www.pwc.co.uk

Internal Audit Report 2016/2017

Information and Cyber Security Review

Hinckley and Bosworth Borough Council

June 2017

pwc

Contents

Distribution list

For action:	Michael Dungey, ICT Manager Julie Kenny, Monitoring Officer
For information:	Audit Committee

Executive summary (1 of 4)

Report classification

High risk

(21 points)

Total number of findings

	Critical	High	Medium	Low	Advisory
Total	-	1	3	2	-

Executive summary (2 of 4)

Headlines/summary of findings

This review looked at Hinckley & Bosworth Borough Council's (HBBC) current cyber security 'as is' position by performing a gap analysis of information and cyber security risks in six areas; priorities, risk, connection, people, technology and response. The detailed scope of our work is included in our terms of reference in Appendix B. HBBC are operating a commercial IT model whereby they are providing IT services to a number of other local Councils. Our review is only looking at HBBC infrastructure and applications.

The outcome of our review has noted one high, three medium and two low risks:

- **Security Monitoring (high risk):** An absence of security monitoring tools to detect and alert on suspicious activity on the network;
- **Access Control (medium risk):** There is a lack of a centralised IT system to manage user access across different applications at HBBC. The leavers process is also disjointed due to the correct individuals/departments not all receiving notifications of movers and leavers;
- **Third Party and Physical Access (medium risk):** Right to audit clauses are included in supplier contracts but are not performed to ensure suppliers are complying with security clauses and delivering service as expected. Absence of security monitoring (e.g. CCTV) in the data centre, which would hinder an investigation if an incident was occurred due to malicious activity;
- **Incident Response Procedure/Plan (medium risk):** The current incident response procedure does not cover all steps required to be followed in an event of a security incident occurring. Some important information is missing from the process document, for example the contact details of internal and external contacts to notify of incidents and actions that need to be taken for security related incidents;
- **Information Training and Awareness (low risk):** Users that have privileged access or may handle sensitive data are not provided with targeted training to raise awareness of the potential security risks and challenges associated with their job role and level of users access; and
- **Information Security Policy, classification and asset register (low risk)*:*** There is no information security policy to outline high level objectives in regards to the measures and governance of information security. A number of policies assessed as part of the audit are not reviewed on an annual basis and do not have version control for completeness. Currently there is no information classification in place to detect and restrict sensitive and personal information leaving the network and no data loss prevention (DLP) tool is implemented. Across the organisation there an absence of a comprehensive information asset register to outline the information assets at HBBC and the risks associated.

We would like to thank the staff involved in this review for their help during this internal audit.

Executive summary (3 of 4)

Management comments

The Authority is already aware of the issues noted in relation to SIEM software and have already secured software that will cover the SIEM issue called Manage Engine ADAudit, to be deployed as part of the agreed work programme for Steria 2017/18. In the meantime, we have firewall and other security procedures in place to reduce the risk of unauthorised access. Therefore as action is being taken we do not feel the high risk rating is warranted as the risk is being addressed, and we have unauthorised access prevention software in place. We are unaware of wide spread use of SIEM software in councils, so feel we are making progress by our proactive action to include procurement of SIEM solution software in the near future. We accept it was not in place at the time of the audit, but feel our current set up was reasonable.

Executive summary (4 of 4)

Good practice

1 There are a number of user awareness and training initiatives in place such as e-learn modules, annual data protection refresher courses and information governance display posters.

2 Role based background checks are conducted on employees.

3 A mobile device management (MDM) solution is in place to manage corporate mobile devices across the organisation.

4 A number of data security policies in place to provide information security governance and guidance to all employees within HBBC.

5 All legal contracts go through the legal department for consultation, approval and signing.

Current year findings (1 of 6)

Technology

1

Finding rating

Rating	High

Finding and root cause

Security Monitoring

Security monitoring applications help to provide visibility to the network and identify, analyse and alert on security incidents triggered on the network and applications. an application monitoring tool in place called Kiwi that monitors basic users activity (e.g. logon times) on applications or processes but there are limited security monitoring tools in place to detect suspicious activity on the network such as:

- Data loss prevention (DLP); and
- Security incident and event management (SIEM) system.

Basic IDS/IPS functionalities are in place via implemented firewalls but there is no dedicated solutions in place. The Council has elements of intrusion prevention within the WatchGuard firewall but this does not provide full prevention protection as it is not a dedicated appliance built for this function. Sophos UTM is also used for web server protection which the Council use for reverse server authentication which validates users. The Council use Sophos AntiVirus to alert on potential malware entering the network. Solarwinds is used to alert and report on the performance of the network, for example server health, diskspace.

Cyber attacks are becoming more common and targeting specific sectors and knowing you are being attacked is critical. There are a range of tools to help identify and manage an attack, which can be costly, but an attack would also be very costly. As HBBC operates a commercial model of IT they should be doing more to ensure their network and data and those of the other Councils are secure.

Risk

Without security monitoring, the Council will be unaware of potential security breaches or unauthorised access attempts. Although the implementation of security monitoring tools may be costly, the implications and results of not having the correct tools in place may pose a greater risk leading to greater overall costs to HBBC.

Action plan

The Council should consider which security monitoring tools are required based on their current structure. The tools will help identify suspicious activity and will provide alerting on a range of security events and should be configured to best meet the needs of the organisation.

Responsible person/title:

Michael Dungey, ICT Manager

Target date:

September 2017

Current year findings (2 of 6)

Risk

2

Finding rating

Rating	Medium

Finding and root cause

Access Control

Controlling access to HBBC systems is essential to ensure legitimate users are granted access to systems through identification, authentication, authorisation, and accountability. This also helps to manage the joiners, movers and leavers process at HBBC.

There are approximately 30 to 40 applications in use at HBBC but the user access is not centrally managed by IT or linked to the Active Directory (AD) to provide a full view of who has access to each system. The majority of the systems are managed by individual system administrators across the organisation (e.g. finance system) and the process for requesting access varies from system to system. For example, access to the Benefits and Revenue system is via email which would be difficult to audit.

It was also identified that due to lack of a centralised IT system, there is a disjoint in the leaver process and the correct system administrators or department are not consistently being notified of movers or leavers in order for access to be removed. The leavers process consists of a form completion that is then sent to the system administrators via email.

Risk

- A lack of consistency in the management of user access and disjointed leavers process could result in user IDs remaining active after the user has left the organisation, which may result in unauthorised access; and
- Where access is not amended during a movers/leavers process, access rights may be accumulated over time resulting in excessive privileges and possible segregation of duty conflicts, increasing the possibility of fraud. There is a risk due to poor audit trails as the requests are made through email and not a centralised system.

Action plan

Consider whether the systems can be linked to a centralised system such as Active Directory or consider if an access governance tool could be used to provide an oversight of user access rights across systems.

Perform a review of which departments and individuals should be notified of movers and leavers and ensure this is reflected in the leavers process.

Responsible person/title:

Michael Dungey, ICT Manager

Target date:

September 2017

Current year findings (3 of 6)

Connections

3

Finding rating

Rating	Medium

Finding and root cause

Data Centre

The data centre at HBBC is onsite but managed by a third party supplier, SOPRA Steria. It was identified that there are no CCTV cameras within the data centre to monitor activity and help identify any malicious incidents should they arise. Backup services are run over night to an offsite location at the Melton Mowbray Council. In an event of data recovery, the network is mirrored but the backups are not. HBBC are looking at enhancing the current backup service and data centre recovery.

Risk

- Malicious activity within the data centre may go unnoticed due to the lack of CCTV monitoring (e.g. installation of malicious device on to a server) and investigation of an incident would be limited; and
- If backups are not taken on a frequent basis and recovery point objectives (RPO's) are not agreed this could result in a large amount of data loss.

Action plan

HBBC should considering installing CCTV cameras in the data centre and on the entry door to enable them to track and record all activity. This will reduce the likelihood of malicious activities within the data centre and aide investigation of incidents.

The Council should ensure RPO's and RTO's are agreed to ensure backups that may be critical are taken more frequently.

Responsible person/title:

Michael Dungey, ICT Manager

Target date:

September 2017

Current year findings (3 of 6)

Connections (cont….)

Finding and root cause

Third Party Management

HBBC do not have a standard contract in place. They rely on third party suppliers contract and the details provided by them. The legal team refer to a practical law database which states precedents of what clauses should be present which includes data protection, information security and the right to audit. Although the right to audit clause is included, this is not currently exercised by HBBC.

Risk

There is a risk that suppliers may not be complying with the clauses in their contract and without exercising their right to audit, HBBC may not have assurance that the suppliers are complying with the contract.

Action plan

HBBC should perform risk assessments on their third party suppliers based on the type of and volume of data they have access to and consider exercising their right to audit for these suppliers. This will provide HBBC with assurance that these third parties are complying with the contract and delivering service as expected.

Responsible person/title:

Michael Dungey, ICT Manager

Target date:

September 2017

Finding rating

Rating	**Medium**

Current year findings (4 of 6)

Crisis Response

4

Finding rating

Rating	Medium

Finding and root cause

Incident Response Procedure/Plan

HBBC have an ICT security incident procedure document, that provides guidance in the event of security incidents occurring. It covers key elements such as a response framework and security risk classification but the document does not cover all requirements outlying how to deal with security incidents. The document is missing:

- Contact details for third parties involved in service delivery or response;
- Identification and remediation action for different types of security incidents;
- IT contacts and their details to notify of incidents;
- Response plan for different types of security incidents; and
- Phrases to be used for communicating security incidents to the staff.

The Leicestershire ICT Partnership have a security working group who are tasked with reviewing information security incident reports, initiating corrective and preventative action as appropriate. Specialist Security services are included as part of the outsourced contract from Sopra Steria in the form of an operational security manager.

Risk

In the event of a security related incident, such as a security breach, there is dependency on the approach used to manage and resolve the issue. Without a complete security incident response policy, a security incident such as a virus infection may not be isolated and dealt with effectively. Staff may be unaware of their responsibilities, resulting in increased downtime and business disruption.

Action plan

Work should be undertaken to enhance the current ICT security incident procedure document to include the following areas:

- Reporting, escalation and notification procedures;
- Communication both internal and external;
- The members of staff responsible and their contact details;
- The criteria for the use of external security breach specialists; and
- Incident closure.

The policy should be tested and reviewed on a regular basis. Specialist training should be provided for individuals dealing with security incidents.

Responsible person/title:

Michael Dungey, ICT Manager

Target date:

September 2017

Current year findings (5 of 6)

People

5

Finding rating

Rating	Low

Finding and root cause

Information Training and Awareness

Information security training is included as part of the induction process for all new starters which includes a number of e-learning training course. e.g. data protection and information governance training. Individuals with privileged access or those with roles that include handling sensitive data are not provided with specific and targeted information security training.

Risk

In the absence of targeted training for privileged users may result in a poor security culture increasing the likelihood of data breaches.

Action plan

Higher risk users should be provided with additional, tailored training to ensure they are aware of the potential security risks and challenges involved in their day to day roles.

Responsible person/title:

Michael Dungey, ICT Manager

Target date:

September 2017

Current year findings (6 of 6)

Priorities

6

Finding rating

Rating	Low

Finding and root cause

Information Security Policy

There is no information security policy to outline high level objectives in regards to the measures and governance of information security.

There are a number of policies that have been implemented across the Council but do not have version control and are not reviewed on an annual basis (e.g. laptop mobile computer security policy, cloud storage policy and USB security policy). This is not in line with security best practices, where it is recommended that security policies are reviewed at least annually.

Risk

Employees may not be aware of their information security responsibilities and the security standards that they are expected to follow. This may lead to poor security practices within the Council exposing the organisation to the risk of unauthorised access to information and resources, disruption of HBBC's day to day operation, reputational damage and the risk of legal action. Out of date policies may hold information that is obsolete and provide false and misleading information to users which could result in incorrect actions being taken.

Action plan

An information security policy should be developed, together with details of how HBBC's performance against the information security policy will be measured. Such documents should be reviewed annually for suitability and business relevance.

Responsible person/title:

Michael Dungey, ICT Manager

Target date:

September 2017

Current year findings (6 of 6)

Priorities (cont….)

Finding and root cause

Information Classification Scheme

HBBC do not have an information classification scheme in place, therefore all data such as personally identifiable information (PII), commercially sensitive and financial data are not classified and handled accordingly. Currently there are no restrictions on the type of information leaving the organisation and no data loss prevention (DLP) tool in place.

Risk

Where an information classification scheme is not enforced, there is the risk that users will be unaware of the requirements for handling and processing sensitive data. As a result, they may export confidential data out of HBBC environment either unintentionally or with malicious intent.

Action plan

Implement and enforce an information classification scheme across all areas within the Council to ensure sensitive data is classified and users are aware of their responsibilities in securely handling and transferring data. Any classified information tagged may trigger an alert on the DLP tool if sent outside of the Council's network.

Responsible person/title:

Michael Dungey, ICT Manager

Target date:

September 2017

Finding rating

Rating	**Low**

Current year findings (6 of 6)

Priorities (cont….)

Finding and root cause

Information Asset Register

There is an absence of a comprehensive information asset register which may contain the details of HBBC's information assets, how to manage them and the risks associated to them. In preparation of the General Data Protection Regulation (GDPR) coming in to effect in May 2018, it requires an information asset register to be in place.

Risk

The lack of an information asset register may result in an inability to identify and understand the information HBBC hold and the controls in place to protect those assets.

Action plan

Develop and implement an information asset register, which includes the risks associated and the safeguards in place.

Responsible person/title:

Michael Dungey, ICT Manager

Target date:

September 2017

Finding rating

Rating	Low

Appendices

Appendix A: Basis of our classifications

Individual finding ratings

Critical

A finding that could have a:

- **Critical** impact on operational performance; or
- **Critical** monetary or financial statement impact ; or
- **Critical** breach in laws and regulations that could result in material fines or consequences; or
- **Critical** impact on the reputation or brand of the organisation which could threaten its future viability.

High

A finding that could have a:

- **Significant** impact on operational performance; or
- **Significant** monetary or financial statement impact*;* or
- **Significant** breach in laws and regulations resulting in significant fines and consequences*;* or
- **Significant** impact on the reputation or brand of the organisation.

Medium

A finding that could have a:

- **Moderate** impact on operational performance*;* or
- **Moderate** monetary or financial statement impact; or
- **Moderate** breach in laws and regulations resulting in fines and consequences*;* or
- **Moderate** impact on the reputation or brand of the organisation.

Appendix A: Basis of our classifications

Low

A finding that could have a:

- **Minor** impact on the organisation's operational performance*;* or
- **Minor** monetary or financial statement impact; or
- **Minor** breach in laws and regulations with limited consequences; or
- **Minor** impact on the reputation of the organisation.

Advisory

A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

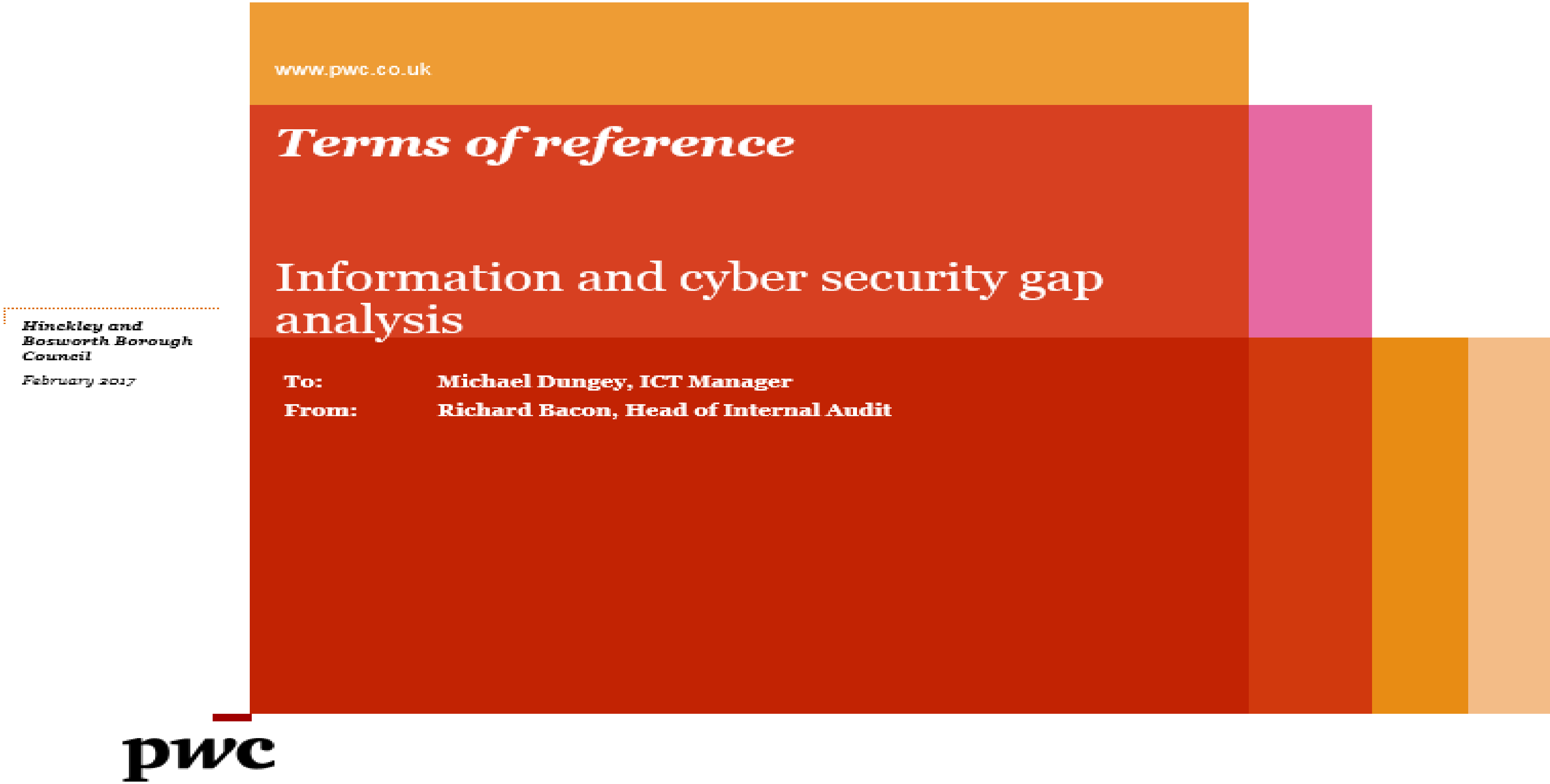
Report classifications

The report classification is determined by allocating points to each of the findings included in the report.

Findings rating	*Points*
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

Report classification	*Option A*	*Points*
□	Low risk	6 points or less
□	Medium risk	7 – 15 points
□	High risk	16 – 39 points
□	Critical risk	40 points and over

Appendix B: Terms of reference



www.pwc.co.uk

Terms of reference

Information and cyber security gap analysis

Hinckley and Bosworth Borough Council

February 2017

To: Michael Dungey, ICT Manager

From: Richard Bacon, Head of Internal Audit

Background and audit objectives

This review is being undertaken as part of the 2016/2017 internal audit plan approved by the Audit Committee on the 27 June 2016**.**

Background and audit objectives

The general cyber threat to all organisations is increasing and the Council needs to re-evaluate the security measures it has in place. The Council requires a cyber security review to determine the current 'as is' position regarding cyber security and to provide both quick wins and pragmatic recommendations in order to improve cyber security across the organisation.

The Council processes and store confidential and sensitive information on residents and staff which, if not securely managed, stored and processed, could lead to unauthorised access, data loss, business disruption and reputational damage.

As part of the internal audit for 2016/17, we will carry out a gap analysis of information and cyber security risks for a number of areas, which are summarised in the scope section on the next page, to evaluate your approach to cyber security and review the current arrangements that are in place.

Audit scope and approach (1 of 3)

As discussed when we met with Michael Dungey, our review will be based around the PwC Cyber Security Confidences framework.

This is designed to give a broad overview of your current level of maturity in respect of understanding and mitigating relevant risks. This includes not only the risks around information in its electronic format, but also hard copy documents which can just as easily put the organisation at risk of a security incident.

We have outlined our scope in each of the six areas.

We have outlined our scope in each of the six areas:

Priorities

- Is information appropriately identified across the organisation?
- Are management aware of where information is held and who is responsible for that information
- Are there appropriate information classification and handing policies in place?

Risk

- Are there appropriate policies in place to manage the information security risk?
- Do management understand the risks that they are taking and does their risk appetite correlate to their control environment?

Connections

- Are management aware of what information is shared and where it is shared?
- Are there appropriate provisions within third party service contracts to safeguard Alumasc's information?

People

- What is the level of awareness of cyber and information security across the business?
- Are employees aware of what constitutes an information security breach; do they know what to the in the event of one?

Technology

- We will consider the technology landscape; including the use of desktop, laptop and mobile devices.
- What protection is in place to safeguard information held on devices?

Response

- What is the response plan in place in the event of a cyber security incident?
- Do management have the capabilities to effectively contain a cyber security incident or information security breach?

Audit scope and approach (2 of 3)

The assessment will be conducted through a review of documentation and interviews with Council staff. The assessment will be based across the six cyber confidences, assessing:

- **Priorities** – consideration of the risk appetite of the Council in relation to information and cyber security. Review of any existing data classification systems used to identify high risk items and evaluate the extent of the safeguards put in place by the Council to mitigate this risk;
- **Risk** – a review of the information security framework currently in place;
- **Connections** – review the processes for contracting with third parties who will have access to Council data, and assess if information security is appropriately considered;
- **People** – assessment of the levels of awareness across Council employees of cyber and information security principles and policies;
- **Technology** – assessment of the appropriateness of the tools used to prevent data loss and unauthorised access; and
- **Response** – review of the Council response plans in the event of a cyber / information security incident. Assessment of the tools used to detect malicious software and unauthorised access.

Audit scope and approach (3 of 3)

The scope of our work will be limited to the areas identified in this Terms of Reference. Limited operational effectiveness testing will be performed as part of this review. There will be no detailed configuration reviews of security components such as firewalls, intrusion prevention systems, MDM solutions and access control testing will not be performed. This review will not provide certification against compliance frameworks such as PCI or GDPR.

Recommendations for improvement will be made in respect of the information and cyber security controls in scope.

Our audit approach is as follows:

- Obtain an understanding of the individuals responsible for day to day management of information and cyber security through discussions with key personnel;
- Review of relevant documentation;
- Identify the key risks and validate these with the IT Manager; and
- Provide you with a written report highlighting risks and recommendations.

Internal audit team and key contacts

Name	Role	Contact details
Richard Bacon	Head of Internal Audit	richard.f.bacon@pwc.com
Jodie Stead	Internal Audit Manager	jodie.a.stead@pwc.com
Matt Wilmot	Information and Cyber Security Manager	matthew.wilmot@pwc.com
Arinder Badyal	Information and Cyber Security Specialist	arinder.k.badyal@pwc.com

Key contacts – Hinckley and Bosworth Borough Council

Name	Title
Julie Kenny	Monitoring Officer
Ashley Wilson	Section 151 Officer
Michael Dungey	IT Manager
Cal Bellavia	Consultation and Improvement Officer
Julie Stay	Human Resources and Transformation Manager

Timetable

Fieldwork start	27th February 2017
Fieldwork completed	17th March 2017
Draft report to client	24th March 2017
Response from client	31st March 2017
Final report to client	7th April 2017

Agreed timescales are subject to the following assumptions:

- All relevant documentation, including source data, reports and procedures, will be made available to us promptly on request.
- Staff and management will make reasonable time available for interviews and will respond promptly to follow-up questions or requests for documentation.

Please note that if Hinckley and Bosworth Borough Council requests the audit timing to be changed at short notice and the audit staff cannot be deployed to other client work, Hinckley and Bosworth Borough Council may still be charged for all/some of this time. PwC will make every effort to redeploy audit staff in such circumstances.

In the event that, pursuant to a request which Hinckley and Bosworth Borough Council has received under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 (as the same may be amended or re-enacted from time to time) or any subordinate legislation made thereunder (collectively, the “Legislation”), Hinckley and Bosworth Borough Council is required to disclose any information contained in this document, it will notify PwC promptly and will consult with PwC prior to disclosing such document. Hinckley and Bosworth Borough Council agrees to pay due regard to any representations which PwC may make in connection with such disclosure and to apply any relevant exemptions which may exist under the Legislation to such report. If, following consultation with PwC, Hinckley and Bosworth Borough Council discloses any this document or any part thereof, it shall ensure that any disclaimer which PwC has included or may subsequently wish to include in the information is reproduced in full in any copies disclosed.

Internal audit work was performed in accordance with PwC's Internal Audit methodology which is aligned to Public Sector Internal Audit Standards. As a result, our work and deliverables are not designed or intended to comply with the International Auditing and Assurance Standards Board (IAASB), International Framework for Assurance Engagements (IFAE) and International Standard on Assurance Engagements (ISAE) 3000.

This document has been prepared only for Hinckley and Bosworth Borough Council and solely for the purpose and on the terms agreed with Hinckley and Bosworth Borough Council in our agreement dated 10th May 2016. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.