# ICT Asset Management

# North Yorkshire Fire and Rescue Service

# Internal Audit Report 2021/22

Business Unit: ICT
Responsible Officer: Head of ICT
Service Manager: Service Delivery Manager
Date Issued: 11 May 2022
Status: Final
Reference: 45580/008

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

# Summary and Overall Conclusions

## Introduction

Asset management is a systematic process of operating, maintaining, upgrading, and disposing of assets cost-effectively.

North Yorkshire Fire and Rescue Service (NYFRS) has a large number of ICT assets. To achieve value for money and full use from the hardware, it is important all ICT assets are tracked and managed appropriately. All ICT assets should be updated to ensure that users are using the optimal equipment and software. It is also important to make sure assets are secure and accounted for to help prevent data breaches and financial loss.

The service has recently invested in a new ICT Asset Management system that will facilitate the management of ICT Assets.

## Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system will ensure that:

- Due diligence is carried before purchasing ICT assets, so to help to demonstrate and obtain value for money
- Asset management processes are supported by effective inventory tools
- There is a complete and accurate list of all tracked assets
- All tracked assets are allocated to a named individual
- There is a clear ICT asset recovery process for when staff members leave

We had initially intended to review whether ICT assets were either redistributed or disposed of in a secure manner once they have reached the end of their lifecycle. Information was not provided in time for us to complete this work.

## Key Findings

All purchases are authorised by a manger before they are made. However, from our sample review of ICT purchases, no evidence of quotes are being sought for ICT spending to obtain value for money. All payments had been made via one company, Computarcenter.

All ICT Assets are provided with a unique reference number and they are assigned to either a named individual or department. All the key details of the ICT assets are stored within the ICT Asset register, which is used to effectively manage the ICT assets. The service have a clear policy in place for how ICT assets can be used.

A key ICT inventory control is, on a regular basis, to verify all assets still exist and are where the asset register says they are. In conversation with the ICT technician, it was explained that prior to the pandemic, visits would take place each year to confirm all ICT asset information was accurate, and assets were located as per the register. Any variances would be recorded and information updated.

Such checks have not been undertaken in the past two years due to the Covid pandemic. We were told these visits and physical checks of all assets would recommence in 2022/23, and this could help to ensure a complete and accurate list of assets exists.

All assets and their configuration information are identified and registered in the Configuration Management Database. There were a few discrepancies between the ICT Asset & Configuration Management process policy and practices. The policy states an item should include details of the hierarchical dependencies between itself and other configuration items within the Configuration Management Database (CMDB), the CMDB must be managed and audited, monthly report.  These processes are not currently in place. When staff leave or change roles within NYFRS there is a clear procedure or reallocating ICT assets to other members of staff. Once ICT assets have reached the end of their lifecycle, there is a clear process to dispose of the assets in a safe way however we did not obtain evidence that this process has been followed.

## 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 Value for money and following service procurement expectations

| Issue/Control Weakness | Risk |
|---|---|
| No evidence quotes are being sought for ICT spending which is required in the financial management policy. It is unclear what the service's expectations are, and/or whether the rules are out of date. | Fire Service rules are not followed and value for money is not obtained. |

**Findings**

Our review of ICT purchases over £10,000 highlighted that multiple quotes had not been requested or received for any of our sample sample. All purchases had been made via one company; Computarcenter.

In conversation with the ICT team it was explained that best value for money is sought before purchasing ICT Assets however evidence of obtaining quotes from different suppliers before purchasing ICT Assets was not saved. Therefore it was not possible for us to verify that different suppliers was considered before purchasing ICT Assets.

**Agreed Action 1.1**

Evidence for obtaining different quotes from multiple suppliers to obtain best value for money would be attached to tickets of the purchased ICT Assets within the service desk.

| | |
|---|---|
| **Priority** | 3 |
| **Responsible Officer** | Service Delivery Manager |
| **Timescale** | 31 August 2022 |

## 2 No ICT Assets Audit carried out

| Issue/Control Weakness | Risk |
|---|---|
| There has been no audit of the location of ICT Assets in two years | ICT Assets are lost/stolen or not recognised, leading to financial loss and data stolen. |

**Findings**

A key ICT inventory control is, on a regular basis, to verify all assets still exist and are where the asset register says they are.

In conversation with the ICT technician, it was explained that prior to the pandemic, visits would take place each year to confirm all ICT asset information was accurate, and assets were located as per the register. Any variances would be recorded and information updated. Such checks have not been undertaken in the past two years due to the Covid pandemic.

We were told these visits and physical checks of all assets would recommence in 2022/23, and this could help to ensure a complete and accurate list of assets exists.

**Agreed Action 2.1**

| | | |
|---|---|---|
| ICT Asset audit will commence in 2022. Features on the ICT Asset Management system, Lansweeper will be used to locate the location of ICT assets. To automate the location of tracking assets where possible. | **Priority** | 3 |
| | **Responsible Officer** | Service Delivery Manager |
| | **Timescale** | 31 August 2022 |

## 3 CMDB review is not being carried out

| Issue/Control Weakness | Risk |
|---|---|
| Configuration Management Database (CMDB) auditing is not being carried out | Issues not identified within the CMDB system. |

**Findings**

A configuration management database is used to store information about hardware and software assets. Details on configuration items and their relationship between critical assets are detailed within the Configuration Management Database (CMDB). The database may include any dependencies between configuration items.

The services Asset & Configuration Management policy requires that:
*"The CMDB must be managed and audited producing monthly reports showing to current validity and accuracy"*

The service is not currently carrying audits of the CMDB and no audit reports have been issued. This lack of review could mean that inaccuracies and errors within the CMDB are not being identified. Inaccuracies within the CMDB could mean that the impact of changes of configurations items is not known.

**Agreed Action 3.1**

| | | |
|---|---|---|
| To develop monthly reports of the CMDB to show the current validity and accuracy of configuration items of the device. | **Priority** | 3 |
| | **Responsible Officer** | Head of ICT |
| | **Timescale** | 31 December 2022 |

## 4 Configuration Items' Hierarchical Dependencies

| Issue/Control Weakness | Risk |
|---|---|
| Configuration items within the CMDB do not include hierarchical of dependencies which is non-compliant with NYFRA policy. | Configuration item dependencies are not known. |

**Findings**

The Asset & Configuration Management Policy also states that:

"[Within the CMDB] Each Configuration Item should include details of the hierarchical dependencies between itself and other configuration items that comprise an IT service as defined in the ICT Service Catalogue"

At the time of the audit this had not been completed. This could potentially mean that dependencies within the CMDB are not known, leading to relationships between Configuration Items and Assets not being known. This could increase the time for root cause analysis for any issues discovered and increase the time taken for change management processes.

**Agreed Action 4.1**

| | | |
|---|---|---|
| Map of Hierarchial Dependencies is being developed so it would be possible to know what impact changes will have on the wider network. The map with then be transferred to the CMDB. | **Priority** | 3 |
| | **Responsible Officer** | Head of ICT |
| | **Timescale** | 31 December 2022 |

# 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.