



Healthy Organisation – A Strategic Review

Final Report

Issue Date: April 2018

Working in Partnership to Deliver Audit Excellence

Contents

Executive Summary

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

Summary Assessment

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

Detailed Assessment

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

Appendices:

- Appendix A – Mapping Areas for Attention to 2017/18 Internal Audit Plan
- Key Contacts and Distribution
- Statement of Responsibility

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 the Vale of Glamorgan 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'.

The Vale of Glamorgan Council has selected to review four of the eight themes this year:

- Risk Management
- Commissioning and Procurement
- Programme and 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. The work was carried out during 2018 with testing completed by the end of March 2018. A senior manager from the Vale of Glamorgan Council was appointed as a key contact for each theme and outcomes were agreed with them ahead of producing the final report.

The Vale of Glamorgan 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 some examples in greater detail 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.

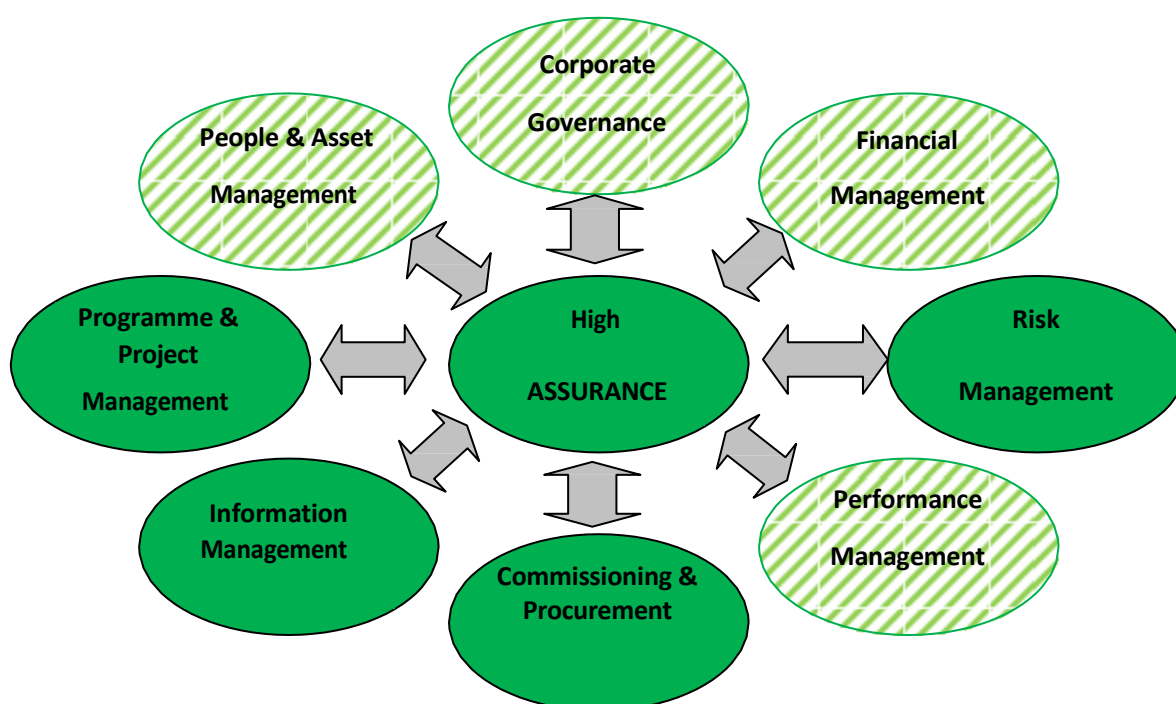
Audit Assurance:

High


The assurance for each of the four themes referred to above have been reviewed and depicted in the following chart (in solid green). This indicates an overall High Assurance opinion. Some areas of further improvement are still required, however in the main strong control frameworks are in operation across the reviewed themes.

In order to present a complete picture of assurance across all 8 themes, the Head of Audit has considered the audit work completed elsewhere in the audit plan for the remaining themes (People and Asset Management, Corporate Governance, Financial Management and Performance Management) and has confirmed that they are all High Assurance. These areas have not been assessed by SWAP but we have included the opinion of the Head of Audit below to enable a more complete representation of assurance across the Council to be depicted. The areas assessed separately by the Head of Audit are shown cross hatched (as opposed to solid green).

Overall assurance graph



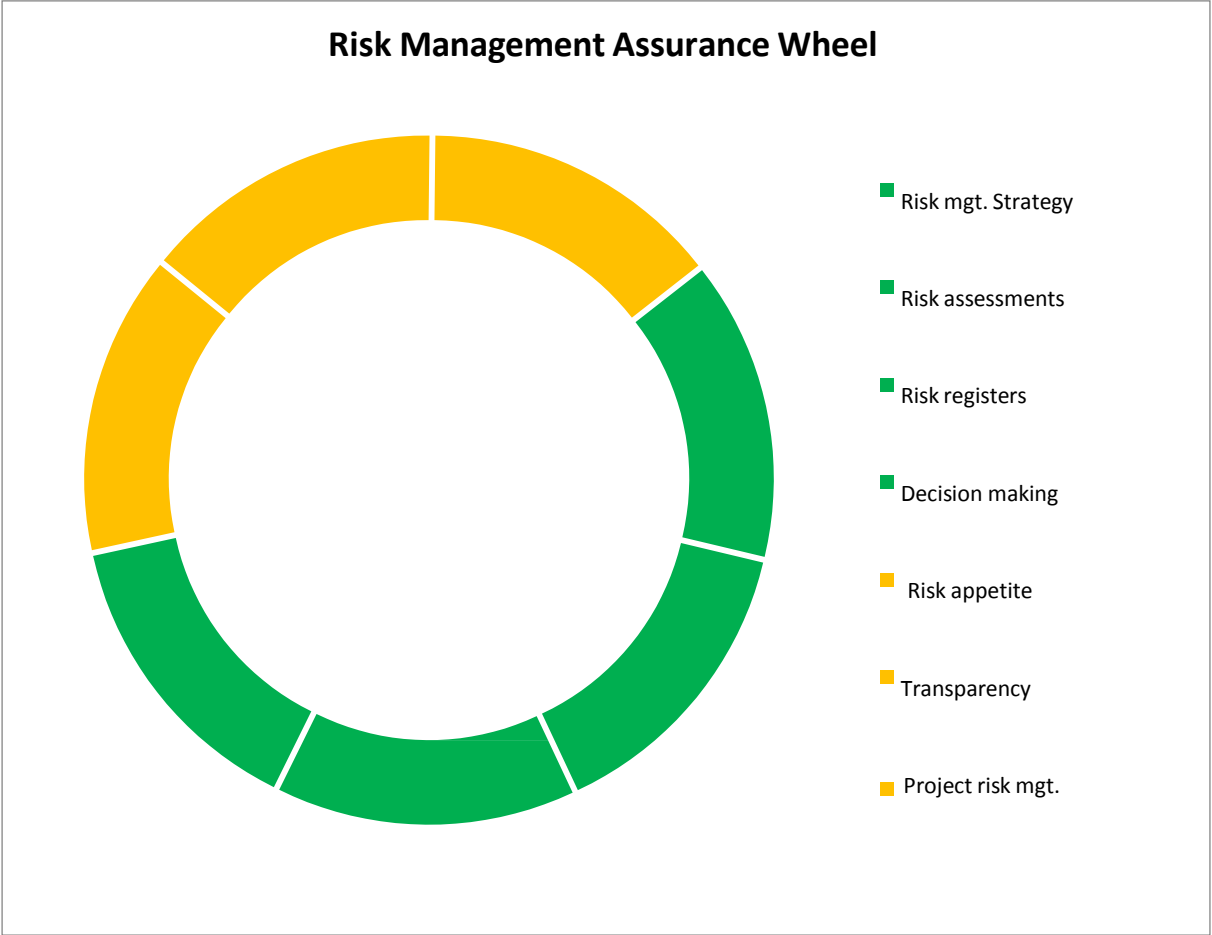
R/A/G Rating Key:

- RED** (Low Assurance / High Risk)
- AMBER** (Medium Assurance / Medium Risk)
- GREEN** (High Assurance / Low Risk)
-  High Assurance rating assessment provided by the Head of Audit

Summary Assessment by Theme

1 Risk Management	GREEN
--------------------------	--------------

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 **Green** RAG rating has been assigned because of the strong control framework in place in relation to risk management. There are some further areas which require improvements, however key processes are in place including a revised approach to risk management.

Risk Management - AREAS OF STRENGTH

Risk Management Strategy

- The revised approach to risk management has been approved by members of the Audit Committee.
- Service Managers are operating in line with the new risk management approach.
- A revised risk management strategy has been created and is to be taken for consideration by Audit Committee in May 2018.

Risk Assessment

- Team plans, service plans and standard project documentation provide adequate consideration to risks.
- Oversight of team plans and service plans is provided by the Performance and Development Team, who are also responsible for the oversight of risk management at the Council.

Risk Register

- The corporate risk register is reviewed on a regular basis within Insight Board meetings by staff of suitable seniority.
- Corporate risk updates are provided to Audit Committee on a quarterly basis.
- Risks are also considered within the quarterly Well-being Outcome Performance reports to Cabinet.

Decision Making

- Reports and supporting documentation are taken to Members to request approval for proposals, thus providing a platform for a risk assessment to be included.

Risk Appetite

- A risk scoring process is in place to categorise risk via a 4x4 likelihood and impact matrix.

Transparency

- Regular risk management updates are provided to Members of the Audit Committee.
- Risk management information is readily available to staff via the intranet.

Project Risk

- The Council's risk management strategy and project management toolkit clearly identifies the expectations in relation to project risk management.
- Project Managers and Sponsors are often Service Managers or Directors, enabling risks to be considered at an appropriate level.

Risk Management - AREAS FOR ATTENTION

Risk Management Strategy

- Once formally approved, the new strategy will require communicating to staff to ensure they understand how risk management is considered at the Council.

Risk Assessment

- There are inconsistencies regarding how risks to the achievement of commissioning plans are referenced, as there is not a standard template for commissioning plans. Whilst this may be difficult to implement due to commissioning being devolved to Service Areas, as a minimum, expectations in relation to the assessment of risks associated to commissioning should be included within the risk management strategy.

Risk Register

- Whilst the process for managing and monitoring the corporate risk register appears to be well considered, it is not currently documented. It was advised that the updated strategy will include this information and will be communicated to staff to mitigate the risk of staff being unaware of the process.

Decision Making

- There is no standing item for risk assessment on the templates used for committee decision reports.
- Inherent and residual risk scores could then be captured along with the actions that have been put in place to show the impact of the decision made by Members.
- Risk assessment of proposals could be improved by ensuring that this takes place at an earlier point in the decision making process and includes an assessment of all options including 'do nothing'.

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 strategy is awaiting revision and therefore does not currently reflect the Council's approach to risk management.
- The corporate risk assessment is not communicated with other local authorities and bodies.

Project Risk

- It appears that there are some instances of the documented approach to risk

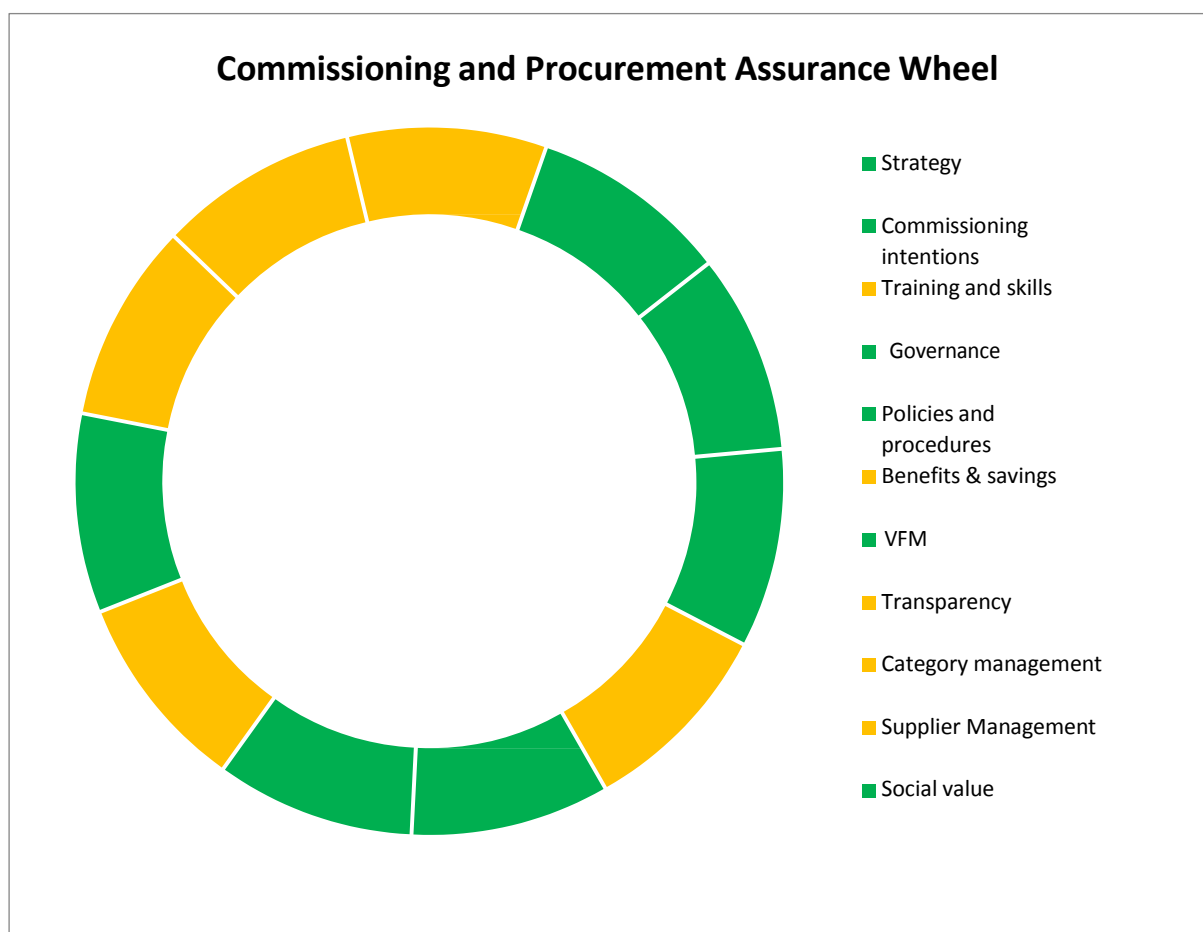
management within projects not being followed in practice. This has been highlighted within the Project and Programme Management theme.

2 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 commissioning and procurement. Commissioning is the responsibility of Directorates, with no central commissioning team in place.

AREAS OF STRENGTH

Strategy

- A Draft Procurement Strategy is in place for the Council.
- We sample checked the commissioning strategies for Older Persons and Children's and Young Persons and found that they are well-aligned with the Corporate priorities within the Council's Corporate Plan and aim to achieve Value for Money.

Commissioning Intentions

- Clear commissioning intention strategies/plans are in place which effectively communicate the intentions of the commissioning for both Children's and Young Persons services, and that of Older Persons.
- These plans are publicly available, showing good integrity to the Public stakeholders who wish to view the Council's intentions, and are available easily to potential suppliers wishing to provide services to the Council.

Training and Skills

- The Procurement Strategy (although in Draft at present) clearly identifies the lifecycle of the Procurement process.
- The Commissioning Plans viewed clearly identify the lifecycle of the Commissioning processes.
- The Procurement Strategy clearly identifies the commitment of the team to ensuring the training and development of its staff.

Governance

- Documented thresholds which require approval or Delegated Authority are reflected in practice.
- Procurement and Commissioning performance is adequately monitored at the required levels.

Policies and Procedures

- Social Services has a Commissioning Framework in place, providing guidance on and explanation about the Commissioning of such services at the Council.
- Public Contract Regulations 2015 are well documented within the Procurement Code of Practice.

Benefits and Savings

- There are Procurement Specialists in place to advise Commissioners on procurement routes for their projects as required.

Value for Money

- Value for Money and Social Value targets are well documented within the Procurement and Commissioning Strategies viewed.
- The performance framework guidance in place is sufficient for Managers to base Contract monitoring requirements on.
- VFM and SV Targets are communicated well via Tender documents.

Transparency

- None – as it was not possible to conclude some areas of testing.

Category Management

- Driving VFM methods with Suppliers and through Contract Management processes are well documented within the guidance in the Procurement Code of Practice.

Supplier Management

- There was evidence of the evaluation documents used to evaluate tenders, and good practice procedures to follow within the Procurement Code of Practice available to staff undertaking Procurement.

Social Value

- A standard procurement process 'methodology' is in place and utilised to maximise the efficiency of the process.
- Member development opportunities are well established, with a strategy in place to and resource material accessible, to help ensure that Members have the levels of understanding to be involved in the commissioning process.

AREAS FOR ATTENTION

Strategy

- The updated Procurement Strategy needs to be finalised, including the time period for which it is to cover.
- Once finalised, the Council could consider publishing the Procurement Strategy online.
- Commissioning is devolved within the Council to Service level. Without corporate oversight there is a risk that other Commissioning Plans/Strategies do not link sufficiently to the current Corporate Priorities of the Council.

Commissioning Intentions

- It is noted that the Social Care Commissioning Strategies/Plans sampled cover time periods which end in 2018, so a review of these is anticipated in due course.

Training and Skills

- There is not any focus on the need to provide targeted Corporate training to the staff in the commissioning teams within the Commissioning Strategies viewed. Consider inclusion of a commitment to ensure that the Corporate teams skills and competencies are developed in line with implementing the plan.

Governance

- None

Policies and Procedures

- The Contract Procedural Rules should be reviewed to ensure that they refer to the updated Procurement Contract Regulations 2015.

Benefits and Savings

- Ensure that Commissioning targets for Directorates other than Social Services are in place, measured and monitored, with KPI reviews.
- Ensure that KPIs are in place to measure and monitor the Commissioning Savings target progress/achievements for Social Services.
- Clearer identification of savings targets could be provided within the Social Care Commissioning Strategies/Procurement Strategy viewed. A yearly review to update the document on the targets for the year ahead and status of the previous year's achievements would provide this.
- Ensure that Commissioning teams notification of Procurement Projects to the Procurement Unit is not circumvented, even if the Procurement Specialists' advice is deemed as not required within the Business Case analysis.

Value for Money

- It appears that, having requested some Commissioning Strategies from other Directorate Service areas, there does not appear to be a Commissioning Strategy in place for each Directorate/Service Team at the Council.
- Commissioning plans for those other than Social Services are not available to the public/potential suppliers via the Website.

Transparency

- Ensure that the Procurement Code of Practice procedures include a standard procedure/guidance around the Local Government Transparency Code 2015 regarding the publishing of Future Contract Notices and spend above threshold.
- Ensure that the Procurement Strategy refers to compliance with the Local Government Transparency Code 2015.
- Update the Contract Procedure Rules to comply with the Public Contract Regulations 2015.
- Ensure compliance with the requirement to publish spends over threshold and Future Contract Notices publicly (via Sell2Wales)
- Consider publicly displaying spend above threshold levels via the Council website, to further enhance transparency.
- Ensure that the Contract Register held on E-Tender Wales portal holds all of the information required to indicate the managerial reporting stages and contract history/milestones.
- Ensure that all contracts held by the Council in excess of £15k are recorded in the Corporate Contract Register.

Category Management

- Consider inclusion of a Category Management strategy/procedure overview within the Procurement Code of Practice and Procurement Strategy when next reviewed, to clarify the Council's processes, Category targets, which Categories are used and the responsibility of Category Managers regarding this.
- Reference to Procurement Category Management's roles and responsibilities regarding the process could be documented more clearly within the Procurement Code of Practice.

Supplier Management

- Ensure that Key Suppliers are identified and addressed by Disaster Recovery Plans within the reviews of the Corporate and Service Area/Directorate Business Continuity Plans.

Social Value

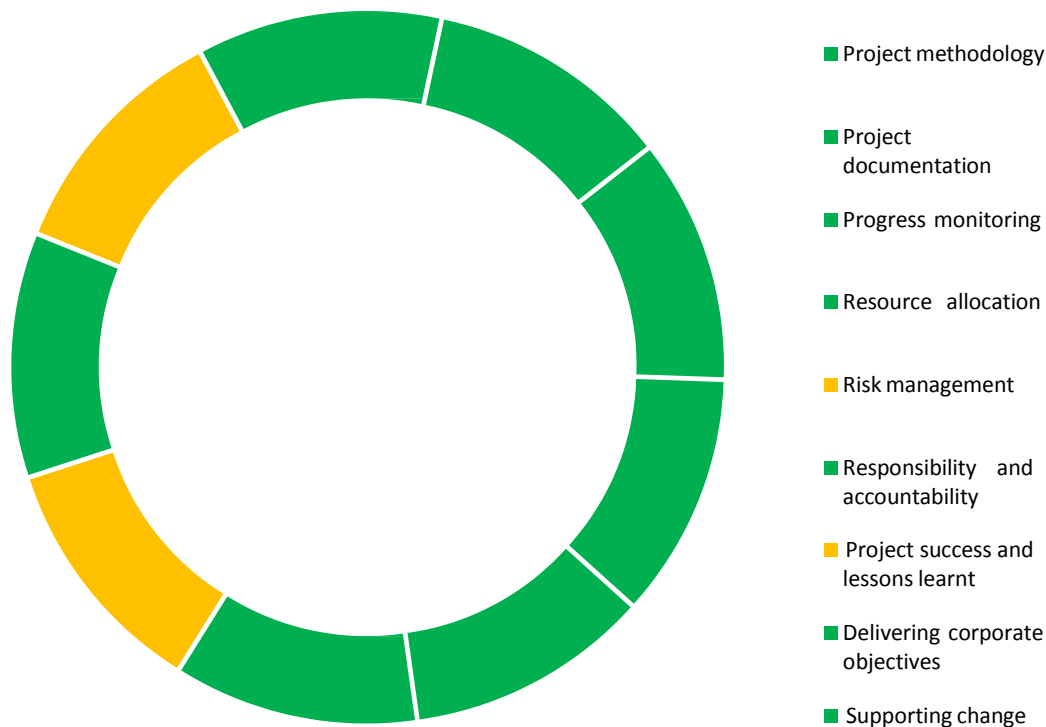
- None

3. 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.

Programme and Project Management Assurance Wheel



The **Green** RAG rating has been assigned because of the strong control framework in place. The RAG ratings given are reflective of this. Sampling in this area has been performed on two current programmes (Transport Programme, Digital Transformation) and two current projects (Cemetery Approach, Leisure Centre Works).

Project Management - AREAS OF STRENGTH

Project Methodology

- Standard project methodology is in place and readily available from the intranet.
- A toolkit including guidance on how to complete each of the project documents is easily accessible.
- Clear thresholds are in place to determine the level of project management required dependent upon level of risk and funding.
- Project Managers and Sponsors are required to attend a day long project management course before they can commence a project.

Project Documentation

- Project Management templates are readily available to staff from the intranet.
- Each of the programmes/projects sampled within this review had sufficient supporting documentation, which outlined the scope, anticipated outcomes and estimated costs of the works.

Progress Monitoring

- Programmes/projects within the Reshaping Services Programme receive frequent monitoring and reporting to Cabinet.
- Strategic Projects are reviewed on a bimonthly basis by the Strategic Projects Monitoring Group.

Resource Allocation

- The skills required to complete the programme/project were outlined within project documentation for the majority of programmes/projects sampled.

Risk Management

- The Council's risk management strategy clearly identifies the expectations in relation to project risk management.
- Risk and issue logs were in place for the two sampled programmes.

Responsibility

- Each of the officers named within the project documentation as supporting the sampled programmes/projects were of adequate seniority to undertake the roles.

Lessons Learned

- Some benefits realisation considerations were provided within sampled project initiation documentation.

Delivering Corporate Outcomes

- Oversight arrangements for the Reshaping Services Programme and Strategic Projects help to ensure that programmes/projects are aligned to corporate objectives.

Supporting Change

- For the sampled programmes/projects, adequate considerations towards cultural change and/or sustainability were made within the project documentation.

- A representative from HR was identified against three of the four sampled programmes/projects.

Project Management - AREAS FOR ATTENTION

Project Methodology

- None

Project Documentation

- None

Progress Monitoring

- For one of the selected projects, there is no evidence of a formal Project Board meeting being undertaken since April 2017 (Cemetery Approach).

Resource Allocation

- One project lacked information regarding the skills and capacity required to undertake the work (Leisure Centre Works).

Risk Management

- Risk and issue logs were not in place for the two sampled projects.

Responsibility

- For one of the sampled projects, there was no evidence of the roles and responsibilities being outlined at the outset (Leisure Centre Works).

Lessons Learned

- The Council may want to consider collating performance information in relation to completed programmes/projects, to enable a clearer picture regarding the successfulness of projects on a corporate front.

Delivering Corporate Outcomes

- The project brief template in place for lower risk projects does not include a section to document alignment to strategic objectives.

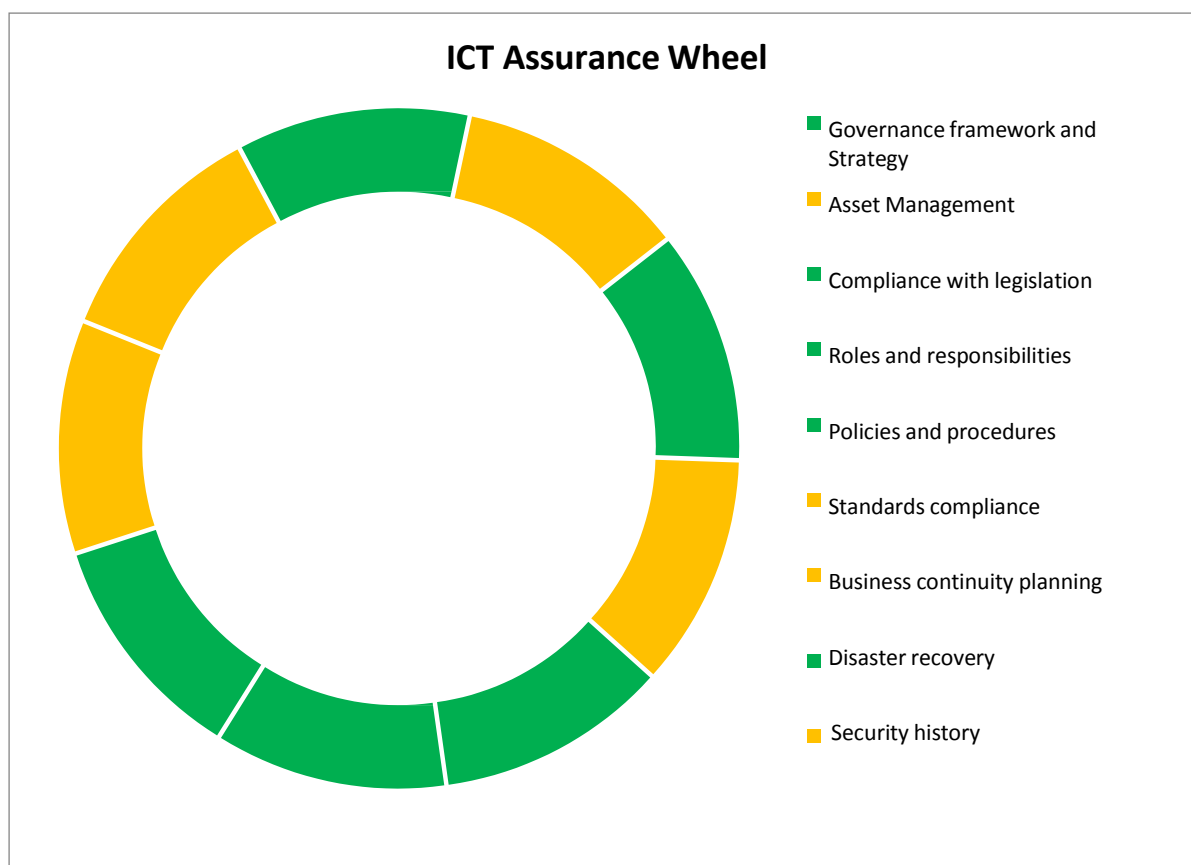
Supporting Change

- Creation of a governance structure for the Leisure Centre Works project would provide clarity over the roles and responsibilities for the project.

4. Information Management

GREEN

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.



The **Green** RAG rating has been assigned because of the strong control framework in place for information management. Further improvements are still to be made, however in the main effective procedures are in place.

AREAS OF STRENGTH

Strategy

- The current ICT Strategy and Service Plans document their commitments to achieving the Councils Objectives within the Corporate Plan.
- The Operational ICT Manager appears to be well-appraised with information that he requires regarding the ICT Services departments' status and performance.
- There appears to be an adequate amount of ICT team meetings, Corporate Team Meetings and various monitoring Boards, who meet on a regular basis, and cross-cutting Management staff attending the meetings/boards ensures that all information and actions are communicated and acted on appropriately.

- Action points in the meeting minutes viewed allocated actions to relevant Management representatives and usually indicate the required timeline for completion/next reporting date.

Asset Management

- The Asset Management function has clear links with the Service Desk, Configuration Management, Change Management, Procurement, Release Management and Starters/Leavers processes as identified via the Intranet and Asset Management Policy.
- The Asset Management Policy clearly defines which assets should be included in the Asset Register Database.

Legislation

- Lawful regulations regarding Computer misuse, data protection, human rights, WEEE and other acts/directives are well documented within the ICT Code of Conduct and referred to within other ICT documents.
- The GDP Regulations have been taken seriously by the Council as a whole, and a robust implementation plan is in place which appears to be on track for the May 2018 deadline.
- GDPR Implementation plans have been sufficiently communicated to Cabinet and have seen broad discussion with the relevant Information Governance, Insight and Corporate Management Boards.
- The new Data Protection training and detail of responsibilities have been well communicated to staff via the intranet, with training modules to update their knowledge.
- The Data Protection Officer has extensive knowledge and is sufficiently senior to perform the role.

Roles and Responsibilities

- A clear structure is in place for the ICT department.
- The Constitution points to a detailed delegation of authority for the Service Head of the ICT Department.

Policies and Procedures

- The ICT & HR Suite of Policies, Strategies and Codes of Conduct cover a broad range of topics.
- There appears to be good communication of Policy updates to staff via the Intranet and via communication by Management.
- Development and appraisal opportunities exist within the Council.
- Metacompliance is utilised to ensure that all new starters have read and accepted the ICT Code of Conduct.

Standards Compliance

- The Council is compliant with PSN, a process which involved the successful implementation of improvements required within remedial action plans.
- Clear communication of the PSN has been made with staff regarding why it's there, what it means for them and who to contact if they require assistance.
- Whilst there has been a gap since the last PCI review, the decision has been taken by the Council to procure a managed service.

Business Continuity Planning

- Access to the Application List is exclusive to the Application Support Team, to control who can amend the list.
- The definition of 'critical' systems is clear/well defined.

Disaster Recovery

- The Corporate Business Continuity/Disaster Recovery Plans are undergoing a large review to ensure that they are up to date/efficient.

Security

- Cyber security incidents are recorded within the Altiris system.
- Implementation of a central log for information disclosure breaches has been identified as a requirement within the GDPR project plans.
- The Employee Information Security Responsibilities document has been identified as requiring update within the GDPR project plan.

AREAS FOR ATTENTION

Strategy

- Accountabilities of ICT Group/Support Managers and their teams are available on the Staff Intranet; however this page requires review to ensure that it is up to date with the most relevant contacts and role descriptions.

Asset Management

- The Asset Management Policy and Procedure documents are not available/easily accessible by staff via the Intranet.
- Considerations should be given to Software Asset Management, including monitoring for the licensing of Software and inclusion of information within the Asset Management Policy.
- The Asset Management Procedure document should be revised to include practical guides for ICT/Front line staff regarding asset transfer and disposal.
- Consider better recording of the reading and understanding of the ICT Policies by staff by inclusion of a question relating to this within the #itsaboutme appraisal.
- Review entire suite of ICT Strategy and Policies to ensure that these are up to date, ensuring that document control is consistent for all.

Legislation

- The Disability Discrimination Act is not referred to within the ICT suite of policy/strategy/plan documents viewed. A more formal approach to addressing this Act should be considered, to ensure that needs of disabled staff are adequately accounted for in a proactive manner.
- Publish the Records Management Policy along with the procedure on the Staff Intranet to make it readily accessible to staff.

Roles and Responsibilities

- As referenced within the Governance Framework and Strategy section, the Staff Intranet requires review to ensure that the descriptions of roles and contact names, are up to date.
- The "Reporting Security Breaches" page on the staff intranet requires update to include the current SIRO's contact details.
- Continue to recruit for the vacant junior posts, having gained approval for the posts to go ahead.

Policies and Procedures

- Consider a review of the document control in place across the entire suite of Policies, Strategies and Codes of Conduct, to ensure that all required documents have the correct controls in place.
- Consider an update of the Policies (HR & ICT) as many are out of date/without review for 2+ years.
- Ensure that once new/updated Policies are uploaded to the Intranet regarding GDPR, that they are updated across the various pages of the Intranet where reference to Data Protection appears, to make sure that out-dated information is removed.

Standards Compliance

- There has been a large gap since the last PCI review, as a result of the Council awaiting further information from Northgate regarding whether they can be part of a managed service.

Business Continuity Planning

- An urgent update of the ICT Business Continuity Plan is required regarding the Applications Recovery Plans and ICT contact details.
- Considerations should be made to ascertain whether there is a more efficient way to ensure that the ICT Business Continuity Plan's contacts list and Application Recovery Plans are more regularly updated.
- The plans to update the application list should be continued, once a full assessment of applications has been completed in accordance with the Digital Strategy goals.
- Considerations should be made to ascertain whether there is a more efficient way to ensure that the application list is more regularly updated.

Disaster Recovery

- Consider whether full tests of the Corporate Business Continuity and Backup Disaster Recovery Plans are necessary to ensure that the plan is sufficient should a 'real' incident occur.
- Ensure that the Corporate Business Continuity/Disaster Recovery Plans include a detailed solution for bringing back each service area, and that the contact lists are up to date.
- Ensure that a regular update of the BCP responsibilities and contacts list is in place, to proactively prevent details from 'expiring'.

Security

- A security breach register/log is not currently kept for information disclosure incidents, however there are plans for this as part of the GDPR compliance work.

- Continue with the review/update of the Employee Information Security Responsibilities document, especially regarding breaches of security.

Detailed Assessment

1. Risk Management

Risk Management Strategy - Low Risk

The Council has recently revised its approach to risk management, which has been reflected within a new risk management strategy. The new approach to risk management has recently been agreed by Audit Committee, which is soon to be followed by consideration of the strategy.

The Council's new approach to risk management is being used by Service Managers, however, upon update of the risk management strategy, requires further communication to staff to ensure that it is embedded throughout the Council, building on the work undertaken to date by the Insight Board and through the Service Planning meeting workshops held with all Heads of Service and their management teams.

Risk Assessment – Low Risk

The need for risk assessment is outlined within the Council's risk management strategy. The strategy also provides information on project risks.

Risk management is built into the standard Team Plan and Service Plan templates. These are reviewed annually by the Performance and Development Team, who are also responsible for oversight of risk management.

There is not a standard template for Commissioning Plans, therefore the inclusion of risk considerations within Commissioning Plans is the responsibility of each Service Area.

Risk Registers – Low Risk

The Corporate Risk Register is directly linked to the Council's Corporate Plan Well-being Outcomes which contribute to the Well-being Goals set by Welsh Government. Individual risks are evaluated in terms of the impact on the Council's ability to contribute to the Goals. It is reviewed on a quarterly basis at Insight Board. A quarterly report is also taken to Corporate Management Team, before being taken to Audit Committee.

Each risk has an allocated risk owner, who is responsible for monitoring their risks and ensuring adequate mitigating actions are implemented.

The Council do not utilise bespoke software for their risk register. Microsoft Word and Excel are used.

Decision Making – Low Risk

As part of the decision making process over proposals by members, some of the key risks in relation to the proposals are referenced within reports and supporting documentation. This could be enhanced by specifically referencing the key risks in relation to the proposal within its own section of the reports and providing current and residual risk scores, along with mitigating actions to be taken. This would also allow for mitigating actions to be reported to members periodically.

Risk Appetite – Medium Risk

The Council uses a 4x4 risk assessment matrix to score their risks based upon likelihood and impact. There is not a predetermined risk tolerance value in place. To provide greater clarity in relation to whether a risk is within the Council's risk appetite, a numerical value could be set, enabling any risks above which to be deemed as "out of tolerance".

Transparency – Medium Risk

The Council's risk management strategy is available from the staff intranet site, however as previously referenced the strategy is currently out of date. Members of the Audit Committee are provided with a risk management update on a quarterly basis, with their most recent update including a risk management session to ensure that the proposed new risk management structure was understood.

Areas of high risk are discussed with other Authorities in relation to specific projects, such as the City Deal. The corporate risk assessment is not currently shared with other local authorities and bodies. Introducing this would provide opportunities for shared learning.

Project Risk Management – Medium Risk

These findings are also reported under the Programme and Project Management theme.

The Council's risk management strategy provides clear detail in relation to the links between projects and risk management. It includes detail on the need to determine the level of risk associated with the project during the start up phase of the project, and the requirement to maintain a risk and issues log throughout the completion of the project.

There is less certainty regarding whether this approach is adopted in practice, with risk and issue logs provided for the two sampled programmes, but not for the two sampled projects.

2. Commissioning and Procurement

Strategy – Low Risk

The Council do not have a central Commissioning Strategy, as commissioning activities have been devolved to Directorates. There is not a Council wide operating model or vision in place for commissioning. Strategy is outlined within the local level Commissioning Strategies/Plans created within each Directorate, as outlined below.

A Procurement Strategy is at Draft stage, which clearly links to the Council's Corporate Plan 2016-2020 and references the four Well-being Outcomes.

Commissioning Intentions – Low Risk

Commissioning intention strategies were only found to be in place within the Social Services Directorate. The strategies for Older People's Services and Children and Young People Services were obtained, which were both found to be well-communicated action plans as to what the Council Social Services are aiming to achieve, how they will monitor this and their overall approach towards commissioning.

Training and Skills - Medium Risk

The Procurement Strategy and the sampled Commissioning Strategies clearly identify the lifecycle of procurement/commissioning at the Council. The Procurement Strategy recognises the importance of the training and development of procurement staff, whilst the Commissioning Strategies focus only on the skills of the 'operational' staff and volunteers involved with the care projects as opposed to that of the Commissioning teams within the Council. The plans for this were instead included within the relevant Team Plans.

Skill needs assessments are done as part of the ongoing #itsaboutme appraisal programme and by Project Teams skills analysis put in place to manage procurement for certain projects, these processes also identify skills/competency training needs. Tasks are matched to those within teams who have the suitable category knowledge.

Governance – Low Risk

The Contract Procedure Rules within the Constitution refer to the Procurement Code of Practice regarding the Delegated Authority levels and where the levels of contract value and authority are documented.

Discussion with the ICT Procurement Manager confirmed the levels of authority required to move to the next stages of Procurement and samples of this taking place were provided for the Managed Print contract for which the contract value exceeded £100k.

Procurement exercises are monitored for performance and achievement via the various approval levels in place throughout the process - authorisation through Management within the Procurement portal ('Chief Officer sign off'), and by Scrutiny Committee and Cabinet as required.

Commissioning/Contract Performance Management is monitored by the designated Contract Manager and reported upwards to the Corporate Director for that Directorate, who in turn passes information up toward Cabinet and other committees.

Corrective actions are put in place if targets are not met are decided at management team level and escalated to Corporate Management teams if/as necessary.

Policies and Procedures – Low Risk

The Contract Procedural Rules refer to the superseded Public Contract Regulations 2006, whilst the Procurement Code of Practice refers to the updated Public Contract Regulations 2015.

Sustainable Procurement and Social Value are not stand-alone policies but are both included within the Procurement Strategy which is currently at Draft stage. Life cycle cost guidance is documented well within the Procurement Code of Practice, showing that the MEAT mechanism is used to assess tenders for contract awards.

There is a Social Services Commissioning Framework available via the Intranet, which indicates that there are Commissioning processes in place covered by the Analyse, Plan, Do, Review methodology.

Benefits and Savings – Medium Risk

The Social Services Commissioning Strategies targets are established from a range of Local and

National Imperatives such as the Councils Communities Change Plans, the Corporate Plan and Social Care Frameworks; and the Procurement targets are established to ensure compliance with Local and National regulations/rules, such as the Council's Financial Procedure Rules, Contract Procedure Rules and the Public Contract Regulations 2015.

Savings are identified within the Older Persons Commissioning Strategy as "Efficiency Savings", although they provide a percentage target of 4% savings over the periods 2011/2012 to 2013/2014, they do not explain what targets are in place for after these periods. This Plan is expecting a review in 2018, and so an update on these targets would be an expected feature of the review.

The Children and Young Persons Strategy identifies efficiency savings also, and points to it 'being likely' that the Social Services Directorate as a whole will need to meet a target of £2mil/year for the 'foreseeable future'. The Plan also identifies what the benefits of effective commissioning could be.

The Procurement Strategy identifies the Units targets as generally being to ensure that Value for Money is obtained when planning a procurement route, and no quantitative targets are given within the Procurement Strategy.

There were no commissioning or procurement KPI samples viewed during audit testing, so it is not possible to provide information on whether targets are being met and whether there are any actions in place to address targets which are not being met.

Value for Money – Low Risk

Within the Procurement Strategy, the Children and Young Persons Commissioning Strategy, and the Older Persons Commissioning Strategy, value for money and social value delivery intentions are well documented. Within the commissioning strategies there is also identification of the need to bridge the requirement to save costs with the requirement to provide adequate care to recipients of the service.

Performance Management Frameworks are available via the Intranet, indicating how Directorates/ Service teams should monitor performance against value for money and social value targets, as well as reference to this within the commissioning strategies viewed.

Value for money and social value requirements are communicated to potential suppliers within the tender guidance documentation provided via the Sell2Wales portal. The standard guidance provides information as to what evaluation and scoring is applicable to tender submissions.

Transparency – Medium Risk

The Procurement Strategy and Procurement Code of Practice refer to the Public Contract Rules 2015; whilst the Contract Procedure Rules within the Constitution document refer to the out-dated 2006 Public Contract Rules. None of these documents refer to the Local Government Transparency Code 2015, nor to the requirement to publicly advertise Future Contract Notices via the Sell2Wales portal.

There is no publication of spends above thresholds via the Councils website. One current contract notice showing the Contract Value could be located via the Councils Sell2Wales page, but no other notices viewed indicated Contract worth. Not enough evidence was available to

arrive at a conclusion as to whether publishing of spend above threshold was compliant.

The Contract register is held via the E-Tender Wales portal and Excel reports were provided from this late in the audit testing period. A swift review of some entries on the Contract list, compared to the Contract Award Notices available on the Sell2Wales Vale of Glamorgan page did not appear to link any Contracts with an Award Notice. The content of the Contract Register was also missing a contract history for each, milestones and the managerial reporting dates; which are information requirements from the Procurement Code of Practice when submitting a contract onto the register. There was one example of a future contract notice available the Sell2Wales Vale of Glamorgan pages, but it appeared to be out of date, advertising an information sharing event in mid-2017. This area would be well placed for further review in the future.

Category Management – Medium Risk

Category Management is a method used at the Council for their procurement activity, however, this is not evidenced within the Procurement Strategy nor Procurement Code of Practice. There is however a table describing the specialist areas for the two procurement specialists or 'category managers' who sit beneath the Council's Head of Procurement, which indicate the 'categories' that procurements fall into. As there was no category management strategy available it was not possible to reach a conclusion regarding the way that category management is performed.

Supplier Management – Medium Risk

No evidence was provided to suggest that a key suppliers list is in place at the Council.

The Business Continuity Plans are currently undergoing a review and the current Plan was not provided, therefore it was not possible to ascertain whether key suppliers are considered.

A Business Continuity Protocol document was provided along with Business Impact Analysis', though these did not address supplier failure and referred to the Service areas/Directorate BC Plans for further guidance. The ICT Continuity Plan was provided, but the links within the document to the service areas individual Disaster Recovery plans do not work/allow me to view the document, as such no conclusion as to whether they include supplier recovery could be reached.

Social Value – Low Risk

Stakeholders appear to be engaged with adequately at the beginning of procurement processes, in line with the Councils Procurement Code of Practice. There is a standard methodology regarding the procurement process, which is sufficiently documented within in the Code of Practice as a step-by-step guide.

Evidence of the standard process influencing contract design and award was found within the report to Cabinet regarding the recent tender for the Managed Print Service. There was evidence in this report that the project board were to be established following the Corporate Procurement Management Methodology, consisting of various department representatives including Legal and HR. Evidence of the methodology influencing contract award was within this report, which noted that finding a collaboration partner was not possible after attempted efforts.

The development of all Council staff who engage in procurement activities is monitored and progressed via an ongoing/annual appraisal scheme called #itsaboutme. Members knowledge and expertise are also developed in accordance with the Member Development Strategy, by their involvement in Council business and access to training resources.

3. Programme and Project Management

Project Methodology – Low Risk

Standard project methodology is in place and available from the Council's intranet site. The exact methodology to be used is determined by the size, funding, and level of risk associated with the project. The Council also operate with a flexible approach to the documentation; the use of the templates is not mandatory, so long as key areas are considered.

Project Documentation – Low Risk

Key project document templates are available from the staff intranet, such as a Project Initiation Document and a Business Case. The Council's approach to Programme and Project Management is to enable the Project Manager and Project Sponsor the flexibility to decide what form the documentation is to take, therefore the templates are available as an option for use and are not mandatory, although the content within the templates is still expected to be evidenced.

Each of the four programmes/projects sampled within this review were found to have sufficient documentation to support them, which 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.

Programmes/projects within the Reshaping Services Programme are monitored within monthly Programme Board meetings, with progress also reported to Cabinet on a frequent basis.

Strategic Projects, those which are not within the Reshaping Services Programme however are still of corporate interest, are monitored within the bimonthly Strategic Projects Monitoring Group.

Each of the four programmes/projects sampled are monitored within the arrangements outlined above. The sampled programmes/projects also had had their own Project Board meetings to discuss progress, however for one of the sample (Cemetery Approach), evidence could only be provided to show the last formal meeting was in April 2017.

Resource Allocation – Low Risk

For three of the four programmes/projects which were sampled within this review, the project documentation in place defined the skills 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.

Two of the sampled programmes/projects also clearly defined the capacity required for the work to be completed, however the other two did not. It appears that, whilst a flexible approach to project management documentation is being adopted by the Council, there is greater potential for some key governance information to be missed as a result of standard project documentation not being mandatory.

Risk Management – Medium Risk

The Council's risk management strategy provides clear detail in relation to the links between projects and risk management. It includes detail on the need to determine the level of risk associated with the project during the start up phase of the project, and the requirement to maintain a risk and issues log throughout the completion of the project.

There is less certainty regarding whether this approach is adopted within Projects. Risk and issue logs were provided for the two sampled programmes, however they were not in place for the two projects sampled. It should be noted that both projects within the sample commenced prior to the introduction of the project management guidance on the intranet, however it would be expected that the approach to risk management be adopted within all key projects currently in place.

Responsibility – Low Risk

The Council's approach to project management means that there is flexibility regarding whether the Project Initiation Document and Business Case templates are used, however the content of the templates is expected to be followed.

Of the sampled four sampled programmes/projects, the roles and responsibilities for three were outlined within governance structure documents. This information was not found to be in place for the fourth sampled programme/project.

Lessons Learned – Medium Risk

It was advised that plans for benefits realisation are included within the project documentation of programmes/projects, however, it was not possible to verify this during testing and therefore may be of benefit to verify in future.

There is not currently a corporate overview of all completed programmes/projects.

Delivering Corporate Objectives – Low Risk

The template business case for higher value and/or risk projects requires staff to document the 'Strategic Fit' of the proposal. For lower value/risk projects, the project brief template does not request any information in relation to the project's alignment to corporate objectives.

The Council's approach to programme/project management means that it is not expected that these templates are always completed, however the required information from within the templates is expected to be seen within the documents created.

Oversight arrangements by Senior Management and Members also help to ensure that the Reshaping Services Programmes and the Strategic Projects are undertaken in line with corporate objectives.

Supporting Change – Low Risk

For the two programmes sampled, both of which would have an impact upon staff, cultural considerations were made within the project documentation.

Whilst neither of the projects sampled had a direct impact upon staff, they both included considerations towards sustainability within their project documentation.

A representative from HR was identified within project documentation as supporting three of the four programmes/projects. It was not possible to determine this for the Leisure Centre Works project, as a governance structure document was not in place.

4. Information Management

Strategy – Low Risk

There are clear links within the Corporate Plan regarding how ICT will play a role in carrying out the Council's Objectives, which is further reflected within the ICT Strategy and ICT Service Plan. The ICT Service Plan provides information on the actions in place for the year ahead, which of the Council Priorities they meet and who is responsible for each.

The ICT Strategy was approved via Cabinet and is currently undergoing a further review, arising from a Service Plan action to align with transformational changes at the Council.

There appears to be an adequate amount of ICT team meetings, Corporate Team meetings and various monitoring Boards, which are chaired by some of the same Group Managers/Heads of Service as those at Team meetings, ensuring that information and action points are sufficiently communicated via cross-cutting between meetings/boards and actions completed as necessary. The information provided to Officers who are not involved directly with ICT is made clear/free of IT 'jargon' to ensure it is understood.

The Council's Constitution document provides job descriptions for the Operational Manager (ICT), with information in relation to the whole ICT team available via the intranet.

Asset Management – Medium Risk

The Asset Management Policy and Procedure documents are not available/easily accessible by staff via the intranet.

The Asset Management function has clear links with the Service Desk, Config. Management, Change Management, Procurement, Release Management and Starters/Leavers processes as identified via the Intranet and Asset Management Policy.

There are hardware asset management procedures within the asset management procedures document regarding the inventory of assets through to the receiving of goods, but no practical direction for ICT staff members in order to complete asset transfer (to the end user/back) or disposal. There is a brief mention of each process within the policy document which is geared towards the Council staff receiving the equipment, rather than protocol for ICT staff. The Asset Management Policy does not reference software management.

Asset Management Policy references full lifecycle, however concerns were raised regarding how well the procedures are adhered to, therefore this may require further review. There is a CMDB which is in place to log the lifecycle of each ICT Asset, however concerns have also been raised regarding its upkeep.

Legislation – Low Risk

Most lawful regulations regarding computer misuse, data protection, human rights, WEEE and other acts/directives are well documented within the ICT Code of Conduct and referred to within other ICT documents. There was guidance and a procedure document regarding Records Management available via the intranet, but the Records Management Policy was not available. There are currently controls in place to comply with the Welsh Government classification

scheme, but new software is due to be installed to make the process easier regarding classification categories.

The Council have appointed a Data Protection Officer in preparation for the GDPR. There is an implementation plan based around the 12 Step Guidance provided by the ICO, from which a number of progress reports have been provided to various Corporate Boards and Corporate Management Team, as well as to Cabinet.

The Information Asset register is being updated by Management teams regarding the information they hold that relates to GDPR, which will be used as a basis to identify the data sets held across the Council. The retention schedule was last updated in March 2017 and will be reviewed again once there is further retention information published by Government.

The DPO has adequate knowledge to be able to execute the role efficiently and there is awareness training going out to all staff at the Council, as well as an update to the induction training modules for new starters.

Roles and Responsibilities – Low Risk

The ICT Department recently underwent a large restructure due to a decrease in resource funding. Currently all posts are filled within the ICT Structure, with the exception of three junior posts.

The Constitution document for the Council identifies the Delegation of Authority for the Head of Service (Operational Manager (ICT)), with the responsibilities of ICT teams given under their section of the staff intranet (and otherwise within their HR job descriptions).

The staff intranet "Reporting Security Breaches" page requires updating, to refer to the current incumbent of the SIRO post.

Policies and Procedures – Low Risk

There is a comprehensive suite of ICT policies in place which cover a wide range of topics, and all could be easily located from the intranet. They are all in need of an update (except for the DSE Policy), with most of the Policies last updated in 2015, and some do not have document control in place to indicate their last review.

There are no alternative methods for communication of the Policies to staff with visual impairment, nor any versions in the Welsh language for Welsh speaking staff.

There is adequate communication of ICT policies to new starters within the Corporate Induction process, and through updates communicated as key messages via the staff intranet, which are also circulated by Management if relevant to their teams. Metacompliance is utilised to ensure that all new starters have confirmed that they have read and accepted the ICT Code of Conduct.

European Computer Driving License training is available to all ICT staff as well as the mandatory Corporate Training which all staff receive.

Standards Compliance – Medium Risk

There is clear guidance for staff indicating what GCSx and GCi compliance is, what it relates to,

set-up procedures, and a personal commitment to state which they would have to complete in the event that they will be required to use the GCSx network. There is also information on who to contact if they have any issues with the networks.

The Council passed their most recent PSN review, with remedial action plans in place (and in progress) to address the recommendations made by their assessors. The most recent PCI compliance test was in 2015, with a follow up in 2016, as the Council has been awaiting Northgate to undertake a site survey with the prospect of the Council joining their managed service. The Council are waiting for an announcement by Northgate regarding whether this can take place, which should determine the following course of action. As a contingency plan, there are other 'backup' suppliers in place to take over if Northgate cannot perform the review.

Business Continuity – Medium Risk

The critical application list features in quarterly key performance reports and appears to be discussed/approved at Digital Strategy Board meetings. This Digital Strategy Board consists of the Managing Director, Head of Services and Theme Leaders (nominated Group Managers) and feeds up information to the Insight Board.

As confirmed verbally by the Operational ICT Manager, only the Application Support Team within ICT have access to the applications list. 'Critical' applications are defined within the list as "*Mission critical applications that are key to the day to day running of the authority*". Although there is a quarterly key performance report which includes the critical applications list within, the Operational ICT Manager explained that the "Top 20" applications are in need of review to assess their criticality. This is planned within actions plans in accordance with the Digital Strategy Project currently being implemented. The list was compared to the ICT Services Continuity Plan and some of the applications did not appear to feature within the software/applications listed with DR Plans. The ICT Continuity Plan was last reviewed in April 2015 and therefore needs to be updated, with contact details for some current staff not included within the Appendix E Emergency Contacts Lists.

As part of this review, it has not been possible to verify whether detailed recovery solutions are in place for each of the applications referenced within the ICT Business Continuity Plan.

Disaster Recovery – Low Risk

There is a nightly backup of the NetApp volumes which are retained for the night and day before. Oracle E-Biz and VMWare retain a week's worth of snapshots. Backups are stored on disc at the production site and then replicated to an identical appliance in the disaster recovery location. Longer term backups are kept for a maximum of two years. The backup disaster recovery plan has not been fully tested, but there is a recovery diary kept which details the individual system recoveries which have occurred, along with issues stemming from them.

Security – Medium Risk

All cyber security incidents are logged within Altiris at the time they are reported to the ICT Service Desk.

There is not currently a central log of information disclosure breaches, although this is already being addressed as part of the GDPR implementation plans. The DPO explained that currently information disclosure breaches are managed via Service Areas/Directorates own 'Security Incident' logs and dealt with within their teams and communication with the SIRO.

The Employees Information Security Responsibility document is available on the staff Intranet which provides guidance on how to report security breaches, but there is no information within this document as to how they will be followed up (other than a meeting).

There is an intranet page advising staff what to do in the event of a security breach and advice on the Information Security Portal regarding what constitutes a 'breach', but the security breach page still refers to the now retired Head of Strategic ICT as the Council's SIRO.

There is a section of the Corporate Risk Register which provides an update on the Council's status regarding security breaches, which provides a brief reference to actions/the status as opposed to a detailed action plan, but it does indicate that the risk status has remained static and that actions are being put in place, which is reported to have 'lowered' the amount of data issues being experienced. No major breaches are reported recently here.

Appendix A - Mapping Areas for Attention to 2017/18 Internal Audit Plan

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
Risk Management – Strategy	The revised risk management strategy needs to be approved and communicated to staff to reflect the changes in approach.	Medium Risk Follow up required.	Head of Performance & Development	TBA
Risk Management – Risk Assessment	There is a lack of consistency regarding how risks to the achievement of commissioning plans are referenced.	Low Risk – Advisory Recommendation	As Above	N/A
Risk Management – Risk Register	The process for managing and monitoring the corporate risk register is not currently documented.	Low Risk – Advisory Recommendation	As Above	N/A
Risk Management – Decision Making	Information on risk assessment provided to members is highly limited and could be improved by ensuring that risks are more explicitly referenced within the documentation. This would enable inherent and residual risk scores to be captured along with the mitigating actions.	Medium Risk – Follow up required.	As Above	TBA
Risk Management – Risk Appetite	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 value should be taken to Audit Committee as part of the current corporate risk register review schedule.	Medium Risk – Follow up required.	As Above	TBA
Risk Management – Transparency	The corporate risk assessment is not communicated with other local authorities and bodies.	Medium Risk – Follow up required	As Above	TBA
Commissioning and Procurement – Strategy	The updated Procurement Strategy needs to be finalised, including the time period that it is to cover.	Medium Risk – Follow up required.	Head of Finance / Section 151 Officer	TBA
Commissioning and Procurement – Strategy	There is no corporate oversight of Commissioning Strategies/Plans.	Medium Risk – Follow up required.	OM – Commissioning & Information	TBA
Commissioning and Procurement – Training and Skills	The Commissioning Strategies/Plans viewed did not provide any information on the need to provide targeted training to staff.	Low Risk – Advisory Recommendation	As Above	TBA

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
Commissioning and Procurement – Policies and Procedures	The Contract Procedural Rules do not refer to the Procurement Contract Regulations 2015.	Low Risk – Advisory Recommendation	Head of Finance / Section 151 Officer	N/A
Commissioning and Procurement – Benefits and Savings	Aside from the Social Services Directorate, commissioning targets are not in place. KPI's are also not in place to help monitor the Social Services commissioning savings target. An annual review of the commissioning strategies to update the targets may assist with this.	Low Risk – Advisory Recommendation	OM – Commissioning & Information	N/A
Commissioning and Procurement – Transparency	The Procurement Code of Practice does not include guidance regarding the Local Government Transparency Code 2015, such as the requirements for publishing of future contract notices and spend above threshold.	Low Risk – Advisory Recommendation	Head of Finance / Section 151 Officer	N/A
Commissioning and Procurement – Transparency	The Constitution Contract Procedure Rules need to be updated to comply with the Public Contract Regulations 2015.	Low Risk – Advisory Recommendation	As Above	N/A
Commissioning and Procurement – Transparency	Ensure compliance with the requirement to publish spends over threshold and Future Contract Notices publicly (via Sell2Wales).	Low Risk – Advisory Recommendation	As Above	N/A
Commissioning and Procurement – Transparency	Ensure that all contracts held by the Council in excess of £15k are recorded in the Corporate Contract Register.	Low Risk – Advisory Recommendation	As Above	N/A
Commissioning and Procurement – Category Management	Consider inclusion of a Category Management strategy/procedure overview within the Procurement Code of Practice and Procurement Strategy.	Low Risk – Advisory Recommendation	As Above	N/A
Commissioning and Procurement – Supplier Management	Ensure that Key Suppliers are identified and addressed by Disaster Recovery Plans.	Medium Risk – Follow up required	As above	TBA
Programme and Project Management – Progress Monitoring	Regular formal progress meetings are not currently being undertaken for the Cemetery Approach project.	Low Risk – Advisory Recommendation	CMT	N/A
Programme and Project Management –	Risk and issues logs are not in place for the two sampled projects.	Low Risk – Advisory Recommendation	CMT	N/A

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
Risk Management				
Programme and Project Management – Responsibility	The Leisure Centre Works project did not have a governance structure document to outline the roles and responsibilities in relation to the project.	Low Risk – Advisory Recommendation	OM – Neighborhood Services & Healthy Living	N/A
Programme and Project Management – Lessons Learned	Performance information in relation to programmes/projects is not currently kept corporately. This would enable the Council to have a clearer picture regarding the successfulness of projects.	Medium Risk – Follow up required	CMT	TBA
Programme and Project Management – Delivering Corporate Outcomes	The project brief template in place for lower risk projects does not currently request any information in relation to the project's alignment to corporate objectives.	Medium Risk – Follow up required	CMT	TBA
Information Management – Strategy	The Staff Intranet page outlining the accountabilities of the ICT Group and their teams is out of date.	Low Risk – Advisory recommendation	OM – ICT	N/A
Information Management – Asset Management	The Asset Management Policy and Procedure documents are not available/easily accessible by staff via the Intranet.	High Risk – Follow up required	As Above	TBA
Information Management – Asset Management	Software asset management is not referenced within the Asset Management Policy.	High Risk – Follow up required	As Above	TBA
Information Management – Asset Management	The Asset Management Procedure could be revised to include practical guides in relation to asset transfer and disposal.	High Risk – Follow up required	As Above	TBA
Information Management – Legislation	The Disability Discrimination Act is not referred to within the ICT suite of policy/strategy/plan documents viewed.	Medium Risk – Follow up required	As Above	TBA
Information Management – Legislation	The Records Management Policy and Procedure should be published on the Staff Intranet.	Low Risk – Advisory Recommendation	As Above	N/A
Information Management – Responsibilities	The 'Reporting Security Breaches' page of the staff intranet needs updating with the current SIRO contact details.	Low Risk – Advisory Recommendation	As Above	N/A
Information Management – Policies and Procedures	A number of the policies in place are now out of date and require review.	High Risk – Follow up required	As Above	TBA
Information Management –	An up to date PCI review has not been undertaken.	Unable to conclude		

Theme	Area for Attention	Inclusion in 2018/19 Plan	Owner	Date of Audit Work
Standards Compliance				
Information Management – Business Continuity	The ICT Business Continuity Plan requires updating with current Application Recovery Plans and ICT contact details.	Unable to conclude – Action Required	As Above	TBA
Information Management – Disaster Recovery	Consider whether testing of the Disaster Recovery Plan and the Business Continuity Plan is necessary.	Unable to conclude – Action Required	As Above	TBA
Information Management – Disaster Recovery	Ensure that the Corporate Business Continuity/Disaster Recovery Plans include a detailed solution for bringing back each service area, and that the responsibilities with contact lists are up to date.	Medium Risk – Follow up required	As Above	TBA
Information Management – Security	A security breach register/log is not currently kept for information disclosure incidents.	Unable to conclude – action required	As Above	TBA

Report Authors and Distribution

Report Authors

This report was produced and issued by:

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

Key Contacts

The key contact for each theme:

- **Risk Management** Huw Isaac, Head of Performance and Development
- **Commissioning** Gaynor Jones, Commissioning and Information Operational Manager, Social Services
- **Procurement** Nigel Smith, Operational Manager Exchequer Services
- **Programme and Project Management** Tom Bowring, Operational Manager, Performance and Policy
- **Information Management** Nick Wheeler, Operational Manager, ICT

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 Responsibility

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.