Company X
Data Protection Audit Report
Final

Auditors:	XXX	(Lead Auditor)
	XXX	(Engagement Lead Auditor)
	XXX	(Secondary Auditor)
Distribution:		Final
Report:	XXX	Director, Business & Law
	XXX	Director (Business)
Date Issued:		20 January 2019

Contents

Visit ref/Type/Date/Duration	Regulation / Standard	Site address
DR4/2018/812 Data Governance& GDPR Audit 31/03/2015 2 day(s) No. Employees: 215	(EU) 2016/679 (GDPR) ISO/IEC 27002:2013 NIST Big Data Reference Architecture	Company X XXXX XXX Road London XXX United Kingdom

Executive Summary

This document records the key findings of a Data Governance Audit of COMPANY X on 29th September 2018 against the requirements of the General Data Protection Act (EU) 2016/679 in relation to a data sharing agreement XXX covering COMPANY X and Commercial Data Supplier COMPANY Y; provided in pseudonymised format. This audit was conducted using approved and mature methodology based on ISO standard 19011:2011 (Guidelines for auditing management systems) and follows the same format for all audits of Data Sharing Agreements conducted by Data Risk Foresight.

In total, X number of Minor Nonconformities were raised; successful resolution will significantly contribute to attaining GDPR compliance.

- Information governance activities must be further developed (Minor)
- Add audit outcomes and risk assessment / treatments as standing agenda items at Commercial and Production meetings (Minor)
- Establish a procedure for ongoing compliance with legal regulatory changes through a clearly identified procedure and owner (Minor)
- Establish a set of quality objectives for products provided (Minor)

Areas of Good Practice

- Data destruction policies and procedures are in place with safe storage systems practiced

- Recruitment, retention and ongoing training development processes are particularly rigorous in demonstrating resourcing competency
- Documented requirements for second party provision of services to COMPANY X are sound
- Double suppression of Small Numbers provides extra assurance of security around patient identification

The Audit Team did not witness any breaches of current data sharing (DS) or data re-use agreements (DRA). In summary, it is the Audit Team's opinion that at the current time and based on evidence presented on the days attended, there is minimal risk of inappropriate exposure and / or access to data provided by COMPANY X and its third party commercial data supplier under the terms and conditions of the data contract legally signed by both parties, nor in re-use of the data by Company X in its operational activities under the requirements of the GDPR.

1. About This Document

1.1 Introduction

The both the GDPR and the UK Health and Social Care Act 2012 contains a provision that those companies providing functions related to the provision of social care to minors and especially vulnerable minors, in England handle confidential information appropriately.

Company X undertook a review of data use and a report produced by Company X's Data Protection Officer, XXXXXX recommended that Company X should implement a robust data audit and governance function that will enable ongoing scrutiny of how data is being used, stored and deleted by those receiving it.

In September 2018, Company X commenced a programme of external audits with third party organisations with which it holds DSAs. The established audit approach and methodology is using feedback received from the auditees to further improve Company X's data audit function and its internal processes for data dissemination, to ensure they remain relevant and well managed.

Audit evidence was evaluated against a set of criteria drawn up by Company X's Data Protection Officer based upon the requirements of the GDPR, together with DSAs signed by the relevant contractual parties and the international standard for Information Security, ISO 27001:2013 and the ISO22301 Business Continuity Management standard.

The Information Commissioner (ICO) may, with the consent of a company's data controller, assess the extent to which good practice is applied when processing personal data and can then inform the data controller of the results of the assessment. The Information Commissioner sees auditing as a constructive process with real benefits for data controllers and so aims to establish, wherever possible, a participative approach.

An Assessment Notice is the medium through which the Information Commissioner's Office (ICO) will seek to instigate a compulsory audit. However, the Assessment Notice Code of Practice, in the interests of clarity, distinguishes between compulsory and consensual audits.

Company X suffered a reported delay in providing copies of personal data in response to a Subject Access Request in July 2018, and related correspondence between Company Xl and the ICO. It was therefore subjected by Company X's Data Protection Officer that Company X may benefit from an ICO data protection audit.

Company X then agreed to a consensual audit by the ICO of its processing of personal data. Following the audit by the ICO, Company X has contracted Data Risk Foresight to assist in a more detailed data control audit and in the provision of training and developing data governance frameworks for its ongoing use of personal data across its operational locations.

An introductory meeting was held on the 29th September 2018 with representatives of Company X's senior management team, to identify and discuss the scope of the audit, data strategy and future technology use that may impact upon data protection and GDPR compliance.

1.2 Background

COMPANY X was launched in January 2006 in response to the growing need in the marketplace for the provision of secure accommodation for minors who had no alternative and were identified as being vulnerable or potentially vulnerable.

The company was acquired by the Company Z in 2012, which currently operates in ten geographical locations within the UK,. COMPANY X Ltd is one of three companies that sit inside Company Z. Other companies within this division are Company A and Company B.. Company X utilises data received from all operating companies within the group, as well as from outside commercial data suppliers. The data is used only in England, however the data is requested from overseas suppliers for the purpose of recruiting personnel who are required to have thorough background checks made prior to engagement. The client base is primarily located around major UK cities and has an age range of 12-24 years old. The number of geographic locations currently stands at 23, with 1200 staff who work on a part-time, full time 3-shift basis.

COMPANY X specialises in the provision of secure accommodation as a subcontracted company of local authorities, who are under a legal obligation to provide such secure accommodation. The company continues to expand and data is shared increasingly between the operating companies, as well as local authorities and government agencies outside of the UK.

Due to the nature of the data and the clients, Company X is seeking to certify for ISO 9001 (Quality Management) certified and is moving towards ISO 27001 (Information Security), the logical next step is for COMPANY X to use the findings from this audit as a catalyst to progress towards ISO certification. Company X is concerned that the data use and protection under ISO27001 will still leave it vulnerable to failing to comply with all the provisions of the GDPR.

Additionally, the senior management intend to utilise data on an increasing basis to facilitate further expansion of the group, in particular, with exchanging of personnel and clients between locations and consequent data transfer, storage, deletion and use issues. Senior management are seeking a set of data governance and stewardship frameworks to be developed in conjunction with Data Risk Foresight to enable suitable training, policies and procedures to be put in place for ongoing regulatory compliance.

1.3 Purpose

This report provides an evaluation of how COMPANY X conforms to the requirements of the GDPR and Health and Social Care Act 2012, covering the provision of statistics to local authorities, Resident Statistics (RS) and Office of National Statistics (ONS) data. The document provides a summary of the key findings.

1.4 Areas Assessed and Findings

Opening Meeting:

The formal opening meeting included the objective of the assessment, methodology and terminology used, confidentiality, number of staff in scope, purchase order details (not required), and the agreed assessment plan.

Company Overview – Organisation Context, Interested Parties and Scope / Leadership / Compliance:

Company X is regulated by a number of national, local and child protection laws, as well as by the GDPR for personal data. The company employs a large number of personnel from overseas locations, both within the EU and outside of it. Requests for personal data are therefore made to commercial and governmental entities for personal data relating to areas required under UK law to be addressed when employing an individual to provide care, housing to vulnerable minors.

Company X has a turnover of about £XXM. Company X stores both paper-based and electronic based data at multiple locations

Interested parties have been identified which include clients, third party organisations, employees, shareholders, regulated authority departments, the Office of National statistics, the ICO, business partners healthcare professional etc.

Their needs and expectations have been clearly captured within this audit. The Operations Director and CISO have the overall authority and responsibility for the control and management of data within the group. The Data Protection Officer has the responsibility for the creation, maintenance and enforcement of data policies and procedures, and reports directly to the Board in respect of regulatory compliance and has overall authority for maintaining it.

1.5 Non-Conformities and Observations

Where a requirement of either the GDPR, or the audit criteria was not fulfilled, it will be classified as a Major Nonconformity, Minor Nonconformity or Observation.

1.5.1 Major Nonconformity

The finding of any of the following:

- The absence of a required process or a procedure
- The total breakdown of the implementation of a process or procedure
- The execution of an activity which could lead to an undesirable situation
- Significant loss of management control
- A number of Minor Nonconformities against the same requirement or clause which taken together are, in the Audit Team's considered opinion, suggestive of a significant risk

1.5.2 Minor Nonconformity

The finding of any of the following:

- An activity or practice that is an isolated deviation from a process or procedure and in the Audit Team's considered opinion is without serious risk

- A weakness in the implemented management system which has neither significantly affected the capability of the management system or put the delivery of products or services at risk
- An activity or practice that is ineffective but not likely to be associated with a significant risk

Observations

Type	Area / Process	Clause/Regulation
Observations:	Risk Assessment – General Information Security Risk Assessment / Information Security Risk Treatment and Statement of Applicability	ISO27002 6.1.3
Scope:	ISMS and GDPR Appropriate Controls	
Details:	There was no evidence that residual high-level risks have been signed off. However, this could not be raised as a non-conformance because on 23/03/2015, ITG conducted an internal audit on behalf of COMPANY X and this was picked up as per clause 6.1.3. COMPANY X is yet to review this in the next review meeting. COMPANY X must ensure that mechanisms are in place to ensure that high residual risks or high risks in general are signed off appropriately.	

Context of the Organisation

The Context of the organization has been defined within the GDPR, ISMS manual and Health and Social Care Act 2012 that articulate the internal interfaces which include (Education: Communications: Finance: Fitness to practice:: HR IT: Operations: Policy & Standards: Post Delivery: Secretarial & Service and Council): Council, and the Third party interfaces include (Suppliers: Partners: Software Licensing: Consultants Professional Services: Landlord: Local Authority: Hosting Suppliers: Telecomms: Professional Service Suppliers and Regulator).

The needs of the these interested parties has been considered and the system scope is seen to be appropriate to the business needs and any issues identified have been directly feed into the risk assessment.

Resources

Defined resources and consultancy services have been available for the implementation of the GDPR and ISMS projects. Resource are also in place for the ongoing support of GDPR and ISMS and responsibilities have been allocated for the management of Data and Information Security. All staff have job descriptions and the minimum skill level for each position has been defined allowing staff competencies to be determined and reviewed

Staff screening relies mainly on two completed references, however some of this can be limited and there may be benefit from looking at a more effective way of conducting staff background checks.

All staff complete CBT training on Data Protection and Information security and there is a security culture developing with the use of posters and security campaigns at all operational locations within their administrative offices and other staff areas.

- Lots of security posters distributed through the company.
- Action Forms List: to be used when employees do not comply with security rules; different templates, depending on the issue.

ISMS monitoring

IT systems are monitored and a monthly report identifying pertinent measures for IT systems, the overall view of IT is a well

controlled and mature operation.

Management Review

A comprehensive monthly meeting is completed and this forms the bases of the management review as all the requirements from the GDPR and Health and Social Care Act 2012 regulations are included in the monthly meetings.

Internal audits

A programme of internal audits has been established, with the frequency of these being every quarter for the outset and with this being anticipated to be changed to bi-annually and an initial 12 month period. It was recommended that the frequency be maintained at quarterly reviews, with biannual audits being more comprehensive in nature.

1.6 Audience

This document has been written for the Managing Director of Company X. A copy will be made available to the local authorities in each geography in which Company X operates. Additional internal distribution will be to the relevant personnel identified by the Managing Director. The report will be published in a publicly available forum controlled by the relevant local authority.

1.7 Scope of the Audit

Following pre-audit discussions with Company X's senior management, it was agreed that the audit would focus on the following areas:

a. Data Protection Governance - with specific reference to data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor GDPR compliance.

b. Training and Awareness - the training and awareness of staff of data protection & information security related policies and procedures, including the storage, use and security of personal data, and how to report security incidents.

c. Records Management - the policies and procedures in operation to manage the manual and electronic records containing personal data, including creation, maintenance, storage, movement, retention and destruction as well as security.

d. Subject Access Requests - the policies and procedures in place to ensure subject access requests are processed in accordance with the requirements of the GDPR.

e. IT Security - The controls in place to ensure adequate protection is applied to personal data processed via the organisation’s IT systems.

1.8 Audit Team

The Audit Team was comprised of a certified General Data Protection Regulation (EU) 2016/679 (GDPR) practitioner, certified Big Data Professional and ISO 27001:2013 (Information security management systems) auditor.

The audit was conducted in accordance with ISO 19011:2011 (Guidelines for auditing management systems), ISO27002:2013, and GDPR gap analysis.

2. Audit Findings

2.1 Audit Opinion

The primary purpose of the audit is to provide the Senior Management of Company X and a number of local government authorities with an independent assurance of the extent to which Company X, within the scope of this agreed audit is complying with the GDPR.

The recommendations made are primarily around enhancing existing processes to facilitate compliance with the GDPR.

Overall Conclusion	
Limited Assurance	The arrangements for data protection compliance with regard to governance and controls provide limited assurance that processes and procedures are in place and are being adhered to. The audit has identified scope for improvement in existing arrangements and appropriate action has been agreed to reduce the risk of non-compliance. We have made one ‘reasonable’ assurance and four ‘limited’ assurance assessments, where controls could be enhanced to address the issues which are summarised below and presented fully in the ‘detailed findings and action plan’ section 7 of this report along with management responses.

2.2 Access Controls

COMPANY X has established a management framework to control the implementation and use of data received from a number of overseas bodies and commercial entities, as well as data relating to the vulnerable minors in the accommodation provided by Company X. A GDPR data protection and an Information Security Policy are in place, with named senior personnel within the organisation responsible for adherence to this policy. All staff appear to go through an effective, rigorous and documented induction and personal development cycle.

There is a need to improve the active management of the internal named or authorised user directory to ensure that only the most current version of the document is used, reflecting all information regarding starters and leavers.

Evidence was provided to demonstrate that only the staff named within the GDPR policies had access to data. Access to digital records is through a secure login protocol which provides an audit trail of activity.

Data is held in a secure data warehouse which is separate from the operational personnel IT system. A separate analytical tool is used by analysts to interrogate multiple fields of information prior to the provision of a placement of a vulnerable minor within the properties owned by Company X. Care workers employed by Company X are registered with the Association of Social Care Workers (ASCW) and they work towards ASCW professional certification.

Personnel log on verification is controlled and recorded by the system. The IT service team provide single point of contact to access the information.

Controls with regards to third party suppliers of products and / or services are in place and documented; suppliers did not have access to actual, only mock/audit test data.

Company X provided lists of authorised users who receive separate notification of their user names and passwords.

The audit trail of user activity appears to be well controlled.

As some activities can be handled at sister companies, COMPANY X should consider changing the GDPR policies and procedures so that the wider group is aware of corporate responsibilities for data sharing.

Conclusion: Access Control and associated login methodology used to gain access to public facing and secure data seems well managed and there appears to be minimal risk of exposure to unauthorised / inappropriate access to data.

2.3 Information Transfer

Receipted information is initially collated in a secure server before being transferred to the public facing / end user interface. All testing and development of data models for use

by subscribers and / or public view is managed in the secure environment and taken through a Quality Assurance process under the management of a named individual prior to release.

The public facing web portal provides only aggregated data through a Quality Dashboard as a snapshot of information at any given point in time. COMPANY X personnel wishing to access governmental Trust-level information can only do so through obtaining the relevant inscription credentials. Personnel must request the HR manager who will then inscribe the individual. The HR manager must submit the names of those employees who have been authorised to access Trust-specific information.

All Small Numbers which may identify an individual undergo a double lock-down procedure to ensure that any sensitive information cannot be inferred whether at an individual or aggregate level.

Conclusion: Information passing over public networks is protected from fraudulent use, modification, disclosure, misrouting and duplication. There is no direct link between public facing tools and information and the source sensitive personal data which is managed on a separate secure environment.

2.4 Disposal of Data

The GDPR policy and procedure specifically refers to a requirement to provide confirmation in writing of secure disposal.

Data destruction policies, procedures and guidelines based on the best practice guidelines on data destruction from the Health and Social Care Act 2012 are in place. The policy references disposal through in-house pattern wiping software and shredding / disintegration.

A documented procedure for the import of sensitive personal data has been written though lacks configuration management and version control. There is a stated requirement to provide written confirmation to the local authority that data has been securely disposed.

Records of destruction are auditable through the internal user and activity logs available through the system. However, due to time constraints, the Audit Team did not see evidence; this will be followed up at the next audit visit.

Conclusion: The safe handling of information from import to disposal, including record keeping has been demonstrated. However, evidence of destruction will be a priority at the next visit.

2.5 Pseudonymisation and Anonymisation

Cryptography Policy: the CISO is responsible for authorising any changes. COMPANY X encrypts data as required on a risk-based approach. 128-bit encryption is the current standard for all encryption in the company. A secure password store is used to store encryption keys for all encrypted datasets or objects. Key generation is managed by the IT department using suitable tools and methods. For the public facing websites, key generation is carried out by an independent certificate authority. The policy for transfer of files via removable media and email is covered in the IT Policy.

Where encrypted files are sent to outside organisations, password should be communicated in a secure manner. KeyPass application is used for Key management for the systems.

2.6 Risk Assessment and Treatments

A Risk Register is in place as required by the Health and Social Care Act 2012, but is still in its early stages and should be amended to include version control. Control measures, owners, improvements and target delivery dates were present though not all fields within the log are complete or up to date.

There is a process in place to review the Risk Register on a quarterly basis; the next review is due at the end of November and will be confirmed at the next audit meeting.

A risk-based audit programme should be established in order to facilitate the organisation's progress towards the stated objective of ISO certification.

Conclusions: Risk Management is present but embryonic. It requires further development to demonstrate that active mitigation is in place.

2.7 Operational Planning and Control

Use of sensitive private data received seems to be well managed and controlled and demonstrated products were seen to be fit for purpose with regard to end user requirements.

Peer review mechanisms established for Quality Assurance and compliance purposes are stored on a separate directory. User Acceptance Testing is secure and managed by named individuals. All development and analysis arising from products using source

data was Quality Assured through a senior named officer; a dedicated QA role is to be implemented shortly. COMPANY X should ensure that governance activities are built into all key stages of projects.

Local authority satisfaction surveys have been carried out regularly though a third party and the development lifecycle is reviewed and influenced by the local authorities. Outputs are reviewed at GDPR and IS meetings to effect improvements and data privacy redesign. GDPR meetings seem to be working well as a management review forum but should consider audit outcomes and risk assessments / treatments as standing agenda items.

It is noted that there are established relationships with local authorities and a LinkedIn User Group though COMPANY X may wish to consider how the end user Help Desk can establish and monitor comments made online. The next audit visit will consider how well the information gathered from personnel is used to inform data protection performance and service provision.

- The absence of version control in all documents requires addressing.
- The public facing tool acknowledges which overseas organizations are the source of data supplied as part of HR activities.
- COMPANY X should consider the best way to ensure ongoing compliance with legal regulatory changes through a clearly identified procedure and owner.
- COMPANY X should consider how best to establish a set of quality objectives for products provided (follow-up at next audit meeting).
- Documented policies stated as being in place, but not seen by the Audit Team due to time constraints, will be followed up at the next visit:
  - Staff training records and competency checks
  - Performance evaluation measurement analysis and monitoring

- Annual Business Plan
- Information Asset Register
- Business Continuity Plan
- Change control process

Conclusions: The business would benefit from being recognised as a secure and trusted data manager / provider; ISO 27001 certification would assist in achieving this objective. It is recognised that resources may be required to achieve certification.

2.8 Physical Security

The client occupies 23 buildings around the UK. The following controls were seen to be in place:

Manned entrance
Visitors Log
Coloured lanyard cards
Secure print
Shredders
Secure waste bins
Double entrance doors
CCTV surveillance system
Access control buttons on doors
FOB access to each building

Filing cabinets
Fire alarm system
Intruders alarm system
Computer locks
Swipe on / off cards to doors and elevators
Safe storage boxes to transfer information
Security bars on windows
Fire extinguishers
Screen blockers in the Registration area
Limited access to computer room.

The following maintenance records were reviewed:

Fire alarm as of 01.4.2017
Health and safety risk assessment as of 27.05.2018
Facilities Risk assessment
Pat testing as of 01.02.2016
Annual service for extinguishers as of 11.05.2015
Electrical installation condition report as of 18.06.2015
Periodic inspection report as of 20.04.2018
UPS maintenance log as of 17.09.2017

The following exceptions were noted:

During the visit in the Fitness to Practise two unattended working stations were noted without applying screen lock as per Policy requirements X1 Tidy Desk Policy/X2 "All devices including mobiles laptops should be locked when not in use" & X3 "If you intend to leave any computer switched on and unattended in the office at any you must lock your computer screen". See minor NC raised below.

Maintenance records were made available at the time of the assessment. The guide confirmed that the Facilities Manager was not onsite and other staff could not provide the records. Maintenance records dated 20/07/2018 for air conditioning were sampled. Cabling in server room was seen to be in an untidy manner. See observation raised below.

Observations

Type	Area / Process	Regulation / Clause
Observations:	Physical Security	Art 24.
Scope:	GDPR	
Details:	Access control to the server room is inadequate to prevent unauthorised entry	

3. Audit Approach

3.1 Documents Reviewed:

Documents reviewed included:

1. DOC XXX Compliance & Redundancies (23/01/2015)
2. DOC XXX ISMS Manual
3. REC XXX 1 List of Legislation & Regulations
4. Risk Register & Risk Treatment Plan (March 2018)

3.2 Tour Facility

2.1 The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

2.2 The audit field work was undertaken at each location operated by Company X, between 1st August 2018 to 15th November 2018.

2.3 The final audit field work was undertaken at Company X's London Headquarters on 16 to 18 November 2018.

3.3 Senior Management

The Director of Operations was interviewed to gauge top management's commitment to the ISMS and also COMPANY X's drivers for GDPR and data governance compliance. Drivers include: Assurance to local government authorities and the general public; securing personal/sensitive data; protection and preservation of CIA; implementing appropriate controls etc According to the Managing Director, COMPANY X considers the following as the biggest risks to non-compliance with the GDPR:

- Not securing personal data of the vulnerable minors residing at the properties of Company X
- Not complying with the GDPR in relation to flows of personal data as part of the hiring process
- Unable to embed information security awareness into COMPANY X's culture
- Human error

As a business, Management has ensured that its data protection and information policy and objectives reflect its strategic direction. The needs of the business informed the setting of the objectives. The objectives, policies etc are all channelled to employees through the Senior Management Team (SMT). Please note that the Managing Director explained the overview of the company and its context. The import of this can be read in the above section on "Company Overview".

3.4 Assessment Participants

On behalf of the organisation:

Name	Position
XXX	Head of Business Process Development
XXX	Information Risk Manager

XXX	Director of Service Operations
XXX	Head of HR
XXX	Assistant Data Protection Officer

The assessment was conducted on behalf of Data Risk Foresight by:

Name	Position
Dr. Phillip King-Wilson	Lead Auditor and Compliance Consultant

3.5 Supplier Relationship

Engagements with third party requires a confidentiality agreement to be signed before any services can be supplied. All contracts contain security requirements and new suppliers undergo an audit before approval. Performance is monitored and no third party supplier has direct access to the information of COMPANY X. Procedure XXX was verified.

3.6 Closing Meeting

The closing meeting was conducted and the report findings summarised satisfactorily to those present. No comments on the report were received. The Data Risk Foresight standard approach including confidentiality, nature of sampling, appeals process (if required), and any forward actions following this assessment were confirmed. The next visit planning arrangements were reviewed and confirmed.

4. Summary of Audit Findings

4.1 Areas of Good Practice.

- There was evidence of a corporate awareness of some current data protection non-compliance issues, supported by a willingness to act on ICO recommendations, in order to improve practices and support compliance with the GDPR within Company X.

- Staff indicated a good level of awareness regarding the security and confidentiality of personal information.

- There is an agreed mutual monthly password scheme between Company X and the Local Authorities, for sharing personal information on individuals, for example, over housing issues. This provides additional security to prevent disclosure of personal information to those unauthorised to receive it.

- There is an established framework for assessing and managing risk within Company X, led by the Internal Risk Manager (Audit & Improvement).Data protection issues are considered and risk rated annually, although some improvements are required to the reported duties of Information Risk Owners.

- There is an effective level of IT security that includes an annual IT health check, strong access controls, encrypted laptops and pen drives, secure remote access to council networks, and the professional and certified removal and destruction of personal data on IT equipment.

4.2 Areas for Improvement.

- The data protection framework should be strengthened by the provision of reporting mechanisms to the Data Protection Officer (DPO) on data protection compliance, including SAR performance indicators, in line with Company X's Legal Responsibilities Policy (paragraph XXX).

- The introduction of a governance, stewardship, or steering group, which meets periodically and includes the Information Security Manager, Risk Manager, DPO or other roles as appropriate, may assist in the identification and mitigation of overlapping issues and in providing assurance on corporate data protection compliance.

- Specific data protection training and further refresher training should be provided to ensure that staff handling personal data are aware of all of the data protection principles, which apply to all aspects of their processing of personal information and to ensure that Company X complies with legislative requirements.

- Policies relating to the Records Management of personal data should be established, in line with current proposals by Company X to develop records management policies based on those in other Councils, and overall management responsibility for records management allocated to a senior position.

- An annual summary of security incidents involving personal data and system processing personal data should be reported to the Data Protection Officer and other relevant staff such as the HR Manager.

4.3 Risk Management and Asset Control

COMPANY X maintains a single inventory of information assets which is subdivided by asset owners into separate asset groups. Changes to identified risks are reviewed and agreed at the monthly Senior Management Team meetings (this also serves as the Management Review Meetings). Residual risks are implicitly accepted for current risks at SMT meetings.

The organisation maintains a risk assessment & treatment document. This well reviewed during stage 1 assessment and also in this assessment. The focus now was to look at COMPANY X's implementation of its risk assessment and treatment process. Risks have been identified, analysed, evaluated and treated using criteria. The risk methodology used is well structured. Owners have been assigned to identified risks with clear criteria and guidelines. COMPANY X uses 3rd party tool "Verisk" in managing its initial risks, treatment and SOA. COMPANY X also manages its risk in a manual document and the outcome forms part of the monthly rep ort for the EMT.

The SOA reviewed dated 21/08/2018 included control objectives and the controls selected with reasons for their selection as mandated by the standard. Inclusions and their justifications have been clearly stated. Selection of controls are based on contractual requirements, legal/regulatory requirements, best practice, results of risk assessments etc. Related documents have been referenced within the SOA.

COMPANY X has no exclusions.

Top risks are highlighted and discussed at SMT meetings.

Some of the risks sampled included:
- Loss of reputation (medium)
- Interruption to electricity supply (high)
- Basement flooding (medium)
- PSA full cost recovery and significant financial impact (medium)
- Rapid increase in number of allegations (medium)

Appropriate treatment and mitigation have been applied to the above identified risks.

Documents reviewed included:

1. Risk Register & Risk Treatment Plan (Jan 2018)
2. DOC XX Risk Management v1.2 (18/05/2018)
3. DOC XX.1 Asset Management
4. Statement of Applicability for ISO 27001:2013 v1.2 (01/05/2018)
5. Risk Management Process (09/06/2018)

4.4 Business Continuity

COMPANY X's Business Continuity Plan was reviewed and found to be well maintained. COMPANY X maintains a war box containing the BCP at the Head Office Site in London. COMPANY X has 5 seats available at the HQ location for personnel. Access lists to the HQ site was reviewed. The BCP is available to selected employees and local authority teams in hard copy format. Tests are carried out on an annual basis. Results of tests were available for review. It was noted that last year's test was based solely on IT Systems. The scenario for the test was based on burst water main rupture, flooding pipe work carrying telecommunication lines. Key resources have been identified and similarly, RTO's and RTO's have been determined.

Development is outsourced. COMPANY X has controls in place and a policy for secure development which is adhered to by 3rd

parties. Developers have restricted access to applications and support is provided via VPN. COMPANY X has escrow accounts and this is managed by a 3rd party (XXXXX). System changes go through rigorous reviews by COMPANY X's CISO. Segregated test environments exist. Test data are protected and redacted.

COMPANY X has a policy for managing Supply Relationships. "Right to audit " clauses were noted in the agreements reviewed. COMPANY X has supplier monitoring as part of its audit programme. New projects are assessed against ICO's Privacy Impact Assessment. Suppliers are risk assessed based on the following:

- Information suppliers handle
- Volume of information
- Frequency of handling the information

The above determines the supplier’s level of risk which is categorised as High, Medium or Low.

Documents reviewed included:

1. DOC XX Business Continuity Management v1.2 (12/04/2018)
2. Brief Report for November 2017 Exercise
3. Annual Business Continuity Test - Audit Committee (March 2018)
4. Report for November 2017 Exercise
5. REC XX Disaster Recovery/Business Continuity Order of Restoration of Principle IT Systems for COMPANY X
6. Access Lists for HQ Site
7. DOC XX Systems Acquisition, Development & Maintenance
8. XX Change Management & XX Emergency Change
9. DOC XX Supplier Relationship vX.X (09/07/2018)
10. Consult CRM Master Services Agreement (22/12/2017)
11. Request for Proposal - In-house Education Systems & Process Review
12. Single Licensee Software Escrow Agreement (with 3rd party XXX)
13. COMPANY X - Charter UK Agreement (03/02/2016)
14. Escrow Agreement for XXX (July 2017)
15. COMPANY X - GDPR Policies and Procedures (07/02/2018)
16. AWS Contract Agreement

4.5 Data Security and Governance Awareness

The staff were sampled to ascertain their knowledge on information security and it was evident that all of them have been through the awareness training. All staff interviewed were able to demonstrate their knowledge on information security and how it relates to their role. The staff were aware of the need to have segregation of duties and had a firm understanding of classification of information requirements in place. They were able to point out where the relevant policies and other documentation related to the ISMS stored on their portal. They knew the reporting procedures for information security incidents.

Overall their knowledge on information Security was satisfactory. Awareness records were sampled during the HR session earlier on in the assessment. Please see the relevant section on HR.

COMPANY X's DPO is responsible for Information Governance matters such as Data Protection, Freedom of Information and Subject Access Matter requests including training. As such it was noted that the DPO has a bias when it comes to Information Security Awareness. The DPO was able to demonstrate strong knowledge on the subject.

The Finance team have robust systems and controls to ensure the protection and preservation of confidentiality, integrity and availability of data they work with. Checks and balances on transactions were seen to be in place. Credit card details are not held beyond a day. The data is securely locked and processed the day after. After this all completed transactions are securely shredded and only unique identifiers and key information without full credit card details are held for archival and regulatory purpose s. The team have all completed their information security awareness training and this was ably demonstrated when a new starter was interviewed.

The other teams: HR, Project Management and Property Management showed great awareness in data protection, confidentiality, clear desk and screen policy (Tidy Policy), information security policy and incident reporting. It was noted that the project management team have embedded information security as a requirement and will be adopting the privacy impact assessment as part of the RFP process going forward.

The Property Management team scrutinises all content from the various department to ensure that any information put out is free of confidential data. This process requires an approval by the local council and legal. The team is also the point of contact if there are suspicions that unauthorised persons (such as Journalists) are "fishing" for information on hearings. Education
department deals with the approval of in-house programmes and mainly deal with personnel giving education. Confidential details held include staff CVs and these are restricted to limited staff within the department.

4.6 Top Management Interview

Top Management interview took place with the Managing Director and the Chief Executive. The CEO made it clear that COMPANY X understands that it will take time for the data protection and ISMS to mature and be fully embedded into COMPANY X's processes and procedures.

The organisation is committed to continual improvement and this is bolstered by the fact that COMPANY X is also certifying for ISO 9001 certification. Financial and Human resources have been committed to the GDPR compliance program. £35 000.00 has been allocated to the management of the ISMS and 23 people (one per operational location) have undergone GDPR training to act as local DPO's for the company, reporting in to the HQ DPO.

The company maintains a monopoly privilege in each location it operates in due to demand for placements exceeding supply and the company is able to acquire suitable properties rapidly to facilitate expansion. Processes are in line with applicable legislation and 99% of the organisations processes are in the public domain so ISO certification for TQM, BI and information security became the "obvious thing to do" in order to achieve continuous improvement and maintain "public trust". Standards were embedded to the company's procedures. The concept of "Providing wellbeing, security, with a Duty of Care" is the company's motto.

During the first year of implementation of the GDPR program a constant push to people is expected to take place to comply with the policies and procedures and then within 2 years of implementation the aim is to become an automatic process and completely embedded in the normal way of business and become a culture of people "saying this is how we do it". The main drivers for the certification were the legal, commercial and public requirements for data confidentiality, integrity and availability.

The organisation handles confidential information and the consequence to the vulnerable minors, as well as overseas sourced personnel in terms of breach or loss of information would be tremendous and the contractual aspects of such event could destroy the company within a short timeframe, with properties holding commercial mortgages funded by the local authorities fees for each child placement. Monthly reporting systems are in place to support the ISMS. IS roles and responsibilities have been defined and monitoring bodies are in place.

The client is subject to the following internal / external audits:

Local government authorities

The ICO
Commercial auditors
Internal audits
Accreditation bodies
Office of National Statistics

Resources:

Investment in money and time has been made from management and staff in terms of documentation and implementation of the standard and a budget is maintained for on-going training and assessments.

High Risks identified during the meeting:

- Data loss and the consequences of the loss
- Loss of trust in people
- Data breach / loss of control over the organisation
- Misuse - mishandling of information

5. Data Governance and Control

5.1 GDPR Policies

REDACTED

5.2 IS Policies

REDACTED

5.3 Big Data Policies

REDACTED

5.4 Distributed Ledger (Blockchain) Policies

REDACTED

5.5 GDPR Procedures

REDACTED

5.6 IS Procedures

The Access control policy XX.2018 was seen to be in place for Access control process.

Related documentation:

IS Policy
Starters and Leavers Process
Health and social work professions order

IT Policy Access to the company's systems can be made only by authorised users. The access rights to applications take into account:

- the classification levels of information
- data protection and privacy legislation and any potential client contractual commitments
- the need to know principle
- everything is forbidden unless expressly permitted
- any privileges that users actually need to perform their roles
- user access requests are subject to formal authorisation and periodic review

Authentication mechanisms for the guest wireless network are applied for users and equipment. Control of user access to information services is enforced. The network with scope of this policy is that installed at the COMPANY Xs premises. A Network Overview Diagram was seen to be in place. Servers are on their own virtual network, separated. Security authentication protocols are used for authorising access to networks.

User Access Management:

The Recruitment and employee change databases were seen to include the new starters listed. The following sample was selected from the list was followed the process through for effectiveness:

Creating an account:

- Temporary agency worker
- Line managers recruitment authorisation form with details regarding facilities (access control cards, hours of working, mobile, keys,),
- IT department (VPN, PC--laptop, Lotus notes, access levels. etc)
- Approved by HR
- Account created by IT

Changing privileges:

Contract variation (used for roles change)
Registration Manager
Internal move from Case Team Manager FTP to Registration Department
Form approved by the Line manager
Approved by HR
Approved by Finance
Approve by the CEO
Verisk software implementation, phone extension, passwords and usernames.
Removal of privileges of previous account.

5.7 Big Data Procedures

REDACTED

5.8 Distributed Ledger (Blockchain) Procedures

REDACTED

5.9 Stewardship

REDACTED

6. Audit Grading

6.1 Grade Definitions

Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the definitions in the table below.

Colour Code	Internal Audit Opinion	Recommendation Priority	Definitions
	High Assurance	Minor points only are likely to be raised	The arrangements for data protection compliance with regard to governance and controls provide a high level of assurance that processes and procedures are in place and being adhered to. The audit has identified limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance.
	Reasonable Assurance	Low Priority	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements.
	Limited Assurance	Medium Priority	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The audit has identified scope for improvement in existing

			arrangements
	Very Limited Assurance	High Priority	The arrangements for data protection compliance with regard to governance and controls provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

6.2 Information Maturity Assessment

The information governance model for this audit provides assessment tools, information standards, organizational structures and roles and responsibilities in relation to managing information assets according to Company X's:

Business Assessment and Strategy Definition Blueprint
Technology Assessment and Selection Blueprint
Information Management Roadmap and Foundation Activities
Design Increment
Incremental Development, Testing, Deployment and Improvement

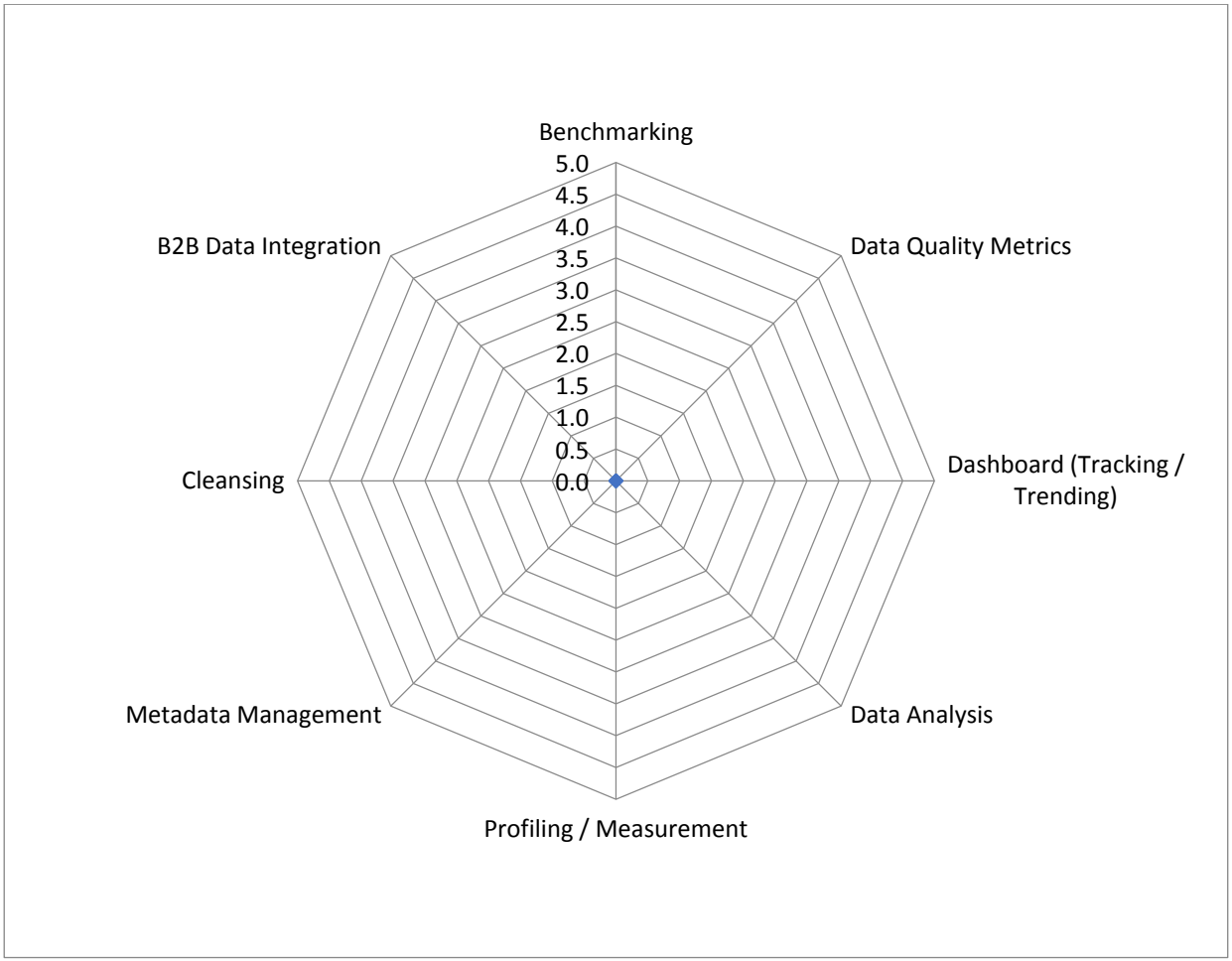
These were in considered in conjunction with the available supporting assets of:

- Tools and technique papers
- Deliverable templates
- Capability statements
- Software assets

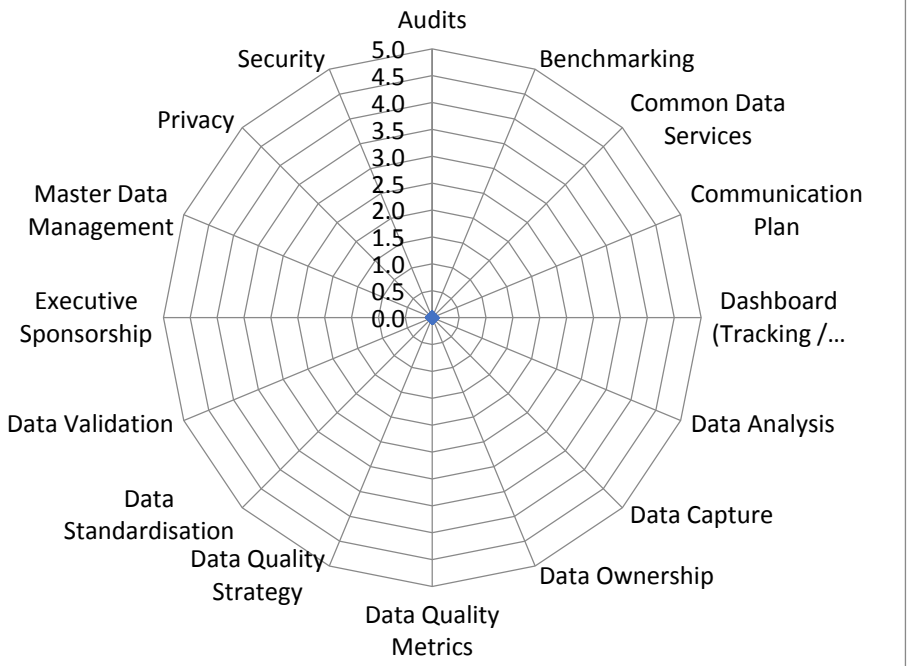
REDACTED

6.3 Summary Results Charts

REDACTED

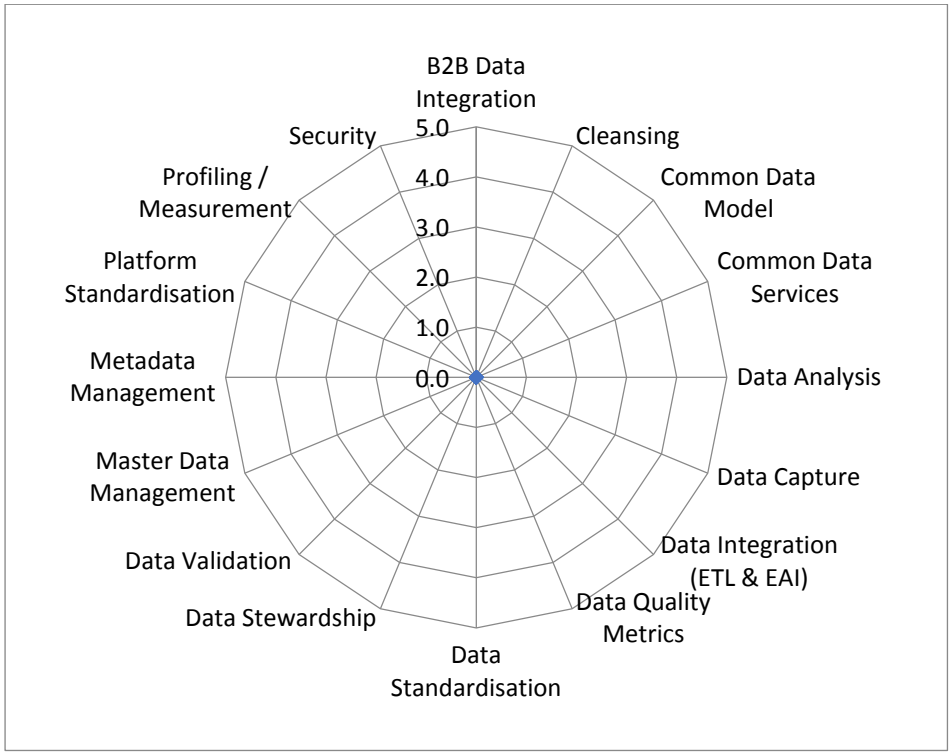


Overall Result

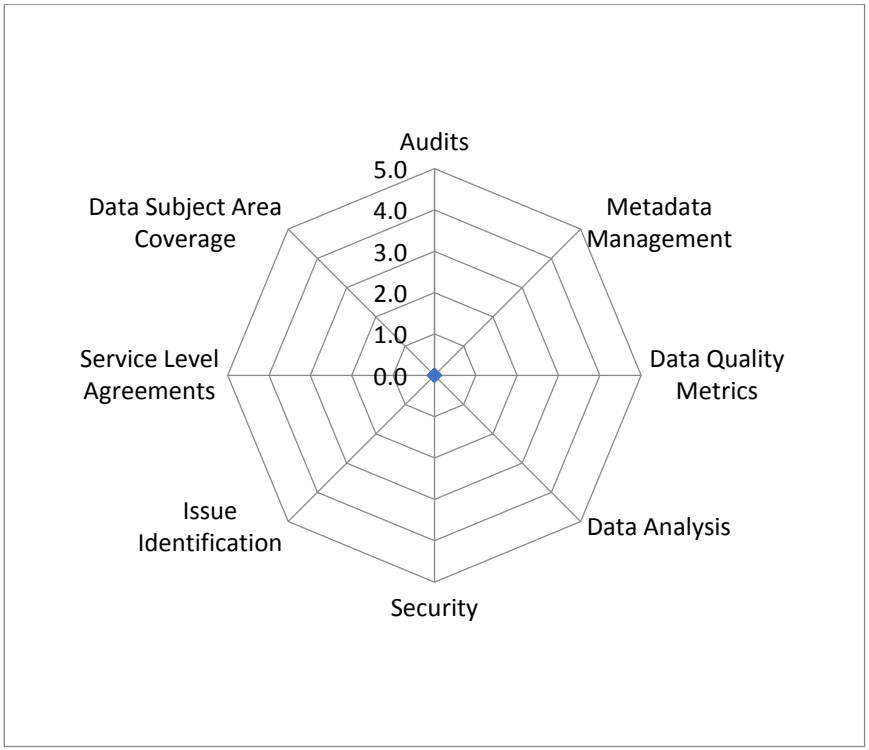


People

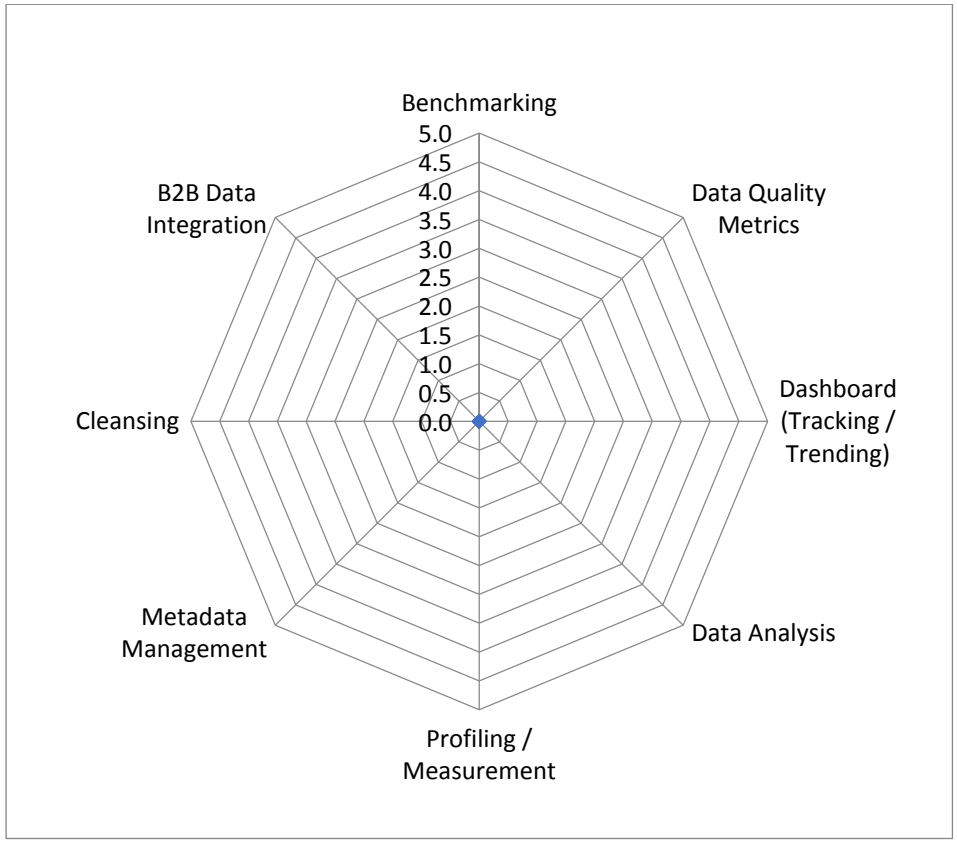
Policy



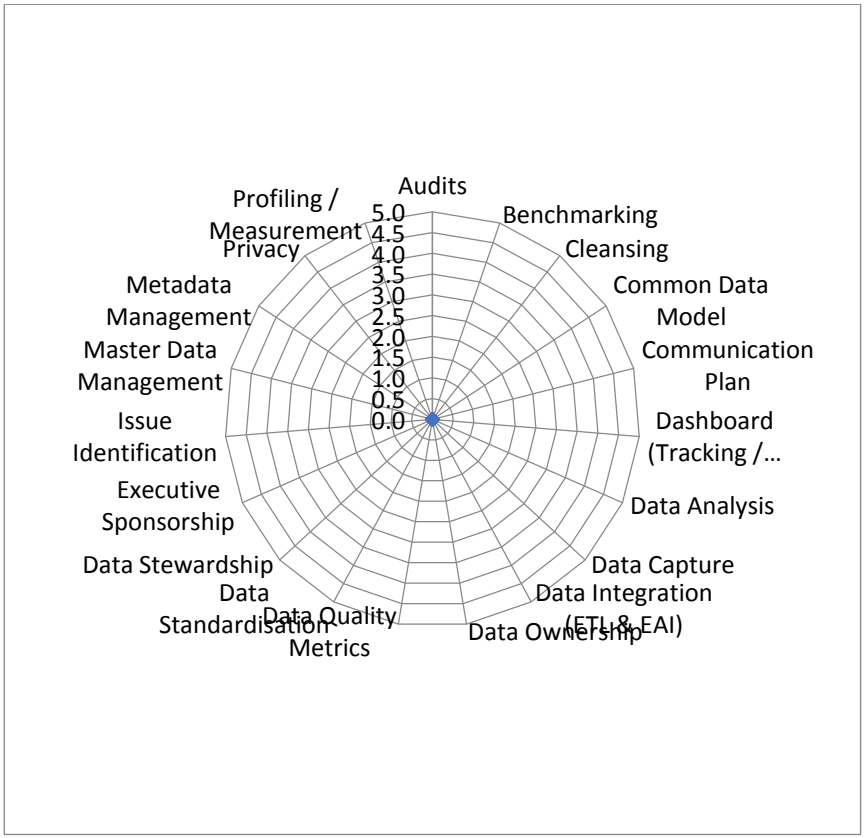
Technology



Compliance



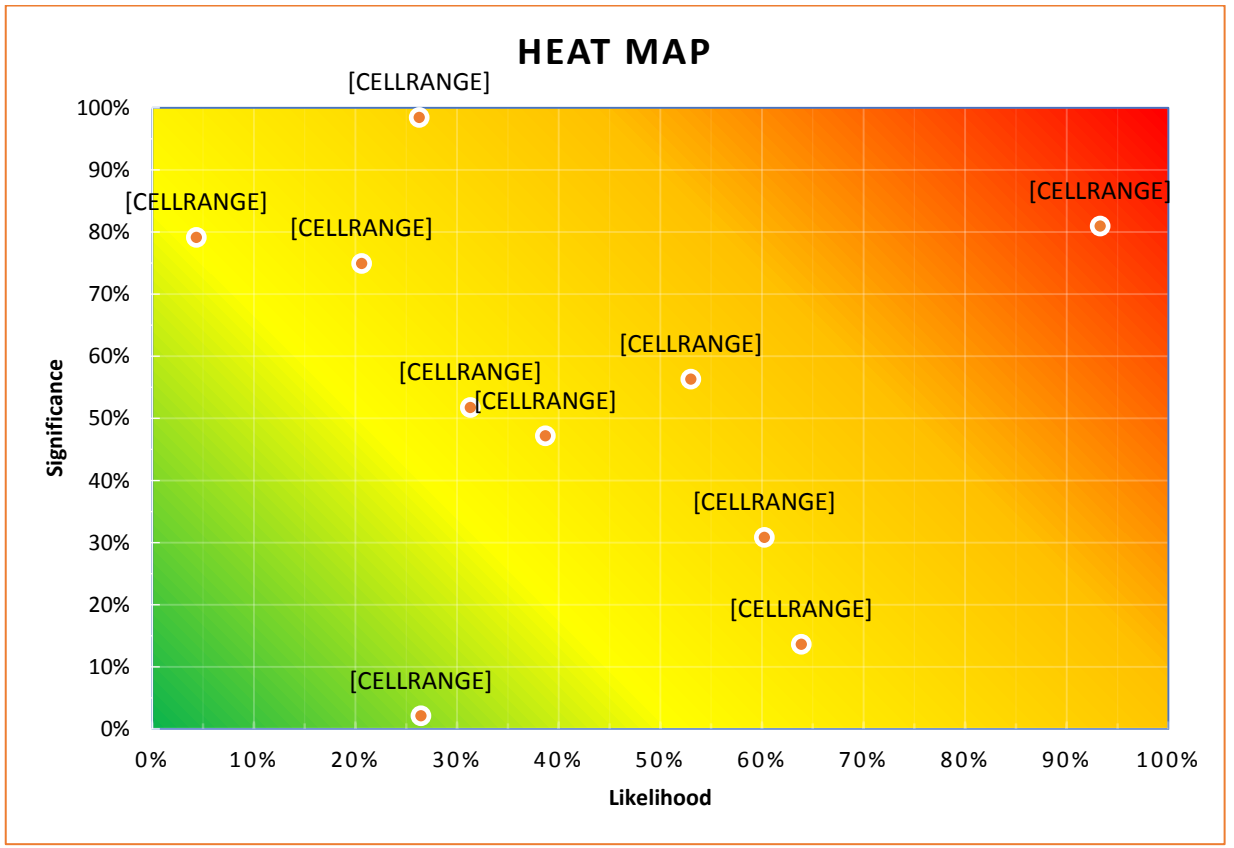
Measurement



Processes and Practice

6.4 Data Risk Heat Map

REDACTED

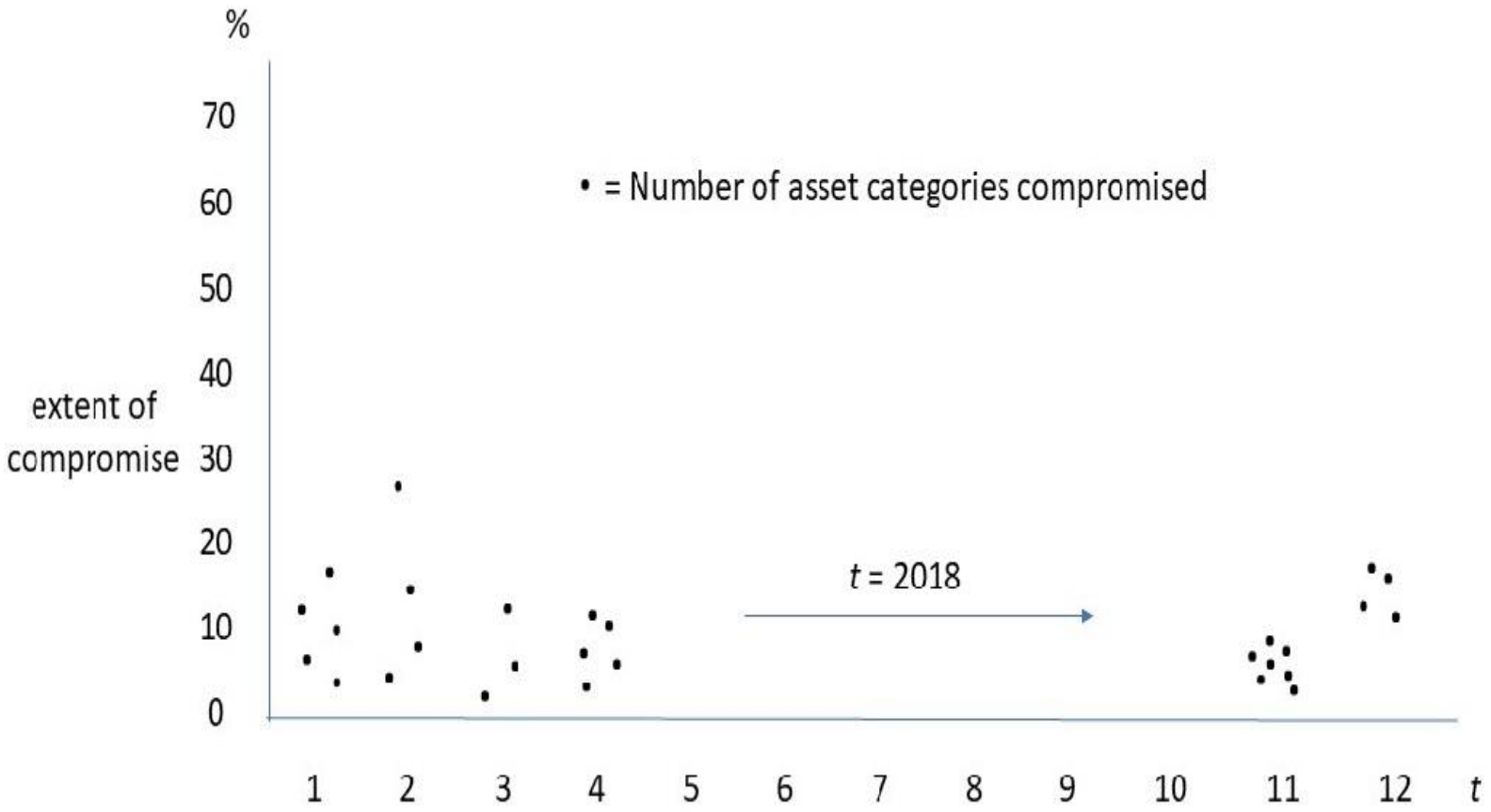


REDACTED

6.5 Data Governance PIN Map

Summary Points

REDACTED


%
70
60
50
40
30
20
10
0
extent of compromise
• = Number of asset categories compromised
t = 2018
1
2
3
4
5
6
7
8
9
10
11
12
t

REDACTED

7. Detailed Findings and Action Plan

7.1 Summary Gap Analysis by Area

	Number of Requirements	QTY Compliant	%	QTY Partially Compliant	%	QTY Non-Compliant	%	QTY Not Applicable
Security Policy								
Organisation of Information Security								
Data Asset Management								
HR Security								
Physical and Environmental Security								
Communications and Operations								
Access Controls								
IS Acquisitions Development Maintenance								
Data Storage and Disposal								
Data Security Incident Management								
Business Continuity Management								
Personal Data Risk Management								
Integrated Data Risk Management								

7.2 Summary Report

Findings from the audit will be risk categorised using the criteria defined in Section 6. The rating will take into account the impact of the risk and the probability that the risk will occur.

Ref	Compliance Risk	Issues/Findings	Recommended Solution	Management Comments, Responsibility for Action, Due Date
X.1 Scope A: Data Protection Governance - with specific reference to data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor GDPR compliance.				
A	If there is a lack of a robust and consistent governance process it raises the risk that personal data may be processed and managed inappropriately, with the potential for damage and distress to individuals.	X.1.1 The CISO has recently been appointed to the Data Protection Officer (DPO) post, following the resignation of the previous DPO. X.1.2 There is an Information Security Manager and a Risk Manager. Each location Head of Company X is a designated Information Risk Officer (IRO) for their location. The company's Directors and Chief Executive sit on the Senior Management Team, who may be consulted about relevant Data Protection / Information Security Governance issues. The Senior Management Team report all matters of governance to the finance and audit committee.		

		X.1.3 There is currently no separate Information Governance and Stewardship Group where Information Security, Risk and Data Protection issues are monitored, discussed and addressed.	X.1.3 The introduction of a Governance, stewardship or steering group, which meets periodically and includes the Information Security Manager, Risk Manager, DPO or other roles as appropriate, may assist in the identification and mitigation of issues and in providing assurance on corporate DP compliance.	X.1.3 Governance Group to include Information Security Manager, Risk Manager and DPO with (as and when) representatives from Finance, Personnel, Revenues & Benefits and Housing & Environment. **Responsibility:** Senior Management Team. Due Date: February 2019
		X.1.4 Company X does not currently have appropriate measures in place (e.g. responses to SAR's) with a management information reporting mechanism for the DPO or Senior Management Team to monitor overall Data Protection compliance.	X.1.4 The Data Protection framework should be strengthened by the provision of monitoring and reporting mechanisms to the Data Protection Officer on DP compliance, in line with the Council's Legal Responsibilities Policy (paragraph XX).	X.1.4 **Responsibility:** Governance Group Senior Management Team Due Date: April 2019
ETC……				
ETC……				

Ref	Compliance Risk	Issues/Findings	Recommended Solution	Management Comments, Responsibility for Action, Due Date
X.5 Scope X: IT Security - The controls in place to ensure adequate protection is applied to personal data processed via the organisation's IT systems.				
B	A failure to provide and implement proper security procedures for major IT systems containing personal records raises the risk of loss of data and inappropriate use by unauthorised individuals causing damage and distress.	X.5.1 Privacy Impact Assessments are not carried out for new properties acquired during expansion, nor for equipment and systems being introduced to new locations by Company X. However security risks and necessary controls are established prior to roll out as part of the normal course of business using relevant sources of information. X.5.2 These assessments focus on security and do not consider other aspects relevant to the GDPR that may be included in a PIA or the privacy by design approach advocated by the ICO.	X.5.2 Company X should consider conducting partial or full PIA allowing a new property to be used by vulnerable minors and also before implementing new systems and software.	X.5.2 Responsibility: CISO; Property Director Due Date: Ongoing
ETC……				
ETC……				

The agreed actions may be subject to a follow up audit to establish the level of implementation and improved compliance.

7.3 Assessment Plan

		Visit Q1 2018	Visit Q2 2018	Visit 3 Q3 2018	Visit 4 Q4 2018
Business Area / Location	**Date (mm/yy):**				
	Duration (days):	3	2.5	4	3
GDPR Assessment					
IS Assessment					
Data Maturity Assessment					
Process Risk Assessment					
Policies & Procedures Review					
Context of the Organisation, Scope and Policy					
Leadership and Commitment					
Planning and Resources					
HR Security					
Access Control					
Data Security					
Data Governance					
Data Stewardship					
Personal Data Risk Management					
Integrated Data Risk Management					
Document and Record Controls					

Monitoring & Measurement					
Risk Assessment, Risk Treatment, Statement of Applicability					
Regulatory Compliance					
Data Stewardship					
Data Security Incident Management					
Personal Data Management and Control					
Communications					
Physical and Environmental Security					
Business Continuity					
System Acquisition, Development and Maintenance					
Data Use and Analytics					
Big Data and Distributed Ledger Risk Assessment					
Program and Project Management					
Data Strategy and Information Maturity					
3rd Party Risk Assessment and Control					

7.4 Next Visit Plan

The objective of the assessment is to conduct a surveillance assessment and look for positive evidence to ensure the elements of the scope of certification and the requirements of the management standard are effectively addressed by the organisation's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organisations specified objectives, as applicable with regard to the scope of the management standard, and to confirm the on-going achievement and applicability of the forward strategic plan.

The scope of the assessment is the documented management system with relation to the requirements of ISO 27001:2013 and the defined assessment plan provided in terms of locations and areas of the system and organisation to be assessed.

Date	Assessor	Time	Area / Process	Item
	PKW	09.00	CORDA distributed Ledger	GDPR Compliance
	PKW	12.00	Big Data Analytics	Re-identification Risk
	PKW	14.30	Data Stewardship	Board Sponsor
			ETC……	

7.5 Notes

The assessment was based on sampling and therefore nonconformities may exist which have not been identified. If you wish to distribute copies of this report external to your organisation, then all pages must be included.

Data Risk Foresight and all its agents shall keep confidential all information relating to your organisation and shall not disclose any such information to any third party, except that in the public domain or required by law or relevant accreditation bodies. Data Risk Foresight and its agents and suppliers bodies have signed individual confidentiality undertakings and will only receive confidential information on a 'need to know' basis.

Data Risk Foresight has transacted with Company X under a non-disclosure agreement (NDA) and will not disclose to any other party the existence or nature of this consultation, except with the explicit written agreement of Company X.

This report and related documents is prepared for and only for Company X. Data Risk Foresight does not accept or assume any responsibility (legal or otherwise) or accept any liability for or in connection with any other purpose for which the Report may be

used, or to any other person to whom the Report is shown or in to whose hands it may come, and no other persons shall be entitled to rely on the Report.

Any queries regarding this report should be directed to Dr. Phillip King-Wilson, Lead Consultant and Auditor, Data Risk Foresight.

During the audit, all the employees interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of Company X's working practices, policies and procedures. The following staff members were particularly helpful in organising the audit:

- XXX, PA to the Director of Business.
- XXX, Director of Business & Law
- XXX, Information Security Manager