East Northamptonshire Council

# Governance and Audit Committee – 3 December 2014

## ICT Physical Security

**Purpose of report:**

To provide members with an update following the 'limited assurance' findings from the Welland Audit – Physical Security (March 2014).

**Attachment(s)**

Appendix A: The Welland Partnership Internal Audit Report

### 1.0 Background

1.1 As part of the Internal Audit programme a review was undertaken to look at the physical security of the Council's IT facilities.

1.2 An overall assurance opinion of '*Limited Assurance'* was received due to concerns over IT equipment in server rooms being damaged due to fire or through insufficient server room security.

1.3 This paper provides a response to these audit concerns, and proposes that these risks are accepted for the foreseeable future while a longer term plan is put in place to migrate all computer hardware to an external location.

### 2.0 Audit Review and Findings

2.1 The internal audit process looked at the current levels of security around the essential computer equipment that supports the Council's business.

2.2 Of the six risk areas, the audit found evidence for 'Sufficient Assurance' in four areas, concerning removable media, compliance with the Data Protection Act and the physical security of equipment located around the business.

2.3 In two Risk area, relating to IT equipment held in service rooms, the audit noted:-

> Neither of the two server rooms are protected against fire. Failure to install any fire prevention or detection equipment in the server rooms puts the Council at significant risk of not being able to continue "business as usual" in the event of a fire. A budget to rectify this issue has been provisionally assigned but has yet to be approved. Following issue of the draft executive summary report the Head of IT Services stated that this issue is a high priority but ultimately the decision on whether to accept the risk or approve capital spend will be made by Members.

### 3.0 Response to the Audit Findings

3.1 Following this Audit Action, work has progressed with the Council's Amenities team, to establish the level of mitigation activity required and potential cost. A sum to cover this was also included in the provisional 2014-15 capital plan. A quote from Chubb Fire limited has been obtained, proposing the installation of appropriate fire suppressant equipment along with making the rooms 'airtight' to enable the fire suppressant technology to work. This would cost in excess of £32,000 (+VAT).

3.2 While the loss of one or both of the Council's computer rooms would be a major concern for the Council, the likelihood of this occurring is very low. In addition, capital has recently been secured at both councils to replicate and store data off-site, i.e. a copy of key East Northants data is stored at Wellingborough and vice versa for Wellingborough. In the event of a fire, replacement of the computer hardware would take time to procure and setup, but the data is irreplaceable and this is the primary resource we need to protect.

3.3 In the longer term, both computer rooms are not fit for purpose, and Wellingborough's stated intent is to vacate their Tithe Barn Building (where the BCW computer room sits). This issue is now being addressed through an overall strategic approach to the provision of our technology infrastructure.

3.4 This approach to this risk was reviewed by the Corporate Management Team in August 2014, and accepted as a pragmatic solution. The longer term solution should also provide additional benefits to the Council in pooling our technology resources with other organisations to obtain greater resilience in the future. Early conversations are taking place with a number of providers, and a recommendation for Council is expected early in 2015.

3.2 It is therefore recommended that the Audit risk identified by the Welland Audit is accepted as a low level of risk, and that the cost of fireproofing the existing facilities is not progressed.

**4.0 Equality and Diversity Implications**

4.1 There are no Equality and Diversity implications arising from this report.

**5.0 Legal Implications**

5.1 There are no legal implications arising from this report.

**6.0 Risk Management**

6.1 Identified risks will continue to be managed by close observation of the computer room environments, and improved house-keeping put in place to ensure that combustible materials are not stored in the area.

**7.0 Financial Implications**

7.1 The planned capital expenditure of £32K (+ VAT) will not be progressed.

**8.0 Corporate Outcomes**

8.1 This paper relates to the following Corporate Outcomes:

- Effective Management
- High Quality Service Delivery
- Good Value for Money

**9.0 Recommendations**

9.1 The Committee is recommended to

1) Accept that the level of risk identified by Welland Audit is sufficiently low to be acceptable in the short term, and support the plan to transfer the whole server room environment to an external provider.

(*Reason: To satisfy auditor recommendations*)

| | | | | | |
|---|---|---|---|---|---|
| **Legal** | Power: Local Government Act 1972<br>Other considerations: | | | | |
| **Background Papers:** | | | | | |
| **Person Originating Report:** | Phil Grimley, Head of ICT Service,<br>01832 742076, pgrimley@east-northamptonshire.gov.uk | | | | |
| **Date:** 13th November 2014 | | | | | |
| **CFO** | | **MO** | | **CX** | |

(Committee Report Normal Rev. 22)

# WELLAND INTERNAL AUDIT CONSORTIUM
# East Northamptonshire Council

## INTERNAL AUDIT REPORT

# Physical Security
# 2013-14

| | | | | |
|---|---|---|---|---|
| ***Issue Date:*** | 11/03/2014 | ***Issued to:*** | Phil Grimley | Head of IT Services |
| ***Author:*** | Elaine Laycock<br>Nicola Scott | | Ian Peters | ICT Technical Manager |
| | | | Glenn Hammons | S151 Officer |
| | | | Kelly Watson | Finance Manager |

# WELLAND INTERNAL AUDIT CONSORTIUM
# East Northamptonshire Council

## Physical Security 2013-14

## EXECUTIVE SUMMARY

### 1. INTERNAL AUDIT OPINION

The key risk associated with the IT Physical Security is that that damage or destruction could occur to the Council's IT equipment leading to disruption to service provision or loss of data. Testing found that neither of the two server rooms have fire protection installed. Without the installation of this control the Council is at significant risk on being unable to continue "business as usual" should a fire occur in either of the server rooms. The ICT Technical Manager asserted that a budget has been "provisionally allocated but is subject to final member approval". Although the former Head of IT Services and the IT Technical Manager asserted that only authorised employees could enter the server rooms, the Officer within Resources and Organisational Development responsible for managing and maintaining the corporate access card system stated that it was not possible to produce a report of all users with access to the server rooms. As a result of this no assurance can be given that appropriate access levels have been granted. It is, therefore, the Auditor's Opinion that the design and operation of controls provides **Limited Assurance**. The audit was carried out in line with the scope set out in the approved Terms of Reference.

The Opinion is based upon testing of the design of controls to manage the six risks about which the Client sought assurance and testing to confirm the extent of compliance with those controls as summarised below.

| Internal Audit Assurance Opinion | Direction of Travel | | | | |
|---|---|---|---|---|---|
| **Limited Assurance** | N/A | | | | |
| **Risk** | **Design** | **Comply** | **Recommendations** | | |
| | | | **H** | **M** | **L** |
| Risk 1. IT equipment in server rooms can be damaged and/or destroyed either accidentally or deliberately leading to a disruption of Council business – server room security | Limited assurance | Sufficient assurance | 0 | 0 | 0 |
| Risk 2: IT equipment in server rooms can be damaged and/or destroyed either accidentally or deliberately leading to a disruption of Council business – fire protection | Limited assurance | Sufficient assurance | 1 | 0 | 0 |
| Risk 3: IT equipment in offices and outlying sites server rooms can be damaged and/or destroyed either accidentally or deliberately and/or stolen leading to a disruption of Council business – physical assets | Sufficient assurance | Sufficient assurance | 0 | 0 | 0 |
| Risk 4: Council owned removable media is lost or stolen with no audit trail as to whom the item has been allocated | Sufficient assurance | Substantial assurance | 0 | 0 | 0 |
| Risk 5: Council employees are unaware of their responsibilities regarding physical IT assets | Substantial assurance | Substantial assurance | 0 | 0 | 0 |
| Risk 6: Confidential information is available to the general public leading to breaches of the Data Protection Act | Substantial assurance | Substantial assurance | 0 | 0 | 0 |
| **Total Number of Recommendations** | | | **1** | **0** | **0** |

# WELLAND INTERNAL AUDIT CONSORTIUM
# East Northamptonshire Council

## 2. ISSUES REQUIRING MANAGEMENT ATTENTION

- Neither of the two server rooms are protected against fire. Failure to install any fire prevention or detection equipment in the server rooms puts the Council at significant risk of not being able to continue "business as usual" in the event of a fire. A budget to rectify this issue has been provisionally assigned but has yet to be approved. Following issue of the draft executive summary report the Head of IT Services stated that this issue is a high priority but ultimately the decision on whether to accept the risk or approve capital spend will be made by Members.

## 3. AREAS WHERE CONTROLS WORKED AS DESIGNED

- The Council has good arrangements in place to ensure that employees are aware of their responsibilities regarding the security of data and physical assets.
- The IT department have a good procedure for the management and maintenance of an asset register.

## 4. LIMITATIONS TO THE SCOPE OF THE AUDIT

The auditor did not;

- Review any other areas than the risks identified above.

Our work does not provide absolute assurance that material error; loss or fraud does not exist.

# WELLAND INTERNAL AUDIT CONSORTIUM
# East Northamptonshire Council

## ACTION PLAN

| **Risk 1:** IT equipment in server rooms can be damaged and/or destroyed either accidentally or deliberately leading to a disruption of Council business – server room security | | | | | | | |
|---|---|---|---|---|---|---|---|
| Rec No. | ISSUE | RECOMMENDATION | Management Comments | Category | Officer Responsible | Due date | WP Ref |
| 1 | Neither of the two server rooms are protected against fire. Failure to install any fire prevention or detection equipment in the server rooms puts the Council at significant risk of not being able to continue "business as usual" in the event of a fire. | Head of ICT Services implements fire suppression/detection equipment in both server rooms. | This issue is something which is high on my priority list. However, it is the Members who ultimately make the investment decision, and if they decide to accept the level of risk, I shall be seeking a written underwriting of the risk. | High | Head of IT Services | 31/08/2014 | 02.01 |

# WELLAND INTERNAL AUDIT CONSORTIUM
# East Northamptonshire Council

## GLOSSARY

**The Auditor's Opinion**

The Auditor's Opinion for the assignment is based on the fieldwork carried out to evaluate the design of the controls upon which management relay and to establish the extent to which controls are being complied with. The table below explains what the opinions mean.

| Level | Design of Control Framework | Compliance with Controls |
|---|---|---|
| **SUBSTANTIAL** | There is a robust framework of controls making it likely that service objectives will be delivered. | Controls are applied continuously and consistently with only infrequent minor lapses. |
| **SUFFICIENT** | The control framework includes key controls that promote the delivery of service objectives. | Controls are applied but there are lapses and/or inconsistencies. |
| **LIMITED** | There is a risk that objectives will not be achieved due to the absence of key internal controls. | There have been significant and extensive breakdowns in the application of key controls. |
| **NO** | There is an absence of basic controls which results in inability to deliver service objectives. | The fundamental controls are not being operated or complied with. |

**Category of Recommendation**

The Auditor categorises recommendations to give management an indication of their importance and how urgent it is that they be implemented. By implementing recommendations made managers can mitigate risks to the achievement of service objectives for the area(s) covered by the assignment.

| Category | Impact & Timescale |
|---|---|
| **HIGH** | Management action is imperative to ensure that the objectives for the area under review are met.<br><br>Recommendation to be implemented immediately with explanation to the Audit Committee should timeframe extend beyond three months. |
| **MEDIUM** | Management action is required to avoid significant risks to the achievement of objectives<br><br>Recommendation should be implemented as soon as possible with explanation to the Audit Committee should timeframe extend beyond six months |
| **LOW** | Management action will enhance controls or improve operational efficiency.<br><br>Recommendation should be implemented within six months but the Audit Committee will be advised where the client specifies that a longer delivery time is necessary and / or justified. |

**Limitations to the scope of the audit**

The Auditor's work does not provide any guarantee against material errors, loss or fraud. It does not provide absolute assurance that material error, loss or fraud does not exist.

# WELLAND INTERNAL AUDIT CONSORTIUM
# East Northamptonshire Council

## AUDIT TERMS OF REFERENCE

| | | | |
|---|---|---|---|
| **Entity** | **IT Physical Security 2013-14** | | |
| **Entity code** | **E/PHSE2014** | | |
| Auditor(s) | TBC | Anticipated testing date | TBD |
| Supervisor | Nicola Scott | Date Last Audited | N/A |
| TOR issued to / officers to contact: | Gareth Jones Head of ICT | | |
| | | Date of TOR | 31/05/2013 |
| | | Number of planned days | 12 |

**CONTEXT**

The IT Strategic Audit Plan identifies the key IT risks faced by the Council and sets out a plan for IT audit work in support of the wider internal audit plan over the 3 year period from April 2013 to March 2016.

IT is central to and essential for the business of the Council and therefore it is important that all physical IT assets are protected to ensure the systems of the Council run smoothly and provide a service to both internal and external users.

**AUDIT APPROACH**

**Objective of the Audit**
The purpose of the audit is to provide assurance that the Council has put in place controls to ensure that the physical IT assets of the Council are protected from accidental or malicious loss or damage.

**Scope of the Audit**
The audit will include an examination of the key controls to give assurance that:

- All server rooms are secure;
- The server rooms have adequate fire and environmental protection;
- IT physical assets in council offices and outlying sites are secure ;
- There is a central record held of each piece of Council owned removable media, which is complete and up to date;
- Users understand their responsibilities regarding physical IT assets;
- Physical output is protected.

| | |
|---|---|
| I have read and approved the above Terms of Reference | |
| TOR agreed by: | **Gareth Jones** |