Healthy Organisation– Information Management Follow Up

Draft Report

Issue Date: July 2018

Working in Partnership to Deliver Audit Excellence

Contents

Executive Summary

- This section provides an overview of the approach taken in relation to the Healthy Organisation strategic review, as well the overall assurance assessment.

Summary Assessment

- This section contains the summary assessment by theme and the key strengths and Areas for Attention identified are highlighted.

Detailed Assessment

- This section contains a more detailed assessment of each area considered by theme.

Appendices:

- Appendix A – Mapping Areas for Attention
- Key Contacts and Distribution
- Statement of Responsibility

Executive Summary

Overview

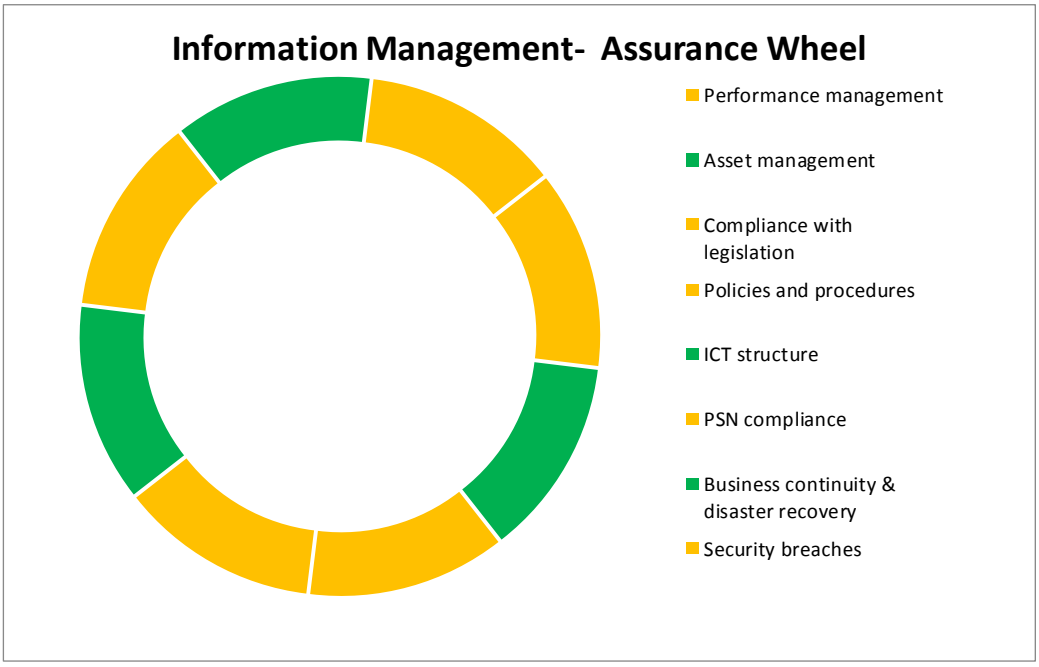
As part of the 2018/19 audit plan a follow up audit has been undertaken to assess the control framework in place for Information Management at the Council. As part of the initial Healthy Organisation review undertaken in March 2018, a meeting was held with the Group ICT Manager, however at this time we were unable to obtain sight of some key pieces of information to verify that the controls were in place. We were therefore unable to conclude on this theme and have now conducted this follow up review on the areas outstanding to enable assurance to be provided to Senior Management.

The Audit Assurance section below provides a summary assurance wheel for Information Management, followed by a more detailed assessment for each of the controls. Appendix A of the document maps the areas requiring attention.

Audit Assurance: **Medium**

The assurance for Information Management follow up referred to above have been reviewed and depicted in the following graph. This indicates an overall **Medium Assurance** opinion.

Information Management assurance graph



R/A/G Rating Key:

RED	*(Low Assurance / High Risk)*
AMBER	*(Medium Assurance /Medium Risk)*
GREEN	*(High Assurance / Low Risk)*

Summary Assessment

Information Management is an important aspect of governance for an organisation. Effective Information Management will facilitate and support efficient working, better decision-making, improved customer service and business transformation to facilitate the delivery of key priorities and objectives.

AREAS OF STRENGTH

Performance Management

- The satisfaction of the service users against the 4 ICT Key Point Indicators is tested regularly via KPI surveys.
- Satisfaction of ICT service users is consistently excellent/ very good/ good as gauged by the KPI survey results.

Asset Management

- The OTRS Configuration Management Database is regularly updated and holds all relevant information about hardware and software assets to prove their full lifecycle.
- Business cases are submitted with new equipment requests by specific Business Managers, to allow for ICT Services analysis of the need for the equipment and approval as necessary.

Compliance with Legislation – GDPR

- The roll-out of GDPR training and planning for GDPR implementation was already underway during the previous Healthy Organisation review.

ICT Structure

- An ICT structure chart identifies all posts within the ICT Services and most management posts are filled.

Policies, Procedures & Training

- There has been a roll out of Apprenticeships within the ICT Service, to aid progression and learning opportunities.
- Mandatory training records are kept on a standardised Corporate Induction Record, and on the e-learning portal individually for all staff.

PSN Compliance

- There has been the addition of new columns in the PSN remedial actions tracker to assist with monitoring who is responsible for completing actions to adhere with deadlines and comments are now being left by those responsible as to the status of the action.
- There was a decrease in the quantity of “High” risk recommendations made by the PSN assessors compared to the previous assessment.

Business Continuity & Disaster Recovery

- The Group ICT Manager has liaised with Business Managers to collate the list of applications within the ICT Business Continuity Plan.
- An up to date Major Incident Recovery plan is in place, which have been developed in partnership with local and regional 'Category 1' authority representatives. The documents are subject to regular review at local and regional planning groups.

Security Breaches

- The ICT Service Desk ticketing system which security breaches are reported through does not hold detailed information about the breach, therefore mitigating the risk of unauthorized individuals acquiring sensitive information.

AREAS FOR ATTENTON

Performance Management

- The Corporate Director for Operational & Partnerships Services should ensure corporate oversight and analysis of ICT performance is on the CMB agenda if appropriate and that KPIs are further reported to Council at the quarterly committee meetings.
- The Group ICT Manager should consider implementation of more a formal performance review process within the ICT Service.
- Due to the high scores on the KPI surveys for both *"Availability of voice and data network"* and *"Availability of storage area network (core computing)"*, the Group ICT Manager could consider adjusting these KPIs to alternative measures which assess areas currently untested.

Asset Management

- The Group ICT Manager should develop an Asset Management Plan for the ICT Service, to define how the Asset Management function works and links with key areas, such as: The Service Desk, the Configuration Management Data Base, change management, procurement and starters/leavers.

Compliance with Legislation – GDPR

- At the time of audit there was uncertainty over the appointment of a new Senior Information Risk Owner (SIRO), with the post holder (the Monitoring Officer, Corporate Director of Operational & Partnership Services) due to retire on 6th July 2018.
- The SIRO should consider whether the unofficial appointment of the DPO is appropriate, along with considering how staff could be more explicitly made aware of who the DPO is and how they can be contacted.
- The DPO should consider a more formal approach to recording the remaining progress of GDPR implementation, as without this information it would be difficult to effectively prove that GDPR implementation was underway in a timely manner, and in accordance with the implementation deadlines which are not currently documented in formal plans.
- The SIRO and DPO together should consider whether the current stance to not publish FOI requests and responses via the Councils website shows sufficient compliance with the Local Government Transparency Act.
- The DPO should ensure that the Retention Guidelines within the amended Data Retention Schedule are correct and in accordance with statutory requirements.
- The DPO should ensure that revised Privacy Statements are made available via the intranet and public facing website.
- The SIRO and DPO should review the members of staff who have not completed the GDPR training to ensure that the list is reasonable.

ICT Structure

- The Corporate Director for Operational & Partnership Services should consider whether there is enough clarity within guidance and structure documentation at the Council, to allow for transparency regarding who holds important Information Governance roles and responsibilities.

- The Information Management Strategy has not have been reviewed since May 2015 and having viewed the document it was unclear who would be responsible for reviewing it. The document should be reviewed to reflect the Information Governance roles not otherwise described within the current version, as well as to reflect changes to Council processes in light of the GDPR implementation; such as the delegation of a new DPO, and the updated Data Protection and Security Breach Policy appendices.

Policies, Procedures & Training

- The Group ICT Manager should undertake a review of all ICT Policy/Codes of Conduct to ensure that these are up to date and reflect the current day ICT Service procedures, as the versions available within the staff intranet dated back to 2009 in some instances. A regular review plan should also be put in place to prevent the documents becoming out of date in the future.
- The Group ICT Manager should ensure Service-wide mandatory training has been completed for those staff in ICT.

PSN Compliance

- The Group ICT Manager should satisfy himself that the next PSN (Public Services Network) assessment due date is within calendar reminders and work plans of those responsible for ensuring compliance, to avoid expiration of the 2018/19 certificate prior to booking the next assessment.
- The Group ICT Manager should ensure that deadlines allocated to “High” risk PSN Assessor recommendations/actions are adequate and ensures the issues are proactively addressed.
- The Group ICT Manager should consider whether the recurring issues have been addressed with adequate actions which will lead to the mitigation/eradication of the risk recurring a third time.

Business Continuity & Disaster Recovery

- The Group ICT Manager should ensure the review of the ICT Business Continuity Plan goes ahead in Summer 2018 to bring the Plan up to date and to clarify the identity of 'critical' applications within the applications list.
- The Corporate Directors of Directorates should ensure that their Services’ Business Continuity/Disaster Recovery Plans are up to date and contain an Emergency Plan in event that their Service’s critical ICT applications should fail. The Directorate Business Continuity/Disaster Recovery Plans should link or direct Management to the ICT Business Continuity Plan with regards to recovery of their Services applications if not addressed within their own plans.

Security Breaches

- The SIRO should consider the adequacy of the current Security Breach tracking spreadsheet in its current state and ensure that it captures all information required to inform the monitoring manager of the status of actions within.
- The SIRO should ensure that access to the Security Breach spreadsheet log is adequately access-restricted.
- The Data Protection Officer (DPO) should ensure that the process in place for recording breaches into the Data Security Breach Incident tracker is sufficient to record all information required about who is reporting and logging the breach, the timescales of action completion, KPI information, reports to the ICO and so on; and also ensure that reference numbers are assigned to each incident within the log that are reflected on its accompanying investigations and related documents completed by the investigating managers.

- The SIRO and relevant Business Managers should ensure that all outstanding remedial actions have been or are being implemented, and these actions are reviewed and monitored to ensure effectiveness in mitigating the risk and reducing the likelihood of recurrence.
- The DPO and Heads of Service should further consider whether all staff should receive the updated GDPR data protection training, as opposed to omitting staff who 'do not process data'.
- The SIRO should ensure that the Data Security Breach Procedures are clearly accessible via the staff intranet, with old versions being removed to avoid confusion.

Detailed Assessment

Performance Management	Medium Risk

Previous findings:
The Group ICT Manager confirmed that there is a quarterly Corporate Performance Assessment report produced which includes information regarding ICT performance, however a copy was not made available at the time of the original audit (March 2018). We were therefore unable to conclude on the extent to which the priorities stated in the ICT Strategy are measured, monitored and achieved and the requirements of the Performance Management Framework are being met.

Follow up review findings:
There are 4 KPI's for the ICT Service, against which stakeholder satisfaction is gained by means of an OTRS Service desk survey after each 5th ticket logged. Provision and discussion of the 2017/18 Quarterly KPI results with the Group ICT Manager identified that results are generally showing good/very good/excellent performance across the 4 KPIs, and there was not much variance in the figures seen. It was noted that the KPIs for both *"Availability of voice and data network"* and *"Availability of storage area network (core computing)"* have consistently scored 100% throughout 2017/18.

On discussion with the Group ICT Manager, it was explained that no ICT service meetings are held regarding KPI performance, however KPI data is forwarded to the Corporate Management Board via an administrator for their review at Corporate Management Board meetings. This data is then put into an accumulative KPI report which is viewed by Council on a quarterly basis, however there was no evidence of this within Council minutes on the Council website. The previous KPI report was viewed, which did not contain the four ICT KPI's. The Group ICT Manager explained that they had enquired as to why the ICT KPIs were not included within this report, however an answer was not provided by the end of this review. The Group ICT Manager stated that efforts will be made to ensure that the ICT KPIs are included in the reports going forward. Two samples of Corporate Management Board agendas and corresponding minutes were provided during the Healthy Organisation Corporate Governance review but did not appear to discuss the ICT Service's performance criteria within the agendas or minutes.

It appears that KPI data is gathered on a sufficiently regular basis and that KPI survey topics are for relevant measures. It is, however, unclear how the ICT Service proactively manage their performance formally within the Service; and there was little evidence of discussion of their Performance at Corporate Management Team meetings or at full Council.

Asset Management	Low Risk

Previous findings:
There is no documented Asset Management Plan in place for the ICT department. For this reason, we were unable to conclude how the ICT asset management functions links with the service desk, configuration management, change management, procurement, release management and starters/leavers process, or whether a full asset management life cycle takes place within ICT.

There is a database in place which is used for ICT asset management, however only one screenshot of information held within the database was provided for audit testing. We were therefore unable to confirm whether further assets life cycles are monitored, or how assets are recorded on this register.

Follow up review findings:
As identified within the previous audit, there is no documented plan or policy for asset management within the ICT Service. Whilst there is not an asset management policy to define assets (software or hardware) within the Service, the ICT Business Continuity Plan holds a list of 'critical' software applications (identified as Tier 1). The list was developed by the Group ICT Manager during meetings with Business Managers prior to the final ICT Business Continuity Plan being published in May 2016.

Discussion with the Group ICT Manager has clarified that the full lifecycle of an asset can be tracked within the CMDB, whether purchased via the ICT Service or via Directorates. New ICT assets are requested via the OTRS Service desk ticketing system and will only be considered if a business case completed by one of five Directorate Business Managers has been attached. Requests for new equipment must be approved by the Group ICT Manager prior to procurement of the asset.

Existing hardware assets are assigned a 5-year expiry date, after which they will be replaced. It is noted that capital funding was restricted in 2017/18 meaning that some assets had reached their 5-year expiry date, however were not replaced. £175,000 of capital funding has been approved by Council to fund the 2018/19 ICT asset renewal, allowing the service to bring their asset renewal up to date.

When a member of staff leaves employment at the Council, a ticket is logged to make ICT aware. Once the ticket has been administered by ICT, the assets record is updated with that information and the equipment is cleared of data and added to stock if not reassigned to another user. To manage and identify assets within the database, assets are assigned an identifier based upon asset type and how and when they were purchased. These categories are not documented within any ICT documentation provided, although they were evident in an asset record pulled from the CMDB which was viewed during the audit.

Compliance with Legislation - GDPR	**Medium Risk**

Previous findings:
During the previous audit, it was unclear whether the Data Protection Officer (DPO) at the Council would continue the role long-term, or whether, as expected, it would be reassigned to the Council's Information Officer. The Information Officer had not received any specific GDPR training at the time of testing.

The progression towards implementing GDPR was also unclear, due to there being no formal implementation plans, nor record of minutes from the Implementation Group that had been created.

Evidence was seen that the Data Protection Policy had been reviewed and approved by Council, along with the Data Retention Plan and Data Retention Schedule; however there were concerns regarding the data retention timescales assigned to certain files in the Data Retention Schedule.

Follow up review findings:
In discussion for this follow up review with the Group ICT Manager, it was made clear that the DPO role has now been designated to the Information Officer, who was interviewed during our last review.

There is concern over whether there are any plans to appoint a new SIRO, as the current post holder (the Monitoring Officer, Corporate Director of Operational & Partnership Services) is due to retire from the post on 6th July 2018. There did not appear to be a formal handover of the SIRO responsibilities prior to the current SIRO taking annual leave before their retirement.

On discussion with the Information Officer, now DPO; the role was unofficially assigned from 1st April 2018 by the Corporate Director for Operational & Partnership Services. We were informed that the decision to appoint the Information Officer as DPO was communicated to staff via a Data Protection update within the Bridgenders mailing tool, though when viewed this update did not explicitly inform staff of the DPO appointment. The DPO recently begun GDPR Practitioner Certification training w/c 14 May 2018, which was expected to be completed in 5 weeks' time.

The DPO was unaware of the Information Management Strategy (version 2015), which holds old versions of the Data Protection & Security Breach Policies and Procedures as well as designating the responsibility of DPO to the Monitoring Officer. The DPO was made aware of this document and they advised that they would be update the document.

At present, Freedom of Information requests are not published on the Council's website. A project plan is underway to add more information to the new website, which the DPO expects to lessen the number of FOI requests received.

During the original audit it was identified that some timescales relating to staff records within the Data Retention Schedule did not match the Retention Guidelines for Local Authorities. It was advised that HR are still in the process of determining the appropriate retention guidelines for the issues raised. Once fully completed, all revised Privacy notices will be published via the Intranet and on the Public facing website. When discussed with the DPO, this was due to go ahead on 25th May 2018, but on review of the Intranet, this is yet to occur.

The DPO provided the following statistics in relation to Council staff who have completed the new GDPR training:
Corporate staff: 21% completed, 79% not completed
Schools: 9% completed, 91% not completed.

The DPO explained that these figures were representative of a full head count, however not all staff would be receiving the new GDPR e-module training, only those who process personal data as part of their role. Statistics in relation to those members of staff who process personal data were requested however it was advised it was not possible to provide this information. This indicates that there has been no formal identification of the quantity of existing staff who are to take the GDPR training at the Council.

ICT Structure	Low Risk

Previous findings:
The ICT structure chart was provided; however, this did not outline the responsibilities/detailed scheme of delegation within the ICT department. Due to no further information regarding ICT roles, we were unable to conclude as to the structure/scheme of delegation of the ICT or Information Management functions at the Council.

Follow up review findings:
The Group ICT Manager advised that no decisions effecting the ICT Service as a whole would be made without their approval. It was explained that there is a Scheme of Delegation within the Council's Constitution document which applies to all Group Managers at the Council, although on viewing the Constitution, this was not found to be the case.
The structure chart provided in the original review is the Service's means of identifying the delegation of authority, along with HR job descriptions which provide further detail of the roles duties/responsibilities. These were provided for the Group ICT Manager, the Data & Network Services Manager and the Systems Manager.

The post of Unified Services Manager is currently vacant and has been since the promotion of the Group ICT Manager who previously held the role. The Unified Services Manager post is currently being supported by the Data & Network Services Manager and the Group ICT Manager.

Policy, Procedures & Training	Medium Risk

Previous findings:
ICT Policy/Strategy and Code of Conduct documents are available via the Intranet, however most of the documents were found to be out of date and without document control.

Some policies were available in Welsh language, however this not for the entire suite. There was also no consideration for the equality/diversity of ICT in relation to the Discrimination Act, regarding alternative equipment/assets or staff procedures.

Follow up review findings:
The suite of ICT & Information Management Policies and Codes of Conducts still required review at the time of follow up review.

Generally, policies are distributed to staff during the Corporate Induction at the beginning of their employment, which would be signed for on completion of the module on their Corporate Induction Record. Codes of Conduct are delivered as a mandatory e-learning module as part of this process. The exact ICT policies required would be determined by the role of the new member of staff. During employment, updates and newly created policies are communicated via email for Service Managers to disseminate to their teams or via the Bridgenders mailing service. The relevant Intranet page would also be updated to reflect the change.

On top of the mandatory training for ICT staff, specialised ICT roles receive further coaching/training via their peers and have accessibility to specialised accreditation pathways. The Group ICT Manager explained that the ICT Services department advocate using apprentices to develop their teams specialisms and foster a good learning culture.

Training matrices were viewed for both the Unified Services and Systems teams within the ICT Service. Both identified areas of Mandatory training that had not been completed for ICT, Safeguarding, Fire Safety and Violence Against Women, Domestic Abuse & Sexual Violence (*VAWDASV*), some of which was not completed for the Support and Digital Officer Manager amongst other staff currently in post.

PSN Compliance	Medium Risk

Previous findings:
Although it was advised that regular PSN check testing is performed internally, we were unable to view a copy of the most recent compliance certificate at the time of the audit and the improvement plan was too vague to confirm implementation of any recommendations, as no timescales or accountabilities were identified in the plan.

Follow up review findings:
As informed by the Group ICT Manager, the previous PSN assessment had expired at the time of the original Healthy Organisation review in April 2018. It was explained that this was due to a changeover of responsibility for ensuring its compliance in the Service, as well as a lack of notification by the PSN Assessors. A PSN review was undertaken at the end of April 2018, as soon as possible following it being identified that the previous certificate had expired. The Group ICT Manager provided the remedial actions tracker for 2017/18 during the original Healthy Organisation review and also the new

remedial actions tracker for 2018/19's review. At the time of testing the 2018/19 tracker and Assessors PSN report had been sent for approval, but that it may not be returned for a few months, as such there had not yet been a decision on whether the PSN actions suggested by the Service yet had been approved yet. It was agreed by the Head of Internal Audit that we would conclude the report on her satisfaction that the PSN was in hand and had been sent for approval.

Details taken from the ICT Service's 2018/19 PSN remedial actions tracker are outlined below:

Risk Level	Total Actions Required	Actions Completed
High	35	7
Medium	16	3
Low	16	0

*figures correct as of 13 June 2018.

The total high-risk actions to be taken is 35, compared to a total of 40 high-risk actions to be taken from the previous assessment. The total medium-risk actions to be taken is 16, compared to a total of 24 from the previous assessment. The total low-risk actions to be taken is also 16, compared to 0 within the previous assessment. The total number of high-risk actions to be completed has fallen compared to the previous year's report, and there has been the addition of new columns in the tracker to assist with monitoring responsibility for completing actions, as well as deadlines and comments left by those responsible.

There are plans for PSN compliance to be phased out across the Public Sector, however it was confirmed that PSN compliance will be adhered to until the point in which the Council no longer utilise services via PSN.

Business Continuity & Disaster Recovery	Low Risk

Previous findings:
We were unable to conclude a full opinion regarding a critical application list, having not been able to view the Configuration Management Data Base (CMDB). The ICT Business Continuity Plan provided did not identify which applications are critical, but did identify application 'owners', contact details for the application suppliers, alternative systems and which servers the application related to. It was noted that the ICT BCP was last reviewed during May 2016. It was advised that there is a printed copy of the ICT Business Continuity Plan held in a fire safe within the Civic Offices. The Group ICT Manager also confirmed that the applications list is not under a regular review process and had not been updated since it was compiled three years ago.

Regarding the Corporate Business Continuity Plans for the Council, the tests could not be concluded as there were no documents identified/provided. The Group ICT Manager confirmed that there are Service/Directorate Business Continuity Plans, but the ICT Plan does not feed into an overarching Corporate Continuity Plan.

Follow up review findings:
<u>Directorate/Service Business Continuity Plans</u>
As previously confirmed, there is an applications list within the ICT BCP, but not within the CMDB. 'Critical' applications are identified within the ICT Business Continuity Plan as 'Tier 1' systems. The Group ICT Manager explained that while most applications are accounted for within the ICT Business Continuity Plan, Directorates should include the applications that they use within their own Directorate Business Continuity Plans and Disaster Recovery Plans. It was also identified by the Group ICT Manager that the ICT Plan has no link with the Corporate Business Continuity Plan, and we were not able to locate a Corporate Business Continuity Plan via the staff Intranet.

One other Business Continuity Plan was made available at the time of the previous audit, for the Social Services & Well-Being Directorate. This document was out of date (due for review in Jan 2016), and did not provide a list of applications used by the Service, nor a plan to follow if applications (for example the DRAIG database) become unavailable. Neither did it link to the ICT BCP server recovery type plans for these applications.

Corporate Business Continuity Plans

The owners of the Major Incident Plans for the Council are the Emergency Planning Team, with the Emergency & Electoral Team Manager responsible for their review and relevant planning. The Emergency & Electoral Team Manager provided the most recent revision of the Strategic Major Incident Plan, Recovery Plans and the Emergency Incident Control Plans; as well as the Corporate (Strategic) Business Continuity Plan. The Corporate Business Continuity Plan for the Council is in place to ensure that during a major incident occurring there are sufficient plans to keep services available to customers, such as bin collection, and other every day services.

The Major Incident Plans and supporting documents have recently been reviewed and, due to restructuring within the Council, there are plans to develop major incident training modules for Service Managers towards the end of 2018 regarding call outs, planning for recovery, and other related topics, to ensure that all necessary staff have sufficient knowledge. The Recovery Plan document outlines the responsibilities of all local Authorities in the case of a major incident and is currently in draft form (dated Feb 2018).

The Emergency & Electoral Team Manager also explained that there are Local Resilience Plans in place which sit beneath the Major Incident Plan, which are developed through seven different 'Category 1' members of local authorities (including Fire teams, Water Boards, and Health Care representatives) who work together at a Regional Planning Group to create recovery plans with regional collaboration.

The Council's Corporate Business Continuity Framework was last reviewed and updated in March 2018, by the Emergency Planning & Electoral Team Manager. The Corporate Business Continuity Framework is supported by individual Directorate plans with more detail on how each directorate will run its own services in the event of a crisis affecting how the Council deliver business as usual. The Framework identifies the Corporate Management Board as the Crisis Management Team and sufficiently outlines teams varying responsibilities if the Plan was to be activated. Contact and distribution list details are not held within this document, but separately by the Emergency Planning team, which would be distributed as necessary when an incident occurred.

It is expected that each service area would hold information regarding emergency response within their own Business Continuity Plan, which was found to be the case within ICT and Social Services & Well-Being. The ICT and Social Services BCPs viewed were both found to be out of date/due for review at the time of testing, with the Social Services plan not identifying their critical/other applications to be bought back in the event of failure. Business Continuity Plans for the remaining service areas were not reviewed as part of this work.

Security Breaches	**Medium Risk**

Previous findings:

The Group Manager for ICT confirmed that the DPO and SIRO monitor security breaches at the Council, deciding on which to report to the ICO and monitoring breaches once reported via a central spreadsheet. The Data Security Breach spreadsheet was not provided for audit testing.

The Strategy/Codes of Conducts and mandatory Data Protection training in place appeared to be robust enough to ensure that breaches are reported and monitored, however these required reviews to align with the implementation of GDPR.

Follow up review findings:
The Security Breach Incident Tracker was provided by the Group ICT Manager. It was advised that it is stored within the Councils O: Drive, of which only certain users can access (DPO, SIRO and the Business Managers).

One case of a laptop theft was discussed during an audit interview with the Group ICT Manager, who explained that the incident was reported to the ICO, who took no further action due to the laptop's encryption. Another instance was discussed regarding a significant breach which took place in late 2016, which lead to a member of staff being suspended pending further investigation/action. It was advised that the incident was being dealt with by HR and had not yet reached a conclusion.

The ICT Service Desk can be used to log security breaches, however they do not hold full details of the incident investigation, which are signposted to the relevant 5 Business Managers to follow up confidentially. The Security Incident Breach tracker is then updated with the cases progress. Upon review of the tracker, it was found that a lot of information was missing from various columns. The tracker holds all security breach information since 2001, but only a handful of entries in total have been identified with a "Security Breach Ref #".

Within the details tab of the tracker there was little information regarding whether the actions (if any) put in place were completed, by whom, the date of completion and whether any further monitoring was being implemented to address any potential for the incident to reoccur and/or affect other areas of the Council.

Guidance is not easily identifiable within the Bridgend staff intranet as to how to report a data security breach. There is information regarding reporting a Security Breach within the Information Management Strategy as an appendix; however this document is out of date (last reviewed in 2015). It is not possible to tell from the Security Breach Incident Tracker whether the process explained within the Information Management Strategy appendix has been followed as there is insufficient information kept within the tracker to conclude this.

During the audit testing completed in the original Healthy Organisation review, it was identified by the Group ICT Manager that there was a mandatory ICT training module for staff members, as well as a Data Protection mandatory module during staff inductions, to ensure that the data breach protocol is communicated to all staff members.

Appendix A - Mapping Areas for Attention to 2018/19 Internal Audit Plan

Theme	Area for Attention	Update
Information Management- Performance	The Corporate Director for Operational & Partnerships Services should ensure Corporate oversight and analysis of ICT Performance is on the CMB agenda if appropriate and that KPIs are further reported to Council at the quarterly committee meetings.	Complete – performance is monitored on line.
Information Management- Performance	The Group ICT Manager should consider implementation of more formal Performance review within the ICT Service.	Actioned. Current methods are deemed appropriate.
Information Management- Asset Management	The Group ICT Manager should develop an asset management plan for the ICT Service.	Already in place.
Information Management - Legislation - GDPR	There is concern over whether there are any plans to appoint a new SIRO. The Executive Director should ensure that this role has been passed on to a suitably senior member of the Management team.	This has already been actioned with the Monitoring Officer covering the SIRO role.
Information Management- Legislation - GDPR	The SIRO should consider whether the unofficial appointment of the DPO is appropriate, and how staff could be more explicitly made aware of who is responsible/ the main point of contact for the role of DPO.	This has already been actioned and an appropriate appointment made which was clearly disseminated to staff via Bridgenders.
Information Management- Legislation - GDPR	The DPO should consider a more formal approach to recording the remaining progress of GDPR implementation, as without this information it would be difficult to effectively prove that GDPR implementation was underway in a timely manner, and in accordance with the implementation deadlines which are not currently documented in formal plans.	A GDPR implementation Board was established with key representation from each Directorate. It has been accepted that formal minutes should have been taken;
Information Management – Legislation - GDPR	The SIRO and DPO together should consider whether the current stance to not publish FOI requests and responses via the Councils website shows sufficient compliance with the Local Government Transparency Act and formally risk assess the impact of not publishing FOI's online.	There is an FOI Publication Scheme on the intranet which publishes FOI responses that we consider would be of interest to the public. The team are currently reviewing the Publication Scheme with a view to publishing more FOIs
Information Management – Legislation - GDPR	The DPO should ensure that the Retention Guidelines within the amended Data Retention Schedule are correct and in accordance with statutory requirements.	The Data Retention Policy has been reviewed in light of GDPR and was approved by Cabinet in January 2018;
Information	The DPO should ensure that revised	Complete

Theme	Area for Attention	Update
Management – Legislation - GDPR	Privacy Statements are made available via the intranet and public facing website.	
Information Management – Legislation - GDPR	The SIRO and DPO should ensure that staff who have not completed the updated GDPR training are mandated to do so.	GDPR training – this is a set agenda item for the IG Board. The completed lists are reported and each Business Manager is then required to chase those within their Directorate who are yet to complete it;
Information Management - ICT Structure	The Corporate Director for Operational & Partnership Services should consider whether there is enough clarity within guidance and structure documentation at the Council, to allow for transparency regarding who holds important Information Governance roles and responsibilities.	Already in place. Some updating is required but this is low risk and therefore not high priority.
Information Management - ICT Structure	The Information Management Strategy was seen to not have been reviewed since May 2015 and having viewed the document it is unclear who would be responsible for reviewing this Strategy. The document should be reviewed to reflect the Information Governance roles not otherwise described within the current version, as well as to reflect changes to Council processes in light of the GDPR implementation; including the delegation of a new DPO, and the updated Data Protection and Security Breach Policy appendices.	The Information Management Strategy is currently being reviewed by Legal as it is felt that it appropriately sits with Legal.
Information Management – Policy, Procedures & Training	The Group ICT Manager should review all ICT Policies and Procedure documents to ensure that they are up to date and reflect the current day ICT Service procedures, as the versions available within the staff intranet dated back to 2009 in some instances. A regular review plan should also be put in place to prevent the documents being out of date in future.	Complete
Information Management – Policy, Procedures & Training	The Group ICT Manager should ensure Service-wide mandatory training has been completed for staff in ICT.	Complete
Information Management – PSN Compliance	The Group ICT Manager should satisfy himself that the next PSN assessment due date is within calendar reminders and work plans of those responsible for ensuring compliance, to avoid expiration	The Group Manager is satisfied. PSN is being replaced by Cyber Essentials Plus.

Theme	Area for Attention	Update
	of the 2018-19 certificate prior to booking the next assessment.	
Information Management – PSN Compliance	The Group ICT Manager should ensure that deadlines allocated to "High" risk PSN Assessor recommendations/actions are adequate.	All high risks are actioned immediately therefore no recommendations or actions are outstanding.
Information Management – PSN Compliance	The Group ICT Manager should consider whether the recurring issues have been addressed with adequate actions which will lead to the mitigation/eradication of the risk recurring a third time.	This is being considered and will be addressed when the Data-centre is moved to Ravenscourt.
Information Management – Business Continuity & Disaster Recovery	The Group ICT Manager should ensure the review of the ICT Business Continuity Plan goes ahead in Summer 2018 to bring the Plan up to date and to clarify the identity of 'critical' applications within the applications list.	This is being considered and will be addressed when the Data-centre is moved to Ravenscourt.
Information Management – Business Continuity & Disaster Recovery	The Corporate Director for the Social Services and Well-Being Directorate should ensure that the Business Continuity/Disaster Recovery Plans for their services are updated and contain an Emergency Plan in light that their Services critical ICT applications should fail. They should link to the ICT Business Continuity Plan with regards to Recovery of their applications.	As above – this will be actioned as part of the update
Information Management – Business Continuity & Disaster Recovery	The Corporate Director for Education and Family Support should ensure that they hold adequate and up to date Business Continuity and Recovery Plans for their Directorate's Services in the event of a major event or disaster.	As above – this will be actioned as part of the update.
Information Management – Business Continuity & Disaster Recovery	The Corporate Director for Communities should ensure that they hold adequate and up to date Business Continuity and Recovery Plans for their Directorate's Services in the event of a major event or disaster.	As above – this will be actioned as part of the update.
Information Management – Business Continuity & Disaster Recovery	The Corporate Director for Operational and Partnership Services should ensure that they hold adequate and up to date Business Continuity and Recovery Plans for their Directorate's Services in the event of a major event or disaster.	No longer applicable. Will cover the Directorate of CEX – Resources and included as above.
Information Management – Security Breaches	The SIRO should ensure that access to the Data Security Breach Incident tracker is adequately access-restricted.	This is already appropriately access-restricted.
Information Management – Security Breaches	The DPO should ensure that the process in place for recording breaches into the Data Security Breach Incident tracker is	Already actioned and monitored by the DP officer.

Theme	Area for Attention	Update
	sufficient to record all information required about who is reporting and logging the breach, the timescales of action completion, KPI information, and reporting to the ICO; and ensure that reference numbers are assigned to each incident within the log that are reflected on its accompanying investigations and related documents completed by the investigating managers.	
Information Management – Security Breaches	The SIRO and relevant Business Managers should ensure that all of their relevant actions in relation to security breaches have been or are being implemented, and these actions are reviewed and monitored to ensure effectiveness in mitigating/eradicating the risk of recurrence.	DPO – there is a Code of Practice for Data Breaches available for staff on the intranet which outlines the new process in light of GDPR. All data breaches are recorded in Legal and should also be held by the relevant Business Manager. Data Breaches is a set agenda item for the IG Board so that breaches can be discussed with a view to ensuring such breaches do not recur.
Information Management – Security Breaches	The SIRO should ensure that the Data Security Breach Procedures are clearly accessible via the staff intranet, with old versions being removed to avoid confusion.	See above.

Report Authors and Distribution

Report Authors

This report was produced and issued by:

- Moya Moore, Assistant Director
- Dan Newens, Senior Auditor
- Emily Hobbins, Auditor

Key Contacts

The key contacts for Information Management:

Martin Bell, Group ICT Manager

Charlotte Branford, Information Officer (DPO)

Julie Cooper, Emergency Planning Team

Distribution List

This report was distributed to:

Helen Smith, Head of Internal Audit

Statement of Responsibility

Conformance with Professional Standards

SWAP work is completed to comply with the International Professional Practices Framework of the Institute of Internal Auditors, further guided by interpretation provided by the Public Sector Internal Auditing Standards.

SWAP Responsiblity

Please note that this report has been prepared and distributed in accordance with agreed Audit Charter and procedures. The report has been prepared for the sole use of the Partnership. No responsibility is assumed by us to any other person.