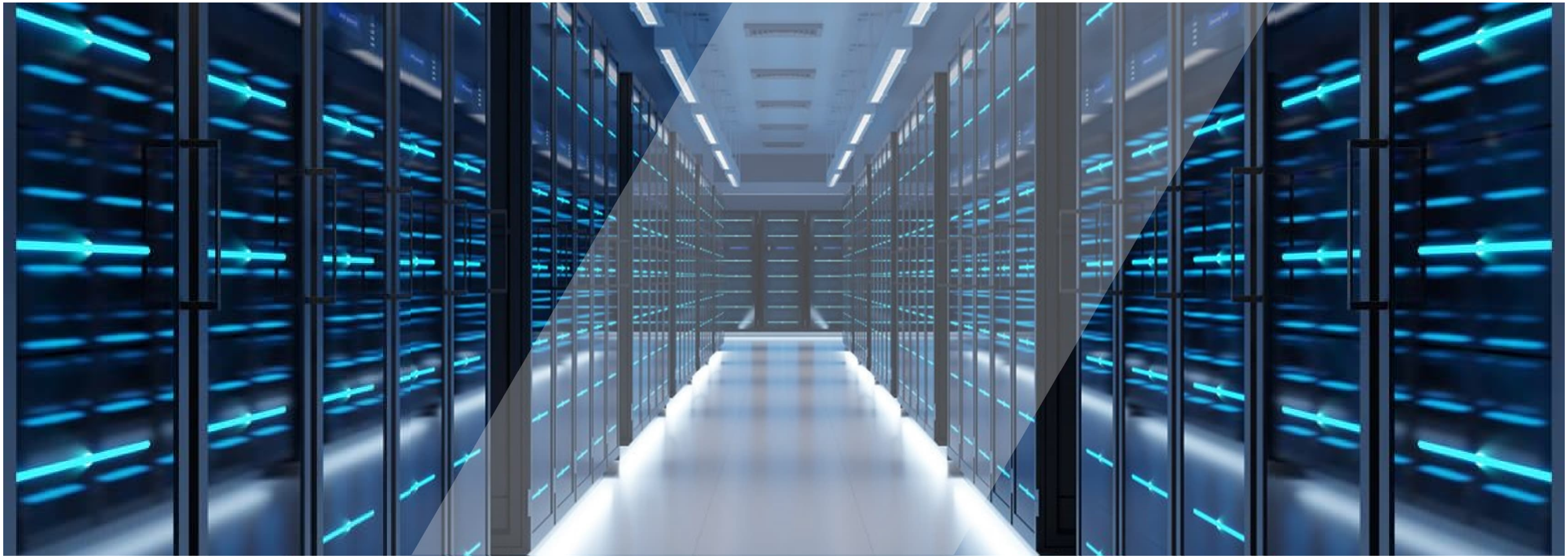

Hinckley and Bosworth BC: Internal Audit Final Report

IT Asset Management: Leicestershire ICT Partnership (LICTP) (2023/24)

Audit Sponsor: John Palmer (Strategic Head of ICT)

Audit Contacts: Alan Long (Operational Delivery Manager)
Grant Churchman (Infrastructure and Security Manager)

June 2025

Reporting Timetable

Debrief Meeting: 13/12/24

Draft Report Issued: 18/12/24

Comments Received: 12/3/25

Final Report Reissued: 11/6/25

forvis mazars

Contents

Disclaimer

This report ("Report") was prepared by Forvis Mazars LLP at the request of Hinckley and Bosworth BC and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of Hinckley and Bosworth BC and to the fullest extent permitted by law Forvis Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk. Please refer to the Statement of Responsibility in Appendix A1 of this report for further information about responsibilities, limitations and confidentiality.

Your One Page Summary

Audit Objective: To assess the design and effectiveness of the control framework for managing IT assets.

Audit rationale

Why the Audit is in Your 2024/25 Plan

This topic was requested by the LICTP steering group.

Your Strategic Risk

OPSICT12: Inaccurate Asset database – LICTP unable to provide adequate asset tracking, manage software and device lifecycles. (October 2023)

Summary of our opinion

Limited Opinion

See Appendix A1 for definitions

🟩	🟨	X	🟥

Summary of Recommendations

High Priority	2
Medium Priority	4
Low Priority	1

Actions agreed by you	100%
High Priority completion	31/10/25
Overall completion	30/6/26

Summary of findings

Examples of good practice

- ✓ A process is in place to report lost mobile phones, ensuring they are suspended or wiped to protect sensitive information.
- ✓ The equipment disposal process is carried out in an environmentally friendly manner by a service provider.

Highest Priority Findings

- Deficiencies in asset management process and assets maintenance.
- Weakness in the physical security measures for protecting hardware assets.

Key root causes

- Relying on inadequate tools and underutilising available technologies for asset management.
- Insufficient adoption of modern security measures and reliance on outdated practices.

01 Summary Action Plan

Below is a high level summary of the actions that are intended to support your management of this risk area. Further detail about our findings, which have been discussed with management, are provided in our detailed action plan (see 03 Detailed Action Plan).

Ref	Recommendation	Priority	Responsible Person	Due Date
1.	1. The server and network device data will be recorded into the Assets SharePoint list. 2. Certero is already used to scan the network on a regular basis. Reports will be generated quarterly to cross-check the records maintained in SharePoint will be undertaken. 3. In-Tune reports will be generated quarterly to cross-check asset records held in SharePoint. 4. A monthly stock check process has already been initiated and the stock recorded will be cross-checked against the LICTP SharePoint asset list referenced in (1) above.	High	Alan Long Operational Delivery Manager(ODM)	1. Complete 2. 31/07/25 3. 31/07/25 4. 28/02/25
2.	1. A regime of monthly checks on equipment stored within designated ‘server’ or ‘comms’ rooms will be undertaken to ensure they are clear of frangible materials, unused ICT equipment. 2. Work with MBC Estates management to identify or construct suitable ICT equipment storage area. 3. Work with estates management for each council, to implement CCTV monitoring of the doors to the server and IT asset storage rooms at each council.	High	Alan Long ODM	1. 28/02/25 2. 01/09/25 3. 31/10/25
3.	1. The pre-approved software to be finalised and published. 2. Include Mobile apps from In-Tune into Approved software list. 3. Bring all device software, (except mobile devices) into Certero and ensure licence process is created and adopted for the allocation, review, and management of licences.	Medium	1. John Palmer Strategic Head of ICT Shared Service (SHICTSS) 2. Alan Long ODM 3. Alan Long ODM	1. Dependent on completion of 2 and 3 2. 01/09/25 3. 01/09/25

4.	The consolidation of the asset register we have in SharePoint (response to finding 1) addresses this recommendation.	**Medium**	John Palmer SHICTSS	Complete
5.	1. Create an assets procedure and guidance to support the device lifecycle policy 2. Review policies annually or on request of revision once new draft policies approved and extant.	**Medium**	1. Alan Long ODM 2. John Palmer SHICTSS	1. 30/06/25 2. 30/06/26
6.	1. Approve and publish the draft AUP 2. Require all employees sign the finalised AUP once published 3. Create learning materials for the use, care and return of equipment and publicise to staff.	**Medium**	1. John Palmer SHICTSS 2. Alan Long ODM 3. Baljit Ghataorre/Alan Long ODM	1. 31/07/25 2. 01/11/25 3. 01/11/25
7.	1. Create and present proposal for an organisational change on asset budget management to ICT Steering Group. 2. Create guidelines and supporting communications materials on responsibility of managers to return leavers and redundant equipment. 3. Create quarterly asset allocation reports, distribute to managers and reconcile any alterations suggested by service managers and verify against ITAM/CMDB. 4. Create and present to ICT Steering Group returns exception procedure for approval.	**Low**	1. John Palmer SHICTSS 2. Alan Long ODM 3. Alan Long ODM 4. John Palmer SHICTSS	1. 12/08/25 2. 31/08/25 3. 30/09/25 4. 12/10/25

02 Value for Money and Sector Comparison

Within each of our reports, we summarise any observations we have made about the effectiveness, efficiency and economy of your operations. This is to support our portfolio of public and social sector organisations with value for money considerations. We also summarise how you compare to similar organisations, which is intended to bring you the benefit of our insight.

Value for Money

Effective IT asset management is critical for ensuring value for money within the Councils by minimising unnecessary expenditure and optimising the utilisation of available IT resources.

During the audit, we identified several areas where improvements may enhance cost-efficiency and resource allocation:

- The absence of a unified system for tracking and managing assets leads to inefficiencies, increased administrative effort, and potential underutilisation of resources.
- The lack of centralised tracking and analysis of software licenses may result in financial penalties for non-compliance, operational disruptions, or over-subscription.
- Insufficient physical security measures to secure IT assets expose the organisation to risks of theft, loss, and unauthorised access, resulting in potential replacement costs and investigation costs/fees related to security breaches.
- Delays in deleting unused Office 365 licenses for leavers and retrieving laptops retained by managers increase unnecessary procurement costs, which could be mitigated by implementing stricter processes for asset recovery and license management.

Sector Comparison

It is comparatively rare for organisations of any size to rely on IT asset records that are not held within a database of the service desk software. Many organisations support this with further software to scan the network for devices and their software which enables inaccuracies in the IT asset registers to be investigated.

Because the partnership relies on manual records, the processes therefore, do not compare well with councils that have implemented such tools.

The policies covering IT asset management are not comprehensive in scope and thus compare poorly with other organisations, especially considering that the topic is covered by good practice frameworks such as the IT Infrastructure Library (ITIL).

It is unfortunately common for server rooms to have a secondary use as storerooms for IT equipment, but this increases risks that servers may be interfered with or subject to risks such as fire that arise from the storage of additional materials not associated with server support.

03 Detailed Action Plan

We have identified areas where there is scope to improve the control environment. Our detailed findings are provided below. Definitions for the levels of assurance and recommendations used within our reports are included in Appendix A1.

1 Weaknesses in asset management and register maintenance

Findings and Risk

A comprehensive asset management process should be established to ensure all IT assets are effectively managed and tracked.

Each council maintains two separate registers; one for laptops and another for docking stations and monitors, in addition to a software asset register managed by Certero is maintained. Mobile phones are managed through Intune and Meraki, with the council in the process of transitioning these fully to Intune.

All these registers are stored on SharePoint with personnel from ICT having access to it.

As per the review of these asset registers, it was noted the following:

1. <u>Lack of centralised asset register</u>

There is no centralised asset register to track all devices and their assigned owners across the councils. Additionally, we were not provided with any registers that included the servers in the server room and other network devices such as switches and routers. They were also not included in any of the registers listed above. During the site visit to Melton, it was observed that the registers available on SharePoint were outdated, and that alternative registers were being used, separate from the SharePoint records.

2. <u>Manual register updates without automated reconciliation</u>

While Certero is capable of scanning laptops within the network, the asset registers are manually updated by authorised personnel. Therefore, there are no regular automated scans, to identify gaps or discrepancies in the asset registers in relation to the devices deployed to prompt the application of corrections.

3. <u>Inconsistent assignment and documentation of assets in registers</u>

Some assets were not assigned to anyone, assigned to generic IDs, or listed as "in stock" but not documented accurately. For example, in some cases, assets were both marked as owned by individuals and simultaneously listed as "in stock." This indicates that the registers are not being maintained accurately.

Recommendations

1. Establish a single approach to IT asset management based on common standard IT asset register before migrating to a centralised configuration management database (CMDB), ideally integrated with the service management software used by the service desk. This should track all assets, including laptops, docking stations, monitors, servers, mobile phones, network equipment and items in stock. This will provide a single source of truth for asset management, provide supporting information to the service desk when resolving incidents and support the identification of devices to be returned by leavers.
2. Leverage tools like Certero to automatically scan devices within the network, and the device register from Intune to identify potential discrepancies in the CMDB.
3. A comprehensive review of the asset registers should be conducted to identify and close gaps, ensuring all assets are accurately assigned and documented.
4. Perform periodic audits to reconcile assets with the CMDB, particularly for those assets in storage or for which automated scanning is not feasible.

Root Cause

Failure to establish common tools and processes for IT asset management at the formation of the partnership and subsequent reliance on inadequate tools and underutilisation of available technologies for IT asset management.

During the site visit of the three councils, it was noted that some labelled assets were not registered in the asset registers, misregistered, or unlabelled.

4. Absence of physical audits and inventory scans

No physical audits or inventory scans are conducted to reconcile the asset register records with the actual inventory, which increases the risk of discrepancies and outdated records.

Risk and Impact: Poor data quality, inaccurate asset records, and unclear asset responsibility, leading to misallocation, increased risk of loss or theft, operational inefficiencies, and financial or security vulnerabilities.

Management Comments / Agreed Actions

Comments

A single SharePoint list has been created including all devices including laptops, PCs, docking stations, monitors and mobile devices LICTP would like to share this evidence before accepting the final report. At this point in time migration of the Assets SharePoint list into Sunrise CMDB is not considered financially viable or operationally beneficial.

Actions

1. The server and network device data will be recorded into the Assets SharePoint list.
2. Certero is already used to scan the network on a regular basis. Reports will be generated quarterly to cross-check the records maintained in SharePoint will be undertaken.
3. In-Tune reports will be generated quarterly to cross-check asset records held in SharePoint.
4. A monthly stock check process has already been initiated and the stock recorded will be cross-checked against the LICTP SharePoint asset list referenced in (1) above.

Responsible Person	Alan Long ODM	**Action Due Date**	1. Complete 2. 31/07/25 3. 31/07/25 4. 28/02/25
		Priority Level	**High**

2 Physical security of IT assets in storage

Findings and Risk

Adequate physical security measures, such as locks, surveillance, and access controls should be in place, to prevent theft of IT assets in storage.
During site visits to the three councils, it was noted the following:

1. The server room at Melton councils was used to store unallocated IT equipment such as new/used equipment and equipment awaiting disposal. At Blaby, whilst IT assets are stored in a side room to the data centre entrance, the door between the two areas was not locked during our visit. This is not in line with good practice.
2. Access to the Blaby server room is controlled by a pin code, which is shared among ICT staff and building maintenance personnel. However, there is no formal process to change this password if employees or building staff leave. Additionally, there are no access logs maintained to track entry into the server room.
3. Server cabinets in Hinckley & Bosworth and Blaby were not locked and thus owing to the above issues are at risk of damage, theft and interference.
4. No cameras were installed outside the doors to the server/storage rooms, or outside the the rooms used by IT staff to configure devices.

Risk and Impact: Potential unauthorised access, theft, or damage to critical assets, which can lead to data breaches, operational disruptions, and financial and reputational damage to the Council.

Recommendation(s)

1. Assess the current access control measures for the Blaby server room and side room used to store IT assets and consider implementing more advanced options, such as biometric or card-based access, to improve security.
2. Install surveillance cameras outside of rooms used to store and/or configure IT assets.
3. Regular audits should be conducted to ensure server rooms comply with security standards, including monitoring access, and ensuring server cabinets are effectively secured.
4. Establish a secure storage area for the storage of IT assets at Melton Borough Council.

Root Causes

Reluctance to install security measures, such as surveillance cameras, and reliance on outdated tools and practices.

Management Comments / Agreed Actions

Comments

Blaby will be leaving the ICT partnership on 31st March 2025. Blaby management have requested LICTP make no changes or implement any new security on their premises before they leave the partnership and therefore our actions below are limited to those councils that remain in the partnership.

Actions

1. A regime of monthly checks on equipment stored within designated 'server' or 'comms' rooms will be undertaken to ensure they are clear of frangible materials, unused ICT equipment.
2. Work with MBC Estates management to identify or construct suitable ICT equipment storage area.
3. Work with estates management for each council, to implement CCTV monitoring of the doors to the server and IT asset storage rooms at each council.

Responsible Person	Alan Long ODM	**Action Due Date**	1. 28/02/25

			2. 01/09/25 3. 31/10/25
		Priority Level	**High**

3 Inadequate Software Licensing and Application Management

Findings and Risk

A formal process should be established for managing software licensing agreements and installations.

Software installations are tracked using Certero, which scans the software applications installed on all the laptops and classifies them as follows:

- SB (Standard Build) software: Part of the default laptop builds.
- Optional installs: Indicates whitelisted applications.
- Investigate: Signifies software that is yet to be classified as either standard or optional.

If users wish to install software, they must raise a ticket with the Service Desk, providing a business justification for the request. The request is then reviewed and approved based on the preapproved applications list and business needs.

Based on the review performed, the following issues were noted:

1. No centralised licensing management

While Certero is utilised for software asset management, it is not utilised for software license management. Consequently, there is no centralised register consolidating information on software license types (e.g., per user, per subscription), the number of permitted installations, and other licensing details. Whilst there are a variety of suppliers of software we assessed the license management approach for Cisco and Microsoft 365 products, and noted for these that this information is tracked separately through individual software portals.

2. Incomplete preapproved applications list:

The list of preapproved applications has not been finalised. For instance, in ticket INC024868, a request to install FileZilla was placed that we were informed was a preapproved application,.however, in the Certero-extracted list, FileZilla was classified under "Investigate," indicating its status is still under investigation.

3. Mobile applications not integrated:

The Certero-extracted list does not cover mobile apps. For example, in ticket INC027336, a user requested to install the Zoom app on a mobile phone, and the request was approved. However, there was no record of this application in the Certero-extracted list.

Risk and Impact: Overspending on unnecessary licenses or non-compliance, leading to legal and financial consequences. Additionally, an incomplete preapproved applications list may allow unmanaged software, increasing the risk of security breaches and malware threats to council data and networks.

Recommendations

1. Utilise software tools in place, such as Certero, to implement a centralised system to consolidate all software licensing details, including license types, permitted installations, and expiration dates, to ensure compliance and optimise license usage.
2. Perform periodic audits of software licenses to identify unused or underutilised licenses and reallocate them as necessary to improve cost efficiency.
3. Expand the preapproved applications list to include mobile applications, ensuring consistent oversight and approval processes for all devices and platforms.
4. Review, finalise, and regularly update the preapproved applications list to ensure it is comprehensive and aligns with the organisation’s operational needs and security policies.

Root Cause

Failure to develop policies mandating a comprehensive approach to software licensing and application management.

Management Comments

Comments

Recommendation 2. LICTP do undertake quarterly user account reviews and rationalise licences as part of this process.

Agreed Actions

1. The pre-approved software to be finalised and published.
2. Include Mobile apps from In-Tune into Approved software list.
3. Bring all device software, (except mobile devices) into Certero and ensure licence process is created and adopted for the allocation, review, and management of licences.

Responsible Person	1. John Palmer SHICTSS 2. Alan Long ODM 3. Alan Long ODM	**Action Due Date**	1. Dependent on completion of 2 and 3 2. 01/09/25 3. 01/09/25
		Priority Level	**Medium**

<table>
<tr><th colspan="4">4 Deficiencies in Access Control</th></tr>
<tr><th colspan="2">Finding and Risk</th><th colspan="2">Recommendation(s)</th></tr>
<tr><td colspan="2" rowspan="3">Access permissions should be restricted based on job responsibilities and on a need-to-know basis.
The asset registers are stored on SharePoint, where 29 members from the ICT team have edit access. However, only a selected number of these members actively update the folders and registers as part of their job responsibilities. This indicates that some personnel may have unnecessary permissions, which could be restricted to read-only in line with their job requirements.
<strong>Risk and Impact:</strong> Unauthorised modifications, accidental deletions, or malicious alterations to asset registers, potentially compromising data integrity and security. For example, an unscrupulous individual could apply a fictitious update to disguise a theft.</td><td colspan="2">Access permissions should be reviewed to ensure edit rights to the IT asset registers are granted only to personnel responsible for their maintenance, while others are provided view-only access based on their roles. Regular access reviews should also be conducted to ensure permissions remain aligned with current job responsibilities.</td></tr>
<tr><th colspan="2">Root Cause</th></tr>
<tr><td colspan="2">Failure to identify inappropriate updates to the IT asset data as a risk.</td></tr>
<tr><th colspan="4">Management Comments / Agreed Actions</th></tr>
<tr><td colspan="4"><strong>Comments:</strong>
The consolidation of the asset register we have in SharePoint addresses this recommendation.</td></tr>
<tr><td rowspan="2"><strong>Responsible Person</strong></td><td rowspan="2">John Palmer SHICTSS</td><td><strong>Action Due Date</strong></td><td>Complete</td></tr>
<tr><td><strong>Priority Level</strong></td><td><strong>Medium</strong></td></tr>
</table>

5 Lack of comprehensive IT asset management policies and procedures

Findings and Risk

Clearly defined and approved IT asset management policies should be in place and reviewed periodically to ensure their validity and consistency.

As per the review of the IT asset management policies, it was noted that the policy documents did not include a version history or records of the approval and review processes, such as the following:

- Corporate Policy for Software Security and Licensing
- Corporate Policy for the Procurement, Replacement, and Configuration of ICT Desktop Equipment
- Corporate Policy for the Disposal of ICT Equipment & Software

Additionally, the following policies were still in draft form and had not been finalised:

- Acceptable Use Policy
- Corporate Mobile Device Policy

Moreover, there were no overarching policies and procedures outlining the complete asset management process and lifecycle. This includes the assignment of assets, the process of updating and maintaining asset registers, leveraging tools for automated scans and tracking of assets and licenses, license compliance, conducting regular reconciliations, ensuring the accuracy of asset registers, and managing the processes for users to request and install software or pre-approved applications.

Additionally, there was no policy for the security of hardware assets and physical access controls across the three councils.

Risk and Impact: Inconsistent practices, lack of clear guidelines for employees, and potential non-compliance with regulatory standards. This can lead to operational inefficiencies, security vulnerabilities, and mismanagement of assets.

Recommendation

1. Create and formalise overarching IT asset management policies that outline the complete process for maintaining and ensuring the accuracy of asset registers, security protocols, and access controls.
2. Implement a regular review schedule to update policies and maintain version history, ensuring alignment with current practices and standards.

Root Causes

Relying on outdated policies while new policies are still in the drafting phase.

Management Comments / Agreed Actions

Comments

LICTP are drafting a new suite of policies, all new polices contain Document controls. See AUP and Corporate Device Policy V1_00. The policies cited are the extant policies and will be retired shortly.

A device lifecycle policy has been drafted and is going through approval process currently.

Agreed Actions

1. Create an assets procedure and guidance to support the device lifecycle policy.
2. Review policies annually or on request of revision once new draft policies approved and extant.

Responsible Person	1. Alan Long ODM 2. John Palmer SHICTSS	**Action Due Date**	1. 30/06/25 2. 30/06/26
		Priority Level	**Medium**

6 Inadequate Acceptable Use Policy (AUP) coverage and lack of asset management training

Findings and Risk

Employees are required to sign the Acceptable Use Policy (AUP) upon employment, which includes statements about corporate network access, email security, and internet usage.

Whilst a revised AUP is currently being drafted, the existing AUP does not provide guidelines for the use of the Councils' assets, such as laptops and mobile phones, nor does it fully address the asset return process. Additionally, out of six sampled employees, only one signed AUP was provided. It was explained that this was because the employees selected had started before the implementation of the current AUP.

Furthermore, no training is conducted to ensure employees are aware of and understand how to appropriately handle the Councils' assets.

Risk and Impact: Employees may misuse council assets, risking damage, loss, unauthorised use, and non-compliance with organisational standards.

Recommendation

1. The draft AUP should be finalised and approved promptly. It should include clear guidelines on the use, care, and return of the Councils' assets, such as laptops, mobile phones, and other equipment. Once completed, all employees, including existing and new staff, should be required to review and sign the updated AUP to ensure consistent understanding and compliance.

2. Develop and conduct mandatory training for employees to ensure they understand how to appropriately handle council-owned assets, covering topics like maintenance, security, and the return process.

Root Causes

Lack of periodic policy review, as the AUP was last updated in June 2019, coupled with the absence of policies mandating user training on asset management.

Management Comments / Agreed Actions

Comments
The draft AUP includes policy statements on device care, use and return. Guidelines are separate from policy. Guidance documents will be created to supplement the AUP.
LICTP is not equipped, nor resourced to provide training, it accepts there is need for awareness materials to be created and shared.

Agreed Actions

1. Approve and publish the draft AUP.
2. Require all employees sign the finalised AUP once published.
3. Create learning materials for the use, care and return of equipment and publicise to staff.

Responsible Person	1. John Palmer SHICTSS 2. Alan Long ODM 3. Baljit Ghataorre/Alan Long ODM	**Action Due Date**	1. 31/07/25 2. 01/11/25 3. 01/11/25
		Priority Level	**Medium**

7 Inefficient asset allocation and resource utilisation cross departments

Finding and Risk

Assets should be effectively utilised and managed in a cost-efficient manner.

Upon the departure of an employee, their line manager manages the exit procedure, and a ticket is raised with the IT service desk listing the assets assigned to the employee for return. However, these tickets do not include specific asset names, which may make it difficult or inaccurate to track and verify the return of assets. Additionally, we were informed that some departments retain devices returned by leavers in the belief that the devices belong to their cost centre and as a contingency against the possibility that future budgetary constraints may prevent future procurement.

Risk and Impact: Inefficient resource utilisation can lead to some departments accumulating surplus devices while others face shortages, causing operational delays, underutilisation or overprovisioning of assets, and potential financial inefficiencies.

Recommendation

1. IT assets should be owned by the ICT department on behalf of each council to facilitate the efficient transfer and full utilisation of IT assets based on each council's needs.
2. Department managers should be made aware of their responsibility to return redundant devices to IT.
3. Department managers should receive periodic reports of the devices assigned to them with the staff members who are the users.
4. A process to handle return exceptions should be defined, such that if devices are not returned within 7 days of the last working day of the staff member, that the matter is escalated to the senior leader of the directorate.

Root Cause

End user assets purchased are charged to business unit cost centres causing managers to assume that these are owned by their own department.

Management Comments / Agreed Actions

Comments
LICTP supports the recommendation that ICT assets should be owned by the ICT department. The practice of providing budget codes is cumbersome, time consuming and creates a culture of perceived 'ownership' of corporate assets by service areas and managers.

Agreed Actions
1. Create and present proposal for an organisational change on asset budget management to ICT Steering Group.
2. Create guidelines and supporting communications materials on responsibility of managers to return leavers and redundant equipment.

3. Create quarterly asset allocation reports, distribute to managers and reconcile any alterations suggested by service managers and verify against ITAM/CMDB.
4. create and present to ICT Steering Group returns exception procedure for approval.

Responsible Person	1. John Palmer SHICTSS 2. Alan Long ODM 3. Alan Long ODM 4. John Palmer SHICTSS	**Action Due Date**	1. 12/08/25 2. 31/08/25 3. 30/09/25 4. 12/10/25
		Priority Level	**Low**

A1 Audit Information

Agreed Audit Objective and Scope

The objectives of our audit were to assess whether Hinckley and Bosworth BC has in place adequate and appropriate policies, procedures and controls in relation to IT asset management with a view to providing an opinion on the extent to which risks in this area are managed. The audit considered the following risks relating to the area under review:

- **Policies and Procedures**
  - Staff working inconsistently or to incorrect practices.
- **Maintenance of the IT Asset Register**
  - Records of hardware/software deployed are not maintained.
  - The organisation is unable to detect new software or hardware installed, and to verify that this is authorised to update the IT asset register.
- **Assignment of Assets**
  - No standard way of assigning software/hardware assets, they are assigned incorrectly to the wrong staff and the IT asset and licensing records are not updated.
  - No responsibility or accountability for IT assets.
  - Software is installed without a valid license.
  - Unauthorised staff install software, such as following its download.
  - Assets are not collected from leavers and licenses recovered resulting in loss/theft of assets.
- **Security of Hardware**
  - Theft of valuable equipment due to lack of physical security controls.
  - IT assets are not identifiable as organisational property.
- **Asset Loss Management**
  - Management unaware of theft of valuable equipment or information.
  - Inability to disable / wipe assets remotely if lost / stolen.

  - Unassigned licenses and/or unused software are maintained that lead to excess costs.

- **Software license compliance** - Software installed exceeds available licenses, which without corrective action, leads to penalties from the license owner.
- **Disposal Procedures** - Assets to be disposed are lost, or there is no evidence that they have been securely wiped.

Scope Limitations

In giving this assessment, it should be noted that assurance cannot be absolute. The most an Internal Audit service can provide is reasonable assurance that there are no major weaknesses in the framework of internal control. Any testing performed was conducted on a sample basis. Our work does not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

In assessing the management of software licenses we considered the management of these for Cisco products and Microsoft 365, but owing to constraints in the process, policies and management tools we did not assess other software in use at the partnership.

Definitions of Assurance Levels and Recommendation Priority Levels

Definitions of Assurance Levels	
Substantial Assurance	The framework of governance, risk management and control is adequate and effective.
Moderate Assurance	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited Assurance	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
Unsatisfactory Assurance	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Definitions of Recommendations		
High (Priority 1)	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Medium (Priority 2)	Recommendations represent significant control weaknesses which expose the organisation to a moderate degree of unnecessary risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low (Priority 3)	Recommendations show areas where we have highlighted opportunities to implement a good or better practice, to improve efficiency or further reduce exposure to risk.	Remedial action should be prioritised and undertaken within an agreed timescale.

Statement of Responsibility

We take responsibility to Hinckley and Bosworth Borough Council for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent.   To the fullest extent permitted by law Forvis Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Registered office: 30 Old Bailey, London, EC4M 7AU, United Kingdom. Registered in England and Wales No 0C308299.

Contacts

Peter Cudlip
Partner, Forvis Mazars
peter.cudlip@mazars.co.uk

Neethu Ram
Associate Director, Forvis Mazars
neethu.ram@mazars.co.uk

John Roth
IT Auditor Manager, Forvis Mazars
John.roth@mazars.co.uk

Amgad Elfiky
IT Auditor, Forvis Mazars
amgad.elfiky@mazars.co.uk

Forvis Mazars is the brand name for the Forvis Mazars Global network (Forvis Mazars Global Limited) and its two independent members: Forvis Mazars, LLP in the United States and Forvis Mazars Group SC, an internationally integrated partnership operating in over 100 countries and territories. Forvis Mazars Global Limited is a UK private company limited by guarantee and does not provide any services to clients. Forvis Mazars LLP is the UK firm of Forvis Mazars Global.

Visit forvismazars.com/global to learn more about the global network.