the scope of our work and/or increase the audit budget. If this is necessary, we will agree this with the Staffordshire Fire and Rescue Service sponsor during the audit.

Debrief held	16 September 2021
Draft report issued	27 September 2021
Responses received	3 February 2022
Final report issued	3 February 2022

Internal audit Contacts	Daniel Harris, IA Partner Angela Ward, Senior Manager Sheila Pancholi, Technology Risk Partner Darren Currell, Technology Risk Principal Consultant
Client sponsor	Howard Watts, Director of Community Safety
Distribution	Howard Watts, Director of Community Safety

rsmuk.com