Healthy Organisation – A Strategic Review

Final Report

Issue Date: April 2018

Working in Partnership to Deliver Audit Excellence

Contents

Executive Summary

Overview

The concept of a Healthy Organisation review was developed by the South West Audit Partnership and the West of England Chief Internal Auditors Group to provide an objective assessment of the management control framework or 'health' of an organisation. In 2015/16 a Healthy Organisation review was carried out at Dorset County Council and Wiltshire Council and was well received at both and it was agreed to complete one for Bridgend County Borough Council as part of this year's audit plan.

The review framework assesses against eight corporate themes: Corporate Governance; Financial Management; Risk Management; Performance Management; Commissioning and Procurement; Information Management; Programme & Project Management; and finally, People and Asset Management. A Red, Amber and Green (RAG) rating is applied to each theme reviewed. These eight themes together contribute towards an overall assessment and understanding of the Council as a 'Healthy Organisation'.

Bridgend County Borough Council have selected to review five of the eight themes this year:

- Governance
- Risk Management
- Commissioning and Procurement
- Programme & Project Management
- Information Management

For each of the corporate themes the strength of the management control framework in place was assessed against a benchmark model by identifying the presence or otherwise of key controls. This included the use of assurance from other sources, such as external audit, as well as recent internal audit reports. The work was carried out during 2018 with testing completed by mid-March 2018. A senior manager from Bridgend County Borough Council was appointed as a key contact for each theme and outcomes were agreed with them ahead of producing this overall report.

The Bridgend County Borough Council Internal Audit Plan is very much focused towards the high-risk areas of the Council. The range of services delivered by the Council, by itself and in partnership with others, is very large and therefore this approach makes the best use of the audit days available. This does mean however that we may not achieve a balanced view of risk management across the organisation. As the Healthy Organisation review is a high level corporate overview, it will help ensure that we all have a balanced view of the control framework in operation across the Council. It has not checked for 'compliance' with the control framework at Service level (although we have looked at Adult Social Care where we needed to sample check).

To stay 'healthy', the Council, like all organisations, must undergo periods of change to remain current, but such change will introduce uncertainty. The existing control framework itself will be challenged by the new demands brought about by the very change needed to move the Council forward. At the start of this change, this framework is in part unproven. Consequently, all healthy

organisations must move between periods of green and amber as they set new priorities which are then subsequently reflected in their governance and service structures. This lifecycle is an ongoing, iterative process.

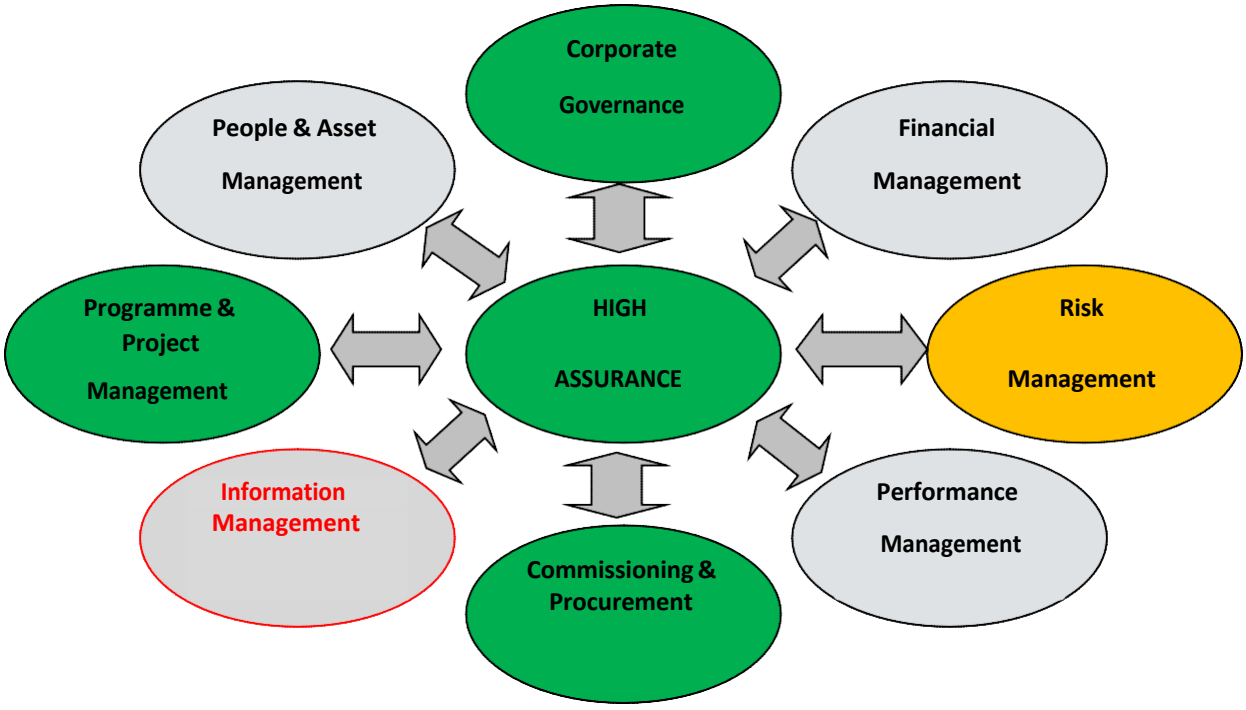
Most of these 'areas for attention' have already been recognised as such by services and work is either ongoing or planned to address this. The intention is for the main areas of weakness to be included in the 2018/19 internal audit plan, to provide assurance that improvements are made and achieve expected outcomes.

Following the section on overall assurance below, each theme is summarised with a management overview and beyond this more detailed findings for each theme has been provided. Appendix A then maps areas requiring attention to the 2018/19 Internal Audit Plan.

Audit Assurance:	High

The assurance for each of the five themes referred to above have been reviewed and depicted in the following chart. This indicates an overall **High Assurance** opinion, although we were unable to form a conclusion on Information Management as we were not provided with the evidenced needed to complete our work at the time of the audit.

Overall assurance graph



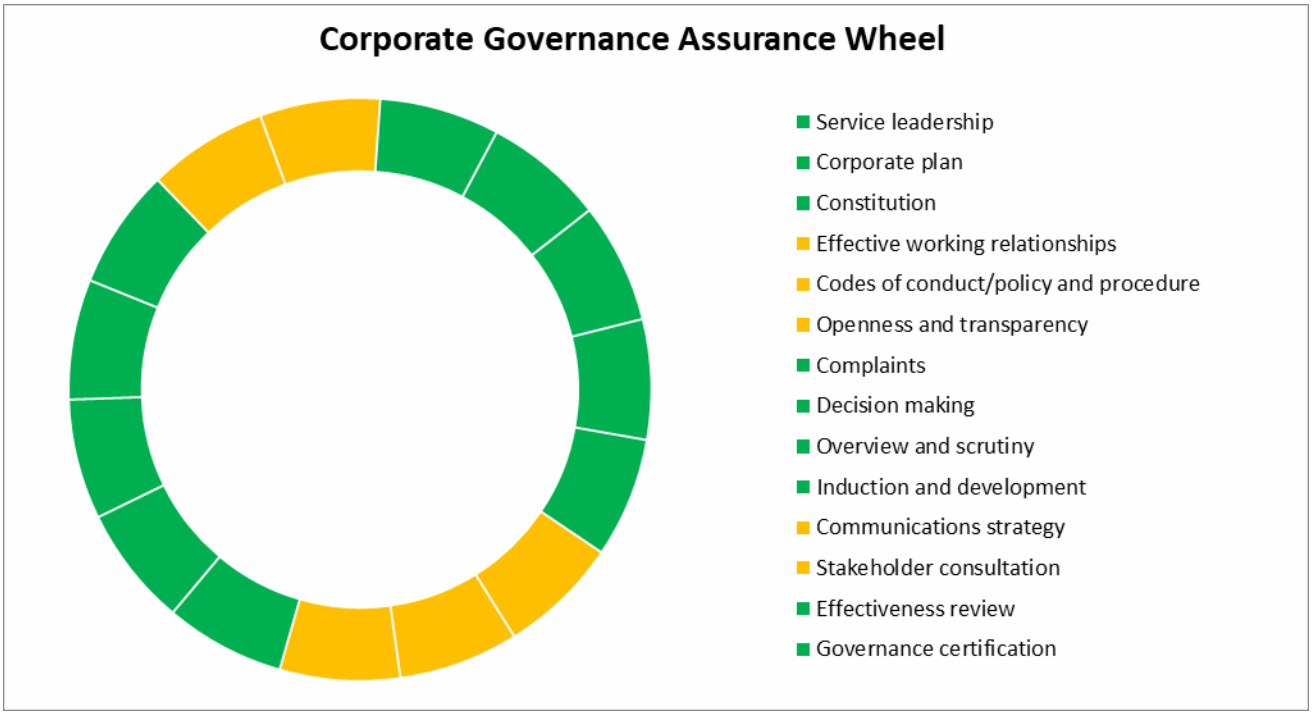
R/A/G Rating Key:

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

Summary Assessment by Theme

1. Corporate Governance	GREEN

Good corporate governance will facilitate effective management that can deliver long term success and performance of an organisation. Corporate Governance refers to the Strategic (rather than operational) management practices and values and beliefs by which the Council operates that balances accountability and the interests of all its stakeholders, including service users, the wider public and business community, management, Members and staff across the Council. It provides the framework for achieving the Council's goals in every respect including service delivery objectives, preservation of reputation and accountability, together with the values and culture in which services are delivered. Many of the elements of a good corporate framework should be replicated in structures and processes within service levels.



The **Green** RAG rating has been assigned because of the strong control framework in place in relation to corporate governance.

Governance - AREAS OF STRENGTH

Leadership

- The Corporate Management Team is currently undergoing a restructure by the Chief Executive. It is evident that interim cover arrangements are in place to ensure continuity of the management arrangements where required.

- In response to the recent Ethics audit recommendation, the Corporate Management Board (CMB) have addressed upward feedback mechanisms available to staff by asking the Corporate Director of Education and Family Support to consider the approach which could be used for this.
- Corporate Management Board meetings are held on a weekly basis with relevant senior officers in attendance. The agenda is flexible enough to accommodate emerging issues, but also includes some standing items.
- Attendance at Corporate Management Board meetings is good.

Corporate Plan

- A Corporate Plan is in place for 2016-2020, which is reviewed annually to ensure it remains aligned to the Council's corporate priorities. A draft Corporate Plan for 2018-2022 was presented to the Corporate Review Board in January 2018.
- Public consultation and member involvement are part of the development of the Corporate Plan.
- The Corporate Plan is published internally and externally using a variety of methods to ensure it is accessible by all stakeholders.

Constitution

- A Constitution is in place and is formally updated as required during the year, in accordance with the Annual Governance Statement review indicator table.
- Accountabilities and responsibilities of both Members and Officers are well documented, including the accountabilities for those Officers responsible for Partnerships, Shared Services and other Joint arrangements.

Effective Working Relationships

- Well documented guidance/protocols are in place to define how Officers and elected Members should work together, including an induction framework.
- Evidence is available within Corporate Management Board meeting minutes to show that Members and officers are working together.

Codes of Conduct

- Codes of conduct regarding behavioural standards are well documented in the Constitution and are aligned with the National Assembly Standards.
- There is a well-documented procedure to follow regarding declaration of Conflicts of Interest within the Councils Constitution document.

Openness and Transparency

- The Constitution, forward plans, policies, strategies, agendas and minutes are published online, easily accessible by the public.

Complaints

- Complaints procedures are readily available for members of the public via the website.
- The procedure wording on the website clearly explains the timescales and what responses the Public should expect from the Council.
- The procedure on the website identifies who to contact in the event that a complainant does not find the Council's response to their satisfaction.

Decision Making

- There is a clear protocol regarding decision making for both Council Policy and for Council Budgets, with minimum requirements for obtaining advice or consultation set out in the Constitution.
- Minimum timeframes are well defined, for example periods of consultation.
- A sample check of Council, Cabinet and Audit Committee minutes found them to be of suitable format, with evidence of informed decision making.

Overview and Scrutiny

- Definitions of Audit Committee and Scrutiny Committee responsibilities are contained within the Constitution.

Induction and Development

- Member induction training is well designed, with a detailed framework in place.
- A variety of internal and external training providers are used.
- Surveys of Member's opinions on the quality of their training are completed, with the surveys further utilised to influence external supplier approval.
- There is a focus within the Member Development Strategy on targeted development plans and having mentors in place to assist with Member development.
- There is plenty of opportunity for Leadership team development provided in the form of Leadership training programmes and e-learning modules.
- Evaluation forms are available to invite feedback from staff on the external training courses that they attend.

Communication

- The Communications, Marketing and Engagement Team Plan includes the general approach to engaging with public and other stakeholders.

Stakeholder Consultation

- The Communications, Marketing & Engagement Team Plan defines the Council's stakeholders.

Effectiveness Review

- The Annual Governance Statement includes a review of the effectiveness of governance arrangements.

Governance Certification

- The Annual Governance statement was found to accurately reflect the opinions of both the External and Internal Auditors.

Governance - AREAS FOR ATTENTON

Leadership

- In some instances, actions are agreed at Corporate Management Board, but the minutes do not record any timescales for completion for those actions.
- The "Action review" part of the minutes should state whether previous meeting

actions have been completed (as indicated within the agenda).

- There were some items on the cancelled meeting 20th December 2017 Corporate Management Board Agenda that were not returned to in either of the following 2 meeting agendas, making it difficult to confirm that the issues had been addressed later on.

Corporate Plan

- None

Constitution

- A number of minor referencing issues were identified in Part 1 Summary and Explanation "What's in the Constitution?";
  - There is no reference to the Democratic Services Committee (Article 9) in Part 1.
  - Part 1 states that The Standards Committee is under Article 9, but it's under Article 10.
  - All references to Articles after 10 require update to the corresponding Article number, as a result of the addition "Democratic Services Committee" in Article 9.
- The commissioning of services processes/procedures are not described within the Constitution document, nor within any structure/responsibilities and duties documents within Directorates information available on the intranet.

Effective Working Relationships

- While there is a stated ambition to encourage effective working relationships (Elected Member Learning Development Strategy), opportunities to measure the effectiveness of this in practice are missing due to a lack of feedback mechanisms to gather feedback on Member/Officer relations. There is evidence within Corporate Management Board minutes that this is already being addressed and was raised as a recommendation in the 2017 SWAP Ethics Audit.
- The Constitution is not referred to within the Corporate Induction Framework, which is important as the Constitution contains the Codes of Conduct and behavioural standards.

Codes of Conduct

- There is a need to update the Council's Whistleblowing Policy and ensure once updated that it is communicated to all Council staff. This was already recommended within the 2017 SWAP Ethics audit and we believe this is already being addressed.

Openness and Transparency

- There is no reference to the Council's view on good governance within the Constitution.
- There is a clear and publicised protocol for Freedom of Information Requests on the website, but the Council does not regularly publish requests and responses on their site (the latest being November 2016). This would reduce time spent answering repeat questions, and adhere with the expected levels of transparency as laid out in the Freedom of Information Act's Publication Scheme.

Complaints

- Note: Whistleblowing has been included in the code of conduct section above.

Decision Making

- None

Overview and Scrutiny

- None

Induction and Development

- While there is a schedule of mandatory and optional training available for Members, the mandatory list should be updated to reflect the updated GDPR training once in place.
- A Development Strategy could be implemented for the Leadership teams (various levels), in the same way that there is a Strategy for Members.

Communication

- There is no guidance within the Communications, Marketing and Engagement Team Plan regarding how officers (or Members) should handle a situation if they are approached for comment on a major issue, which could impact on the reputation of the Council.
- Consider the development of an 'overarching' Council Communications Strategy, separate from the Team Communications Plan. To include defined Strategies/protocol for instances such as Officer/Member communication if they're approached for comment on a major issue, and other communication related potential risks.

Stakeholder Consultation

- There is no guidance within the Communications, Marketing and Engagement Team Plan regarding how Officers (or Members) should engage and communicate with various stakeholders. This links to the above area for attention regarding a Council Communication Strategy.

Effectiveness Review

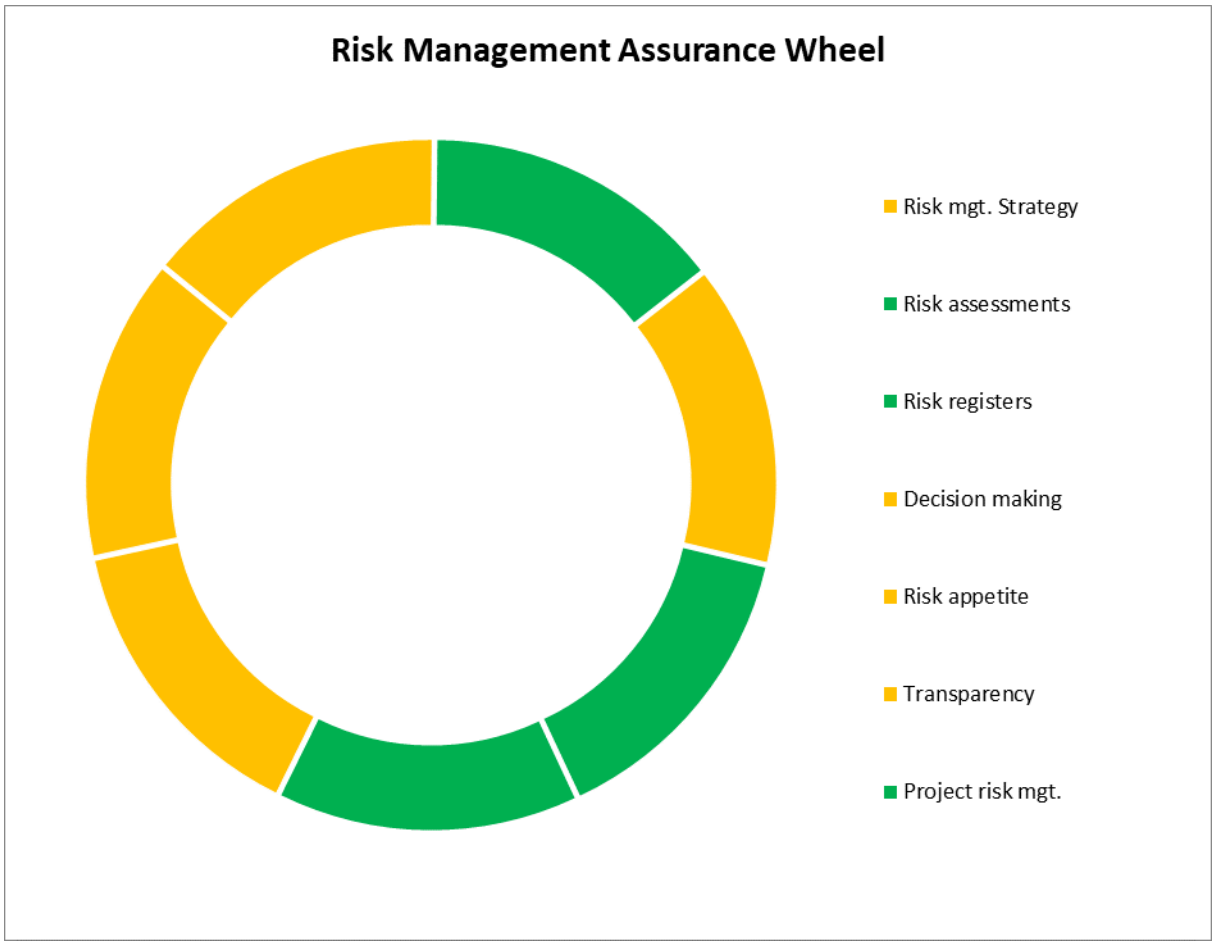
- The Annual Governance Statement could be improved if action points, timescales and responsibilities were included in either a table at the end, or within an appendix; to give clear communication of the issue which the action addresses, who's responsible for completing the action, the status of the actions and expected dates of completion.

Governance Certification

- None

2. Risk Management	AMBER

Effective Risk Management forms a key aspect of assurance and governance for an organisation. Organisations which can demonstrate and operate under a structured and active risk management approach are far more likely to be able to focus upon their key priorities and outcomes and, in doing so, take informed and robust decisions.



The **Amber** RAG rating has been given in recognition that this work is ongoing and needs to continue to further strengthen control frameworks to ensure that risk management practice is fully embedded across the Council. Given the progress seen to date there is good reason to believe that this will be achieved.

Risk Management - AREAS OF STRENGTH

Risk Management Strategy

- A Risk Management Policy is in place which is up to date, has been approved by Audit Committee and is reviewed annually.
- Responsibilities of staff and members are clearly defined within the Policy document.

Risk Assessment

- Project management standard documentation and guidance includes the need for a risk/issue tracker to be created and regularly reviewed.
- Directorate Business Plan templates include a section for a service risk register, which is reviewed as part of the quarterly Corporate Performance Assessment process.

Risk Register

- Corporate risks are reviewed and updated by management and the Insurance and Risk Officer at least quarterly.
- The corporate risk assessment is reviewed and taken to Audit Committee for approval twice a year.
- Corporate risks are also embedded within each Directorates Corporate Performance Assessment (CPA), monitored quarterly.

Decision Making

- Business cases include an assessment of the key risks; therefore, when taken before Members these risks are able to be reviewed as part of the decision making process.

Risk Appetite

- A 6x4 risk priority matrix in place to assess risk against likelihood and impact and the level of monitoring required for risks is clearly defined by three zones (red, amber, and green), which are depicted on the risk management policy's risk matrix.

Transparency

- The Council's approach to risk management is clearly defined and communicated to staff, members and the public via the Risk Management Policy, which is available online.
- The risk profile is communicated to Members twice a year in the form of the corporate risk assessment. This document is also available online for the public to view.

Project Risk

- The project management toolkit document includes a section on risk management, including the need for risks to be considered at all stages of a project.
- Project Managers are required to complete a risk/issues tracker prior to the commencement of the project, before using it as a live document throughout the duration of the project.
- Project Managers and Sponsors are often Service Managers or Directors, enabling risks to be considered at an appropriate level.
- For two of the sampled programmes/projects from the Programme & Project Management theme, there was a standing item for risk management within the project board meetings.

Risk Management - AREAS FOR ATTENTON

Risk Strategy

- Although the Policy is understood at a corporate level, it is possible that it is not within staff below management level.
- The same risk matrix should be utilised consistently throughout the Council (at least one other matrix is in use).

Risk Assessment

- Commissioning plans could be improved by making it a requirement for there to be a risk section.
- Although the Project Management documentation includes a requirement to identify and monitor risk, project risk is not included in the Risk Management Policy itself (see below).

Risk Register

- The register is maintained using word. A bespoke software solution would enable improved access controls, easier reporting and alerts when updates were required.
- The numerical threshold for risk tolerance is not explicitly referenced within the risk management policy, which may mean that there is a lack of clarity for staff and risks are not flagged for corporate review when they should be.

Decision Making

- The standard report to Members pro-forma does not currently include a section regarding the assessment of risk. Introducing this would ensure that risk assessment forms part of Members' decision making process. The assessment should include all options, including 'do nothing'.
- Current and residual risk scores should be provided within the risk section, which would also enable mitigating actions against these risks to be monitored, and reported back to Members as necessary, following their approval.

Risk Appetite

- To improve the guidance to staff further, the Council could set a numerical risk appetite value, which could be included within the Risk Management Policy's risk matrix to act as a visual aid to staff when considering risks.
- This numerical risk appetite value should be taken to Audit Committee as part of the current corporate risk register review schedule.

Transparency

- The Risk Management Policy does not assign a numerical value to outline what score is beyond the Council's risk appetite.
- The corporate risk assessment is not communicated with other local authorities and bodies.

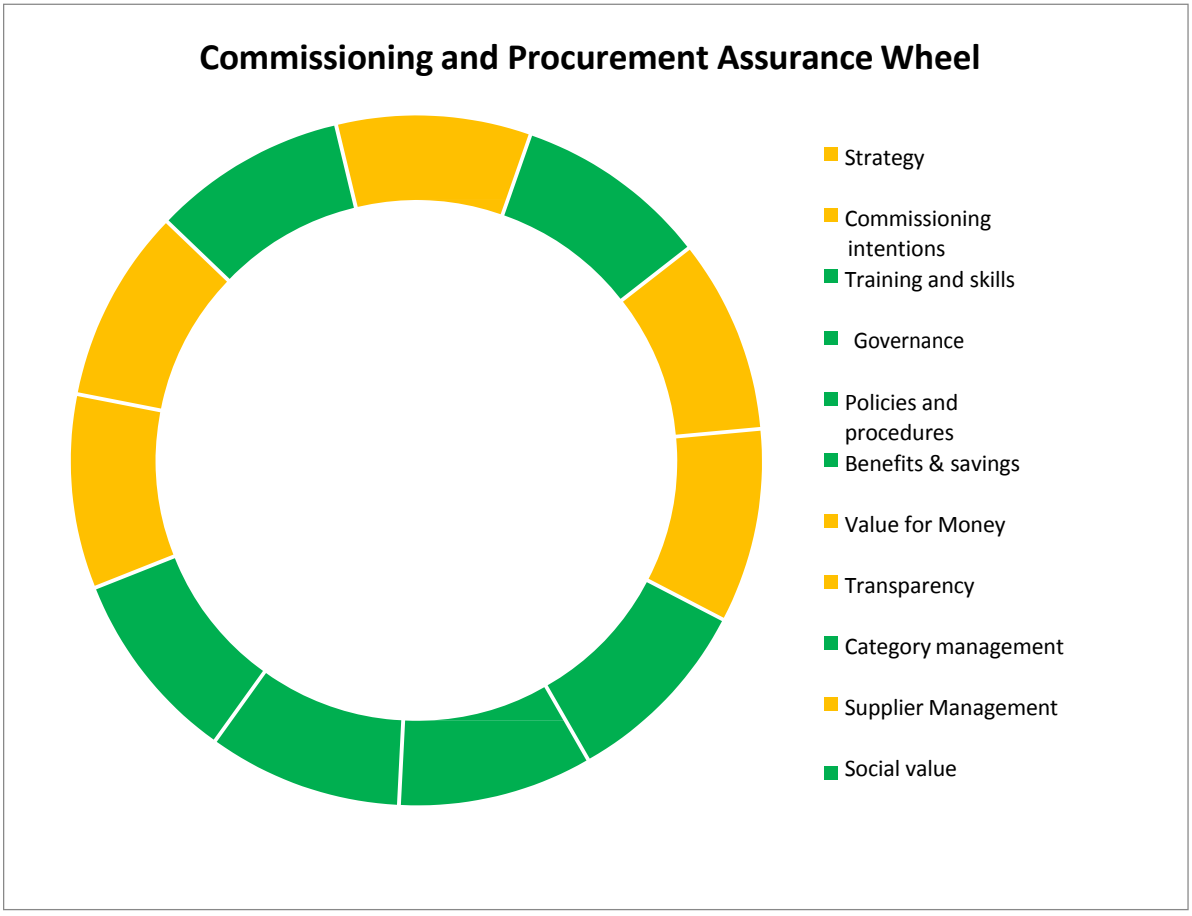
Project Risk

- The Risk Management Policy does not provide information regarding how project risks should be assessed and dealt with. There is also no information on raising project risks to risk registers.
- All projects should include risk management as a standing item on their project board meeting agendas.

3 Commissioning & Procurement	GREEN

Assessing Procurement & Commissioning activity of a Local Authority is a critical determinant in establishing its effectiveness in both being able to deliver benefit for its community but also in showing whether it can maximise VFM for its taxpayers.

Successful organisations understand the complex needs of their service users and design services which take into account the effectiveness of its internal provision against the market place to ensure taxpayers get the best value for money and the local economy is supported. The activity is complex and risky and therefore clear strategies, policies and plans are required which can be measured with appropriate targets that give the right level of assurance.



The **Green** RAG rating has been assigned because of the strong control framework in place in relation to corporate governance.

Commissioning & Procurement - AREAS OF STRENGTH

Strategy

- We sampled the Adult Social Care Commissioning Plan and the Procurement Strategy and found sufficient references to achieving value for money.
- There are plans in place to review/update the Procurement Strategy, to align with the present day Corporate priorities and services (following finalisation of the Contract Procedural Rules review scheduled for completion in April 2018).

Commissioning Intentions

- The Adult Social Care Commissioning Plan adequately documents the commissioning intentions of this Directorate and how the objectives will be achieved.

Training and Skills

- NVQ level 3 and 5 (Supply Chain Management) are being rolled out across the Corporate Procurement team.
- Procurement and Commissioning life cycles are clearly identified within the sample Procurement and Adult Social Care Commissioning Strategies viewed.

Governance

- The Corporate Procurement team enforce the requirement of a Delegated Authority being provided prior to commencing procurement.
- The levels of authority required for Procurement thresholds are adequately documented within procedure documents.
- There are effective mechanisms in place to communicate and monitor performance, and to take action where necessary.

Policies and Procedures

- Model Service Level Agreements (SLA) are in place between the Social Care and Wellbeing Directorate and its suppliers, as a condition of contract.

Benefits and Savings

- Of the samples viewed, Key Performance Indicators have been established within Business Plans and are reflected in KPI/Contract monitoring evaluation documents.
- Of the SLA sample report viewed, where targets had not been met there were sufficient actions put in place to resolve these and there is indication that the status of these will be reported on at future reviews.

Value for Money

- Value for Money targets are communicated well to potential suppliers via the website and in the Adult Social Care Commissioning Plan and are included within the contract monitoring arrangements of existing suppliers.
- Sufficient evaluation of tenders and final tender bids were performed to ensure that Value for Money was achieved in the case of the Transport for Schools Bus Contracts.
- A performance management system is in place for the Transport for Schools contracts to ensure Value for Money throughout the duration of the contracts.

Transparency

- Procurement frameworks and practices are operating in accordance with the National Procurement Service and Public Contract Regulations 2015.
- A maintained Corporate Contracts Register is in place.

Category Management

- The approach to Category Management is included in the Procurement Strategy.
- Category Managers are in place for each Directorate and are nominated due to their Service specialisms.

Supplier Management

- The 'Supplier Manager Framework' is modelled around the NPS (National Procurement Service) frameworks, with adequate amount of supplier and contract monitoring in place.

Social Value

- There is a standard procedure which clearly denotes the stages of procurement including stakeholder engagement at the start of the procurement process.
- Development of stakeholders is considered for staff, existing suppliers and for Members to actively engage with Procurement processes.

Commissioning and Procurement - AREAS FOR ATTENTON

Strategy

- Although we understand there are plans to update them, the current Adult Social Care Commissioning Plan and the Council's Procurement Strategy do not represent the current Priorities of the Council as they were developed prior to the current Corporate Plan 2016-2020.
- Commissioning is devolved within the Council to Service level. Without corporate oversight there is a risk that other Commissioning Plans/Strategies do not link to the current Corporate Priorities of the Council.

Commissioning Intentions

- Although Commissioning intentions were located for Adult Social Care, no other Directorate Commissioning Plans could be located.
- The Commissioning Plan viewed (Adult Social Care) was not found to be readily available to the public. Rather than finding it published via the website, it was part of a 2010 Cabinet Agenda pack. Potential suppliers are unlikely to be able to locate it to understand the Council's commissioning intentions for this Service area.

Training and Skills

- There are no 'required personal qualities/qualifications' indications within the Adult Social Care Commissioning Plan or elsewhere on the Intranet, to identify what skills and/or qualifications the Commissioning teams require to be effective in their roles.

Governance

- None

Policies and Procedures

- Although plans are in place to update them, the existing Procurement Strategy and Contract Procedure Rules do not reflect the Public Contract Regulations 2015.
- With the exception of the Social Care and Wellbeing Directorate, we were not able to confirm whether Service Level Agreements are in place between other Directorate services and their suppliers.

Benefits and Savings

- None

Value for Money

- Ensure that there are adequate performance monitoring, supplier support and management arrangements in place to address potential issues of the Waste Management Services supplier being able to fully meet their contract requirements.

Transparency

- See Policies and Procedures above.

Category Management

- The Contract Procedure Rules do not currently include information about identifying savings targets and category opportunities or indicate where these should be recorded for each Directorate.

Supplier Management

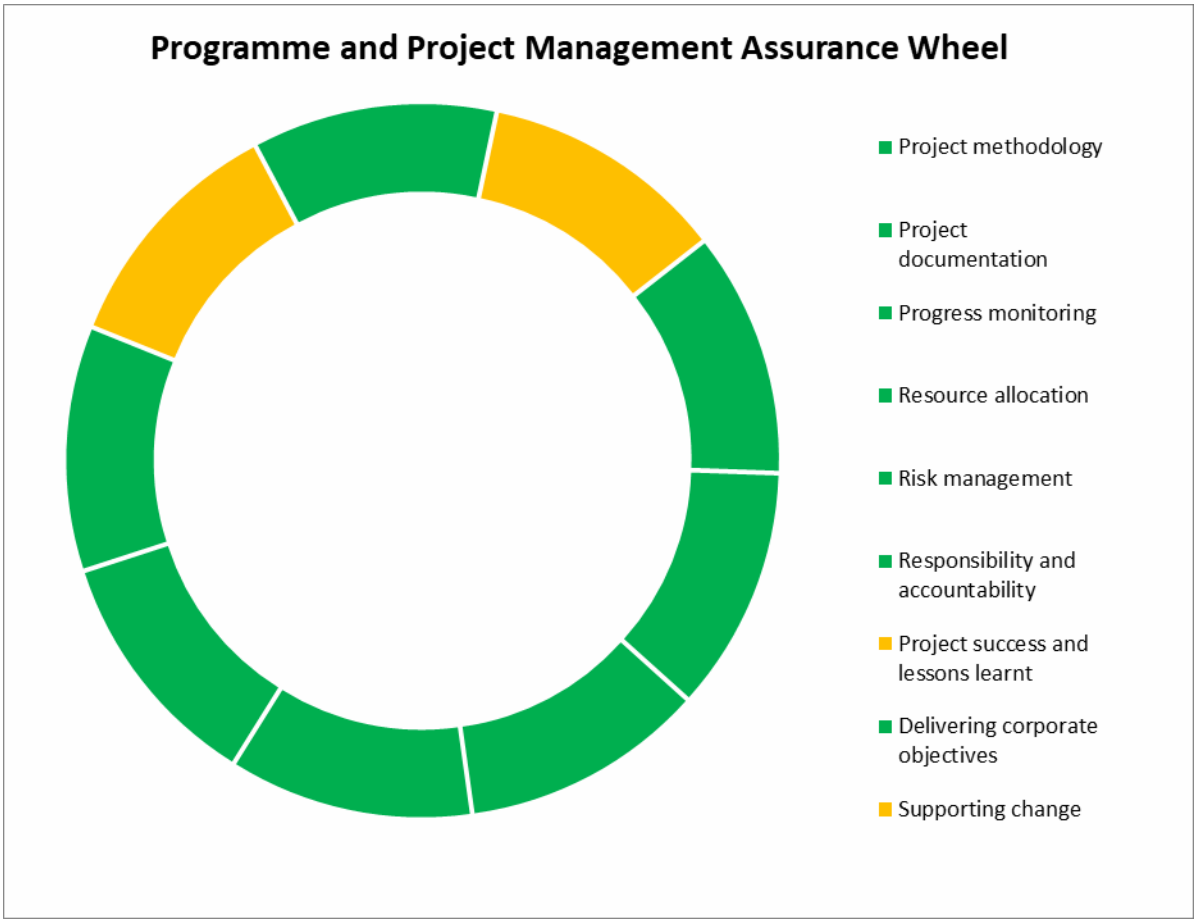
- The authority can identify their 'Key suppliers' via the Corporate Contracts Register, but should consider creating either a central document, or separate Directorate documents, identifying key suppliers in their areas in terms of value, risk and business criticality.
- The Business Continuity Plans for the Communities Directorate and for the ICT Service Group are both out of date.
- Consider inclusion within Directorate Business plans of a Key Suppliers List in terms of criticality and risk, with clear steps (or 'action cards') to follow in the event that a supplier becomes unavailable.

Social Value

- None

4 Programme & Project Management	GREEN

Effective Programme and Project Management forms a key aspect of assurance and governance for an organisation. Organisations which can demonstrate and operate under a structured and active approach are far more likely to be able to focus their efforts and successfully achieve the delivery of anticipated outcomes and their associated benefits. It is important that programmes and projects are clearly defined and resourced. Equally they need to demonstrate a clear link to the delivery of corporate aims and objectives and be adequately governed.



The RAG ratings given are reflective of this. The **Green** RAG rating has been assigned because of the strong control framework in place.

Project Management - AREAS OF STRENGTH

Project Methodology

- Standard project methodology is in place with templates available which are reviewed on an annual basis.
- Guidance is available for staff in the form of a comprehensive toolkit which is

updated annually.

Project Documentation

- Central oversight of corporate programmes and projects is provided by the Corporate Transformation Team, who maintain a database of corporate projects.
- Each of the programmes/projects sampled had sufficient documentation to support them, such as Project Initiation Documents and business cases.
- The scope, anticipated outcomes, and estimated costs were detailed within the documentation of the sampled programmes/projects.

Progress Monitoring

- Clear approval, reporting and monitoring arrangements were in place for each of the sampled programmes/projects.
- Quarterly Corporate Performance Assessment meetings take place with Senior Management and Members, which include updates on progress of projects.
- Monthly updates to Programme Management Board take place for each of the Corporate Programmes.

Resource Allocation

- The Project Initiation Documents for each of the sample programmes/projects included details of the members of staff required to undertake the work, along with their area of expertise.
- The capacity requirements in relation to the programmes/projects were clearly defined for most of the cases sampled, including information on whether parts of the work would be outsourced.

Risk Management

- The project management toolkit document includes a section on risk management, including the need for risks to be considered at all stages of a project.
- Project Managers are required to complete a risk/issues tracker prior to the commencement of the project, before using it as a live document throughout the duration of the project.
- Project Managers and Sponsors are often Service Managers or Directors, enabling risks to be considered at an appropriate level.
- For two of the sampled programmes/projects, there was a standing item for risk management within the project board meetings.

Responsibility

- Programme/project initiation documentation requires the project roles to be defined.
- For each of the sampled programmes/projects, the roles are defined within initiation documentation. Each of these roles are being undertaken by staff of appropriate seniority.

Lessons Learned

- The need for benefits realisation were included within the initiation documentation of the sampled programmes/projects.

Delivering Corporate Outcomes

- Senior Leadership Team and elected Member oversight of core Council programmes

ensures that the objectives of the programmes are linked to corporate objectives on an ongoing basis.

- The Corporate Transformation Team's project databases clearly outline which corporate priority the project is linked to.

Supporting Change

- For the sampled programmes/projects, a representative from HR had been identified to assist with the proposal. This should enable the project to be aligned to the organisational development needs of the Council.

Project Management - AREAS FOR ATTENTON

Project Methodology

- Although projects with a corporate impact will have some involvement from the Corporate Transformation Team, it is possible that some smaller projects are being completed in silo with the standard templates not being utilised.

Project Documentation

- Some smaller scale projects may not follow the corporate approach to programme and project management.

Progress Monitoring

- None

Resource Allocation

- Minor instances of a lack of clarity were identified within one of the sampled programmes/projects (Digital Transformation), in terms of capacity requirements for the programme.

Risk Management

- The Risk Management Policy does not provide information regarding how project risks should be assessed and dealt with. There is also no information on raising project risks to risk registers.
- All projects should include risk management as a standing item on their project board meeting agendas.

Responsibility

- None

Lessons Learned

- Information on the success of projects is not collated centrally so that corporate oversight of can be maintained over the outcome of completed projects.

Delivering Corporate Outcomes

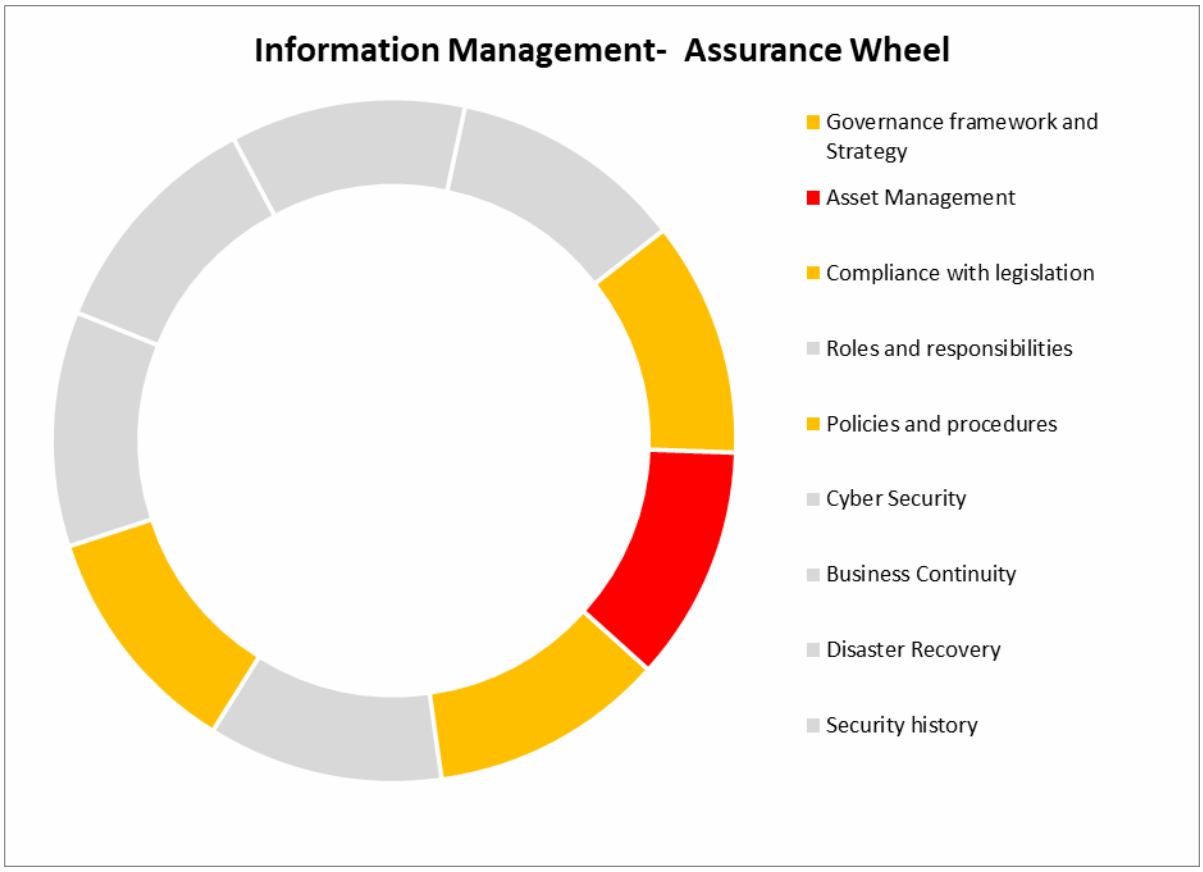
- None

Supporting Change

- The project initiation documentation templates could require additional information in relation to cultural change and the likely impact upon staff.
- Providing additional feedback mechanisms to staff may make proposals to change be better received, as recommended within the 2017/18 Ethics audit.

5 Information Management	No Conclusion

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.



Although we met with the Group ICT manager to discuss the programme of work, we were unable to obtain sight of some key pieces of information to verify the controls in place. We are therefore unable to conclude on this theme and have instead highlighted the areas we sought to confirm and included them in the Improvement Plan as areas for the Council to satisfy themselves over.

Information Management - AREAS OF STRENGTH

Strategy

- There is clear reference within the ICT Strategy to the Corporate Plan and supporting its priorities.
- Goals and priorities of the ICT Service are included in the ICT Strategy.
- There is a bi-monthly Information Governance Board in place, which is a requirement of PSN/CoCo compliance.

Asset Management

- Mandatory ICT Policies have been identified and are included within the Corporate Induction training for all employees and further Policies are including for those staff in specific posts.

Legislation

- GCSx classified email accounts are in place for those who are required to send information externally.
- There is an Electronic Document Records Management system in place.
- Policy and Privacy notices are already under review in advance of the GDPR deadline, with the Data Retention Policy having been approved by Cabinet.
- Information is being gathered to inform an Information Asset Register.

Roles and Responsibilities

- None

Policies and Procedures

- Although out of date, the current suite of ICT Code of Conduct and Policy/Strategy is available to all staff via the Intranet.
- Information Security is addressed broadly throughout the Code of Conduct available to staff via the Intranet.

Cyber Security

- None

Business Continuity

- None

Disaster Recovery

- Although untested, we have been advised that a system back up process is in place.

Security

- Mandatory training covers Data Protection.
- Adequate processes appear to be in place to report security breaches to the SIRO.

Information Management - AREAS FOR ATTENTON

Strategy

- There are no formal plans or timeline for updating the IT Strategy or having it formally approved.
- The existing ICT strategy does not include a 'roadmap' plan of the technologies/ transformational programmes underway or due to start.
- There is a list of anticipated 'programmes'/technology being implemented under priority action plans, but no roadmap given to indicate timescales for implementation.
- More regular and formal meetings between ICT teams and ICT Management would help to ensure that targets are being met and progress monitored.
- The Information Management Strategy requires review to ensure that it reflects accountability for the various Information Governance roles clearly, including the Data Protection Officer Role.
- Although we have been advised that KPI reports are being reported for quarterly review by the Head of Operational and Partnership Services and further by Cabinet, at the time of the audit we were unable to verify whether Key Performance Indicators were in place and being monitored for the ICT Service as the most recent Performance Indicators report to Cabinet did not include those for ICT. The ICT Group Manager is looking into why this is.
- We are not aware of any Service Level Agreement in place for ICT Services.

Asset Management

- There is no documented plan regarding ICT Asset Management. Therefore, it has not been possible to review the impact of ICT assets on areas such as service desk, change management, procurement processes, release processes or staff leavers.
- Due to there not being an ICT Asset Management Plan in place, there is no documented direction as to how hardware or software asset management functions should be run, nor intended goals of this service. There is also no indication given therefore to the punitive impact of breaching said Policy/Plan.
- From a sample of policy documents reviewed, document control measures are not in place.
- From a review of the Intranet, no policies or guidance was found on the following in relation to asset management: procurement, release to the environment, finance, licensing, or disposal.
- At the time of the audit we were unable to confirm the following:
    - Whether asset lifecycle management is in place for all ICT Assets.
    - How the Council knows whether its ICT policies have been read and understood.
    - Although we understand that a Configuration Management Data Base in is place, we were unable to verify further details.

Legislation

- The ICT Strategy Does not define which legislation/regulations the ICT Dept comply with.
- Although the Information Management Policy does include details of relevant

legislation, it does not confirm what action will be taken should there be a breach of the Policies.

- In the absence of an Asset Management Plan, we found no reference towards the consideration to the following legislation:
    - Disability Discrimination Act means that any employee has a right to equipment that will give them the same access to resources as their more able bodied colleagues.
    - Waste Electrical Electronic Equipment, Regulations (WEEE).
    - Copyright Designs and Patents Act is what protects the misuse of software and the Council needs to ensure officers understand what they can and cannot do with software while using Council systems or delivering work for the Council.
- The ICT Code of Practice – Handling and Classification Policy requires review as the version we obtained was dated 2011.
- There is little evidence of discussions regarding the GDPR Project Plan deadlines, due to the lack of minutes/record of the process.
- Due to conflicting information, there is confusion over who will be responsible for the Council's DPO role in the long term
- The Retention Schedule requires review to ensure compliance with the relevant Retention Guidelines for Local Authorities and other Acts as necessary.
- GDPR awareness has not already been rolled out amongst staff but is being developed for implementation in May.

<u>Roles and Responsibilities</u>

- At the time of the audit we were unable to confirm the following:
    - Whether all posts within the ICT service were filled, or whether the service had vacancies.
    - Whether the role profiles match expectations in terms of delegations and responsibilities.
- Due to conflicting information, there is confusion over who will be responsible for the Council's DPO role in the long term
- There were no structure charts available on the intranet. An ICT Structure chart was provided from the I-Trent software, but this lacked the detail required for audit testing.

<u>Policy and Procedures</u>

- Several ICT Policies were noted as being out of date back to 2008-2011, with the exception of the Social Media Protocol and related documents which were reviewed in 2017.
- Equality & Diversity should be considered as part of any policy update (Discrimination Act regarding ICT Asset rights etc).
- No policies were identified surrounding removable media devices, mobile ICT equipment/assets use, or security/protection
- An action plan (or an appendix to) should be included within the revised ICT Strategy with timescales, responsible persons for actions and method of review.
- The Intranet requires update with revised documents when available, ensuring that all documents referred to within the Strategies and Policies are available as stated

within the Intranet.

- At the time of the audit we were unable to confirm what advanced training has been undertaken by relevant ICT staff, and there were some instances within the ICT Training matrix provided where mandatory training was incomplete. Generally, the ICT Training matrix lacked detail.
- Although the Corporate Induction Framework indicates that all staff receive mandatory basic ICT training as part of the Corporate Induction, the Group ICT Manager confirmed that only 'relevant' staff receive this.
- Neither the Appraisal form nor the Employee Appraisal Protocol includes a requirement to confirm whether relevant policies have been read and understood.

Cyber Security

- Although we have been 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 not of the granularity to confirm implementation of any recommendations, with no timescales or accountabilities were identified in the plan.

Business Continuity

- Although we have been advised that a 'critical' applications list is stored within the Configuration Management Data Base and that a system owner from ICT is in place for each application along with a representative from each service, we have been unable to verify this at the time of audit testing, or check the list is up to date.
- We have been advised that Tier 1 applications are those listed within the ICT Business Continuity Plan, and the process of identifying these applications took place approximately 3 years ago, and as such may require update. We were provided a copy of the ICT Business Continuity Plan at a late stage in the audit testing, but this provided only partial plans for the recovery of some applications within it and did not clarify which of those were critical applications.
- We have been advised that the ICT Business Continuity Plan is approximately 2 years out of date and requires review. It was last tested in May 2016 but is not expected to be reviewed until completion of a large server 'reshuffle' later this year.
- The back-up schedule provided to us and discussion with the Servers and Storage Manager identified that backup storage is completed by transfer onto discs held for a maximum of 2 years, which are held within an unsecured appliance in the access controlled production site, and that the same was true for the Disaster Recovery storage location.

Disaster Recovery

- Although we have been advised that there is an ICT Business Continuity Plan, at the time of the audit we were unable to verify this or check whether the contacts contained within it were up to date. We understand that it does not link into a Corporate/Council-wide Continuity/Disaster Recovery Plan.
- A search on the Intranet could not identify Disaster Recovery or Business Continuity guidance.
- Although the back-up process was explained to us, at the time of the audit we were unable to very whether a back-up schedule is in place and adhered to.

Security

- Security breach Codes of Practice/ relevant Strategies need to be updated regarding the implementation of GDPR.
- We understand that all security breaches are recorded on a central spreadsheet by the SIRO. However, at the time of the audit we were unable to obtain a copy and were therefore unable to test the extent to which breaches are reported to the ICO.
- Similarly, we were unable to test whether security breaches are monitored, and action plans followed to mitigate/reduce potential breaches, having been input into the central spreadsheet.

Detailed Assessment

1. Corporate Governance

Service Leadership – Low Risk
The Council's Chief Executive has been proactive in addressing potential gaps in the Corporate Director team by instigating interim posts to avoid any shortfalls in between recruiting permanent Heads of Finance and Education/Family Support Directors. These interim positions are based on open-ended agreements, to ensure continuity of the department's management.

Corporate Management Board meetings are held weekly and are more of a 'Strategic Forum' than a decision making committee. These meetings have agendas and minutes, but no formal Terms of Reference structure, to allow the flexibility to raise and discuss urgent matters arising. However, a review of the minutes found there to be a lack of information regarding follow-up of actions agreed, with deadlines sometimes unclear. Where meetings were cancelled, some agenda items were not picked up at the following meetings.

It was pleasing to note in recent Corporate Management Board minutes that the Head of Education & Family Support has been asked to action the recommendation raised as part of the recent Ethics Audit regarding upwards feedback from staff to management. However, no follow up conditions were noted/set for this within the minutes.

Corporate (County) Plan - Low Risk
The Corporate Plan was written by the Chief Executive and the Leader of the Council, and an amendment/review was approved at Full Council in March 2017. The Corporate Plan identifies the Council's priorities and is subject to an annual review, confirmed verbally by the Group Manager for Corporate Performance, Partnerships & Transformation. There is no document control table within the Corporate Plan, although the date of the review is given on the first/cover page of the document. The Corporate Plan has been communicated via various means to different stakeholders, electronically and in paper form.

The current Corporate Plan is a four-year plan, under regular (annual) review to align the Council's priorities for the year ahead. The Chief Executive is involved in the development of the Plan and there is sufficient use of public consultations to inform the Plan. New performance indicators have been developed within the plan to allow for better performance analysis in coming years. The Corporate Plan is communicated widely to the public, via social media campaigns, local radio channels, local newspapers, the BCBC website and in the local libraries.

Constitution – Low Risk
The Constitution document agreed by the Council is in place to set out how the Council operate including Member/Officer responsibilities in relation to each other, how decisions are made and the procedures which are followed in order to ensure that these are transparent, efficient and accountable to stakeholders. The Constitution is under regular review and is updated when there are changes made to processes which affect its contents. However, there

was a lack of consideration within the document surrounding the commissioning procedures, responsibility and protocol.

Effective Working Relationships - Medium Risk
The Corporate Induction Framework aims to deliver sufficient information to inform Council staff and Members of their roles, responsibilities and duties; as well as setting out protocol for collaborating with one in other. However, there is no direct mention of the Constitution within the Induction framework, which is the Council's 'bible' of procedure and protocol. There is a lack of feedback mechanisms, as already identified within the recent Ethics audit, for Members to provide feedback to officers, and vice versa. Once these are in place it is anticipated that this area will move from medium to low risk.

Codes of Conduct – Medium Risk
The Codes of Conduct for members/officers are well documented within the Constitution and are influenced by the National Assembly National Standard. Codes of Conduct are a mandatory part of the staff induction training and period reminders come in the form of personal appraisals or by email if an amendment/new Code of Conduct has been created. Declarations of a Conflict of Interest guidance can be found within the Constitution, and also forms part of the contract of employment for staff.

The Whistle Blowing Policy has been identified as out of date within the recent Ethics audit. Once this policy has been updated it is anticipated that this area will move from medium to low risk.

Openness & Transparency – Medium Risk
The Constitution is readily available to the Public via the Council website. The Constitution gives no clear indication to the Council's views on good governance, although it refers within the Functions of Committees and Responsibilities of Officers sections to aspects of governance. The Constitution does refer to the Council's approach to transparency. The Council publish the agendas, minutes and forward plans publicly via their website, so that the public can locate information about issues that are important to them.

The Council have not self-published their Freedom of Information requests and responses on their social media or web page since November 2016. On discussion with the Information Officer, the Council currently rely on the person receiving the Freedom of Information response and on a website which is not controlled by the Council to publish the requests and responses. We recommend publishing the requests and responses on the Council's website to move the risk rating on this element from medium to low risk.

Complaints – Low Risk
Complaints procedures are readily communicated to the public via the Council's website, along with guidance on raising a complaint to the Ombudsman in the event that they feel their complaints hasn't been addressed sufficiently. This Policy clearly notes the timeframes in which the Council will respond.

Decision Making – Low Risk
The Constitution document clearly defines the process and responsibility for the Budgetary and Policy decisions that are to be made by the Council. Minimum requirements for obtaining

advice and consultation to inform Policy and Budgetary changes are clearly identified within the Constitution, along with timeframes for each activity, such as periods of consultation. The committee decisions within a cross-section of meeting minutes appear to be well-informed, taking consideration from Members and Officers together and coming to mutual decisions by all.

Overview & Scrutiny – Low Risk

There is an Audit Committee and a Standards Committee in place at the Council, which are held at least quarterly. Attendance of the expected persons at these Committees appears to be good. The Audit Committee and Standards Committee Terms of References are within the Constitution document, and these Terms of References clearly identify the purpose of the committees and the expected outputs.

Member & Officer Induction and Development – Low Risk

There is a Corporate Induction Framework in place which includes Members training programmes. This Induction ensures that mandatory training modules are completed, that essential and additional workplace information is provided (roles, responsibilities and duties of Members) and that there is a follow up after the training has taken place. The Induction is structured to give sufficient training and information to Members, to allow them to be effective in their roles.

Training is designed and delivered by a range of internal and external providers, approval of which comes in the form of feedback survey review. External providers are usually selected using the Welsh Local Government Association suppliers list. There is an "Event Feedback" form available to Members, who are invited to provide feedback on any training that they receive. There is plenty of opportunity for development and a lot of support is available to Members in order to aid their personal targeted training and development plans; as well as sufficient review/monitoring of their development.

The Corporate Induction Framework is used to deliver induction training to Leadership teams, to ensure the delivery of mandatory training modules and provision of the individual's responsibilities, duties and their department's functions within the Council. In addition to this, the Chief Executive and HR department collaborate to implement further top-level training as/when required.

As is the case with the Members training design and delivery, Leadership Team training is conducted both internally and in some cases by external providers. Feedback mechanisms are available to the Senior Leadership Team, to feedback their experience of training received.

Communication - Medium Risk

The Council do not have an overarching Corporate Communications Strategy, but a Communications, Marketing and Engagement Team Plan exists for the 2017-18 period. There is an explanation which indicates the Council's agreed approach to engaging with the public and other stakeholders, but no table of scenarios/issues that have been identified as requiring corporate engagement and/or consultation. The Communications, Marketing and Engagement Team Plan identifies the actions/steps that the Communications teams will take to promote the Council's corporate identity. There is no clear guidance/procedure which Council staff or Members should follow to handle a situation if they are approached for

comment on a major issue which could impact on the reputation of the Council. Separation of the corporate strategy from the operational activities of the Communication Team, and their Team Plan, would be sufficient to move the risk rating from medium to low risk.

Stakeholders Consultation – Medium Risk
While stakeholders have been identified within the Communications, Marketing and Engagement Team Plan, there is no identification of the stakeholder groups that should be engaged with for a range of potential scenarios. As this is not a corporate document, there is a risk that stakeholders are not engaged with in a way that best meets their needs or the Council's needs.

Effectiveness - Low Risk
The Head of Finance's Annual Governance Statement (AGS) for 2016-17 report to Audit Committee shows the AGS being submitted for approval by the Audit Committee, and minutes show subsequent approval of the AGS 2016-17. The AGS can be found within the Statement of Accounts 2016-17 on the Council's website. While there was a description of the Actions within the Statement, and the Corporate Management Board appear to monitor achievement of these actions, there was no document available publicly as an appendix to the AGS showing the issues from which the actions arise, the responsible person for seeing the actions through, the status of the actions nor the expected timescales for completion.

Governance Certification – Low Risk
The Annual Governance Statement 2016-17 sections accurately included the opinions of both internal and external assessors. Minor improvements could be made to ensure the source of all findings and actions are consistently referenced within the report.

2. Risk Management

Risk Management Strategy – Medium Risk
The Council has a Risk Management Policy which is updated on an annual basis. Following review by Senior Management Team, the Audit Committee reviewed and approved the document. The document clearly defines the roles and responsibilities in relation to ensuring the policy is effectively implemented. The policy is available to staff via the Council's intranet site, although we were advised by the Insurance and Risk Officer that staff below managerial level may not have a full awareness of the Council's risk strategy. We also noted that more than one risk scoring matrix is in use within the Council. The Education and Family Support Directorate utilise a 5x5 scoring matrix rather than the 6x4 matrix outlined within the policy.

Medium risk has been assigned to this area on the basis that it may not be fully embedded throughout all levels of the Council, and differences appear in the methodologies across services.

Risk Assessment – Low Risk
Service risk registers are built into annual Directorate Business Plans, with a section for this included within the template document. They are considered on a quarterly basis through the Corporate Performance Assessment process. The project management toolkit includes the need for a risk/issue tracker to be completed and regularly reviewed, for which there is a template to be used. However, this approach is not reflected within the Risk Management

Policy. There is not a standard template for commissioning plans and this review has shown that the considerations towards risks to the achievement of commissioning intentions could be enhanced (see Commissioning and Procurement section of the report).

Risk Registers – Low Risk
The Council's Corporate risk register is managed by the Insurance and Risk Officer using Word. On a quarterly basis, meetings are held with a representative from each Directorate, to discuss any changes in risks within the quarter, both for risks currently on the corporate risk register and any new risks within the Directorate. Following this process, the corporate risk register is updated as necessary and then taken to Senior Management Team for review.

Each risk within the corporate risk register has an owner, who is responsible for monitoring and challenging performance of the risks they own.

Twice a year, a full corporate risk assessment is taken to Audit Committee for review and approval.

As noted in the risk appetite section, there is no numerical threshold or tolerance above which risks are included in the risk register.

Decision Making – Medium Risk
The standard report to Cabinet template does not contain a section for the consideration of risks or issues within a proposal. Some areas of risk are outlined within a business case for a project, however it would be of benefit for the consideration of risk to be a standing heading within the report which goes to Members, to ensure that an assessment of risk occurs at the earliest opportunity in the decision-making process for both formal projects and other approval requests. This could also include current and inherent risk scores, which would allow mitigating actions against these risks to be monitored once the request has been approved.

Risk Appetite – Medium Risk
The Council uses a 6x4 risk scoring matrix to access risk against likelihood and impact. Their score defines each risk into zones (red, amber and green), which determines the level of monitoring the risk should receive. This is depicted within the Council's Risk Management Policy. There is, however, not a numerical tolerance level in place, a figure in which if the risk scored higher than, it would be deemed as "out of tolerance".

Transparency – Medium Risk
The Council's Risk Management Policy and corporate risk assessment are available to members of public via the Audit Committee minutes on the Council's website. The documents are also available to staff via the intranet. Risks are monitored and reviewed on a regular basis between managers and reported to Members every six months.

The corporate risk assessment is not currently shared with other local authorities and bodies. Introducing this would provide opportunities for shared learning. The medium risk rating has been awarded because the lack of a numerical risk tolerance threshold makes it difficult to determine whether a risk sits within acceptable limits.

Project Risk Management – Low Risk
Within the Council's project management toolkit document, there is a section on risk management. This includes the need for risks to be considered at stages of a project, with project teams expected to utilise a risk/issue tracker to assist this process. The Sponsors and Managers of projects are often Service Managers or Directors, thus enabling key project risks to be considered at an appropriate level within the Council. For two of the four sampled programmes/projects within the Programme & Project Management theme, risk management is a standing item on project board meeting agendas.

The risk management policy does not provide information regarding how project risks should be assessed and dealt with. There is also no guidance regarding the need to raise some project risks to the corporate risk registers (see risk appetite section above).

3. Commissioning and Procurement

Strategy – Medium Risk
The 2012-14 Procurement Strategy requires an update to bring it in line with the current Council priorities and services. This is already in hand, as explained by the Corporate Procurement Manager.

We sample checked the Adult Social Care Commissioning Plan and the Procurement Plan and found both to have good links to Value for Money within their approach.

Although links to the Corporate Priorities of the Council are reflected within the Adult Social Care Commissioning Plan sampled, the Council will need to ensure that this is replicated elsewhere too as there is no central Corporate oversight process in place.

A medium risk rating has been made on the basis that there is no corporate overview process for commissioning and the Procurement Strategy requires update.

Commissioning Intentions – Medium Risk
There are no central commissioning documents outlining the commissioning strategy of the Council as a whole, and no other commissioning plans available other than the Adult Social Care plan were identified in the course of the audit. There are commissioning intentions within the Adult Social Care plan which provide sufficient information regarding the aspirations and plans of action for the Directorate, but these are not published making them inaccessible by potential suppliers.

Training and Skills – Low Risk
The Procurement Strategy together with the Adult Social Care Commissioning Plan clearly identify the Commissioning and Procurement life cycles. The Procurement Strategy identifies the required training and competencies for the procurement department. The Commissioning Plan is more focussed around the skills required of the Operational care staff/volunteers and does not mention the corporate training required for the staff 'behind' the Commissioning processes at the Council. A procurement skills need assessment delivered the verdict that an NVQ should be rolled out across the Procurement team, to align skills across the board. This was subsequently approved and is due to go ahead.

Governance – Low Risk
The Corporate Procurement Manager described the Delegation of Authority processes in place and confirmed that these were adhered to. The Delegated Authority, Scrutiny and Cabinet approval levels explained by the Corporate Procurement Manager align with the requirements of the Public Contract Regulations 2015. The approval levels are documented within the Contract Procedure Rules (within the Councils Constitution document).

We found that the Commissioning team performance and achievements are monitored within the Adults Social Care Directorate by Key Performance Indicator reviews on a regular basis and in accordance with the Performance Management Framework. Reports on performance are also fed upwards via the Corporate Director for Social Services and Well-Being to Cabinet within relevant reports which also feature the record of savings by Procurement.

Policies and Procedures – Low Risk
The Council's Contract Procedure Rules were last updated in 2012, as were the Procurement Strategy (including Sustainable Procurement Strategy) but are all undergoing a review/update at present, as informed by the Corporate Procurement Manager.

These are all readily available; the Contract Procedure Rules within the Constitution are available to the Public via the Council's website, and the Procurement Strategies to staff internally via the Intranet, though not readily available to the Public.

There is no document published specifically regarding cost guidance on the Procurement life cycle, but tenders are awarded using the MEAT (Most Economically Advantageous Tender) mechanism.

There is no stand-alone Social Value Policy, instead with social values being communicated throughout the Procurement Strategy within procurement objectives.

The Contract Procedure Rules and Procurement Strategies are out of date and therefore do not refer to the most recent edition of the Public Contract Regulations (2015). However, there is evidence that the outdated edition is no longer being used in practice and that Public Contract Regulations 2015 compliance is in place.

There is a Commissioning Team tool to show the Commissioning/Procurement life cycle, which was provided by the Commissioning Manager for Social Services and Well-Being Directorate. This Commissioning tool echoes the Procurement Management Framework which is in place surrounding the Analyse, Plan, Do, Review cycle.

There was a sample Model Service Level Agreement provided by the Commissioning Manager for Social Services and Well-Being Directorate, which was completed by the supplier and submitted back to Procurement for review as a condition of the Contract Terms and Conditions which indicates that Service Level Agreement reviews are taking place.

Benefits and Savings – Low Risk
Key Performance Indicators and Service Level Agreement reviews are in place for all service teams, including for Procurement and Commissioning/Contract Management teams. KPIs are

established via a number of methods and are agreed by Corporate Management at Directorate Board meetings, for inclusion within the Directorate Plan.

Monitoring is undertaken in the form of Service Level Agreement/KPI reviews and contract reviews on a regular basis, including supplier self-assessments of their services provided and an analysis of gaps/areas for improvement. For example, targets within the Contract Review document for Adult Social Care provider People First indicate that targets are largely being met. The Service Level Agreement review document for People First showed some areas in Quarter 3 which require improvements, and there were actions put in place to achieve these. Corrective Actions for when targets have not been achieved are decided on and initiated during Corporate Management Team meetings.

Value for Money – Medium Risk

Value for Money is documented within the Procurement Strategy and Sustainable Procurement Policy, both of which require an update to align with the current Council Priorities. There are no 'quantitative' measures mentioned within these documents whereby the Council assess Value for Money, nor social value, although Value for Money would be assessed during supplier contract reviews. There is communication of the Council's requirement to achieve Value for Money within the guidance provided to potential suppliers and it is stated publicly via the Council's website procurement page. Value for Money is communicated also within the service Commissioning Plans, although these are not published and accessible by the public/potential suppliers. Guidance, evaluation tools and scoring used by those assessing was evidenced within the Specific Conditions of Tender document provided, which is given to Tendering Contractors.

There is concern regarding the performance management and therefore Value for Money in relation to the Waste Management Contract's performance management, as it was advised that the supplier is currently under a self-certification agreement with the Council and that the Contractor submits payment slips with the relevant defaults under the performance management framework and that the information submitted is checked/audited by the Neighbourhood Service team. The Council are unable to fully rely on the information being supplied by the Contractor at present as they are having difficulty in putting the systems/processes in place to operate with the way the contract has been designed.

The Terms & Conditions/Contractual agreement in place for the Transport for Schools contracts were provided, which outlines the monitoring the Contracts will be subject to so that the Council can ensure Value for Money. Due to resources, performance monitoring is undertaken in reaction to complaints raised by the Public/service users as/when they are raised. There is a log of the complaints received and what penalty points and fines have been awarded to operators. The tendering and evaluation processes for the Transport for Schools contracts were also reviewed, which were found to be suitable.

Transparency - Medium Risk

The Procurement Strategies and Contract Procedure Rules have already been identified as out of date and are undergoing review currently with the Corporate Procurement Manager. They do not comply at present to the Public Contract Regulations 2015. Nevertheless, there is evidence that in practice, the Public Contract Regulations 2015 and the National Procurement

Service (NPS) frameworks are being adhered to. There is a 'live', maintained and detailed Contracts Register in place, which is not published via the website. Adverts are placed on the National Procurement website Sell2Wales as prescribed by the Public Contract Regulations 2015 and in accordance with the NPS framework, but this is not referenced to within the out of date Contract Procedure Rules. Once the policy documents are updated, it is anticipated that the risk rating for this area will move from medium to low.

Category Management – Low Risk
The Procurement activity at the Council follows a Category Management approach for their key spend areas. These were identified as Adult & Children's Social Services, Supporting People, Construction/Highways, Building Maintenance, Facilities Management, Corporate Needs, ICT and Transport.

The Procurement Strategy reflects most of the above Categories identified by the Corporate Procurement Manager but will require updating as part of the review of the Procurement Strategy. There are Category Managers within each Directorate, who have the required specialisms for their services.

The Procurement Strategy identifies Category management methods being used at the Council, but this does not suggest the targets for savings across categories nor the process for identifying category opportunities - as these fall within each Directorates' Business or Commissioning Plans. The Procurement Strategy identifies the objectives of Services to drive value for money by means of Market Testing, encouraging competition, promoting constructive engagement and partnerships, and allowing markets to respond with innovative solutions where possible. There is evidence of a pre-tender engagement future notice via Sell2Wales, encouraging organisations to discuss the matter of advice and support for recipients of Personal Independence Payments. The Contract Procedure Rules section relating to Competitive Dialogue refers to the previous version of the Public Contract Regulations, but is currently going through an update by the Corporate Procurement Manager, so should be rectified during the review.

Supplier Management – Medium Risk
There is no documented reference to the Council's Key Suppliers in terms of value, risk or business criticality, although suppliers can be identified via the Corporate Contracts list in terms of their contract value. There is no Council-wide Business Continuity Plan available via the Intranet and it appears that Directorates develop their own plans. However, only one sample of this could be located via the Intranet, for the Communities Directorate. The Communities Business Continuity Plan did not have adequate procedures to follow in the event that a Supplier failure triggered the Plan. The viability of suppliers is assessed during periodical quality and performance reviews as covered within other Controls in this review. The Procurement team utilise the National Procurement Service framework to undertake their procurement processes.

Social Value – Low Risk
There is a documented process showing how Stakeholders are engaged with at the start of a Procurement process, which was confirmed with the Commissioning Manager for the Social Care and Well-Being Directorate. There is a standard procedure for the Procurement stages, which is documented within the Tender Management Overview guidance and the Contract

Procedure Rules. Evidence of the standard procurement procedures influencing a contract was seen during testing.. Development of stakeholders is considered for staff, existing suppliers and for Members, to enable them to be actively engaged in the processes.

4. Project and Programme Management

Project Methodology – Low Risk
The Council has a Corporate Transformation Team who provide Project Management, Project Support, or Project Assurance on projects as deemed necessary from the project initiation documentation.

There are standard project methodology templates in place for use across the Council. There is also a Project Management Toolkit, which is based upon the PRINCE2 project methodology and provides staff with support and assistance with the completion of their project.

It is acknowledged that some projects that fall outside of the core council programme and are not a major project may be 'unknown' corporately and therefore may take place outside of this framework. However, these are likely to be lower risk projects.

Project Documentation – Low Risk
Key project document templates are available and expected to be used, such as a Project Initiation Document and a Business Case. Each of the four programmes/projects sampled within this review were found to have sufficient documentation to support them, in the form of PIDs and business cases. The documentation outlined the scope, anticipated outcomes and estimated costs of the programmes/projects.

Progress Monitoring – Low Risk
Approval of key documents for a project is performed by the Project Board, however to do so they must have authority for the resources required for the project, which may require Cabinet approval. If the project is of substantial corporate interest, or high in value or risk, it will go to Cabinet to be approved.

Reporting and monitoring is undertaken between the Project Manager and the Project Board. A key tool in this process is the completion of Highlight Reports, which provide an update on the current status of the project. For programmes/projects which are part of the Corporate Programme, monthly Highlight Reports are sent to the Programme Management Board (PMB), which meets monthly to help ensure that any live issues or changes with programmes can be discussed and addressed.

Communication of programme/project progress to Members is through the Council's Corporate Performance Assessment (CPA) process for each Directorate, which include updates on the progress of projects affecting each Directorate.

For each of the four sampled programmes/projects, the approval, reporting and monitoring arrangements were clearly evidenced.

Resource Allocation – Low Risk
A central resource is available to assist with programmes/projects in the form of the Corporate Transformation Team.

The project documentation for each of the four programmes/projects which were sampled within this review defined the skills and capacity required in order to be able to successfully complete the work. This was usually in the form of identifying the individual(s) from HR, Legal, Finance etc who would be assisting with the programme/project.

Risk Management at Project Level – Low Risk
Within the Council's project management toolkit document, there is a section on risk management. This includes the need for risks to be considered at stages of a project, with project teams expected to utilise a risk/issue tracker to assist this process. The Sponsors and Managers of projects are often Service Managers or Directors, thus enabling key project risks to be considered at an appropriate level within the Council. For two of the four sampled programmes/projects, risk management is a standing item on project board meeting agendas.

The risk management policy does not provide information regarding how project risks should be assessed and dealt with. There are also no details regarding the need to raise some project risks to risk registers.

Responsibility and Accountability – Low Risk
The sampled programmes/projects clearly identified the roles and accountabilities in relation to the successful completion of the works. The individual's tasked with performing the roles were also of appropriate seniority to do so.

Lessons Learned – Medium Risk
Plans for benefits realisation are included within the project documentation of programmes/projects. There is not a corporate level oversight of completed projects to determine a longer term picture regarding the successfulness of projects in terms of time, budget and outcomes.

Delivering Corporate Objectives – Low Risk
Section 1.1 of the business case template requires links to be made between the project and the corporate objectives of the Council. Section 2 of the project initiation document template requires details of how the project will 'Fit to Strategy', including its links to the Medium Term Financial Strategy.

If the programme/project is high in value and/or is of corporate interest (i.e. is part of the transformational programme), oversight is provided by Senior Leadership Team and Members throughout the course of the project.

Supporting Change - Medium Risk
For each of the sampled programmes/projects, a representative from HR was outlined within the project documentation. The documentation also provided some links to cultural change and how staff 'buy-in' would be maximised, however there was no set approach to this. To

enhance this, the project initiation templates could include a section for cultural change and the likely impact upon staff.

Providing additional feedback mechanisms to staff may make proposals to change be better received, as recommended within the 2017/18 Ethics audit.

5. Information Management

Governance Framework and Strategy – Medium Risk
The Corporate Plan identifies the Digital Transformation Programme and how ICT will play a large role in achieving this plan.

From a review of the minutes, we were unable to confirm whether the current ICT Strategy was approved via Cabinet. The Group ICT Manager confirmed that the ICT Strategy is overdue for review.

Although the Principles & Priorities within the ICT Strategy link well to the current Corporate Plan Priorities, it does not provide a 'roadmap' of the major technologies/ transformational programmes expected during its course. Though it identifies that there will be some, there are no target deadlines, monitoring techniques or accountabilities given within the document for these.

The Group ICT Manager confirmed that there is a live system (I – Trent) where the ICT structure is recorded, including responsibilities, however, sight of the ICT responsibilities was not provided at the time of audit testing, only a basic structure flowchart. We were therefore unable to conclude on the structure and scheme of delegation and the extent to which it is fit for purpose. Over the course of the audit we found another area of accountability that was unclear: The Information Governance Strategy states that the Data Protection Officer (DPO) role will be held by the Monitoring Officer, which is contrary to the what we were advised by the both the Information Officer and Group Manager of ICT.

There is a bi-monthly Information Governance Board, however, which is a requirement of the PSN/CoCo compliance and three of the ICT Management team attend these along with the chair Head of Operational and Partnership Services and representatives from Directorates. The Information Governance board is minuted, but we were unable to review a sample minutes for the board at the time of audit testing.

The Group ICT Manager confirmed that quarterly Key Performance Indicator reports are created which includes information regarding ICT performance. The copy of this report that Cabinet received did not include KPIs for the ICT service, which was an anomaly that the Group ICT Manager said he would investigate. There doesn't appear to be a Service Level Agreement in place for ICT services. We are therefore unable to conclude on the extent to which the priorities stated in the ICT Strategy are measured, monitored and achieved and whether the requirements of the Performance Management Framework are being met.

Asset Management – High Risk
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 is considered for all ICT assets.

There are some ICT Codes of Conducts regarding Software use, Social Media Use, Mobile Device use (overseas only) and information governance available via the Intranet, which appear to be out of date, with the exception of the Social Media Policy, which is more recent. From a review of the Intranet, no policies or guidance were found for the following areas in relation to asset management: procurement, release to the environment, finance, licensing, or disposal.

The method for ensuring that staff see the Policies relevant to them is determined during their Corporate Induction, but we were unable to identify whether there is a test to check understanding of the policies at a check-up or during an appraisal process.

Document Control does not feature on the policy documents, nor the ICT/Information Management Strategy viewed.

There is a database in place which is used for ICT Asset Management, however only one screenshot of the information held within the database was provided for audit testing, with no further reports on the management of other assets provided. We were therefore unable to confirm whether all asset lifecycles are monitored, or how assets are recorded on this register.

Compliance with Legislation – Medium Risk

The ICT Strategy does not define which regulations the ICT service complies with. The Information Management Strategy refers to the Data Protection Act, Freedom of Information Act, Companies Act 1985 and 2006, Limitations Act 1980, the Electronic Communications Act 2000, the Computer Misuse Act and the Human Rights Act 2000. There is no reference to the following Acts within the documentation viewed: Disability Discrimination Act, WEEE Directive nor the Copyright Designs and Patents Act.

Protective Marking of Information shared externally is in place through GCSx email accounts in accordance with the Local Government Classification Scheme. Information classifications are outlined in the Information Management Strategy.

Due to conflicting conversations and documented evidence, there is some confusion over who will be designated the Data Protection Officer role in the long-term. However, for the time being, the Principal Solicitor within the Legal team is confirmed by the Group ICT Manager as having been assigned (though not via Member approval).

There is no documented GDPR implementation plan, and meetings where the plan is discussed are not 'formal' in the sense that they are not minuted. However, the Information Manager confirmed that a representative from each Directorate (Group Managers) have been attending monthly Implementation Meetings since October 2017 and they are all aware of their own plans and deadlines, and we were informed that attendance at these meetings has been sufficient.

It should be noted that there has been a recommendation raised relating to the Freedom of Information Requests made to the Council within the Corporate Governance strand of this Healthy Organisation Review, which should be considered within the GDPR implementation plan, ensuring compliance with the Government Publication Scheme and relevant GDPR

clauses.

On discussion with the Information Manager, it is evident that an Information Asset Register is being developed as part of the plan, which should identify the Controllers and Processors for each data set held and should support the provision of information requests responses as necessary once implemented.

The Data Retention Policy and Schedule was presented to Cabinet for approval in January 2018 and was subsequently approved. There were incidents of conflict between the information within the schedule and that relating to it within the Retention Guidelines for Local Authorities, which was passed to the Information Manager for review.

The Council should satisfy itself that training for the Data Protection Officer is adequate. Awareness training for staff in general is the responsibility of each Directorates Group Management teams and a draft training module is being prepared for implementation in May 2018.

Roles & Responsibilities – Unable to Conclude
The Group ICT Manager confirmed that there is a live system (I – Trent) where the ICT structure is recorded, including responsibilities, however, sight of this was not provided at the time of audit testing and there were no structure charts available to view on the intranet. We were therefore unable to conclude on the structure and scheme of delegation and the extent to which it is fit for purpose.

Over the course of the audit we found at least one area of accountability that was unclear: The Information Governance Strategy states that the Data Protection Officer (DPO) role will be held by the Monitoring Officer, which is contrary to the what we were advised by the both the Information Officer and Group Manager of ICT.

Policies & Procedures – Medium Risk
While the Policy/Strategy and Codes of Conduct are available via the Intranet, the majority of documents are quite significantly out of date and without document control. The only alternative viewing for some documents is related to the Welsh language, and this does not cover the entire suite of Policies/Codes of Conduct. There is no consideration for the Equality/Diversity of ICT in relation to the Discrimination Act, regarding equipment/assets or staff procedures within the documents viewed. The following areas are not addressed within the suite of documents reviewed: Change Management, Asset Management, some Acceptable Use Policies, Malware/Virus Protection, Capacity Management.

At the time of the audit, we were not provided with the ICT Training Matrix to confirm the extent to which staff have undergone appropriate training. We were therefore not able to conclude on this area of testing.

Cyber Security -Unable to Conclude
Although it was advised that regular PSN check testing takes place internally, we were unable to view a copy of the most recent compliance certificate at the time of the audit and the actions tracker provided regarding the recommendations around PSN compliance did not

provide dates for completion of the actions or much detail around them, making it difficult to confirm implementation of some recommendations.

We have been advised the cash receipting function has been outsourced and therefore the responsibility for PCI Compliance Returns and quarterly compliance scans does not rest with the Council. At the time of the audit we were unable to verify whether these are taking place on behalf of the Council as envisaged.

Business Continuity – Unable to Conclude
We have been unable to conclude a full opinion regarding the Critical Application list, having not been able to view the database. The ICT Business Continuity Plan also does not define 'critical' applications.

The Group ICT Manager confirmed that this critical applications list is not under a regular review process and had not been updated since it was compiled three years ago.

It was unclear whether the System Owners would have updated the list with changes to/removal of/addition of applications as required.

There is no evidence of the definition of a 'critical' application within the ICT Strategy or other ICT Policies reviewed as part of the audit.

Disaster Recovery – Unable to Conclude
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.

The back-up schedule provided to us and discussion with the Servers and Storage Manager identified that backup storage is completed by transfer onto discs held for a maximum of 2 years, which are held within an unsecured appliance in the access controlled production site. It was advised that the same processes are followed at the disaster recovery storage location.

Security History – Unable to Conclude
The Group Manager for ICT confirmed that the Data Protection Officer 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 spreadsheet was not provided for audit testing.

The Strategy/Codes of Conducts and mandatory Data Protection training in place appear to be robust enough to ensure that breaches are reported and monitored, though these will all require review to align with the implementation of GDPR.

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

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
Governance - Leadership	Corporate Management Board meetings should include the following: • timescales for completion of actions recorded in the minutes. • The "Action review" part of the minutes should state whether previous meeting actions have been completed. • Cancelled meeting agenda items carried forward to the next meeting.	Low risk – Advisory Recommendation	CMB	N/A
Governance – Constitution/ Transparency	Future updates should include the following: • Referencing inconsistencies • Commissioning of services processes/procedures • The Councils view on Good Governance.	Low Risk – Advisory Recommendation	CMB	N/A
Governance – Effective Working Relationships	Feedback mechanisms should be put in place to measure the effectiveness of member/ officer relations.	Medium Risk – Follow up required	CMB	N/A
Governance – Effective Working Relationships	The Corporate Induction Framework should be updated to refer to the Constitution and its associated Codes of Conduct.	Medium Risk – Follow up required.	CMB	TBA
Governance - Code of Conduct	There is a Whistleblowing policy, but it requires updating as well as broader communication to all Council staff and for the update to be published publicly.	Medium Risk – Follow up required.	CMB	TBA
Governance – Transparency	The Council should regularly publish Freedom of Information requests and responses on their website.	Medium Risk – Follow up required.	CMB	TBA
Governance – Induction and Development	The mandatory training list for members should be updated to include GDPR.	Medium Risk – Follow up required	CMB	TBA
Governance – Induction and Development	A development programme could be developed for the Leadership teams (various levels), in the same way that there is one for Members.	Low Risk – Advisory Recommendation	CMB	N/A
Governance- Communication/ Stakeholder Consultation	The Communications, Marketing and Engagement Team Plan should be updated to include the following: • how officers (or members) should	Medium Risk – Follow up required.	CMB	TBA

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
	handle a situation if they are approached for comment on a major issue, which could impact on the reputation of the Council. • how officers (or members) should engage and communicate with various stakeholders.			
Governance- Communication	The Communications, Marketing and Engagement Team Plan should be separated from an overarching Communication Strategy.	Medium Risk – Follow up required	CMB	TBA
Governance – Effectiveness Review	The Annual Governance Statement should include action points, timescales and responsibilities in either a table at the end, or within an appendix, to give a clear communication of the issue resulting in the action being made, who's responsible for completing the action, the status of the actions and expected dates of achievement.	Low Risk – Advisory Recommendation	CMB	N/A
Risk Management - Strategy	Steps should be taken to ensure the Risk Management Strategy is understood at all levels of the Council, and not just at Senior levels.	Medium Risk – Follow up required.	CMB	TBA
Risk Management - Strategy	The Council should ensure the same risk matrix is used consistently throughout the different Directorates.	Low Risk – Advisory Recommendation	CMB	N/A
Risk Management – Appetite/ Transparency	To improve the guidance to staff further, the Council should consider setting a numerical risk appetite value, which could be included within the risk management policy's risk matrix to act as a visual aid to staff when considering risks. This numerical risk appetite value should be taken to Audit Committee as part of the current corporate risk register review schedule.	Medium Risk – Follow up required.	CMB	TBA
Risk Management - Register	A bespoke software solution for the Risk Register should be considered to enable improved access controls, easier reporting and alerts when updates were required.	Low Risk – Advisory Recommendation	CMB	N/A
Risk Management – Register/ Project Risk	The Risk Management Policy should be updated to include the following: • the numerical threshold for risk tolerance (above which the risk requires inclusion in the risk	Low Risk – Advisory Recommendation	CMB	N/A

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
	register). • how project risks should be assessed and dealt with and when they should be included in the corporate risk register.			
Risk Management - Assessment	Commissioning plans should be improved by including a mandatory risk section.	Low Risk – Advisory Recommendation	CMB	N/A
Risk Management – Project Risk	All projects should include risk management as a standing item on their project board meeting agendas.	Low Risk – Advisory Recommendation	CMB	N/A
Risk Management – Decision Making	The standard report to members pro-forma should be updated to include a section regarding the assessment of risk. Current and residual risk scores should be provided within the risk section.	Medium Risk – Follow up required.	CMB	TBA
Risk Management - Transparency	The corporate risk assessment should be shared with other local authorities and bodies.	Medium Risk – Follow up required.	CMB	TBA
Commissioning and Procurement – Strategy/ Transparency/ Policies and Procedures.	Although we understand there are plans to update them, the current Adult Social Care Commissioning Plan and Procurement Strategy include no reference to the present Priorities of the Council or the Public Contract Regulations 2015, which has an impact on transparency.	Medium Risk Follow up required.	CMB	TBA
Commissioning and Procurement - Strategy	Arrangements should be made to ensure there is sufficient corporate oversight of Commissioning across the Council.	Medium Risk Follow up required.	CMB	TBA
Commissioning and Procurement – Commissioning Intentions	Commissioning Intentions should be publicly available for all areas of the council where commissioning takes place, and not just Adult Social Care.	Medium Risk Follow up required.	CMB	TBA
Commissioning and Procurement – Training and Skills	The Procurement Strategy and Commissioning Plans should be updated to include required personal qualities/ qualifications.	Low Risk Advisory Recommendation	CMB	N/A
Commissioning and Procurement – Policies and Procedures	With the exception of the Social Care and Wellbeing Directorate, we were not able to confirm whether Service Level Agreements are in place between services and suppliers.	Low Risk Advisory Recommendation	CMB	N/A
Commissioning and Procurement	Consider implementing a quantitative approach to assessing Social Value, to	Medium Risk Follow up		TBA

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
– Value for Money	ensure that targets are provided and met.			
Commissioning and Procurement – Value for Money	Ensure that there are adequate performance monitoring, supplier support and management arrangements in place to address potential issues of the Waste Management Services supplier being able to fully meet their contract requirements.	Medium Risk Follow up required.	CMB	TBA
Commissioning and Procurement – Category Management	The Contract Procedure Rules should be updated to include information about identifying savings targets and category opportunities or indicate where these would be recorded for each Directorate.	Low Risk Advisory Recommendation	CMB	N/A
Commissioning and Procurement – Supplier Management	The authority can identify their 'Key suppliers' via the Corporate Contracts Register, but should consider creating either a central document, or separate Directorate documents, identifying key suppliers in their areas in terms of value, risk and business criticality.	Medium Risk Follow up required.	CMB	TBA
Commissioning and Procurement – Supplier Management	The Business Continuity Plans for the Communities Directorate and for the ICT Service Group require update.	Medium Risk Follow up required.	CMB	TBA
Commissioning and Procurement – Supplier Management	Consider inclusion within Directorate Business plans of a Key Suppliers List in terms of criticality and risk, with clear steps (or 'action cards') to follow in the event that a supplier becomes unavailable.	Medium Risk Follow up required.	CMB	TBA
Project Management – Project Methodology	Although projects with a corporate impact will have some involvement from the Corporate Transformation Team, it is possible that some smaller projects are being completed in silo with the standard templates not being utilised.	Low Risk Advisory Recommendation	CMB	N/A
Project Management - Resource Allocation	Minor instances of a lack of clarity were identified within one of the sampled projects/programmes (Digital Transformation), in terms of capacity requirements for the programme. Clear guidance should be available setting out requirements.	Low Risk Advisory Recommendation	CMB	N/A
Project	The risk management policy needs to	Low Risk	CMB	N/A

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
Management – Risk Management	be updated to include information regarding how project risks should be assessed and dealt with. There is also no information on raising project risks to risk registers.			
Project Management – Lessons Learned	Information on the success of projects should be collated centrally so than corporate oversight of can be maintained over the outcome of completed projects.	Medium Risk Follow up required.	CMB	TBA
Project Management – Supporting Change	The project initiation documentation templates could require additional information in relation to cultural change and the likely impact upon staff.	Medium Risk Follow up required.	CMB	TBA
Project Management – Supporting Change	Providing additional feedback mechanisms to staff may make proposals to change be better received, as recommended within the 2017/18 Ethics audit.	Medium Risk Follow up required.	CMB	TBA
Information Management-Strategy	A formal plan and timeline should be put in place for updating the IT Strategy.	IN THE PROCESS OF BEING FOLLOWED UP	CMB	Quarter 1
Information Management-Strategy	The existing ICT strategy should be updated to include a 'roadmap' plan of the technologies/ transformational programmes underway or due to start.	AS ABOVE		
Information Management-Strategy	At the time of the audit it was not possible to confirm whether all required posts are filled and that the ICT Structure reflects the responsibilities and scheme of delegation within the department. The Council should satisfy itself that this is the case.	AS ABOVE		
Information Management-Strategy	There is a list of anticipated 'programmes'/technology being implemented under priority action plans, but no roadmap given to indicate timescales for implementation.	AS ABOVE		
Information Management-Strategy	More regular and formal meetings between ICT teams and ICT Management would help to ensure that targets are being met and progress monitored.	AS ABOVE		
Information Management-Strategy/	The Information Management Strategy requires review to ensure that it reflects accountability for the various	AS ABOVE		

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
Legislation	Information Governance roles clearly as there is currently a lack of clarity around the Data Protection Officer Role.			
Information Management- Strategy	Although we have been advised that KPI reports are being reported for quarterly assessment, at the time of the audit we were unable to verify this and conclude whether Key Performance Indicators were in place and being monitored for the ICT Service. The Council should satisfy itself that this is the case.	AS ABOVE		
Information Management- Strategy	We are not aware of any Service Level Agreement in place for ICT Services. The Council should ensure that this is in place.	AS ABOVE		
Information Management – Asset Management/ Legislation	An ICT Asset Management Plan should be created to include: • the impact of ICT Assets on areas such as Service Desk, change management, procurement processes, release processes or staff leavers. • How Hardware of Software Asset Management functions should be run and intended goals of this service. • The punitive impact of breaching said Policy/Plan. • Indication of which regulations/directives/legislation are relevant (including Disability Discrimination Act, Waste Electrical Electronic Equipment, Regulations (WEEE). Copyright Designs and Patents Act)	AS ABOVE		
Information Management – Asset Management	From a sample of policy documents reviewed, document control measures are not in place.	AS ABOVE		
Information Management – Asset Management	From a review of the Intranet, no policies or guidance was found on the following in relation to asset management: procurement, release to the environment, finance, licensing, or disposal.	AS ABOVE		
Information	At the time of the audit we were unable	AS ABOVE		

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
Management – Asset Management	to confirm the following: • Whether asset lifecycle management is in place for all ICT assets. • How the Council knows whether its ICT policies have been read and understood. • Although we understand that a Configuration Management Data Base in in place, we were unable to verify further details about what it is used for and how it is managed. The Council should satisfy themselves that the above are being managed effectively.			
Information Management - Legislation	There is little evidence of discussions regarding the GDPR Project Plan deadlines, due to the lack of minutes/record of the process. The Council should ensure that decision making processes are transparent.	AS ABOVE		
Information Management - Legislation	The Retention Schedule requires review to ensure compliance with the relevant Retention Guidelines for Local Authorities and other Acts as necessary.	AS ABOVE		
Information Management - Legislation	GDPR awareness has not already been rolled out amongst staff but is being developed for implementation in May.	AS ABOVE		
Information Management – Roles and Responsibilities	At the time of the audit we were unable to confirm the following: • Whether all posts within the ICT service were filled, or whether the service had vacancies. • Whether the role profiles match expectations in terms of delegations and responsibilities.	AS ABOVE		
Information Management – Roles and Responsibilities	There were no structure charts available on the Intranet. The Council should ensure these are readily available.	AS ABOVE		
Information Management – Policies and Procedures	Several ICT Policies were noted as being out of date back to 2008/2011, with the exception of the Social Media Protocol and related documents which were reviewed in 2017. As part of a general policy update, The ICT Code of Practice –	AS ABOVE		

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
	Handling and Classification Policy requires review as the version we obtained was dated 2011.			
Information Management – Policies and Procedures	Equality & Diversity should be considered as part of any policy update (Discrimination Act regarding ICT Asset rights etc).	AS ABOVE		
Information Management – Policies and Procedures	No policies were identified surrounding removable media devices, mobile ICT equipment/assets use (within the UK), security/protection that is in place and guidance, which identify the process to follow beginning to end, responsibilities, reference to relevant Policies, laws and regs, timescales were relevant and the punitive impact of breaching the policy.	AS ABOVE		
Information Management – Policies and Procedures	An action plan (or an appendix to) should be included within the revised ICT Strategy with timescales, responsible persons for actions and method of review; and a section regarding the ICT stance and commitments re equality/diversity.	AS ABOVE		
Information Management – Policies and Procedures	The Intranet requires update with revised documents when available, ensuring that all documents referred to within the Strategies and Policies are available as stated within the Intranet.	AS ABOVE		
Information Management – Policies and Procedures	The Council should satisfy itself that the ICT Training matrix is up to date and that staff have received relevant training.	AS ABOVE		
Information Management – Policies and Procedures	The Council should clarify the section in the Corporate Induction Framework which indicates that all staff receive mandatory ICT training, during the Corporate Induction (since only some staff received this).	AS ABOVE		
Information Management – Policies and Procedures	Neither the Appraisal form nor the Employee Appraisal Protocol includes a requirement to confirm whether relevant policies have been read and understood.	AS ABOVE		
Information Management – Cyber Security	Although we have been advised that regular PSN check testing internally, we were unable to view a copy of the most recent compliance certificate or improvement plan at the time of the audit to confirm implementation of any	AS ABOVE		

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
	recommendations.			
Information Management – Business Continuity	Although we have been advised that an applications list is stored within the Configuration Management Data Base, that 'Tier 1' 'critical' applications are defined within the ICT Business Continuity Plan, and that a system owner from ICT is in place for each application along with a representative from each service; we have been unable to verify this at the time of audit testing, or check the list is up to date.	AS ABOVE		
Information Management – Business Continuity	We have been advised that Tier 1 applications are those listed within the ICT Business Continuity Plan, and this the process of identifying these applications took place approximately 3 years ago, and as such may require update.	AS ABOVE		
Information Management – Business Continuity	We have been advised that the ICT Business Continuity Plan is approximately 2 years out of date and requires a 'rehaul'. It was last tested in May 2016 but is not expected to be reviewed until completion of a large Server 'reshuffle' later this year.	AS ABOVE		
Information Management – Disaster Recovery	We have been advised that the Contacts List within the ICT Business Continuity Plan is 'mostly' up to date. However, this would require review as the plan has not been updated for approximately 2 years. We understand that it does not link into a Corporate/Council-wide Continuity/Disaster Recovery Plans.	AS ABOVE		
Information Management – Disaster Recovery	A search on the Intranet could not identify Disaster Recovery or Business Continuity guidance, so these are untested by us.	AS ABOVE		
Information Management – Disaster Recovery	The back-up schedule provided to us and discussion with the Servers and Storage Manager identified that Backup storage is completed by transfer onto discs held for a maximum of 2 years, which are held within an unsecured appliance in the access controlled production site and that the same is true for the Disaster Recovery storage location.	AS ABOVE		
Information Management -	Security Breach Codes of Practice/ relevant Strategies need to be updated	AS ABOVE		

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
Security Information Management - Security	regarding the implementation of GDPR. We understand that all security breaches are recorded on a central spreadsheet by the SIRO. However, at the time of the audit we were unable to obtain a copy and were therefore unable to test the extent to which breaches are reported to the ICO.	AS ABOVE		
Information Management - Security	We were unable to test whether security breaches are monitored and action plans followed to mitigate/reduce potential breaches, having been input into the central spreadsheet.	AS ABOVE		

Report Authors and Distribution

Report Authors

This report was produced and issued by:

- Assistant Director
- Senior Auditor
- Auditor

Key Contacts

The key contact for each theme:

- **Corporate Governance** – Andrew Jolley, Corporate Director Operational and Partnership Services
- **Risk Management** – Insurance and Risk Officer
- **Commissioning and Procurement** – Corporate Procurement Officer
- **Programme and Project Management** – Senior Project and Programme Officer
- **Information Management** – Group ICT Manager

Distribution List

The draft report was distributed to the above and the following have also received a copy of the final report:

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.