# Brentwood Borough Council

## INTERNAL AUDIT REPORT

## Data Security

## Audit 12.2015

| LEVEL OF ASSURANCE | |
|---|---|
| Design | Operational Effectiveness |
| Limited | Limited |

BDO

# CONTENTS



| REPORT STATUS | |
|---|---|
| Auditors: | Titi Junaid |
| Dates work performed: | February – March 2015 |
| Closing Meeting | 13 March 2015, Phil Ruck and Tim Huggins |
| Draft report issued: | 13 April 2015 |
| **Final report issued:** | **12 June 2015** |

| DISTRIBUTION LIST | |
|---|---|
| Phil Ruck | Contracts and Corporate Projects Manager |
| Tim Huggins | ICT Manager |

# EXECUTIVE SUMMARY

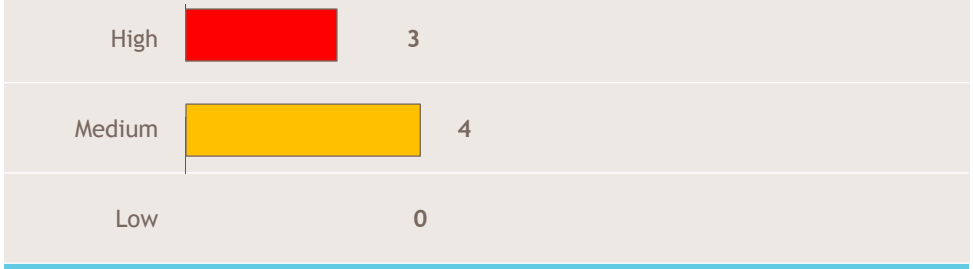
## CLIENT STRATEGIC RISKS

| | | |
|---|---|---|
| **Risk** | 5 & 9 | Information Management<br>• Lack of resources for IT integration.<br><br>Lack of strategic direction<br>• Poor performance management.<br>• Poor delivery of priorities.<br>• Failure to communicate effectively. |

## LEVEL OF ASSURANCE (SEE APPENDIX II FOR DEFINITIONS)

| | | |
|---|---|---|
| **Design** | Limited | System of internal controls is weakened with system objectives at risk of not being achieved. |
| **Effectiveness** | Limited | Non-compliance with key procedures and controls places the system objectives at risk. |

## SUMMARY OF RECOMMENDATIONS (SEE APPENDIX II)




**Total number of recommendations: 7**

## OVERVIEW

Information resources are vital for the delivery of Brentwood Borough Council's services. The availability, integrity and security of its information is essential for maintenance of services and compliance with legal and regulatory requirements. Whilst information security is the responsibility of every member of staff, responsibility for all aspects of information assets and resources lies with the Council's senior management.

Our review of the adequacy and effectiveness of data security controls showed the following areas of good practice:

- Responsibilities for information security and data protection has been appropriately assigned. The information security governance and management arrangements are adequate
- Citrix technology with 2 factor authentication is deployed for remote access to the Council's network
- Data held on mobile devices is automatically encrypted with passcode protection against unauthorised access
- Physical access to council offices is restricted and controlled electronically. Access to the server room is controlled and restricted to appropriate staff
- Technical security controls such as patch management, vulnerability scanning, antivirus/antimalware, web filtering and email scanning are in place.

We found some areas for development or improvement:

- Information security and related policy documents are out of date (high priority recommendation).
- Standard IT access request forms for starters are not in use. Procedures for granting, suspending and amending user accounts for starters, leavers and role changes are not documented. Both of these points put the Council at risk to unauthorised access to its network (high priority recommendation).
- The Council does not have a regular, on-going information security awareness and staff training programme (high priority recommendation).
- The Council does not adopt best practice password configuration and controls (medium priority recommendation).
- The remote access policy is not documented. No manager authorisation is required to set up remote access accounts (medium priority recommendation)
- The incident management policy document is out of date (medium priority recommendation).
- The Council does not obtain assurance from 3rd party services providers (with access to its information assets) regarding their internal controls (medium priority recommendation).

# DETAILED FINDINGS & RECOMMENDATIONS

| **Risk:** Failure to comply with legal and regulatory requirements due to poor information security policies and procedures | | | |
|---|---|---|---|
| **Ref.** | **Finding** | **Sig.** | **Recommendation** |
| 1 | Information Security Policies and Procedures<br><br>The Council is in collaboration with neighbouring councils which it shares information with (essexonline) to develop generic information security and related policies. These policies are used as templates to be modified and adopted as appropriate by individual organisations. The following policies (dated April 2014) were provided for review:<br>• Corporate information security<br>• Conditions of acceptable use – Personal Commitment Statement<br>• Information security policies<br><br>We noted however that these are generic "essexonline" policy documents which were prepared in October 2012 and had not been tailored to Brentwood Council.<br><br>We also found that the following information security related policy documents which were provided for review were out of date. All were dated and issued in February 2009:<br><br>• Acceptable use policy<br>• Access control policy<br>• Corporate information security policy<br>• Email policy<br>• ICT infrastructure policy<br>• Physical security policy<br>• Personal commitment statement<br><br>The risk of non-compliance is higher when policies are out of date. | H | The Council should review and revise the following information security and related policies to ensure that they are fit for purpose.<br><br>• Corporate information security<br>• Conditions of acceptable use – Personal Commitment Statement<br>• Information security policies<br>• Acceptable use policy<br>• Access control policy<br>• Corporate information security policy<br>• Email policy<br>• ICT infrastructure policy<br>• Physical security policy<br>• Personal commitment statement |
| **MANAGEMENT RESPONSE** | | | **RESPONSIBILITY AND IMPLEMENTATION DATE** |
| Agreed. Updated versions are being reviewed currently along with a plan to update staff electronically | | | *Responsible Officer: Tim Huggins*<br>*Implementation Date: 31 December 2015* |

# DETAILED FINDINGS & RECOMMENDATIONS

| **Risk:** Unauthorised access to sensitive information and data security breaches resulting in damage to the Council's reputation | | | |
|---|---|---|---|
| **Ref.** | **Finding** | **Sig.** | **Recommendation** |
| 2 | User Account Management<br><br>Procedures for granting access to the Council's network require that Managers make requests through the IT service desk. Starters are also required to complete and sign "Personal Commitment forms" as evidence that they have read and understood the Council's acceptable use policy.<br><br>A test of compliance with IT access procedures was carried out by selecting a random sample of 10 starters in the past 12 months and reviewing documents obtained and retained by the service desk. The test showed the following results:<br><br>• Personal commitment forms were available in 8 out of the 10 samples tested<br>• 2 of the sample forms examined did not have the signature of the Director authorising access.<br><br>We also noted that standard access request forms are not in use hence access requests made by Managers do not always include the department or role of the new starter.<br><br>We were informed that leaver accounts are suspended when notification is received from line managers. HR does not routinely inform the IT department of leavers.<br><br>Local IT procedures for granting, suspending or amending the access rights of starters, leavers and staff changing roles are yet to be documented.<br><br>The risk of unauthorised access to the Council's network is high in light of these weaknesses. | H | The IT procedures for granting, suspending and changing user access rights to the Council's network should be documented and made available to all relevant staff .<br><br>Standard IT access request forms should be prepared and made available to all Managers responsible for requesting and authorising users' IT access. The form on completion should indicate the department, role and level of access for which access has been authorised.<br><br>The IT service desk should be reminded of the need for ensuring that personal commitment forms are appropriately authorised prior to granting access to new users. All personal commitment forms should be retained as evidence of the action taken.<br><br>The HR department should be required to notify the IT department of leavers as soon as leaver notification is received from managers. A list of leavers should be sent to the IT department every month for review. |
| **MANAGEMENT RESPONSE** | | | **RESPONSIBILITY AND IMPLEMENTATION DATE** |
| A procedure will be created and published.<br><br>Form will be designed and published.<br><br>IT Service Desk will be reminded of the importance of the personal commitment statement<br><br>A starters and leavers process and notification system is being implemented currently. | | | *Responsible Officer: ICT/Business Development - TBC*<br><br>*Implementation Date: 31 December 2015* |

# DETAILED FINDINGS & RECOMMENDATIONS

| **Risk:** Poor information security education, training and awareness resulting in security breaches by authorised users | | | |
|---|---|---|---|
| **Ref.** | **Finding** | **Sig.** | **Recommendation** |
| 3 | Information Security Training and Awareness<br><br>We noted that the Council does not have a regular, on-going information security education and awareness programme. Information Security and Data Protection training is not given to new staff at induction; the Information Governance e-learning tool has been discontinued.<br><br>The risk of breaches of information security and the Data Protection Act are higher where staff with authorised access to information assets and sensitive data do not receive adequate, regular and on-going training and information.<br><br>We are aware that data protection and information security training at staff induction is under review. | H | The Council should establish a training programme for Information Security, Information Governance and Data Protection for all staff. This should include training for both new and current staff.<br><br>Arrangements should be put in place for training during staff induction. On going refresher and regular awareness training should also be established.<br><br>The Information Governance staff e-learning tool should be re-established. |
| **MANAGEMENT RESPONSE** | | | **RESPONSIBILITY AND IMPLEMENTATION DATE** |
| The risk is understood, and mitigation should be shared all managers.<br><br>The Council is implementing an e-learning system for online courses which information security training and awareness training will be part of.<br><br>The Council's induction process is currently being reviewed. | | | *Responsible Officer: HR - TBC*<br><br>*Implementation Date: 31 December 2015* |

# DETAILED FINDINGS & RECOMMENDATIONS

| **Risk:** Unauthorised access to sensitive information and data security breaches resulting in damage to the Council's reputation | | | |
|---|---|---|---|
| **Ref.** | **Finding** | **Sig.** | **Recommendation** |
| 4 | Password Configuration and Controls<br><br>The domain password configuration (on Active Directory) as well as password general controls were reviewed for evidence of their adequacy and effectiveness in securing access to the Council's information assets.<br><br>Our review highlighted the following weaknesses:<br><br>• Password complexity requirement is enabled but the minimum length of password requited is 7 characters. Best practice recommendation is 8 characters.<br>• The system enforces password changes every 90 days. Best practice recommendation is every 30 days.<br>• Session timeout is after 1440 minutes. Best practice recommendation is after 10 minutes.<br><br>Best practice recommendations ensure that the risk of unauthorised access is further mitigated. | M | The Council should consider adopting best practice recommendations for password configuration in the following areas in order to further mitigate the risk of unauthorised access:<br><br>• Password complexity: passwords should be a minimum of 8 characters.<br>• Password expiry date: the system should force passwords to expire every 30 days.<br>• Session time out: sessions should time out after 10 minutes. |
| **MANAGEMENT RESPONSE** | | | **RESPONSIBILITY AND IMPLEMENTATION DATE** |
| Password length to be changed from 7 to 8<br><br>Session timeout to be changed to 10 minutes<br><br>Password expiry is debatable.<br><br>By forcing people to change passwords more regularly will cause staff to choose easier passwords to remember or worse right down. At present I do not agree with this action. | | | *Responsible Officer: Tim Huggins*<br><br>*Implementation Date: 31 July 2015* |

# DETAILED FINDINGS & RECOMMENDATIONS

| **Risk:** Loss of information assets including exposure of sensitive corporate and personal data to the public domain | | | |
|---|---|---|---|
| **Ref.** | **Finding** | **Sig.** | **Recommendation** |
| 5 | Remote Access Policy and Authorisation<br><br>The Council encourages mobile and flexible working. To this effect, any user who already has a domain account can make a request for remote access to the network (and their desktop). Requests are made through the IT service desk. No additional authorisation is required.<br><br>We also noted that the Council's policy for remote working is not documented.<br><br>Although the technical solution deployed by the Council for enabling remote access to its network is adequate, there is a need to identify and mitigate the inherent risks to information security from authorised users. Remote network access should be subject to line manager approval. | M | The Council's policy for remote network access, mobile and flexible working should be documented and made available to all relevant staff.<br><br>Remote access to the Council network should be authorised by the users' line managers.<br><br>An authorisation box for line managers to indicate whether or not new users should have remote network access should be included in the new standard IT user access request form (when established). See ref 2. |
| **MANAGEMENT RESPONSE** | | | **RESPONSIBILITY AND IMPLEMENTATION DATE** |
| • Is it to be made part of the information security policies<br>• A policy will be written, or added into a current one if more appropriate<br>• A management authorisation process will be designed and;<br>• Added to new starters process | | | *Responsible Officer: Tim Huggins*<br>*Implementation Date: 30 September 2015* |

# DETAILED FINDINGS & RECOMMENDATIONS

| **Risk:** Inadequate arrangements for minimising the impact or loss from data security breaches | | | |
|---|---|---|---|
| **Ref.** | **Finding** | **Sig.** | **Recommendation** |
| 6 | Incident Management Policy<br><br>We found the Council's arrangements for information security incident reporting and management to be adequate. However the incident management policy document was issued in February 2009. The document is out of date. | M | The information security incident management policy document should be reviewed and revised. Once updated, the document should be made available to all relevant staff. |
| **MANAGEMENT RESPONSE** | | | **RESPONSIBILITY AND IMPLEMENTATION DATE** |
| Information security incident policy will be updated and relevant staff will be notified | | | *Responsible Officer: Tim Huggins*<br>*Implementation Date: 30 September 2015* |

# DETAILED FINDINGS & RECOMMENDATIONS

| **Risk:** Failure to manage the risks posed by 3rd parties and service providers with consequential reputational damage and financial loss for the Council | | | |
|---|---|---|---|
| **Ref.** | **Finding** | **Sig.** | **Recommendation** |
| 7 | 3rd Party Assurance<br><br>The Council currently has no arrangements in place for obtaining assurance from hosting service providers on the adequacy and effectiveness of their internal controls. Assurances such as Service Auditor's Reports (SARs) or Statements on Standards for Attestation Engagements 16 (SSAE 16) are neither requested nor obtained from service providers.<br><br>The main hosted services are :<br><br>• E-financials hosted by ABS<br>• Revenues and Benefits system hosted by Meritec<br>• Chipside -the car parking system<br><br>There is a risk to the Council's information assets where 3rd party service providers' (with access to its network) internal controls are inadequate or ineffective. | M | The Council should obtain annual assurance reports such as :<br><br>• Service Auditor's Reports (SARs)<br>• Statements on Standards for Attestation Engagements 16 (SSAE 16) from 3rd party service providers or organisations which have access to its information assets. |
| **MANAGEMENT RESPONSE** | | | **RESPONSIBILITY AND IMPLEMENTATION DATE** |
| 3rd party's will be engaged to obtain relevant information for information assurance | | | *Responsible Officer: Tim Huggins*<br>*Implementation Date: 30 September 2015* |

# APPENDIX I – STAFF INTERVIEWED

| NAME | JOB TITLE |
|---|---|
| Philip Ruck | Contracts and Corporate projects Manager |
| Tim Huggins | ICT Manager |

BDO LLP appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.

# APPENDIX II – DEFINITIONS

| LEVEL OF ASSURANCE | DESIGN of internal control framework | | OPERATIONAL EFFECTIVENESS of internal controls | |
|---|---|---|---|---|
| | Findings from review | Design Opinion | Findings from review | Effectiveness Opinion |
| **Substantial** | Appropriate procedures and controls in place to mitigate the key risks. | There is a sound system of internal control designed to achieve system objectives. | No, or only minor, exceptions found in testing of the procedures and controls. | The controls that are in place are being consistently applied. |
| **Moderate** | In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective. | Generally a sound system of internal control designed to achieve system objectives with some exceptions. | A small number of exceptions found in testing of the procedures and controls. | Evidence of non compliance with some controls, that may put some of the system objectives at risk. |
| **Limited** | A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year. | System of internal controls is weakened with system objectives at risk of not being achieved. | A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year. | Non-compliance with key procedures and controls places the system objectives at risk. |
| **No** | For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework. | Poor system of internal control. | Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework. | Non compliance and/or compliance with inadequate controls. |

| Recommendation Significance | |
|---|---|
| **High** | A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently. |
| **Medium** | A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action. |
| **Low** | Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency. |

# APPENDIX III – TERMS OF REFERENCE

**BACKGROUND**

Information security management is an integral part of the Council's IT infrastructure. It is also an essential component of governance and management which affects all aspects of its information management system. Responsibility for all aspects of the Council's information systems, including information security, lies with Senior Management.

**PURPOSE OF REVIEW**

The purpose of this review is to provide assurance on the adequacy of data security controls.

**KEY RISKS**

Based upon the risk assessment undertaken during the development of the internal audit operational plan, through discussions with management, and our collective audit knowledge and understanding the key risks associated with the area under review are:

- Ineffective governance and management arrangements resulting in poorly defined roles and responsibilities for data security
- Failure to comply with legal and regulatory requirements due to poor information security policies and procedures
- Unauthorised access to sensitive information and data security breaches resulting in damage to the Council's reputation
- Loss of information assets including exposure of sensitive corporate and personal data to the public domain
- Inadequate arrangements for minimising the impact or loss from data security breaches
- Failure to manage the risks posed by 3rd parties and service providers with consequential reputational damage and financial loss for the Council
- Poor information security education, training and awareness resulting in security breaches by authorised users
- Exposure of sensitive data due to poor physical and technical security measures.

# APPENDIX III – TERMS OF REFERENCE

**SCOPE**

The areas below will be covered as part of the review:

- Data /information security governance and management arrangements
- Information security policies and procedures
- User account management and access control
- Remote access and mobile devices
- Data security incident reporting arrangements
- Assurance received from 3rd parties and IT service providers in regard to the security of Council data
- Information security awareness and training
- Physical security measures
- Technical security controls.

**EXCLUSIONS**

Our work will be restricted to the areas of consideration within our scope of the review. The review will exclude business continuity planning, detailed network security controls and the security of systems hosted by 3rd parties.

**APPROACH**

Our approach will be to conduct interviews to establish the controls in operation for each of our areas of audit work. We will then seek documentary evidence that these controls are designed as described. We will evaluate these controls to identify whether they adequately address the risks.

**MANAGEMENT COMMENTS**

No management comments have been raised regarding the areas under review.

**LOCATIONS**

Fieldwork will be performed primarily at Council's offices but other sites will be visited if required.

# APPENDIX III - TERMS OF REFERENCE

**DOCUMENTATION REQUEST**

Where available, please ensure that electronic copies of the following documents have been forwarded to us in advance of the review:

- Information security policy and procedures
- User account management procedure document
- Remote access and mobile device policies
- Incident management policy and procedures.

These documents will assist the timely completion of our fieldwork, however this list does not necessarily constitute a complete list of all documentation and evidence that we may need as part of our review

**KEY CONTACTS**

| BDO LLP | | |
|---|---|---|
| Greg Rubins | Audit Partner | t: 0238 088 1892<br>e: greg.rubins@bdo.co.uk |
| Liana Nicholson | Audit Manager | t: 01473 320715<br>e: liana.nicholson@bdo.co.uk |
| Titi Junaid | Senior IT Auditor | t: 0207 893 2741<br>e: titi.junaid@bdo.co.uk |
| **Brentwood Borough Council** | | |
| Philip Ruck | Contract and Corporate Projects Manager | t:+44 (0) 1277 312569<br>e: philip.ruck@brentwood.gov.uk |
| Tim Huggins | ICT Manager | t: +44 (0) 1277 312719<br>e: tim.huggins@brentwood.gov.uk |

# APPENDIX III - TERMS OF REFERENCE

## PROPOSED TIMETABLE

| Audit Stage | Date |
|---|---|
| Commence fieldwork | 02/02/2015 |
| Number of audit days in plan | 20 |
| Planned date for closing meeting | 27/02/15 |
| Planned date for issue of report to Council | 06/03/15 |
| Planned date for receipt of management responses | 20/03/15 |
| Planned date for issue of proposed final report | 27/03/15 |
| Planned Audit Committee date for presentation of report | 28/07/15 |

## SIGN OFF

| On behalf of BDO LLP: | | On behalf of Brentwood Borough Council: | |
|---|---|---|---|
| Signature: | ..... | Signature: | ..... |
| Title: | ..... | Title: | ..... |
| Date: | ..... | Date: | ..... |

**www.bdo.co.uk**