Hinckley and Bosworth Borough Council

General Data Protection Regulation (GDPR) Review as at Quarter 2

23 November 2018

FINAL

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

Jenny Strahan
IT Audit Manager
T: 0117 305 7600
E: jennifer.m.strahan@uk.gt.com

Contents

Report distribution:

For action:

- Information Governance (IG) Officer

Responsible Executives:

- Director (Corporate Services)

Executive Summary

Background

A review of the adequacy of the Council's General Data Protection Regulation (GDPR) arrangements has been undertaken as part of the approved internal audit plan for 2018/19 and this report sets out our findings.

The GDPR came into force across the European Union on 25 May 2018. It replaces EU Data Protection Directive 95/46/EC and supersedes national laws such as the UK Data Protection Act 1998. The GDPR provides for tougher penalties for breaches of the legislation. For the most serious violations, data protection regulators will be able to impose penalties of up to €20m (approximately £17m) or 4% of global turnover, whichever is higher.

Owing to this legislation's complexity, our review did not cover all GDPR related activities that the Council is engaged in and consequently we cannot provide assurance (and hence an opinion) on whether the Council is GDPR compliant. As recent legislation, the Council (like all organisations) is still embedding good practice to demonstrate on-going compliance. Consequently, owing to the timing of this review and our restricted scope, we cannot provide the Council with ISAE 3000 assurance on this matter (i.e. that which is applied for audits of internal control and compliance with laws and regulations such as the GDPR).

We have therefore designed and implemented a program of work designed to examine the Council's GDPR compliance against the key risks identified and outlined within this report as follows.

Objectives

This review assesses Hinckley and Bosworth Borough Council's implementation of its GDPR plans. We have undertaken a high-level review of the Council's GDPR activities and controls with regards to the following **risk** areas:

1) **Processing of personal data is not appropriately governed** – *this includes checking that your organisation has appropriately designated roles and responsibilities*;
2) **Collection of personal data is not conducted properly** – *this includes checking that privacy policies are in place and assessing whether your organisation needs consent to collect personal information;*
3) **Processing of personal data is not conducted responsibly** – *this includes making sure relevant members of staff have been trained to understand what they can and cannot do with personal information;*
4) **Processing of personal data is not safe** – *this includes establishing the technical and organisational measures in place;*
5) **Quality of personal data is not maintained, is not up to date and relevant** – *ascertaining how well your organisation effectively manages its information assets*
6) **People are not given their information rights** – *checking what procedures in place to handle information rights requests properly*; and
7) **Personal data is not shared, disclosed, or transferred securely** – *establishing what arrangements there are to ensure the personal information your organisation is responsible for remains adequately protected, wherever it is located.*

Further details on responsibilities, approach and scope are included the Audit Planning Brief issued to the Council in September 2018.

Limitations in scope

Please note that our conclusion is limited by scope. It is limited to the risks outlined above. Other risks exist in this process which our review and therefore our conclusion has not considered. Where sample testing has been undertaken, our findings and conclusions are limited to the items selected for testing.

Executive Summary

Conclusion

Significant assurance with some improvement required

We have reviewed the Council's GDPR arrangements and the controls tested are set out in our Audit Planning Brief.

We have concluded that the processes provide **SIGNIFICANT ASSURANCE WITH SOME IMPROVEMENT REQUIRED** to the Audit Committee.

Good practice

1. Effective oversight of GDPR is provided by skilled, knowledgeable staff including the IG Officer; the Head of ICT; the Human Resources and Transformation Manager; the Consultation and Improvement Officer; and, the Director (Corporate Services).
2. The majority of all expected policies and procedures are in place to support the Council's compliance with GDPR.
3. The Council has an effective information security framework in place that safeguards its systems and data against cyber threats.
4. Staff training is practically complete and GDPR awareness amongst staff is good.
5. Individuals are informed of their GDPR rights when contacting the Council and comprehensive Policy Notices are in place that advise the individual accordingly. These are clear and well written.
6. The Subject Access Request (SAR) process meets GDPR requirements and is in place.
7. The Data Security Breach Reporting process meets GDPR requirements and is in place.
8. The Director (Corporate Services) provides independent review of GDPR arrangements including data security breach reporting and, as a member of the Senior Leadership Team (SLT), provides strategic oversight.

Areas for development

1. Complete data mapping exercise to help develop an Information Asset Register (IAR) to identify and locate personal data. An IAR will also assist with the identification of those contracts that should be updated to reference GDPR requirements (**Medium recommendation**). *The Council are already taking steps to assess software tools to assist with this task*.
2. Update employee job descriptions to properly reflect their GDPR Roles and Responsibilities (**low recommendation**).
3. Complete the following documentation: Data Classification Policy and Data Protection Impact Assessments (DPIA) Procedure (**low recommendation**).
4. **Four minor improvement notes** were raised to tighten ongoing GDPR compliance arrangements further.

Recommendations

As we have concluded that the processes provide significant assurance with some improvement required, we have raised only one medium level and two low level recommendations and a further four improvement points to address the weaknesses identified.

	High	Med	Low	Imp
Detailed findings	0	1	2	4

Acknowledgement

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

Key Findings & Recommendations

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2

Risk Area	Findings and Recommendation	Action Plan
Processing of personal data is not appropriately governed – *this includes checking that your organisation has appropriately designated roles and responsibilities*.	**Key findings** ▪ GDPR initiatives are led by the Information Governance (IG) Officer who is supported by an IG Assistant and the Freedom of Information (FOI) Officer, both of whom have other non-GDPR duties. ▪ The IG Officer reports progress to the Director (Corporate Services) who as the Council's Monitoring Officer is also its Data Protection Officer, and hence the executive lead for GDPR. ▪ The Director, as a member of the Senior Leadership Team (SLT), will raise GDPR issues to the SLT as necessary. Currently, there is no standing item on the SLT's Agenda for GDPR issues that could be used to demonstrate continual oversight of GDPR compliance by all strategic officers. ▪ Job descriptions of key staff members responsible for GDPR arrangements have not been updated to include these additional GDPR responsibilities. **Recommendations:**	Actions: We will add a standard agenda item onto the SLT agenda on a quarterly basis which will show key issues / statistics on GDPR related maters. Responsible Officer: Julie Kenny Executive Lead: Due date: December 2018
	Issue identified: The SLT do not receive a formal update of the Council's GDPR compliance position. **Root cause:** GDPR has only recently come into effect and the Council is in the process of setting up ongoing compliance good practice**.** **Risk:** GDPR compliance may not be subject to regular on-going monitoring by the SLT who may only be notified when problems arise. **Recommendation:** The SLT Meeting Agenda should be updated to include a standing item on GDPR compliance. Statistics could be prepared by the IG Officer on behalf of the Director (Corporate Services) to present to the SLT. Such statistics could reference for example: the number of GDPR complaints received and dealt with; Subject Access Request (SAR) received & dealt with; Data Security Breach occurrence and actions taken; Staff GDPR training position, etc. **Overall conclusion:** SLT are aware of the GDPR position since the legislation is quite recent. Therefore we consider this to be an **improvement point only (number 1).**	

Key Findings & Recommendations

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2

Risk Area	Findings and Recommendation	Action Plan
Processing of personal data is not appropriately governed – *this includes checking that your organisation has appropriately designated roles and responsibilities*.	**Recommendations Continued:**	Management Response: Accepted. Job Descriptions of relevant staff will be updated. Recommendation 1: Responsible Officer: Julie Kenny Executive Lead: Due date: December 2018.
	Issue identified: Job descriptions of staff responsible for GDPR compliance have not been updated to properly reflect all their GDPR roles and responsibilities**.** **Root cause:** GDPR has only recently come into effect and the Council is in the process of completing all tasks to ensure ongoing compliance**.** **Risk:** Staff performance may not be effectively measured for a critical part of their job role and responsibility. This could mean that training needs are not identified. **Recommendation 1:** The job descriptions of all staff should be updated to properly reflect all their GDPR roles and responsibilities. **Overall conclusion:** Staff are aware of their job role and responsibilities since the legislation is recent as are the activities they undertook to ensure the Council complied with this legislation in time Therefore we consider this to be a **low risk recommendation.**	

Key Findings & Recommendations

In this section we set out the detailed findings arising from our work. Details of what each of the ratings represents can be found in Appendix 2

Risk Area	Findings and Recommendation	Action Plan
Collection of personal data is not conducted properly – *this includes checking that privacy policies are in place and assessing whether your organisation needs consent to collect personal information.*	**Key findings** ▪ There is a Data Protection (DP) Policy and at the time of our review it had been updated to reflect GDPR legislation. It will be authorized for distribution in January 2019 in accordance with the next policy review cycle. ▪ Data Privacy Notices have been incorporated into the forms used by each council service. Full Privacy Policies for each service are currently being uploaded onto the Council Web pages. ▪ We are satisfied that the Data Protection Policy is in line with expectations and best practice, and we have no significant findings to note other than to support the Council's endeavours to distribute it. ▪ Code of Conduct states in Section 31 and 31.1 Data Protection, that all staff must adhere to the Data Protection policy. Non adherence could lead to disciplinary action being taken which could result in staff dismissal. **Recommendation**	Actions: We do have an adopted DP policy already in place. https://www.hinckley-bosworth.gov.uk/downloads/file/855/hbbc_data_protection_policy The revision to incorporate GDPR is scheduled for the next reporting cycle which will be complete at Executive in February 2019.
	Issue identified: GDPR implications for Data Protection working practices and procedures have not been formally incorporated into the Council's Data Protection Policy and distributed. **Root cause:** GDPR has only recently come into effect and the latest version of the Data Protection Policy has not been formalised because of the need to be in time with the next policy review cycle. **Risk:** GDPR high profile may be harder to maintain if the Council relies upon GDPR training alone and the message of compliance could therefore loose some visibility. **Recommendation:** The Data Protection Policy is formalised and approved by strategic officers and Members in accordance with the next review cycle. **Overall conclusion:** Overall the GDPR message remains visible with recent staff training and public awareness promoted by the Government. We therefore we deem this to be an **improvement point only (number 2).**	Responsible Officer: Julie Kenny Executive Lead: Due date: February 2019

Key Findings & Recommendations

Risk Area	Findings and Recommendation	Action Plan
Processing of personal data is not conducted responsibly – *this includes making sure relevant members of staff have been trained to understand what they can and cannot do with personal information.*	**Key findings** ▪ GDPR training has been provided by a third party provider CYLIX to 77 out of 80 managers. Non-management staff GDPR training has been provided via the E-learning portal. Refresher training is due to be scheduled to ensure that staff remain vigilant. ▪ The possibility of using IT security reminders as a means to ensure that GDPR retains a high profile at the Council had not been considered. ▪ Council Members have received GDPR training and further training will be provided following the Councillor elections in 2019. **Recommendation**	Actions: Accepted. The possibility of such messages will be explored with the Head of ICT. Responsible Officer: Julie Kenny Executive Lead: Due date: February 2019
	Issue identified: GDPR reminders to staff are reliant upon training only. **Root cause:** GDPR has only recently come into effect and the Council is in the process of setting up ongoing compliance good practice**.** **Risk:** GDPR high profile may be harder to maintain if relying upon training alone and the message of compliance could loose visibility **o**ver time. **Recommendation:** The IG Officer should liaise with the Head of ICT to explore the use the periodic security messages that are currently issued to all staff to also highlight GDPR issues and reminders. **Overall conclusion:** Since the legislation is recent, we found that the GDPR message was still clearly understood by staff at the time of this review. Therefore we deem this to be an **improvement point only (number 3)** to re-inforce the GDPR message going forward.	

Key Findings & Recommendations

Risk Area	Findings and Recommendation	Action Plan
Processing of personal data is not safe – *this includes establishing the appropriate technical and organisational measures in place.*	**Key findings** ▪ The Council has adequate facilities in place to enable staff to securely transmit personal data. ▪ The Council has established adequate IT Security related policies and procedures that cover all IT activity supporting GDPR compliance (please see Appendix A for complete list). ▪ The Council takes the relevant steps to safeguard it's network, infrastructure and systems. Independent assurance of this is provided by its Public Sector Network (PSN) Code of Compliance Certificate that enables it to connect to the Government's network. In support of this, the Council must provide details of an annual independent network penetration test that is then subject to review by the Government's own security expert inspectors. ▪ The Council does not have an Information Classification Policy that would assist staff in the proper handling of such data and hence ensure that the arrangements to capture, store and maintain the data is sufficient in accordance with its classification. ▪ GDPR requires that information classified as 'Personal' should be subject to Data Protection Impact Assessments (DPIA) to ensure that it is properly managed by the organisation holding such data. However, only one DPIA has taken place (for the Waste Management IT System). The DPIA Policy is in draft but once formalised, it will provide a framework where new processes are assessed to ensure they meet privacy, confidentiality and Data Protection requirements. **Recommendation**	Management Response: Recommendation 2: Accepted. We will ensure a Data Classification Policy is adopted. Ideally this will be part of the main Data Protection Policy, rather than a separate document. Responsible Officer: Julie Kenny Executive Lead: Due date: March 2019. Due date:
	Issue identified: There is no Data Classification Policy and the DPIA Policy is in draft. **Cause**: The Council has not defined a Data Classification Policy nor informed staff of how these classifications would impact the management of its data. R**isks:** Staff may not handle data appropriately which could give rise to, for example, inadequate security measures being deployed when transmitting data. It could also mean that the risks associated with handling personal data are not assessed **Recommendation 2:** A Data Classification Policy should be written to comply with the Government's own recommended data classifications. This Policy should also reference the need to undertake DPIA for personal data and cross reference to the DPIA Policy, which should also be formalised. Once both policies have been ratified, training should be provided to all impacted staff. **Overall conclusion:** Staff awareness of the need to properly handle Personal data is currently high since this legislation is recent. In addition, staff have also received sufficient Information Security training and guidance on the treatment of such data. We therefore consider this to be a **low risk recommendation.**	

Key Findings & Recommendations

Issue	Findings and Recommendation	Action Plan
Quality of personal data is not maintained, is not up to date and relevant – *ascertaining how well your organisation effectively manages its information assets.*	**Key findings** ▪ No data mapping exercise has been completed to identify what personal data is held or where it is located.. This exercise would help complete the Information Asset Register (IAR). ▪ An IAR can be used to identify those organisations with whom personal data is shared which allows for the timely review and update (as necessary) of contracts supporting such activity. The Council is currently reviewing contracts as they come up for renewal. ▪ The ICT function is outsourced to Sopria Steria under a managed service. The Head of ICT is responsible for the four local authorities under a Leicestershire Partnership arrangement which includes Hinckley & Bosworth Borough Council. A contract variation has been signed with Sopria Steria with regards to meeting the Council's GDPR requirements. ▪ The Head of ICT confirmed that software (Veronis) is being trialled to assess how effectively it can assist the Council in the identification and location of personal information. This software can provide each System Owner with details of what personal data is held on their systems which can then be used to verify whether they are GDPR compliant (with respect to the collection, rectification, storage, retention and disposal of such data). ▪ The Retention Schedule is being developed and is to be aligned with the Local Government Association (LGA) guidelines. The Schedule is based upon Kent County Council's retention schedule and is contained within the LGA Inform Plus System used by Hinckley & Bosworth Borough Council. Consequently, there is no overall Retention Policy in place. The IG Officer confirmed that both the Retention Schedule and Policy will be developed by September 2019. **Recommendation**	Actions: We will give consideration to such software. The retention schedule will be complete by September 2019. Responsible Officer: Cal Bellavia Executive Lead: Julie Kenny Due date: September 2019
	Issue identified: The Retention Schedule and overarching Retention Policy have not been completed. **Root cause:** GDPR has only recently come into effect and the Council is in the process of setting up ongoing compliance good policies and procedures including those that relate to the retention of personal data. **Risk:** Staff may fail to properly retain personal data in accordance with the GDPR and/or fail to act consistently. **Recommendation:** The IG Officer should complete this documentation and arrange for its approval and distribution. Staff should be trained accordingly. **Overall conclusion:** Activity is already underway to deliver this documentation. Therefore we deem this to be an **improvement point only (number 4).**	

Key Findings & Recommendations

Issue	Findings and Recommendation	Action Plan
Quality of personal data is not maintained, is not up to date and relevant – *ascertaining how well your organisation effectively manages its information assets.*	**Recommendations (Cont.)**	Management Response: Recommendation 3: We will give consideration to such software.
	Issue identified: The Council has not completed the exercise to document an IAR. An IAR is used to identify what personal data an organisation has and officers are currently reviewing contracts as they come up for renewal rather than focussing initially upon those that involve personal data. The need to complete an IAR has been described as a mitigating factor to address Risk S50 (GDPR compliance) on the Council's Risk Register. **Cause:** Data mapping exercise has not been completed to identify and locate personal data that would be recorded in an IAR. **Risks:** The Council may not easily determine whether personal data is being managed in accordance with the GDPR. It may also mean that the Council does not respond promptly to a Subject Access Request (SAR) or in the event of a data security breach, quickly identify what personal data has been affected. It may therefore fail to meet its statutory obligations. **Recommendation 3:** The Council should complete the exercise to identify and locate all personal data and record this in an IAR. This exercise can be supported by the use of software tools such as Varonis to construct/inform an IAR. This can then be used to identify and review those contracts that involve personal data. **Overall conclusion:** The failure to comply with the GDPR could give rise to a fine being imposed by the Regulator leading to financial loss and reputational harm. Therefore, we deem this to be a medium recommendation.	Responsible Officer: Cal Bellavia Executive Lead: Julie Kenny Due date: September 2019.

Key Findings & Recommendations

Issue	Findings and Recommendation	Action Plan
People are not given their information rights – *checking what procedures in place to handle information rights requests properly*.	**Key findings** ▪ The Council has developed Privacy Notices that cover all potential activities where an individual may contact the Council for advice, guidance etc., please see Appendix A for the complete list. ▪ Individuals are informed of all their GDPR rights. These include: – the right to see their data (they are informed that this is called a Subject Access Request (SAR); – the right to correct that data (rectification), erase it, restrict it, object to its use as well as their data portability rights etc. ▪ The Council has developed a comprehensive SAR Process that is supported by working practices and procedures and all relevant documentation. ▪ All SAR's are received by the IG Officer who raises these with the relevant Business Owner who, in turn, has access to a system administrator (SA) for each of their applications. The SA will interrogate the system and provide the required details to the Business Owner and IG Officer. **Recommendations:** None to date.	Not applicable

Key Findings & Recommendations

Issue	Findings and Recommendation	Action Plan
Personal data is not shared, disclosed, or transferred securely – *establishing what arrangements there are to ensure the personal information your organisation is responsible for remains adequately protected, wherever it is located.*	**Key findings** ▪ ICT maintain information security policies and measures to ensure ongoing compliance with GDPR and good security practice. These include the following IT solutions: anti-virus protection; web use monitoring; internet monitoring; Active Directory audit monitoring tool; security tools to assess the network; robust firewall for the network's perimeter; patch management processes to maintain defences; annual penetration testing with the last test undertaken in 2017 and the next scheduled for November 2018. ▪ The Council has established adequate IT Security related policies and procedures that cover all IT activity supporting GDPR compliance (please see Appendix A for complete list). The overarching Information Security Policy has been approved and published in April 2018. ▪ Adequate Data Security Breach Policy and Procedures are in place, including a Data Security Breach Log used to identify any instances where data may not have been transferred securely. Currently, a Data Security Breach Form is completed by the IG Officer following an investigation which is independently reviewed by the Director (Corporate Services). The Director as the Council's Monitoring Officer, Data Protection Officer and GDPR Lead, will then decide on the appropriate notification (for example to individuals and the Regulator). ▪ All staff have received training in the application of the Council's information security policies and procedures as well as any supporting tools to facilitate the proper safeguarding of personal data. **Recommendation** None to date.	Not applicable

Appendices

Appendix 1: Staff Involved & Documents Reviewed

Staff Involved

- Julie Kenny – Director (Corporate Services)
- Faye Biddles – Information Governance (IG) Officer
- Julie Stay – Human Resources and Transformation Manager
- Mike Dungey – Head of ICT
- Cal Bellavia – Consultation and Improvement Officer

Documents Reviewed

- Business Continuity (BC) & Disaster Recovery (DR) Plan
- Contract sample (Gatherwell)
- Cloud Storage Policy
- Code of Conduct
- Contractor Compliance Form & Letter
- Corporate Mobile Device Policy
- Data Breach Procedure & reporting documentation
- Data Protection Policy
- Disciplinary & Grievance Policy
- Disposal Policy
- GDPR Working Group documentation
- Information Governance Framework
- Isolation LAN Policy
- IT Acceptable Use Policy
- IT Asset Management & Procurement Policy
- IT Change Management Policy
- IT Disaster Recovery Plan
- IT Security Policy
- IT Starters & Leavers Procedure
- Job Application Guidance
- Job Descriptions of key staff: Director (Corporate Services), Head of ICT, IG Officer, Consultation & Improvement Officer
- Laptop & Mobile Device Policies

Appendix 1: Staff Involved & Documents Reviewed

Documents Reviewed (Cont.)

- Privacy Notices: Business Rates, Council Tax, Customer Services, Environmental Services, Finance, Housing, HR, Legal, Neighbourhoods, Planning, Waste Management
- Privileged Users Policy
- PSN Code of Compliance Certificate
- Records Retention Schedule
- Recruitment & Selection Policy
- Replacement Policy
- Risk Register
- Security Incident Policy
- Security Monitoring Report (August Working Group documentation
- Social Media Policy and Guidelines
- Subject Access Request (SAR) Policy
- SAR documentation (SAR Form, acknowledgement & exemption letter)
- Technical Evaluation Questionnaire
- Your Rights (Web)

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