Grant Thornton
An instinct for growth™

Hinckley and Bosworth Borough Council

Revenues and Benefits (Memorandum of Understanding)
Internal Audit report

January 2020

DRAFT FOR MANAGEMENT COMMENT

Andrew Smith
Head of Internal Audit
T: 0161 953 6900
E: andrew.j.smith@uk.gt.com

Zoe Thomas
Internal Audit Manager
T: 0121 232 5277
E: zoe.thomas@uk.gt.com

Kerry Sharma
Internal Auditor
T: 0116 257 5576
E: Kerry.sharma@uk.gt.com

Contents

1 Executive Summary

2 Key Findings & Recommendations

3 Appendices

Report distribution:

For action:

- Director (Corporate Services)
- Head of Leicestershire Revenues and Benefits Partnership

Responsible Executives:

- Director (Corporate Services)

Executive Summary

Background

Harborough, Hinckley and Bosworth and North West Leicestershire Councils are jointly responsible for managing the revenues and benefits services through partnership arrangements. In 2018/19 the partnership budgeted £3.6m for managing the services. At the year end there was a caseload of 14,235 benefits claimants.

The operations of the partnership is overseen by the management board, comprising senior officers from all three councils and a joint committee which meets quarterly, and reviews the financial and operational performance of the partnership.

Hinckley and Bosworth Brough Council are the host authority for the partnership and, as their auditors, we will undertake our review and report our findings to the management board and the joint committee. Our report will be considered by the head of Internal audit for each council when forming their opinion for the 2019/20 financial year.

There is in place a Memorandum of Understanding (MOU) between the Department for Work and Pensions (DWP) and the individual local authorities. The partnership has access to data from DWP and Her Majesty's Revenue and Customs (HMRC) to enable staff to administer:

- Housing Benefit (HB) and any associated counter fraud & error and overpayment recovery activity
- Local Council Tax Reduction (LCTR) schemes and any associated recovery of LCTR errors
- Local Welfare Provision (LWP); and
- Discretionary Housing Payment (DHP).

The MOU sets out the framework and operating policy through which an organisation will access, exchange and share DWP, HMRC and appropriate customer data.

The memorandum of understanding must be signed by the operational manager with responsibility for the service area covered and be countersigned by the s151 Officer. The Chief Executive is also expected to understand their obligations.

The DWP may seek confirmation that each local authority continues to comply with the MOU.

Objectives

Our review will focus on the following potential risks:

- Hinckley Borough Council, as the host organisation, does not have adequate arrangements in place to ensure compliance with the terms of the Memorandum of understanding
- Management is not fully sighted on arrangements and may inappropriately sign off compliance with the terms and conditions, putting the council at risk of the service being withdrawn or facing prosecution.

The MOU sets out a series of key compliance requirements. In our review we have considered each of the compliance areas and concluded whether there is evidence that the partnership is complying in each of the areas.

Limitations in scope

Our findings and conclusions will be limited to the risks identified above. The scope of this audit does not allow us to provide an independent assessment of all risks and controls across the entire management of the MOU.

Where sample testing is undertaken, our findings and conclusions will be limited to the sample tested only. Please note that there is a risk that our findings and conclusions based on the sample may differ from the findings and conclusions we would reach if we tested the entire population from which the sample is taken.

Executive Summary

Conclusion

Significant assurance

We have concluded that the processes provide **SIGNIFICANT ASSURANCE** to the Partnership Board and the Audit Committee.

We are able to conclude that Hinckley and Bosworth Borough Council, as the host organisation, has adequate arrangements in place to ensure compliance with the terms of the Memorandum of understanding; and

There is appropriate oversight by Management in ensuring that terms and conditions of the MOU are complied with.

This is because only minor matters in the risk management activities and controls designed to achieve management objectives were identified from our work.

Good Practice

- We noted that there are good process in place and controls around the documenting and record maintaining of the DWP random access management checks, which means that when DWP request one of the management checks to be sent to them for checking the Partnerships Checking Officer is able to respond promptly.
- The Partnerships Management team have a strong understanding of the MoU which ensures that the impact that Corporate decisions may have on the compliance with the MoU is always taken into consideration.

Areas for development

There are no significant areas for development, recommendations made are for improvement

Recommendations

We have raised one low risk recommendation and an improvement to address the minor weaknesses identified as well as two improvement points.

	High	Med	Low	Imp
Detailed findings	-	-	-	3

Acknowledgement

We would like to take this opportunity to thank your staff for their co-operation during this internal audit.

Key Findings & Recommendations

Risk Area
Hinckley Borough Council, as the host organisation, does not have adequate arrangements in place to ensure compliance with the terms of the Memorandum of understanding.

Compliance Area	Findings and Recommendation	Action Plan
Contracted Service Provider individual LA's should obtain assurance that services sub-contracted to another 3rd party organisation are compliant with required standards	**Key findings** We obtained the Council's most recent MoU Annual Assurance statement, held discussions with team members and reviewed the statement for appropriate signatures. Our findings were that the HBBC's statement had been appropriately signed by both the Partnership and the Council's Section 151 Officer. From discussions we confirmed that the Partnership provided the other Council's within the Partnership with a signed Annual Assurance statement and that they have received both statements back from the Councils and are with the Council's section 151 Officer. **Compliant - YES** **Recommendations: N/A -** We have noted no issues with compliance area	**N/A**

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
Information Assurance compliance • use of the current government approved infrastructure - Public Services Network (PSN) • valid PSN Code of Connection (CoCo) compliance certificate or Cloud-based email assessment pass held • where DWP API services are utilised over the public internet compliance with all obligations set out in MoU	**Key findings** We obtained the Council's current PSN Connection Compliance certificate and guidance given to Partnership staff on the access requirements of Searchlight and held discussions with the Partnership's Management team. Our findings were that HBBC's has a current PSN Connection Compliance certificate covering the period 09/07/2019 to 09/07/2020. That Partnership staff have access to the Seachlight Guide which covers the requirements for accessing the system. Our discussions with team members found that staff are made aware of any reminders sent out by DWP about access requirements. We have confirmed from our discussions that with Partnership management that the Partnership uses the DWP CIS Internet Automation API which is in line with the obligations set out in the MoU. **Compliant - YES** **Recommendations: N/A -** We have noted no issues with this compliance area.	**N/A**

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
Configuration and Change Management • configuration management and change management processes are robust leading to potential unauthorised changes to ICT systems and their constituent components being prevented and reported • robust upgrade and patch management policies in place resulting in updates and patches not being applied in a controlled and timely manner	**Key findings** We obtained and reviewed the Patch Management policy for the Leicestershire ICT Partnership, of which the Leicestershire Revenues & Benefits Partnership is a member. We have confirmed that the Partnership is using the most up to date version of the software and have applied patches as required. We understand that the Change Advisory Board meets weekly and would consider and approve any changes. Our findings were that the policy is robust and that the policy ensures that patches are implemented in a timely manner with each new patch being reviewed and evaluated within one working day to categorise the criticality of the patch. **Compliant - YES** **Recommendations: N/A -** We have noted no issues with this compliance area.	

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
Anti-Malware • mechanisms are in place to identify, detect and respond to malware relating to networked infrastructure, and ICT and information systems that create, sort, transmit or otherwise processes data originating from DWP, or for which the DWP is identified as the data controller • that anti-virus software installed on ICT and information systems is fully licensed and supported, and that all available software updates and patches have been applied in a timely manner	**Key findings** We held discussions with the Partnership management team, with input form the Leicestershire ICT Partnership (LICTP) relating to the anti-malware and anti-virus software and obtained the software license for Sophos antivirus.. Our findings were that the Council uses the Clearswift Secure email gateway which scans all inbound and outbound mail for viruses. Two anti-virus engines are used and all servers and workstations have the Sophos Central Antivirus application installed. Reports of high and medium alerts are generated on a daily basis for engineers to review and action as required, with actions taken reported monthly within the Security reports. **Compliant - YES** **Recommendations: N/A -** We have noted no issues with compliance area.	**N/A**

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
End-Point Access (1) Access to data originating from the DWP, or for which the DWP has been identified as the Data Controller, is: • only afforded to ICT, information systems and mobile devices which are included within the sharing partner's configuration management policies, procedures and processes; and which meet the requirements of the anti-malware controls identified above • controlled such that only ICT and information systems wholly owned and administered are permitted access	**Key findings** We held discussions with the Partnership management team, obtained and reviewed asset register containing the Partnerships ICT assets. Our findings were that Hinckley and Bosworth Borough Council as the Host Authority of the Partnership own all ICT and Information systems that are permitted access to DWP data and all such ICT and information systems are subject to the partnerships ICT policies including anti malware / anti virus / Change & Patch management identified above. All assets used by the Partnership are individually identified and recorded on the asset register. Partnership users have one access that covers the 3 LAs within the partnership. Each user has a unique user ID used when logging on. This enables the partnership / LAs to record the users activity undertaken / attempted including the date and time of activity. Daily random DWP Management checks followed up and relevant paperwork completed and retained. We are satisfied that the arrangements in place are compliant with DWP requirements. **Compliant - YES** **Recommendations: N/A -** We have noted no issues with this compliance area.	**N/A**

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
End-Point Access (2) mechanisms are in place to record and audit end-point activities within its networked infrastructure, as a minimum recording, the end-point's unique identifier, the date and time of an activity, and the activity undertaken/ attempted	**Key findings** We obtained the Partnerships current PSN certificate, held discussions with team members, checked one days DWP Access Management checks and made checks to ensure that the Partnership replies to DWPs adhoc requests for supporting documents of Access Management checks. Our findings were that the Partnership has a current PSN certificate and therefore has an audit logging process in place that meets the requirements of the PSN. That the Partnership maintain good records to support DWP Access Management checks and responds to DWPs adhoc requests appropriate manner. **Compliant - YES** **Recommendations: N/A -** We have noted no issues with this compliance area.	**N/A**

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
• **Encryption requirements** • Data originating from the DWP, or for which the DWP has been identified as the data controller, is encrypted in-transit. Including when being transmitted within its networked infrastructure, to the DWP or to third parties/other. • Encryption products, mechanisms and standards meet DWP standards, e.g. standards detailed within the DWP Use of Cryptography standard (SS-007) Annex H of MoU. • Can evidence / demonstrate effective key management policies, processes and procedures in support of encrypted data	**Key findings** We held discussions with the Partnership management team, with input form the Leicestershire ICT Partnership (LICTP) and reviewed supporting documentation. We have confirmed that all DWP data and that for which the DWP has been identified as the data controller is encrypted when in transit within the network infrastructure. Whilst the DWP encryption standards are complex and constantly evolving the LICTP ensure that the DWP "must" requirements are met as a minimum. Encryption keys are kept securely and access is restricted to engineers that have the designated responsibilities. The process in place is that the LICTP provides an annual assurance statement via email to the Revenues and Benefits partnership that arrangements in place are compliant, with DWP requirements. The partnership relies on this assurance that it meets the requirements. However whilst the LICTP provides some assurance to the Partnership over the MoU compliance areas this mainly relates to the ICT infrastructure and it makes no explicit reference to meeting the DWP standards for encryption products, mechanisms and standards as detailed within the DWP Use of Cryptography standard (SS-007) which forms Annex H of the MoU. **Compliant - improvement recommendation made** **Issue identified:** The partnership receive assurance from the IT partnership via email on compliance with DWP requirements for encryption. The assurance provided is not explicit in all areas. **Root cause:** there is no explicit reference to meeting the DWP standards for encryption products, mechanisms and standards as detailed within the DWP Use of Cryptography standard (SS-007) which forms Annex H of the MoU in the statement of assurance from the IT Partnership to the revenues and benefits partnership. **Risk:** the DWP requirements may not be met in all areas **Recommendations:** that the assurance given by LICTP to the R&B Partnership is extended to include, as a minimum, the encryptions products, mechanisms and standards meet DWP standards within the DWP use of Cryptography standard (SS-007) Annex H of MoU. HBBC should also consider if there are any other ICT compliance areas that they require specific assurance over from the LICTP. **Overall conclusion:** The ICT partnership provides assurance to the partnership over areas within its remit and makes clear what aspects, particularly in relation to security are under the partnerships control. There appears to be a gap in assurance in one area in relation to cryptology as there is no specific reference to this in the statement of assurance. Our audit procedures have confirmed that there is no evidence of non compliance with the standard, we consider this to be a **low risk recommendation** as the matter is about communication of assurance rather than compliance.	Actions: Responsible Officer: Mike Dungey Executive Lead: Due date:

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
Risk Management • Can demonstrate a formal risk management and standards-based approach to the assurance of the infrastructure where the data will be created, stored, transmitted or otherwise processed. • LA's shall have identified a board-level officer who is accountable for the security of data originating from the DWP, or for which the DWP is identified as the data controller, whilst the data is in the custody of the organisation	**Key findings** We held discussions with the Partnership management team, with input form the Leicestershire ICT Partnership (LICTP) and obtained and reviewed the Councils ICT Risk Register. Our findings were that the Council records ICT risks within it's Risk Register and actions taken to mitigate risks are monitored with the risk updated. The Council has identified Julie Kenny – Director of Corporate Services and Monitoring Officer as the Board level officer who is accountable of the security of data originating from the DWP. **Compliant - YES** **Recommendations: N/A -** We have noted no issues with this compliance area.	**N/A**

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
Government email policy • Domain name "gov.uk" are in use and have been since at least March 2019 • Secure email over the internet standards must be followed (e.g. using Transport Layer Security 1.2 or later when sending and receiving email, and using Domain-based message authentication reporting and conformance [DMARC])	**Key findings** We reviewed the domain of email addresses of Partnership staff. Our findings were that the domain ".gov.uk" is used in the email addresses of the Partnership staff. **Compliant - YES** **Recommendations: N/A -** We have noted no issues with this compliance area.	**N/A**

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
Her Majesty's Government Security Policy Framework The Security Policy Framework is followed in order to ensure that HMG information and other assets is secure and to ensure HMG can function effectively, efficiently and securely.	**Key findings** We held discussions with the Partnership management team, with input form the Leicestershire ICT Partnership (LICTP) to ascertain whether the Partnership follows the HMG Security Policy Framework. Our findings were that LICTP, of which the Partnership is a member, follows the HMG Security Policy Framework including having an Operational Security Manager assigned to LICTP and a Security working group that oversees Security Governance. **Compliant - YES** **Recommendations: N/A -** We have noted no issues with this compliance area.	**N/A**

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
Government Security Classifications (GSC) scheme Partnership aligns with the GSC scheme thereby helping individuals determine and indicate to others, the level of protection required to prevent the compromise of valuable or sensitive assets / data.	**Key findings** We held discussions with the Partnership management team, with input form the LICTP to ascertain that the Partnership aligns with the GSC scheme. Our findings were the Partnerships emails are not marked as 'private official'. However, the Partnership gives all emails the same level of protections and security. **Compliant –** YES - improvement point made	Actions: To be implemented Responsible Officer: Storme Coop Executive Lead: Sally O'Hanlon
	Issue identified: all correspondence is treated with a high level of security which is compliant with MOU standards and appropriate to the type of information being transferred. However there is no facility for individuals to indicate to others a specific level of protection **Root cause:** the facility for individuals to rate the sensitivity of the data transferred is an expectation within the MOU. However as all data transferred in the partnership is treated as sensitive then this is not regarded as necessary. **Recommendations:** The Partnership should enable staff to mark emails as 'private official' were data is valuable or sensitive **Overall conclusion:** we are satisfied that the process is appropriate and partnership data is treated as sensitive. Therefore, we consider this to be an **improvement** suggestion.	Due date: June 2020

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
Baseline Personnel Security Standards (BPSS) • Whilst the current Public Service Network (PSN) Code of Connection (CoCo) criteria only requires IT systems administration staff to be BPSS checked the DWP has additional requirements for staff with access to DWP/HMRC systems and/or data. • Pre-employment checks must been undertaken including identity, unspent criminal convictions and right to work as a minimum, with personnel vetting standards being based on the BPSS. • Users must be trained on their obligations with regards to system security and data handling before being given access to DWP data. (Covered by Access control below) • Agency and CSP staff must be subject to the same pre and post-appointment checks as permanent staff • LA's must have processes in place for confirming that CSP's providing all or part of a service covered by the MoU have carried out BPSS screening before granting access to DWP/HMRC data. • Newly assigned existing employees assigned to a post where access to government assets will need to be subject to BPSS verification checks. • Records detailing the dates that checks have been carried out must be maintain as this is a requirement of the Employment Authentication System (EAS), which grants access to some DWP systems including Customer Information system (CIS), Verify Earnings and Pensions service (VEP's) and Tell Us Once (TUO).	**Key findings** We held discussions with the Partnership management team to ensure that pre-employment checks are undertaking. Our findings were the pre-employment checks, including the requirement of BPSS certificates for staff employed to the Partnership are undertaken by the three individual Councils that make up the Partnership. Officers have provided details of the training provided to users and this aspect is further covered below (access control). All current staff having access to DWP systems are permanent employees. Should agency staff be required in the future, then officers have confirmed that the same standards would be required. No staff have been reassigned DWP roles within the year. The Partnership has processes in place to ensure that no one is given access to the system until the Partnership has received confirmation that an individual has a BPSS certificate and records of these confirmation are maintained. Appropriate records are retained by the partnership confirming certificates are in place **Compliant - YES** **Recommendations: N/A -** We have noted no issues with this compliance area.	**N/A**

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
Access control policy A robust access control policy must be maintain specifying; • access rights as defined within EAS guidance, including hierarchy, for individual users or groups of users with considerations on restrictions to access information that users do not have a business requirement for accessing and take into account where a segregation of duties needs to be applied • the frequency with which reviews of access rights must take place for users • action to be taken to remove access when there is no longer a business need, including changing job roles • the period after which inactive accounts must be suspended, and • a process ensuring all users and contractors who terminate their employment or relationship with the organisation are aware of their obligation not to divulge information gained during their employment	**Key findings** We obtained and reviewed the Access Control Policy and held discussions with the Partnership management team. Our findings were that there is a robust access control policy in place that all Partnership staff are required to sign. Access rights are reviewed and appropriately managed to ensure that individual team members have access rights that are in line with their role, including following a change in roll and inactive accounts are suspended in a timely manner. During the year there were two leavers that had their access rights revoked and no new starters. Employment contracts include a confidentiality clause that ensures when individuals leave the employment of the Partnership they are obliged not to divulge information gained during their employment. The partnership has a relatively small number of HB Partnership staff who have access to the data, and this access is overseen by two senior members of the team, consequently there is good understanding of any access change requirements within the team. However there is no formal requirement for periodic review of HB Partnership officers' access. Good practise would be for there to be a formalised annual review of existing access rights of current staff. Additionally, staff at each of the three LA's can view data that is sourced from DWP systems, an annual review should be undertaken to ensure the access is still relevant and in accordance with DWP requirements for usage. **Compliant - YES** **Issue identified:** No **formal** requirement for existing officers' access to DWP systems to be periodically reviewed. **Root cause:** The team is small and management consider that this provides the necessary oversight without a formal review process being put in place. **Risk:** staff may retain access inappropriately. **Recommendations:** HB Partnership should introduce a formal review of access to ensure access is limited to only those HB partnership staff and host authority staff who need it to undertake their roles. **Overall conclusion:** based on our work undertaken we consider that management have a good oversight of access rights of staff so that it is unlikely that staff would have inappropriate access. However an annual review would provide management with assurance that only appropriate staff have access to DWP data. Our audit procedures have confirmed that there is no evidence of non compliance with the standard, we consider this to be a **low risk recommendation**.	**Actions:** Review to be undertaken to all that have Academy access, with reporting to management board on an annual basis. **Responsible Officer:** Andrew Hough. **Executive Lead**: Sally O'Hanlon **Due date:** June 2020, and annually thereafter.

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
Home and Remote working - • The MoU applies equally to staff accessing DWP and HMRC data from outside of the office environment • Home and remote working solutions must comply with HMG Information Assurance Policy guidance, compliance standards within the MoU and PSN or Cloud-based email service assessment standards. • No personal devices should be used for accessing DWP data and/or systems. • A formal Home / Remote working policy must be in place • Additional security training to be given to staff working outside the office environment who handle DWP/HMRC information. • No solution allowing individual or CSP's access from outside of the United Kingdom is permitted. • Data originating from the DWP can only be created, stored, transmitted or otherwise processed by ICT and/or information systems which are located within the UK, EU and those companies covered by Privacy Shield.	**Key findings** We obtained and reviewed the HBBC Flexible Working Policy, reviewed staff training slides, obtained the Partnerships current PSN certificate, obtained and reviewed asset register containing the Partnerships ICT assets and held discussions with Partnership management team. Our findings were that the Council has a clear Flexible Working policy that complies with HMG Information Assurance policy guidance and the that it holds a current PSN certificate. All Partnership staff, including home workers, receive training that covers data security both in the office and outside of the office environment. Our work on compliance area End Point Access (1) confirmed that only devices owed by HHBC were used, and our discussions with Partnership management team has confirmed that no access to the Partnerships systems is permitted from outside of the United Kingdom (UK) with all DWP data only being created stored, transmitted or otherwise processed by systems located within the UK. **Compliant - YES** **Recommendations: N/A -** We have noted no issues with this compliance area.	**N/A**

Key Findings & Recommendations

Compliance Area	Findings and Recommendation	Action Plan
Cloud Service	**Key findings** Confirmed no Cloud service and none planned for partnership. **Compliant – N/A**	**N/A**

Key Findings & Recommendations

Risk Area
Management is not fully sighted on arrangements and may inappropriately sign off compliance with the terms and conditions, putting the council at risk of the service being withdrawn or facing prosecution.

Issue	Findings and Recommendation	Action Plan
Partnerships compliance with MoU T&Cs not monitored / reviewed for changes within the Partnership - including IT changes, and changes to MoU	**Key findings** We held discussions with the Partnerships Management team. Our findings were that any changes to the MoU are notified to Council's by DWP annually as part of the MoU Annual Assurance Statement process. The Partnership's management team review the changes and take any required action to ensure that the Partnership remains compliant. There was no significant changes to the 2019/20 MoU requirements. For IT infrastructure changes planned by HBBC the Partnership Management team are involved in discussions with LICTP to ensure any proposed changes would not result in non compliance. **Recommendations: N/A -** We have noted no issues.	**N/A**

Key Findings & Recommendations

Issue	Findings and Recommendation	Action Plan
Identified breaches are not investigated to DWP satisfaction	**Key findings** We held discussions with the Partnership Management Team about breaches. Our findings were that at the time of our review there were no current breaches at any of the three authority's within the Partnership. A previous breach reported to HBBC by DWP was investigated by the Council with the DWP's involvement and that DWP were satisfied with the findings of the Councils investigation. **Recommendations: N/A -** We have noted no issues..	**N/A**

Appendices

Appendix 1 – Staff involved and documents reviewed

Staff involved

- Julie Kenny – Director (Corporate Services)
- Sally O'Hanlon – Head of Leicestershire Revenues and Benefits Partnership
- Storme Coop – Partnership Manager (Benefits Lead)
- Leigh Butler – Partnership Manager (Revenues lead)
- Emma Weaver – Benefits Team Leader / Checking Officer
- Michael Dungey – Head of IT for Leicestershire ICT Partnership

Documents reviewed

- 2019/20 MoU Annual Assurance statement
- PSN Connection Compliance certificate
- Patch Management policy
- Sophos antivirus software license
- Asset register containing the Partnerships ICT assets
- Access Control Policy
- HBBC Flexible Working Policy
- HBBC Risk Register for ICT

Appendix 2 - Our assurance levels

The table below shows the levels of assurance we provide and guidelines for how these are arrived at. We always exercise professional judgement in determining assignment assurance levels, reflective of the circumstances of each individual assignment.

Rating	Description
Significant assurance	Overall, we have concluded that, in the areas examined, the risk management activities and controls are suitably designed to achieve the risk management objectives required by management. These activities and controls were operating with sufficient effectiveness to provide significant assurance that the related risk management objectives were achieved during the period under review. Might be indicated by no weaknesses in design or operation of controls and only IMPROVEMENT recommendations.
Significant assurance with some improvement required	Overall, we have concluded that in the areas examined, there are only minor weaknesses in the risk management activities and controls designed to achieve the risk management objectives required by management. Those activities and controls that we examined were operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review. Might be indicated by minor weaknesses in design or operation of controls and only LOW rated recommendations.
Partial assurance with improvement required	Overall, we have concluded that, in the areas examined, there are some moderate weaknesses in the risk management activities and controls designed to achieve the risk management objectives required by management. Those activities and controls that we examined were operating with sufficient effectiveness to provide partial assurance that the related risk management objectives were achieved during the period under review. Might be indicated by moderate weaknesses in design or operation of controls and one or more MEDIUM or HIGH rated recommendations.
No assurance	Overall, we have concluded that, in the areas examined, the risk management activities and controls are not suitably designed to achieve the risk management objectives required by management. Those activities and controls that we examined were not operating with sufficient effectiveness to provide reasonable assurance that the related risk management objectives were achieved during the period under review Might be indicated by significant weaknesses in design or operation of controls and several HIGH rated recommendations.

Appendix 2 - Our assurance levels *(cont'd)*

The table below describes how we grade our audit recommendations.

Rating	Description	Possible features
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in the design or application of activities or control that requires the immediate attention of management	▪ Key activity or control not designed or operating effectively ▪ Potential for fraud identified ▪ Non-compliance with key procedures / standards ▪ Non-compliance with regulation
Medium	Findings that are important to the management of risk in the business area, representing a moderate weakness in the design or application of activities or control that requires the immediate attention of management	▪ Important activity or control not designed or operating effectively ▪ Impact is contained within the department and compensating controls would detect errors ▪ Possibility for fraud exists ▪ Control failures identified but not in key controls ▪ Non-compliance with procedures / standards (but not resulting in key control failure)
Low	Findings that identify non-compliance with established procedures, or which identify changes that could improve the efficiency and/or effectiveness of the activity or control but which are not vital to the management of risk in the business area.	▪ Minor control design or operational weakness ▪ Minor non-compliance with procedures / standards
Improvement	Items requiring no action but which may be of interest to management or which represent best practice advice	▪ Information for management ▪ Control operating but not necessarily in accordance with best practice

grantthornton.co.uk