

# Flintshire County Council

Risk Management

Internal Audit Report  
August 2013

FINAL

## CONTENTS

Section	Page
Executive Summary	2
Action Plan	6
Findings and Recommendations	11

Debrief meeting	16 <sup>th</sup> April 2013	Auditors	Flintshire Internal Audit
Draft report issued	29 <sup>th</sup> April 2013		
Responses received	17 <sup>th</sup> July 2013		
Final report issued	7 <sup>th</sup> August 2013	Client sponsor	Chief Executive
		Distribution	Policy and Performance Manager Risk Manager Head of ICT and Customer Services

## 1 EXECUTIVE SUMMARY

This report covers the Risk Management review carried out between January and March 2013. This was approved as part of the Internal Audit plan for 2012/13 as a healthcheck review to follow up the lowest classified areas of the 2011/12 risk maturity advisory review.

Risk management is an integral part of good governance and is a process whereby:

- there is shared awareness and understanding within the Council of the nature and extent of the risks it faces; and
- there is regular and ongoing monitoring and reporting of risk, including early warning mechanisms.

The process should be ongoing, embedded in the culture of the Council and drive performance improvement. It is not about eliminating risk but about understanding risk and managing it more effectively. Each organisation must decide what benefits it would like as a result of its risk management programme and plan its approach accordingly. Through effective risk management, the Council will be able to deliver:

- an appropriate balance between risk and control;
- more effective decision making;
- better use of limited resources; and
- more innovation.

### 1.1 BACKGROUND – THE 2011/12 RISK MATURITY REVIEW

In 2011/12 we carried out an advisory review of Risk Maturity by assessing the following key components of risk management:

- Governance
- Risk Identification
- Risk Assessment
- Risk Mitigation
- Assurance
- Monitoring and Reporting

The advisory review concluded that the Council has a real opportunity to enhance the existing processes in place for risk management but needed to revisit the SARC to better align strategic objectives and improve version control. Risk Assessment and Risk Mitigation were the weakest areas with regard to risk maturity.

### 1.2 INTRODUCTION

The audit has assessed the extent to which Risk Management identifies and evaluates risks faced by the council and establishes effective mitigation actions including the following areas:

1. RISK ASSESSMENT - Risk scoring methodology is defined and applied and risks are effectively assessed using the corporate framework for the following risk types:
  - Strategic Assessment of Risks and Challenges (SARC)
  - Operational risks – through service plans
  - Project Risks - through the Project Management System
  - Partnership risks
2. RISK MITIGATION - Efficient and effective mitigations are established and are achieving required outcomes.

**1.3 CONCLUSION** – The council is making progress with embedding risk management at the council. The Risk Management Strategy has been updated and the strategy covers risk appetite and all key components of risk management.

The current risk assessment and mitigation template proposed for operational risk assessment in the Risk Management strategy represents good practice and is applied by a number of other councils in assessing strategic and other risk types. The SARC still has a number of weaknesses as a corporate risk register. We recommend at the next SARC refresh the format is converted into the best practice template provided for operational risk assessment which will highlight the gaps we have identified in this report and mandate effective completion of risk assessment, and mitigation information including better evidencing inherent, residual and target risk classifications.

In the medium term the council should establish a risk management database linked to the intranet that removes the current time consuming SARC spreadsheet update process which is clearly leading to validation issues. The PP&P section have confirmed a request has been submitted to ICT and this is under development. The same best practice template for risk assessment and mitigation should be used for operational, strategic, partnership and project risks.

The Council should now implement actions to further embed risk management throughout the organisation and ensure consistently high quality of risk assessment and mitigation for all sources of risks be they strategic, partnership, project or operational. In order to achieve this, the council needs to review how it can mandate risk management for all significant partnerships and projects, and also how all significant partnerships can be mapped into one corporate register.

To further embed risk management at the service and operational level, those service plans assessed by PP&P as having weak or no risk management information should be required to revisit risk management, potentially by sharing good practice examples identified elsewhere in the council.

Until effective risk assessment and mitigation is consistently applied and embedded across strategic risks, operational risks, partnerships and projects these two components of risk maturity will continue to need improvement.

#### 1.4 APPROACH TO REVIEW

The following areas were considered as part of this review:

- Risk Assessment  
The likelihood and impact of risk is assessed to prioritise the risks facing the organisation
- Risk Mitigation  
Understanding and analysing the impact of implementation of controls and other risk mitigation activity

Sources of strategic, operational, partnership and projects risks were reviewed on a sample basis to review risk assessment and risk mitigation.

The audit planning meeting also identified that officers were concerned that the quality of risk assessment and mitigation is variable between Directorates. To ensure this was covered as part of the audit a sample of Directorate service plans were reviewed as part of the audit.

##### Limitations to the scope of the audit:

This audit excludes the following four components of risk maturity:

1. Governance  
Establishment of a defined approach that ensures risk management can be used to inform business planning and support business decisions.
2. Risk Identification

Identifying the risks facing the organisation, the causes of those risks and consequences should those risks occur.

3. Assurance

Directing assurance to provide comfort on how well risks are being managed.

4. Monitoring and Reporting

Reporting of risk management to support decision making

In addition, Business Continuity was excluded from this review as it has been the subject of a separate audit.

**1.4 RECOMMENDATIONS SUMMARY**

The following table highlights the number and categories of recommendations made. The Action Plan at Section 2 details the specific recommendations made as well as agreed management actions to implement them.

**Recommendations made during this audit:**

	Fundamental	Significant	Merits Attention	Total
RISK ASSESSMENT AND MITIGATION	0	6	6	12
<b>TOTAL</b>	0	6	6	12

## 2 ACTION PLAN

The priority of the recommendations made is as follows:

Priority	Description
Fundamental	Action is imperative to ensure that the objectives for the area under review are met.
Significant	Requires action to avoid exposure to significant risks in achieving the objectives for the area under review.
Merits Attention	Action advised to enhance control or improve operational efficiency.
Suggestion	These are not formal recommendations that impact our overall opinion, but used to highlight a suggestion or idea that management may want to consider.

Ref	Recommendation	Categorisation	Accepted (Y/N)	Management Comment	Implementation Date	Manager Responsible
<p><b>Risk Assessment</b> - The likelihood and impact of risk is assessed to prioritise the risks facing the organisation.</p> <p><b>Risk Mitigation</b> - Understanding and analysing the impact and of implementation of controls and other risk mitigation activity.</p>						
1.05	The current risk assessment and mitigation template proposed for operational risks in the Risk Management strategy represents good practice and is applied by many councils in assessing strategic and other risk types. There are a number of shortcomings with the current format of the SARC as indicated in our report. We recommend at the next SARC refresh the format is converted into the best practice template provided for operational risks which will highlight the gaps we have identified and mandate effective completion of risk assessment, and mitigation information including better evidencing inherent, residual and target risk classifications. In the medium term the council should establish a risk management database linked to the intranet that removes the	Significant	Yes	1.05i) During the recent business planning refresh, the strategic risks have been aligned to the improvement priorities of the Council and are captured in the high level Improvement Plan.  ii)The detailed risks (work in progress) will be in a format similar to the best practice Operational Template and presented to Cabinet in October. This is consistent with Directorate and Service	1.05i) Completed  ii)October 2013	KA

Ref	Recommendation	Categorisation	Accepted (Y/N)	Management Comment	Implementation Date	Manager Responsible
1.01	<p>current time consuming SARC spreadsheet update process which is clearly leading to validation issues. The PP&amp;P section have confirmed a request has been submitted to ICT and this is currently being developed.</p> <p>The same template for risk assessment and mitigation should be used for operational, strategic, partnership and project risks.</p>	Merits Attention	Yes	<p>Planning</p> <p>iii) ICT to restart "Sprint" exercise to develop database for capturing risks aligned to priorities and performance.</p> <p>1.01. The same template is being used in projects and has been adapted to be suitable for partnerships</p>	<p>iii) First stage of development – October 2013</p> <p>1.01 Completed</p>	KA/CG
1.01	At the next refresh of the risk management strategy residual, inherent and target risk should be clearly defined. The Gross and Net risk sections of the operational risk template should be better explained in the Risk Management strategy so officers will understand that they are identifying inherent and residual risks when determining Gross and Net risk.	Merits Attention	Yes	This is a technical/definition issue. Inherent/residual gross/net mean the same thing; however the Risk Management Strategy will be revisited to clarify the definitions.	1.01 September 2013	KA
1.04	Council objectives should be noted against strategic risks within the SARC, rather than in the Annual Performance Report. This is necessary to enable users of the SARC document to understand clearly how each SARC risk relates to a corporate objective/priority, and how these corporate risks are being managed or mitigated thereby enabling these corporate objectives/priorities to be met.	Significant	Yes	Response as in 1.05	Completed	

Ref	Recommendation	Categorisation	Accepted (Y/N)	Management Comment	Implementation Date	Manager Responsible
1.04	The current 'objectives' included against each strategic risk in the SARC should be renamed to avoid confusion with corporate or directorate objectives to a user of the document.	Merits Attention	Yes	This is now obsolete as the Council has 'refreshed' its objectives/priorities.	Completed	
1.06	Partnership registers should be compiled that completely and accurately captures all significant regional, sub-regional and local partnerships in which the council participates.	Significant	Yes	The partnership register set needs to be better maintained to ensure currency and integrity of data. They will be subject to periodic revision.	December 2013	KA
1.06	Formal risk management as defined by the risk management strategy should be applied to all significant regional, sub-regional and local partnerships where FCC is the lead authority.	Significant	Yes	There is a formalised structure and periodic reporting, but application is not consistent and improvements are needed in some areas. This applies to all significant partnerships, including those where we are the 'lead' authority.	December 2013	CE / KA
1.06	Training in risk management should be provided to current partnership lead officers.	Merits Attention	Yes	Already in place	In progress	KA
1.07	Robust risk management should be applied to all medium and large scale projects with evidence retained in the PMS.	Significant	Yes in part	Agreed that robust risk management should be applied to all projects, but some of these may be manual and not on the electronic PMS system.	Ongoing	KA / Project Managers



Ref	Recommendation	Categorisation	Accepted (Y/N)	Management Comment	Implementation Date	Manager Responsible
1.07	There should be a review of the projects in the PMS periodically to challenge instances where it is identified that PMS risk management templates are not being used.	Merits Attention	Yes	See above		
1.08	The operational risk assessment template included in Appendix B of the Risk Management Strategy is a best practice template and service managers should be required to use this approach to manage risks and evidence this by including the completed template in the service plan  PP&P should review draft service plans and challenge those where risk management information is either inadequate or non-existent	Significant	Yes	Refer to 1.05ii)	September 2013	KA / Heads of Service
1.08	All service managers should be asked to evidence that Data Protection issues have been included in operational risk assessments	Merits Attention	Yes	To be included in ongoing refresh of Service Plan guidance	February 2014	KA

## FINDINGS AND RECOMMENDATIONS

### 1. RISK ASSESSMENT - *The likelihood and impact of risk is assessed to prioritise the risks facing the organisation.*

#### RISK MITIGATION - *Understanding and analysing the impact and of implementation of controls and other risk mitigation activity*

OVERVIEW AND ASSESSMENT OF ACTUAL CONTROLS IN PLACE	RECOMMENDATION
<p><b>1.01 General Risk Assessment and Mitigation</b></p> <p>The risk management strategy (update September 2012) provides the framework for risk management and how to assess and mitigate risks, including the templates to be used. However, there are two different templates proposed within the appendices of the strategy itself - one for Strategic (SARC) risks, and a recent template for operational risks. The SARC template and general risk guidance in the strategy contains no reference to residual and inherent risk and there is no guidance therefore as to how to identify initially the inherent risk through use of the risk matrix, and then current internal controls that help mitigate inherent risk to a residual risk level. This should be addressed, particularly as the recent template for operational risk management included in the appendices to the strategy contains references to gross risk, net risk (equivalent to inherent and residual risk respectively) and target risk (which should be the risk after mitigation action has been implemented in full and outcomes achieved). Service plans, Partnerships and Projects all use different templates.</p> <p><b>Conclusion</b></p> <p>The framework for risk management set out in the risk management strategy is not applied consistently across SARC, operational, partnership and project risk management. In any event two different approaches are now proposed in the risk management strategy depending on whether the risk is operational or strategic.</p> <p><b>1.02 Risk Appetite</b></p> <p>IRM defines risk appetite as 'The amount of risk that an organisation is willing to seek or accept in the pursuit of its long term objectives.' The fact that not all risk can be eliminated or reduced to GREEN is noted in the latest Risk Management strategy:</p>	<p>At the next refresh of the risk management strategy residual, inherent and target risk should be clearly defined. The Gross and Net risk sections of the operational risk template should be better explained in the Risk Management strategy so officers will understand that they are identifying inherent and residual risks when determining Gross and Net risk.</p> <p>The same template for risk assessment and mitigation should be used for operational, strategic, partnership and project risks.</p>

OVERVIEW AND ASSESSMENT OF ACTUAL CONTROLS IN PLACE	RECOMMENDATION
<p>1.2 <b>Not all risk can be eliminated</b> but it is vital that risks are recognized and recorded and that their potential to cause loss is fully understood, some risks are external to us, e.g. The impact of other partners' actions or Governing bodies. Based on this information, action can be taken to direct appropriate levels of resource at controlling the risk or minimising the effect of potential loss.</p> <p>6.6 <b>It should be noted that not all risks can be mitigated to a low (green) level and may be tolerated at a medium (amber) level. The predictive status on the SARC template should be amended to show this and the reasoning behind this should be clearly stated.</b></p> <p>6.9 <b>Most risks cannot be eliminated altogether and risk management involves making judgements about what level of risk is acceptable.</b> There are four categories of response to risks – treat, tolerate, transfer, terminate – known as the Four T's.</p> <p>7.2 <b>Corporate Management Team</b> is responsible for.....<b>Discussing the appropriate level of risk for the Council</b></p> <p>Review of the current SARC (Sept 2012 – final version issues Dec 18<sup>th</sup> 2012) shows that in all but one of the 49 risks, a “Green Predictive” rating is attached to each area which determines when the likelihood and impact will both be low on the matrix. Attempting to make all areas “Green” could be a lengthy process and may potentially never be realised because of the nature of the risk.</p> <p>However, there is evidence that Amber risk will be tolerated in that SARC risk CG23 ‘The Council being in breach of the Data Protection Act resulting in enforcement action by the Information Commissioner’s office, including the imposition of financial penalties and adverse publicity.’ is rated attaining AMBER in March 2013. The CMT report that considered this risk states ‘<i>The Council has agreed to a request from the Information Commissioner’s office to undertake a voluntary audit of the Council’s Data Protection compliance. This voluntary audit will take place early in 2013. When carrying out its audit the ICO would expect the risk of a Data Protection breach to feature in corporate and service risk assessments.</i>’ The report then demonstrates risk appetite: ‘With an organisation the size of Flintshire, with several departments routinely processing personal information, there is a need for constant vigilance and the risk will probably never be less than amber.’</p> <p>Of all the risks identified by the council covering SARC, operational, project or partnerships our sample testing identified only one example of risk appetite being applied as noted above.</p>	

OVERVIEW AND ASSESSMENT OF ACTUAL CONTROLS IN PLACE	RECOMMENDATION
<p><b>1.03 Corporate framework for scoring risk</b></p> <p>We assessed whether there is a corporate framework for scoring risk with clear methodology defining impact and likelihood and how to calculate overall risk. The Council approach to scoring risk is covered Within the Risk Management Strategy including the likelihood and impact matrix. A 3x3 matrix is used although these are represented by high, medium and low rather than a multiplication of 1 by 2 or using 3.</p> <p>Where likelihood and impact cross, this determines the risk level. The criteria that had been assigned to the matrix were included in the strategy to promote consistency in risk evaluation across the council. Descriptions are provided for what each assessment would mean and examples are provided in the Appendices for SARC risks on how to assess the risk. An operational risk template is also provided in the Appendices to the strategy.</p> <p>Conclusion</p> <p>There is a corporate framework for scoring risk with clear methodology defining impact and likelihood and how to calculate overall risk.</p>	
<p><b>1.04 Strategic Risks (SARC) - Risk Assessment and Mitigation</b></p> <p>The (Strategic Assessment of Risks and Challenges) SARC is a top down assessment of strategic risk with the key risks being recorded on a standard template. The SARC provides a detailed assessment of the council's strategic risks and challenges together with mitigating action and as such represents a long term statement capturing the organisational challenges where change and improvement is required. The PPP section is responsible maintaining and also improving the SARC in liaison with the CEO, CMT and Directorate managers. This document provides an overview of the strategic risk profile of the Council. At every refresh a summary overview is provided of deletions, creations, mergers and amendments. Each quarter the SARC is completed by each Risk Title owner, this is usually the secondary owner. Each update shows progress against actions. Once updated, the risk section is forwarded to the Risk Manager for review. Each risk title is subject to review, this involves considering progress made against actions in the previous quarter and a challenge of the RAG ratings. If queries are raised / identified then the Risk Manager will initially make contact with the performance leads or secondary owners as these are the members of staff that have the greatest involvement in the ongoing</p>	

OVERVIEW AND ASSESSMENT OF ACTUAL CONTROLS IN PLACE	RECOMMENDATION
<p>maintenance of the risk areas. If any issues cannot be resolved at this point then the Risk Manager can escalate the issue to the Head of the area in question.</p> <p>Monthly meetings are also held with the performance leads, these are attended by scrutiny leads. Risk management and SARC issues may be raised during these meetings. The SARC is formally issued 6 monthly and is made available on the FCC web site.</p> <p>The County through the Local Service Board has set five high level priorities which aimed to demonstrate how the county enabled economic prosperity, health and wellbeing; learning and life skills; living sustainably and safe and supportive communities. The four main directorates within the council had then developed ten council objectives which flowed through into the directorate priorities.</p> <p>Within the Annual performance report the Council priorities had been mapped to all risks and this was verified by a 100% SARC mapping check, therefore, one can conclude that SARC risks are mapped to corporate objectives in some form. However, it is a time consuming task matching all the risks listed against each objective in the annual performance report and agreeing back to the SARC to ensure all SARC risks are covered and no user of the document could be expected to carry this out just to understand what objectives a SARC risk is a barrier to achieving. This is also back to front and does not satisfy in the right way the objective that the SARC is driven by barriers to achieving corporate objectives– it should be carried out through the SARC process i.e. a risk should not be included in SARC unless it is clear its failure to mitigate would represent a barrier to delivery of one or more corporate objectives therefore that corporate objective(s) should be recorded against the SARC risk. This would enhance a user's understanding and reading of the SARC document. Further ambiguity occurs because the SARC has objectives recorded against most risk entries but these differed from the corporate objectives within the Council. Many of the objectives recorded appeared to be operational but the source or nature of the objectives is never defined.</p> <p><b>1.05 Sample testing of SARC risks</b></p> <p>The SARC was subject to review prior to the issuing of the latest version in December 2012. This process has resulted in the deletion of a number of risks that are now obsolete and new risks added. The following risks were reviewed in detail</p> <p><b>1.) CD08 Loss of opportunity to implement the first Housing Renewal Area for the county and to regenerate Shotton and Deeside urban areas</b></p>	<p>Council objectives should be noted against strategic risks within the SARC, rather than in the Annual performance Report. This is necessary to enable users of the SARC document to understand clearly how each SARC risk relates to a corporate objective/priority, and how these corporate risks are being managed or mitigated thereby enabling these corporate objectives/priorities to be met.</p> <p>The current 'objectives' included against each strategic risk in the SARC should be renamed to avoid confusion with corporate or directorate objectives to a user of the document.</p>

OVERVIEW AND ASSESSMENT OF ACTUAL CONTROLS IN PLACE	RECOMMENDATION
<p>The mitigation and progress statements are as follows:</p> <p><i>a) Evaluate current methods of procurement and identify any areas where increased value for money can be obtained e.g. maximum use of both local labour and supply chains, provision for local apprenticeships - Ongoing</i>  <i>b) Continue to seek opportunities for the introduction of private finance in to the scheme</i>  <i>This action is partially completed with the establishment of CESP energy efficiency schemes which lever in a significant amount of private sector funding from the utility companies.</i>  <i>A longer term aspiration is to introduce private finance from lending institutions, however, this relies on using the value of the Council's loan book as security and therefore this unlikely to be achieved in the near future.</i></p> <p>Currently rated a RED risk, which we assume is a combination of a RED external risk (funding issues) and an AMBER internal risk (due to mitigation actions). As a result of the above mitigation statement and progress a Green rating by 2020 is predicted. However, the facts and uncertainty and the lack of specific mitigation actions programmed to change the risk do not support a GREEN rating by 2020.</p> <p><b>2.) CL08 Climate Change &amp; Flood Risk Management</b></p> <p>This risk covers the increased likelihood of flooding due to inability to identify and mitigate against the impacts of climate change nor reduce carbon emissions. Detailed robust mitigation action is listed including progress updates. The current risk is AMBER and GREEN predicted as 'unable to be classified at present'. The external risk is classified as RED and internal as AMBER, and overall risk as AMBER. It is not clear how internal and external risk is weighted to produce an overall risk classification and there is no guidance in the SARC or Risk Management strategy for risk leads to apply.</p> <p>Conclusion - good mitigation actions and detailed progress reported. This risk has been rated as an Amber risk since December 2008. This risk does not include a date for achievement of a Green risk rating and no longer term rating is provided as a target. However, assume this is because there is an external risk which is classified as RED. Overall it is not possible for the actions of Flintshire alone to reduce the overall risk to GREEN and this should be acknowledged in the risk description – the aim should be to reduce the INTERNAL risk to GREEN. Overall the risk would never get to GREEN as Flintshire alone cannot reduce the 'likelihood of flooding due to inability to identify and mitigate against the impacts of climate change nor reduce carbon emissions' and this is one example where the Risk leads should have applied Risk Appetite and acknowledged that AMBER may be the maximum the overall risk could be reduced to.</p> <p><b>3.) CD37 Food waste treatment project - Breakdown of Regional partnership delivering the food waste project.</b></p> <p>This primarily records the risks relating to the procurement of joint waste treatment not being successful and</p>	<p>There should be guidance for officers as to how to weight external and internal risk to calculate overall risk.</p> <p>(See overall recommendation below)</p> <p>Where there is no detailed and programmed mitigation action and progress for a risk a set date for a GREEN target risk rating should not be provided. Generally in the SARC the phrase 'Unable to determine at present' is included in this instances.</p> <p>(See overall recommendation below)</p> <p>Where it is not possible to mitigate a risk to 'Green' this should be identified in the SARC, clearly showing the need to tolerate an 'Amber' level of risk and therefore application of risk appetite.</p> <p>(See overall recommendation below)</p>

OVERVIEW AND ASSESSMENT OF ACTUAL CONTROLS IN PLACE	RECOMMENDATION
<p>the mitigations actions and progress updates relate effectively to this and currently the risk is AMBER rated with GREEN predicted for 2016/17. The outcome of the procurement will be a food waste partnership with Denbighshire and Conwy. NB the summary SARC shows GREEN predictive September 2012 which cannot be correct as the procurement had not been finalised at that date. The detailed risk shows green predictive as at 2016/17, but the summary SARC shows green predictive September 2012. Improved validation of information presented needs to be undertaken.</p>	<p>Improved validation of information presented in the detailed and summary SARC needs to be implemented (See overall recommendation below)</p>
<p><b>4.) CG13 Customer Focus - The delivery of high and consistent levels of customer services</b></p>	
<p>This risk has amber colouring in the detailed SARC after September 2012. The AMBER status of the detailed risk description conflicts with the summary SARC statement of GREEN for this risk and this should be resolved. Mitigation actions and progress statement including outcomes are robust. However, this risk has been classified as GREEN since June 2011, but insignificant mitigation action would have been completed at that time so it not clear why the GREEN risk rating was originally applied. Review of the archived copy of the SARC risk from 2011 evidences the residual risk was classified as GREEN even though most of the mitigation actions were still to be implemented to achieve target risk:</p>	<p>For customer services risk the AMBER status of the detailed risk description conflicts with the summary SARC statement of GREEN for this risk and this should be resolved. (See overall recommendation below)</p>
<p>a.) Improvements to reception areas at County Hall, Mold. - Funding for major improvements to Entrance 3 was not secured. Minor improvements have been undertaken. The first Flintshire connects centre was not established until 2012. b.) Procurement of new telephony system to support improved customer service and flexible working – only recently implemented in 2013 c.) A web usage campaign to increase use of website and reduce face to face and telephone access, and so delivering efficiency gains – no evidence any significant channel shift had not occurred by Sept 2011 and a target of 2013 has been set to make the website the most popular access channel. d) Full implementation of comprehensive Customer Services Strategy – not completed by June 2011 and was then in early stages of implementation in full (the strategy covers much of above including channel shift). Customer Training Programme - Housing as a pilot only had been completed.</p>	<p>Where substantial mitigation actions remains outstanding the current overall risk should not be classified as GREEN risk rating achieved (See overall recommendation below)</p>
<p>Overall it is not clear that risk could be justified as GREEN from June 2011 when the mitigation action proposed covered all aspects of customer services and was implemented a significant time after June 2011 and much still remains to be implemented eg the remaining Connects centres, improvements to reception, material channel shift so that website is most popular access channel.</p>	
<p><b>5.) DATA PROTECTION RISK –</b></p>	
<p>This risk covers the Council being in breach of the Data Protection Act resulting in enforcement action by the Information Commissioner’s office, including the imposition of financial penalties and adverse publicity. The</p>	

OVERVIEW AND ASSESSMENT OF ACTUAL CONTROLS IN PLACE	RECOMMENDATION
<p>mitigation actions are listed as follows with no deadlines for implementation and no progress updates against them in the progress section of the risk:</p> <ol style="list-style-type: none"> <li>1. That service areas regularly processing personal information have included Data Protection breach as a service risk in their service plans.</li> <li>2. That staff processing personal information have received appropriate training.</li> <li>3. That training is given to Members on their Data Protection responsibilities.</li> <li>4. That a register is maintained of all Data Protection complaints.</li> <li>5. That news items are regularly distributed on the Infonet and to Heads of Service as a reminder of the importance of complying with Data Protection.</li> </ol> <p><b>Conclusions</b> Although the mitigation actions are satisfactory and cover both members and officers responsibilities, there is no timeframe provided against any of the actions or any form of progress update in implementing the mitigation steps. Therefore, currently this risk description and mitigation action plan does not support the predictive Amber Rating for March 2013. One example is the mitigation action that 'service areas regularly processing personal information have included Data Protection breach as a service risk in their service plans.' – of the five 2012/13 service plans sampled in this internal audit, only two noted DPA risk – Leisure and Culture, and Children's Services. The service plans for Customer Services, Housing and Streetscene did not identify DPA as a potential risk, even if the actual risk was GREEN as they may have determined that personal information is not processed regularly. However, it would seem likely that Customer Services would process personal information, and Housing services.</p> <p>The SARC and the supporting report to CMT re Data Protection Risk Management 20-03-12 evidences that risk appetite has been a consideration when establishing the risk management for this risk. However, out of all the risks reviewed covering projects, partnerships, service operational risks and SARC risks, only the DPA risk evidences risk appetite consideration so the conclusion is that risk appetite review is not embedded.</p> <p><b>Overall</b> Overall the SARC evidences the identification of strategic risks where the internal risks have been identified through application of the scoring matrix required by the risk management strategy (which has clearly defined definitions for impact and likelihood). However there is an issue with consistently applying risk assessment methodology and with effective mitigations including whether sufficient action has been implemented to justify risk ratings. Risk lead officers are interpreting the guidance in different ways to completing SARC risks so the risk assessment and mitigation is not consistently robust.</p>	<p>Mitigation action plans should always include progress information to underpin current risk ratings. (See overall recommendation below)</p>



OVERVIEW AND ASSESSMENT OF ACTUAL CONTROLS IN PLACE	RECOMMENDATION
<p>Risk Mitigation actions are not specifically separated between existing controls and identified actions to enable the classification of inherent risk and residual risk to be clearly understood. It was generally unclear how the action plans had been developed when these controls had not been clearly identified on the SARC. Identifying actual controls in place to define inherent risk enables a focus on what the Council already has in place prior to developing any sort of action plan to reduce inherent risk to residual risk. Actual controls in place enable management to understand how the causes to the risk are already being managed before identifying any gaps that may need addressing. The current format of the SARC does not enable user of the document to determine this.</p> <p>Review of the SARC generally and detailed review of a sample of 5 risks identified that the current format of the SARC does not:</p> <ul style="list-style-type: none"> <li>- Show which corporate objective the risk is a barrier to achieving</li> <li>- State clearly which is inherent risk, residual risk and target risk</li> <li>- Differentiate clearly between controls which are currently in place that mitigate inherent risk to residual risk, and those controls that need to be implemented to mitigate residual risk to target risk</li> <li>- Correctly show risk appetite – some risks cannot get to GREEN eg Climate</li> <li>- Show clearly how internal and external risk are weighted to give overall risk</li> <li>- Correctly classify a GREEN rating for some risks</li> <li>- Identify what the objectives relating to all SARC sub-risks actually mean – ie are they service, directorate, or risk specific objectives or are they in fact overall mitigation objectives</li> <li>- Clarify whether sub-risks listed under each SARC risk are weighted to provide overall risk, or individually whether some sub-risks are more important than others</li> <li>- Receive enough validation to ensure there are no inconsistencies between the detailed SARC risk ratings and the summary SARC analysis of risks</li> <li>- Always show progress against mitigation actions to support current risk ratings</li> <li>- Evidence that risk appetite is embedded</li> </ul>	<p>The current risk assessment and mitigation template proposed for operational risks in the Risk Management strategy represents good practice and is applied by many councils in assessing strategic and other sources of risk. There are a number of shortcomings with the current format of the SARC as indicated. Overall we recommend the Council at the next SARC refresh converts the entire format into the best practice template provided for operational risks which will easily highlight the gaps we have identified and mandate effective completion of risk assessment, and mitigation information including better evidencing inherent, residual and target risk classifications. In the medium term the council should establish a risk management database linked to the intranet that removes the current time consuming SARC spreadsheet update process which is clearly leading to validation issues. The PP&amp;P section have confirmed a request has been submitted to ICT and this is currently being developed.</p>
<p><b>1.06 Partnerships - Risk Assessment and Mitigation</b></p>	

OVERVIEW AND ASSESSMENT OF ACTUAL CONTROLS IN PLACE	RECOMMENDATION
<p>The partnership coordinator was asked for the corporate register of partnerships and two registers were provided - one for strategic partnerships and one for non-strategic partnerships. There is also a WLGA Regional Collaboration Compendium that identifies Flintshire Partnerships and some of these are not on any of the Strategic and Other partnership internal lists eg Telecare. The non-strategic partnership list is not updated regularly and a previous discussion with PP&amp;P by internal audit in April 2012 identified that the focus of the Partnerships team is solely on Strategic Partnerships and not on all other regional and sub-regional partnerships. Clearly there is a need to develop a definitive list of partnerships as there are currently three different lists – one strategic, one covering all other partnerships which is out of date, and one compiled by WLGA which contains important partnerships that are not listed on the two internal partnership lists. There is no assurance that all partnerships on the internal partnership lists have been captured.</p> <p>PP&amp;P have produced a framework approach for the self assessment of partnerships. Recently risk assessment has also been incorporated into the framework with templates provided with the aim being to embed risk assessment for all strategic partnerships. However, sample testing of five partnerships (HSCWB, CYP, Housing, Families First and Occupational Health) identified that actual risk management has yet to be applied to these significant and strategic partnerships even though some have been in existence for a number of years eg HSCWB partnership. The partnership coordinator has recently set clear action points regarding risk management for strategic partnerships with the aim being for all these partnerships to have applied risk management within the first 6 months of 2013. As at March 10<sup>th</sup> internal audit had received no evidence of formal risk management being applied to the 5 partnerships included in the sample for this audit.</p> <p>This issue has been previously identified and reported as part of a 2010/11 audit and the working paper noted the following <i>'It was noted that a Strategic Partnership Performance 'Mid Year Review Report was submitted to the Executive' in January 2011. This report included a 'Timetable for Implementation of the Strategic Partnership Governance Framework'. This report identifies dates for the implementation of Risk Registers. To ascertain if risk registers were actually in place and operating effectively, FCC representatives for each of the Strategic Partnerships were contacted by e-mail:</i></p> <ul style="list-style-type: none"> <li>- Children &amp; Young people's Partnership;</li> <li>- Community Safety Partnership;</li> <li>- Health, Social Care and Well Being Partnership;</li> <li>- Regeneration Partnership</li> </ul> <p><i>Only one response was obtained, it was found that a risk register is not in place for the Health, Social Care and Well Being Partnership. However, it is noted in the Strategic Partnership Performance Mid Year Review Report was submitted to the</i></p>	<p>Partnership registers should be compiled at Flintshire that completely and accurately captures all significant regional, sub-regional and local partnerships the in which the council participates.</p> <p>Formal risk management as defined by the risk management strategy should be applied to all significant regional, sub-regional and local partnerships where FCC is the lead authority.</p>

OVERVIEW AND ASSESSMENT OF ACTUAL CONTROLS IN PLACE	RECOMMENDATION
<p><i>Executive in January 2011, that a risk register has been in place since July 2010.'</i></p> <p>Clearly the lack of risk management has been identified previously by PP&amp;P and internal audit but still there is no evidence that strategic partnerships have implemented the requirement for formal risk management. In fact in response to the request for evidence of risk management in order to review risk assessment and risk mitigation one of the partnerships sampled submitted a blank risk register as evidence, and another partnership lead emailed a partnership self-assessment as evidence initially. This indicates there is a need for training in risk management for partnership leads</p>	<p>Training in risk management should be provided to current partnership lead officers.</p>
<p><b>1.07 Projects - Risk Assessment and Mitigation</b></p> <p><b>Overview of Project Risk management Framework</b></p> <p><i>ICT services provide the corporate project management system</i></p> <p>Review of the Project management toolkits and guidance identified there is a corporate Project Management System (PMS) in place, and supported by a Project Management Handbook available on the Infonet. Risk Management is adequately built in to the PMA. The completion of a risk log is required as part of the project initiation process and the maintenance of this log is deemed essential for medium and high scale projects. The guidance is based on the Prince 2 model and the consideration and management of risk is built in to the process. NB The risk management approach in the PMS does not follow the corporate approach to risk management as defined in the risk management strategy.</p> <p>Sample testing of 5 projects from the PMS covering HIGH/MEDIUM scale impact projects identified that for the Agile Working and School Modernisation projects there was no project risk log or evidence of risk management included in the project documents. For the Flintshire Connects, Transforming Transportation and P2P projects adequate evidence of risk management including risk assessment and risk mitigation as prescribed by the PMS guidance was identified.</p> <p>Therefore, although there are robust PRINCE 2 standard templates and guidance for risk management in relation to projects it is not being used, or included in the PMS, for all Medium/large scale projects.</p>	<p>There should be a review of the projects in the PMS periodically to challenge instances where it is identified PMS risk management templates are not being used.</p> <p>Robust risk management should be applied to all medium, large scale projects with evidence retained in the PMS</p>

OVERVIEW AND ASSESSMENT OF ACTUAL CONTROLS IN PLACE	RECOMMENDATION
<p><b>1.08 Operational Risk Assessment and Mitigation</b></p> <p>As part of the service planning process service managers are required to identify and monitor operational risks as detailed in the risk management strategy. The revised risk strategy contains a template in Appendix B proposed for the management of operational risks although this has not been applied as yet by services as the strategy was amended in September 2012 so it will apply to the next service planning round. However, the template is only a suggestion to 'supplement local risk registers'.</p> <p><b>Sample testing of service plans to review operational risks identified the following:</b></p> <p><b>Social Services for Children plan</b> – Risk management comprises a one page cursory list of operational risks although safeguarding risks are covered by the Safeguarding Board</p> <p><b>Housing Services Plan</b> – The plan contains no mention of operational risks</p> <p><b>Customer Services Plan</b> – No operational risk assessment included in the service plan.</p> <p><b>Culture and Leisure service plan</b> – risks are identified against service improvement areas, but no formal risk assessment is applied nor mitigation action proposed so there is no evidence that risks are being managed after initial identification</p> <p><b>Streetscene service plan</b> – SARC risks and comprehensive service specific operational risks are identified with mitigating action. Further review of Environment directorate plans identified that generally this Directorate does apply effective operational risk management</p> <p><b>Conclusion</b></p> <p>There is no standard approach to the risk management of operational risks. Environment Directorate Service Plans did follow a general format and the identification of operational risks and their management were generally included.</p> <p>A detailed review of the Service Plans above showed a varied consideration of risk ranging from a well prepared and considered risk management plan for Streetscene to a cursory coverage of risk in Children's Services and Culture/Leisure, or no risk information at all for Housing and Customer Services. There is a lack of appreciation of the importance of addressing operational risks - lack of risk management can have a detrimental effect on the achievement of service plan objectives. Also of note is that the Data Protection Act inspection programmed for 2013 requires services to evidence that Data Protection issues have been included in operational risk assessments.</p>	<p>The operational risk assessment template included in Appendix B of the Risk Management Strategy is a best practice template and service managers should be required to use this approach to manage risks and evidence this by including the completed template in the service plan</p> <p>PP&amp;P should review draft service plans and challenge those where risk management information is either inadequate or non-existent</p> <p>All service managers should be asked to evidence that Data Protection issues have been included in operational risk assessments</p>