Control Room

North Yorkshire Fire and Rescue Service

Internal Audit Report 2020/21

Business Unit: Control Room
Responsible Officer: Deputy Chief Fire Officer
Service Manager: Group Manager, Control Room
Date Issued: 3 March 2021
Status: Final
Reference: 45600/001

	P1	P2	P3
Actions	**0**	**0**	**4**
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction

The efficient operation of a Control Room relies on a number of factors, such as the availability of staff and the capability and reliability of the Information Technology (IT) systems in place. At the time of this work the failure or loss of the Control Room function including Staff and IT provision was one of the highest risks stated on the services risk register. In the risk register dated 7 September, 8 control measures had been identified to reduce the risk from high (30) to amber (18). The Control Room for North Yorkshire Fire and Rescue Service (NYFRS) is located in their premises which are adjacent to the Fire Station, at Crosby Road, Northallerton.

In 2014 NYFRS and Cornwall Fire, Rescue and Community Safety Service (CFRCS Service) approved a business case to share a single mobilising system within their Control Rooms. The collaboration agreement is one of the eight actions included in the risk register to help manage and reduce the risk of failure or loss of the Control Room function.

The Control and Mobilisation Plan sets out details of the actions to be taken when spate conditions (occurrence of sudden water flow) or other emergency situations occur and cause disruption to the service. These actions are designed to achieve successful business continuity.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls ensured that:

- Control Room service risks and priorities had been identified, and these service risks and priorities were being managed through the Control and Mobilising Plan.
- The Control and Mobilising Plan was being regularly reviewed to ensure it is accurate, and up to date, thereby ensuring the expected standard of quality of service continued to be provided.
- The Control and Mobilising Plan was being tested to ensure any weaknesses were being identified and addressed.

Key Findings

All Control Room service risks and priorities have been identified in the NYFRS risk register. The Control and Mobilisation Plan is the key document to manage the business continuity arrangements and addresses all service risk and priorities identified within the risk register.

We have received assurance that the Control and Mobilisation Plan is being regularly reviewed. However, there is no record of who carried out the review, when that review was done, what was amended and when the next review is due. Information about the previous reviews was transferred from the Sharepoint system to the Cloud over the last 18 months. Records of those reviews appear to have been lost. The Plan is a

document that should be accessible (in hard copy in the Control Room) and the inclusion of these details will help ensure staff know they are using the most up to date version.

The Control and Mobilisation Plan did not contain comprehensive details about the actions to be taken in the event of IT failure. When raised during our work, the Group Manager, Control took immediate action by inserting a section covering the action to be taken in the Control Room at the time of an IT failure. There are contracts in place with the main external providers to the Control Room, namely Capita, Daisy Telecom and NYNET. The contracts with Capita, Daisy Telecom NYNET set out the response times. More details on these actual response times from the external contractors should also be recorded.

There is an understanding between the Control Room and internal NYFRS IT department that IT will provide 24 hour cover in the case of any IT failure. However, it is unclear what response times and expectations are, as these are not documented within the Control and Mobilisation Plan and there is no service level type agreement in place

The present staffing of the control room is 0.5 FTE above establishment. They have also recruited and trained 6 extra resilience staff in response to the Covid-19 crisis. Management should consider the future of these resilience staff after the Covic-19 crisis, as this could be another business continuity response that could be available to them in the future. There are presently sufficient managers in post to provide 24 hour cover.

A peer review carried out by the Chief Fire Officers and Local Government Association into Cornwall Fire, Rescue and Community Safety Service (CFRCS Service) in 2016 recommended that they improve their business continuity arrangements. NYFRS has in place a 'Guidance for Daily Working with CFRCS Service' which sets out the ways of working which was agreed with CFRSC Service during an Operational Board Meeting in November 2017. This document had initially been created in 2016 but has been subject of several updates since. NYFRS have not shared their Control and Mobilisation Plan with CFRCS Service and, to date NYFRS have not received assurance from CFRCS Service that they have suitable business continuity arrangements in place.

There is a regular series of testing being carried out. The programme consists of weekly, monthly and annual testing. IT issues are being reported through the submission of report forms to IT. Failing to continually invest in maintaining present IT systems, or in future advancements in technology will increase the risk of IT failure within the control room.

Regular training and exercising, including Flexible Duty Staff (FDS) and other resilience staff does take place. FDS sessions were cancelled during the period 18 March to 31 July 2020 (linked to the Covic-19 pandemic). A programme of training has since restarted and a schedule completed.

Overall Conclusions

There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited. Our overall opinion of the controls within the system at the time of the audit was that they provided Reasonable Assurance.

1. Business Continuity Arrangements following IT failure

Issue/Control Weakness	Risk
It is unclear what response times and expectations are, for the service being provided by IT to the Control Room. These are not documented within the Control and Mobilisation Plan and there is no service level agreement in place.	The possibility of delays in restoring connectivity within the control room may be delayed if the procedures are not fully outlined in the Control and Mobilisation Plan.

Findings

Over time an understanding has been developed between the management of the Control Room and the NYFRS IT Department that members of the IT Department will be available on a 24/7 response basis. When an IT failure occurs within the Control Room, the first point of contact should be the designated on call member of NYFRS IT department. The expectation is the IT department will facilitate the action required to resume normal service, and this may include liaising with external providers.

Capita have a contract with NYFRS to cover the main IT Software functions like Vision and DS3000. This contracts sets out the response times based on the priority of the fault, the highest been Critical or Grade 1. In these cases the initial response should be within 20 minutes and the fault repaired within the absolute maximum time of 24 hours. NYNET have the contract which covers the internet connections and Crosby Road has an enhanced 24 x 7 response specified within the contract. Daisy Telecom have a contract in place to respond which sets out a 6 hour response time for communication failures related to BT lines.

We found the actions to be taken in response to any IT failure were not comprehensively recorded within the Control and Mobilisation Plan and further detail was needed. During the audit the Group Manger has inserted an additional section within the Control and Mobilisation Plan to show the action that needs to be taken within the Control Room at the time of an IT failure. However, a further section needs to be included, giving details of the external IT contractors, and their contractual obligations. The approach of going direct to Capita, Daisy Telecom or NYNET out of hours is more operationally efficient, however, IT must be informed of this as soon as possible via the Fault Reporting System. This information should be covered in any written service agreements between the Control Room and IT department. A copy of the contracts with the external providers should also be retained by management in Control Room so that they are aware of the agreed response times.

In respect of the Control Room and IT Department there are not any written documents or expectations setting out their response times and expectations of the support arrangements. With a written agreement in place the expectations of the service provision are clear, and supplement the Control and Mobilisation Plan.

Agreed Action 1.1

We will work with the Head of IT Services and Support to obtain a comprehensive list regarding response times and processes, including those from external IT contractors and NYFRS internal out of hours response times. Once obtained the Control and Mobilisation Plan will be updated.

Priority	3
Responsible Officer	Group Manager, Control Room
Timescale	30 June 2021

2. Reviews of the Control and Mobilisation Plan

Issue/Control Weakness	Risk
There is no document review log for the Control and Mobilisation Plan.	The Plan becomes outdated, and lacks relevance and credence. Operators will be unsure if they are looking at the latest version of the Plan, and may follow a Plan that is outdated and incorrect.

Findings

The Control and Mobilisation Plan sets out details of the actions to be taken when spate conditions (occurrence of sudden water flow) or other emergency situations occur and cause disruption to the service. These actions should help achieve successful business continuity.

The Group Manager, Control Room, last reviewed the Control and Mobilisation Plan just after the start of the Covid-19 crisis. There have been previous reviews and that information was stored on the SharePoint system. The information about the reviews was transferred from the Sharepoint system to the Cloud over the last 18 months. When requested the IT department have been unable to recover the required information from the cloud and it appears that this information may have been lost.

The Control and Mobilisation Plan should be reviewed on an annual basis and also at times like the Covid-19 crisis. As this is a document that needs to be available to operators in hard copy, as well as online, then the dates of when the Control and Mobilisation Plan was reviewed and what was amended should be recorded on the form, as well as the date of the next scheduled review.

Agreed Action 2.1

Once the information is obtained from the Head of IT Services and Support then the Control and Mobilisation Plan will be updated and hard copies provided to the Control Room. There is now a section in the six monthly Control audit to check the Control and Mobilisation Plan is up to date.

Priority	3
Responsible Officer	Group Manager, Control Room
Timescale	30 June 2021

3. Business Continuity Plan Cornwall

Issue/Control Weakness	Risk
NYFRS have not received assurance that Cornwall have business continuity arrangements in place.	NYFRS may have to provide cover for CFRCS Service for a prolonged period. Reactive decisions taken by Cornwall may have unintended consequences on NYFRS IT or operational arrangements,

Findings

The partnership between North Yorkshire Fire and Rescue Service (NYFRS) and Cornwall Fire, Rescue and Community Safety Service (CFRCS Service) provides an opportunity for both Services to realise organisational and operational benefits through collaboration whilst maintaining a Critical Control and Fire Control function. The collaboration agreement was signed in 2014 and intended to provide resilience to both services at times of spate conditions, or other emergency situations.

In 2016 CFRCS were subject of a peer review by the Chief Fire Officers Association and Local Government Association. The report states: *'Formal business continuity arrangements were not provided for the new Critical Control function. CFRCS Service will need to demonstrate that it has considered all risks to delivering its Control function, and how it has mitigated against those risks, especially when looking to expand the role of the CCC. For example, where NYFRS and CFRCS Service both have significant incidents, or if CFRCS Service headquarters has outages or is rendered inoperable. The team recommend working closely with the council's Resilience and Emergency Management (REM) team in order to identify and mitigate against potential risks'*.

In the recommendations in the report the following recommendation was made:
'Review the Business Continuity arrangements for the new Critical Control function to ensure they are fit for purpose and appropriately documented'.

NYFRS do have in place a 'Guidance for Daily Working with CFRSC' which sets out the ways of working agreed with CFRSC during an Operational Board Meeting in November 2017. This document had been initially created in 2016 but has been subject of several updates since. This guidance document has been shared with CFRCS but they have not shared the Control and Mobilisation Plan. The only documentation that the Group Manager, Control Room was able to provide from Cornwall was a 2 page Covid Plan which dealt with staffing issues.

On 4 October 2020, Cornwall agreed a course of action to be taken with Capita and NYFRS about recovery of loss of connectivity between CFRCS and NYFRS. Despite this agreement CFRCS took a different course of action causing NYFRS to not having a fully functional Control Room till 3.30pm the following day. This has been escalated to Service Manager level at Capita.

Agreed Action 3.1

The Cornwall's updated BC Plan was received on the 22 January 2021 This plan has been reviewed and sufficiently covers their required actions at the time of a business continuity failure. The plan has been uploaded to sharepoint, where it can be easily accessed by the staff within the Control Room.

Priority	3
Responsible Officer	Group Manager, Control Room
Timescale	Completed

4. Amendments to Control and Mobilising Plans

Issue/Control Weakness	Risk
The Control and Mobilisation Plan did not include sufficient detail and was not up to date for key functions.	Whilst experienced staff are aware of historical and established procedures, any other staff having to cover will be unaware of those arrangements and rely on the Plan to guide them.

Findings

We reviewed the Control and Mobilisation Plan with a view to identifying any weaknesses within the Plan and to suggest any possible improvements. The Plan identifies the action to be taken within the Control Room at the time of any service failure. The Group Manager and the two Watch Managers were consulted throughout this process.

The actions to be taken in response to any IT failure were not comprehensively recorded within the Plan and further detail was needed. This has already been covered within Finding 1 of this report.

The wording in the system of contacting stations needs to be updated to reflect the current practice. This is that personnel are contacted through the text messaging system and stations then further supplement this by passing the message through their own WhatsApp groups.

Presently the Plan gives the impression that at the time of having to relocate the control room to other premises then an appliance should be used for the transport of staff. It is suggested this is amended to 'brigade transport or use of the control room staffs own vehicles if suitably insured to do so'.

Following discussion and agreement with the Group Manager, Control, amendments have already been made to the control and mobilisation Plan. Further work will be required on recording the actual agreed response times from the external contractors once all the details have been established.

Agreed Action 4.1

The Control and Mobilisation Plan has been updated as suggested, and just awaits the response from the Head of IT Services and Support, as outlined in finding one of this report.

Priority	3
Responsible Officer	Control Room Manager
Timescale	Completed

Audit Opinions and Priorities for Actions

Audit Opinions
Our work is based on using a variety of audit techniques to test the operation of systems. This may include sampling and data analysis of wider populations. It cannot guarantee the elimination of fraud or error. Our opinion relates only to the objectives set out in the audit scope and is based on risks related to those objectives that we identify at the time of the audit. Our overall audit opinion is based on 4 grades of opinion, as set out below.

Opinion	Assessment of internal control
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.