AGENDA ITEM 11

FALKIRK COUNCIL

Subject: **CRM POLICY AND FRAMEWORK REVIEW**
Meeting: **AUDIT COMMITTEE**
Date: **20th April 2015**
Author: **DIRECTOR OF DEVELOPMENT SERVICES**

1. INTRODUCTION

1.1 The current CRM Policy and Framework was approved in November 2013, and it was agreed at this time that an annual review would be undertaken.

1.2 An updated CRM Policy and Framework is attached, and key amendments are highlighted below:-

a) Inserted reference to 6-Monthly Service Risk Update to CRMG;
b) Maintenance of risks schedules at Corporate, Service and Project / Partnership levels;
c) An updated CRM Risk Reporting Framework is provided in Appendix 1; and
d) The Corporate Working Groups Chart has been inserted, in Appendix 2.

2. RECOMMENDATIONS

2.1 Members are invited to:

2.1.1 Note the contents of this report.

……
Director of Development Services

Date: 8th April, 2015

Falkirk Council

CORPORATE RISK MANAGEMENT

CRM POLICY & FRAMEWORK

NOVEMBER 2014

CONTENTS

DOCUMENT HISTORY

Document Title:	CRM Policy & Framework	Lead Reviewer:	CRMG Members
Owner:	Director of Development Services	Superseded Version:	2 Sept 2014
Version No:	V21, Nov 2014	Next Review Date:	Q4, 2015

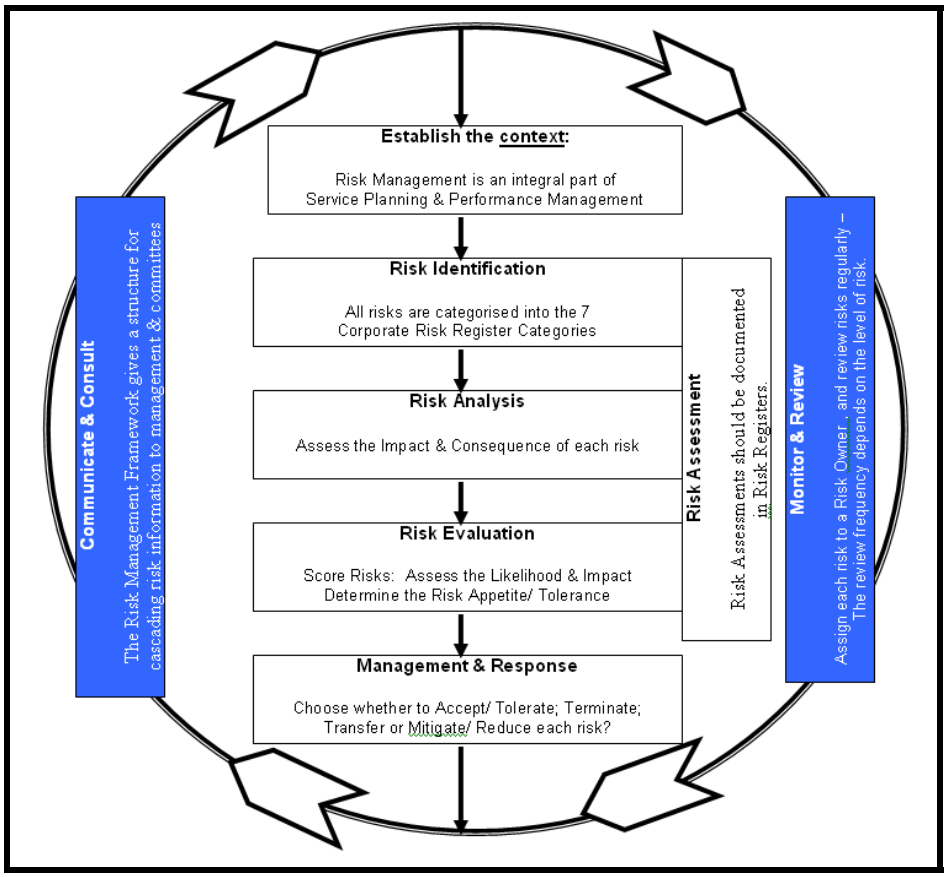
1. POLICY STATEMENT – THE COUNCIL'S APPROACH TO RISK MANAGEMENT

1.1 The purpose of this Risk Management Policy is to set out the framework for embedding risk management across Falkirk Council.

1.2 The Council encourages decision makers to be 'risk aware' rather than 'risk averse'. This includes encouraging innovation and recognising 'opportunity related risk', provided that the risk is assessed and justified in the context of the anticipated benefits for the Council.

1.3 The Council aims to embed a culture whereby risk management is recognised as a continuous process, demanding awareness and action from employees at every level, to reduce the possibility and impact of injury and loss. Risk management should be seen as an enabler to achieving the Council's objectives.

1.4 Risk management requires the identification, assessment, management, monitoring and reporting of risk by the Council, per Table 1 below, in order to effectively manage risks to service, employees, finances, operations, assets and reputation.



1.5 Each stage is outlined within the 'Step by step guide to managing risk', on the intranet.

1.6 Risk affects every activity to a greater or lesser degree and failure to acknowledge this can lead to serious consequences. The Council's Corporate Risk Register sets out risk under the following 7 categories:

- Failures in proper **financial** management
- Failures in proper **information** management (availability, integrity and security)
- Failures in **human resources** management (e.g. recruitment, retention, safety)
- Failure to properly manage **assets**
- Failure to properly recognise, plan for, and manage significant **change**, both internal and external
- Failures in **governance**, leadership, accountability or decision making
- Failures in **partnerships** or contracts with external bodies

1.7 The Corporate Risk Register (CRR), available on the Council's intranet, gives a general description of each risk category. Also, the Corporate Risk Schedule (CRS), circulated to CRMG Members, provides more detailed information on each risk, including the risk evaluation (scoring), controls, actions and ownership for each.

1.8 Risk management is a key component of Corporate governance and resilience, and, therefore, should be embedded within the Council's management at every level, including Community, Corporate and Service Planning and Performance Management.

1.9 If the Council is to manage risk effectively, it needs to demonstrate that risks are managed in a systematic and structured manner and that risks are subject to regular monitoring & challenge.

2. RESPONSIBILITIES

2.1 Elected Members and Officers

a) Elected Members

The CIPFA/ SOLACE Guidance – available on the intranet - and in particular Principle 4, makes explicit the elected member's decision-making role and the need to ensure that risk information contributes to the decision-making process. To support this, an analysis of relevant risks should be included within all committee papers, where appropriate.

CIPFA Guidance Note 10 (Risk Management Guidance for Elected/ Board Members) also advises that Elected / Board Members should get involved in the identification of high level, strategic risks, and outlines the following responsibilities for them:-

- To **gain** a broad understanding of risk management and its benefits;
- To **require** officials to develop and implement an effective framework for risk Management;
- To **challenge** officials to ensure risks are considered and recorded in reports;
- To **require** that risk is formally considered at the start of major projects and re-evaluated throughout the life of the project;
- To **require** officials to report significant risks on a regular basis.

b) Chief Executive

The Chief Executive has overall accountability for the Council's Corporate Risk Management Policy & Framework, and ensuring that effective arrangements are in place to manage risks.

c) Director of Development Services

The Director has delegated responsibility for overseeing corporate risk management arrangements; the effectiveness of CRMG; and for bringing risk issues to CMT. The Director will provide an Annual Report to CMT and the Audit Committee, including the risk management work-plan and self-assessment.

d) Internal Audit Manager

The IA Manager is responsible for developing and completing an Annual Risk-Based Internal Audit Plan. The aim is to provide assurance on the Council's arrangements for risk management, governance and controls.

e) Corporate Risk Manager

The CR Manager will provide training, advice and support across the Council on the management of Corporate, Service, projects and/or partnership risks. He/she will implement & maintain a process for review, maintenance and reporting of corporate risks. Key outputs will be the CRR, CRS and Annual CRM Work-Plan & Performance Review.

f) Directors and Chief Officers

Directors & Chief Officers are accountable for embedding risk management within their Service, and monitoring its effectiveness. They should ensure that controls and review mechanisms are fit for purpose and are operating effectively; and that the risks they own on the CRS are kept up to date and that risk information is shared appropriately, including:-

i) **Communications with SUMs:**

Risk management should be a standing agenda item on all DMT meetings; risk training needs should be assessed through the APDS process; and SUMs should be involved in risk schedules.

ii) **Communications with CRMG, CMT and the Executive**

Each service should, as a minimum, provide a 6-monthly Service Risk Update to CRMG, including updates on Risk Schedules, Business Continuity, Corporate Working Groups and Lessons Learnt from Incidents. A template has been agreed separately by CRMG.

iii) **Communications with the Scrutiny Panel**

Each service should include an extract of the CRS in their Scrutiny Panel Reports and Service Plans, and this should be reviewed as part of planning & performance reviews.

g) Service Unit Managers and Project / Partnership/ Contract Leads

Managers are responsible for ensuring that risk awareness and training is delivered to employees, and for maintaining Risk Schedules relevant to their areas of responsibility (e.g. Divisional, Team, Partnership and/or Project Risk Schedules). Managers should ensure that all current and emerging risks are identified and evaluated; and that proportionate controls, review mechanisms and performance indicators are implemented. Risk management should be a standing agenda item on all Team, Project and Partnership meetings and cascaded upwards, as appropriate, including reports outlined above.

h) Employees

Employees should be aware of the risks that relate to their role, and how to protect themselves and others e.g. health and safety guidance. Employees should be involved in the risk assessment process for their roles and should be encouraged openly report any concerns.

2.2 Committees and Officer-Led Groups

a) Audit Committee

The Audit Committee's Terms of Reference are defined as:-

- To review and seek assurance on the framework of risk management, governance and control.
- To review and seek assurance on the system of internal financial control.
- To review the Authority's Assurance Statements to ensure they properly reflect the risk environment,
- To produce an annual report on the above to support these statements.
- To take account of the implications of publications detailing best practice for audit, risk management, governance, and control.
- To take account of recommendations contained in the relevant reports / minutes of:
  - the External Auditor;
  - the Scottish Parliament; and
  - other external scrutiny agencies.

b) Corporate Management Team

- Ensure that the CRM Policy and Framework is reviewed at least every two years by the Director of Development Services, to ensure that it remains fit for purpose and reflects corporate objectives;
- Embedding a risk aware culture, proactively supporting and encouraging best practice;
- Provide appropriate risk information to Members to support decisions;
- Risk Appetite: Ensure there is good awareness of the Council's risk profile and appetite, and encourage proportionate risk taking and innovation by Services;
- Review the CRR and CRS, taking account of both current and emerging risks.

c) Corporate Risk Management Group (CRMG)

- Monitor the implementation of the CRM Policy and Framework, Annual Work-Plan & KPIs;
- Approve reports to CMT and Audit Committee on the effectiveness of the risk framework;
- Ensure that CRMG members attend and contribute to the activities of CRMG, including the submission of 6-monthly Service Risk Updates and progressing agreed actions;
- Provide a knowledge sharing platform corporately, to inform strategy and guidance;
- Ensure that Risk Schedules, Action Plans and Performance Indicators are regularly reviewed, and that the CRS and CRR reflect e.g. Service and Project Risk Schedules.

d) All Working Groups (see Appendix 2)

- Develop and maintain a risk schedule (or extract from the Corporate Risk Schedule) to support the group's aims and objectives;
- Facilitate the sharing of best practice and lessons learnt;
- Implement proportionate controls and performance indicators to manage risk; and
- Ensure that risks are communicated to CMT and CRMG on a regular basis.

3. CORPORATE RISK REGISTER AND RISK SCHEDULES

3.1 Corporate Risk Register

The CRR will be an over-arching document, maintained by CRMG, which identifies risks, impacts, controls and review mechanisms for each of the 7 Risk Categories.

3.2 Risk Schedules

Risk Schedules are an extension of the CRR, but also provide more specific information on each risk e.g. a risk statement and evaluation of the impact, probability and ownership for each risk.

The risk schedule information is provided by the service(s) and/or Chief Officers who lead on specific risks. The Risk Assessment Template provided in Appendix 3 gives a pro-forma that may be useful for making changes to the risk and/or to assist during risk assessment workshops.

3.2 Risk Schedule Types

Using a consistent template for Risk Schedules enables consistent reporting, clear linkages and the ability to drill up / drill down as necessary to provide reports for different audiences. This is similar to the 'golden thread' method applied to planning and performance reporting.

a) Corporate Risk Schedules (CRS):

- Risks rated as High and Very High (or medium, but affecting 2 or more Services);
- These have the potential to impact on the Corporate Plan or SOA; and
- These will be reported to CRMG, CMT, Scrutiny Panel and others as appropriate.

b) Service, Project and Partnership Risks (SRS/PRS):

- Risks rated as Low (or Medium, but affecting only one Service);
- These have the potential to impact on a Service, Project or Partnership Plan;
- Project risks are threats (positive or negative) to the delivery schedule, cost or anticipated benefits that the project will deliver; and
- These should be routinely reported to Service DMTs and Project / Partnership Boards, and corporately through e.g. Project / Partnership Highlight Reports.

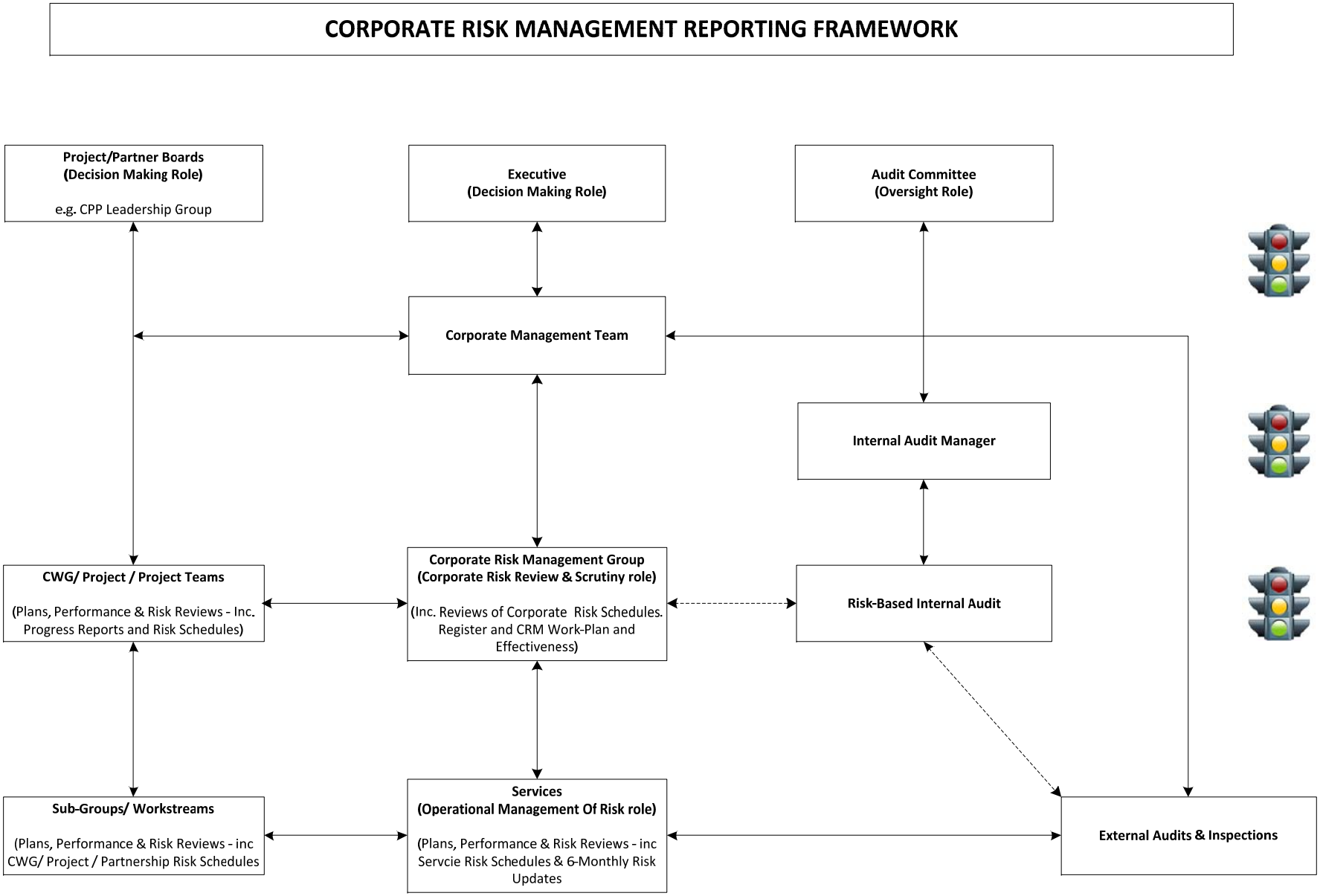
3.3 Linkages Risk Schedules to Planning & Performance Information

Risks are recorded on Covalent and risks should be linked / cross-referred to actions and PIs. This approach ensures that there are measurable actions and PIs associated with each risk; minimises possible duplication and inconsistencies; and enables integrated planning, performance and risk reports to be produced for various audiences, including CMT, CRMG, Scrutiny Panel and Project / Partnership Boards.

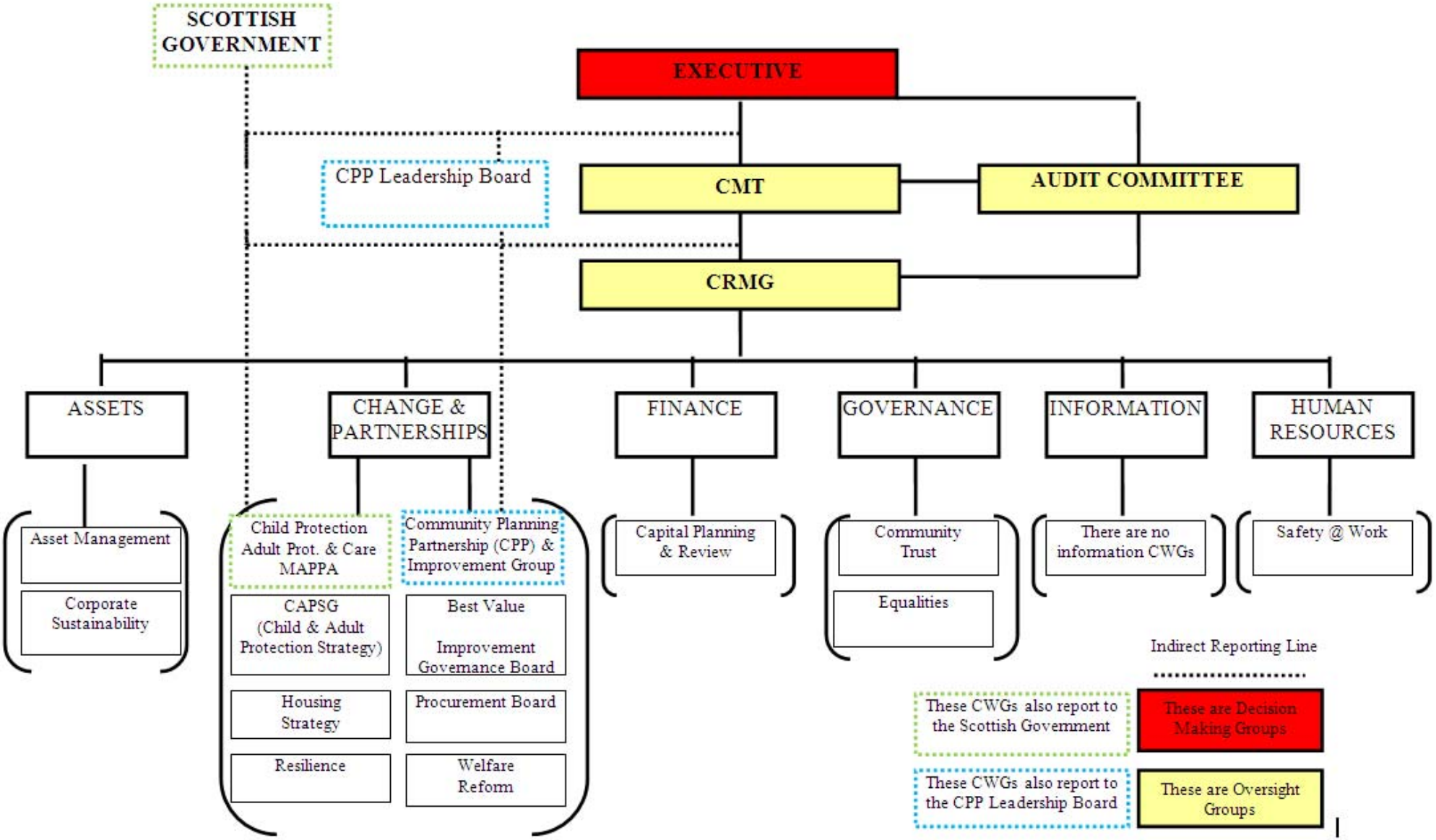
3.4 Risk Assessment Guidance and Templates

Appendix 3: Risk Assessment / Schedule Template;
Appendix 4: Risk Appetite and Prioritisation Matrix; and
Appendix 5: Guidance on scoring impacts.

Appendix 1: CRM RISK REPORTING FRAMEWORK



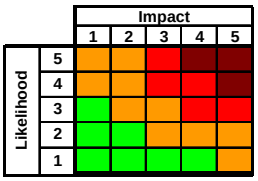
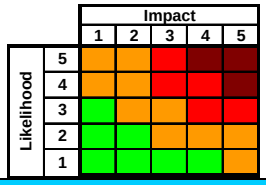
Appendix 2: CORPORATE WORKING GROUPS CHART



Appendix 3: RISK ASSESSMENT / REGISTER TEMPLATE

Risk Identification			
Date Identified		**Identified By**	e.g. CMT, SMT, Project Board?
Risk Type / Category	i.e. Assets, Change, Finance, Governance, HR, Information or Partnerships		
Risk Schedule Type	i.e. does it impact on Corporate, Service and/or Project Plans?		
Risk Title	i.e. provide a heading / identifier - not a description – of the risk		
Risk Statement Per Corporate Risk Schedule	i.e. provide a short a summary of the risk, impact and consequences.		
Impact	e.g. financial, legal, people, reputation, service / project delivery.		
Consequence	e.g. financial loss, prosecution/ sanction, good / bad PR or media interest, good / bad audits.		

Risk Evaluation (Likelihood x Impact) (see risk scoring matrix and guidance)

Current Risk Rating (after controls) (i.e. realistic likelihood & impact given current controls)		**Target Risk Rating (after actions)** (i.e. realistic likelihood & impact after additional actions)	
Risk Matrix  	Likelihood and Impact Scores Risk Level	Risk Matrix  	Likelihood and Impact Scores Risk Level Target Date (Optional):

Control & Review Mechanisms

Controls	**Review Mechanisms**
i.e. what arrangements are currently in place to mitigate the likelihood and / or severity of the risk? e.g. policy, guidance, training, contract conditions, insurance etc.	e.g. monitoring / oversight by specific groups and committees, or inspections / audits etc.

Associated Actions (i.e. cross-reference to items on the Service Performance Plan or Project Plans etc, on Covalent software)

Ref. / Description	Owner	Date Identified	Status	Review Date	Target Date

Associated Performance Indicators (i.e. cross-reference to items on the Service Performance Plan or Project Plans etc.)

Ref. / Description	Owner	Date Identified	Status	Review Date	Target

Risk Impacts & Leads

Lead Service(s) (or Project / Partner Work-stream)	**Lead Officer(s)** (i.e. Job Title)

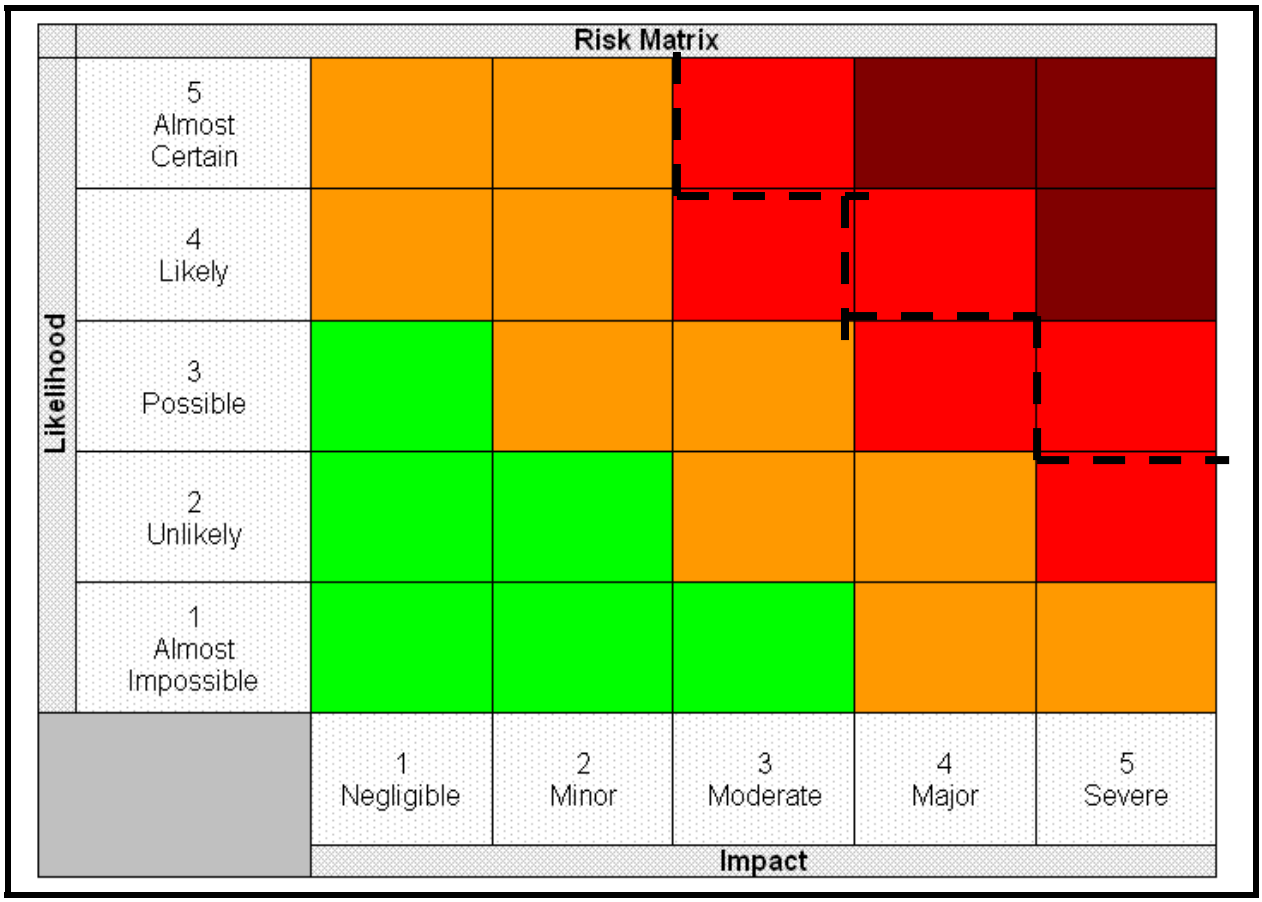
Other(s) Impacted (only complete this section if relevant)

Chief Executive		1		FC (default)		1	
CEO-FIN		2		Fire		2	
CEO-GOV		3		Police		3	
CNS		4		NHS FV		4	
DVS		5		Voluntary (CVS)		5	
EDS		6		Business (SE)		6	
SWS		7		Skills (SDS)		7	
		8		Training (FVCollege)		8	
FCT		9		Transport (SEStran)		9	
HSCP		10				10	
CPP		Other		Other		Other	

Additional Notes

Note Date	(only complete this section if relevant) e.g. Recent Changes made, date added to Covalent software, Covalent reference number assigned.

Appendix 4: RISK APPETITE AND PRIORITISATION MATRIX



Risk Rating	Action to be taken
Very High Risks (Priority 1) **High Risks (Priority 2)**	Risks that are above the Council's (or Project/ Partnership Boards) risk appetite. Senior managers must be made aware of the risk and robust action plans are to be developed and uploaded to Covalent to manage the risk. Risks are required to be included in reports to e.g. CMT, Audit Committee, and Project/ Partnership Boards.
Medium Risk (Priority 3)	Risks that are within Council's (or Project/ Partnership Boards) risk appetite, but could progress above the risk appetite without further actions. Effective monitoring procedures are to be put in place and professional judgement calls are to be made on the requirement of additional actions. Risks are required to be included in e.g. 6-Monthly Service Risk Updates to CRMG, and performance updates to the Scrutiny Panel.
Low Risk (Priority 4)	Risks that are well within the Council's risk appetite and therefore poses no real threat of occurrence or impact. Risk should be managed by existing processes and procedure. There is no requirement to include these risks in reports to e.g. CMT and CRMG. However, they may be included in e.g. Project / Partner Work-Stream Reports.

- - -	'Risk Appetite' Threshold. Any risks above this threshold should have additional actions, within Service Plans, to help reduce the level of risk to a tolerable level.

Appendix 5: GUIDANCE ON SCORING IMPACTS

CONSEQUENCE & IMPACT DEFINITIONS FOR EACH RISK CATEGORY

These take account of Imapct on Reputation/ Finances/ Services / People & Regulatory Compliance

		1	2	3	4	5
Risk Category	**Risk Description**	**Insignificant**	**Minor**	**Moderate**	**Major**	**Extreme**
Financial	Failures in proper financial management	Negligible loss (£<1k)	Minor loss (£1k - £10k) Minor impact on service/ security / reputation	Significant loss (£10k - £100k) Moderate Service / Reputation impact	Major loss (£100k-£1m) Significant impact on service and/or reputation	Severe loss (£>1m) Severe impact on customer, services and reputation
Information	Interruption/ failure in information (availability, integrity and security	Loss of non key systems or data. Service/ Reputation: Negligible impact on service / security / reputation. BCP plans not required.	Loss of key system or data for a limited period of time. Service/ Reputation: Minor impact on service/ security / reputation	Loss of key system or data for a limited period of time. Service/ Reputation: Moderate impact on service/ reputation security. Within tolerability of BCP plans.	Major impact - sustained loss of key system/ data, resulting in major Reputation/ Service: Significant impact. BCP plans implemented	Major impact (permanent loss of data/ facility) resulting in failure to meet Severe impact on customer, services and reputation
HR	Failures in HR management (including recruitment, retention, absence, competence and safety)	People: Affects a small no. of staff. Service: No disruption to service. Reputation: No adverse media.	People: Affects up to 5% of staff. Service: Minor impact on services - issues can be easily resolved. Reputation: Possible adverse local media attention.	People: Affects 5-25% of staff. Service: Ongoing problems, resulting in late delivery /moderate error in service due to lack of/ ineffective staff. Reputation: May affect our standing with a customer/ citizen group. It may also damage relations with consumer & trade bodies etc. Adverse local press reports.	People: Affects 25-50% or more staff. Service: Uncertainty over delivery of service or major error due to ineffective training. Reputation: Results in increased claims/ complaints. It may also damage relations with consumer & trade bodies etc. Adverse reports in national media.	People: Affects 50% or more staff. Service: Non delivery of service; loss of key staff; critical error due to insufficient training; multiple claims or single major claim. Reputation: Concerted, widespread or recurrent critical media coverage of the Council for a specific event.
Assets	Failure to properly manage assets, resulting in damage, loss, theft; and inefficiency by not maximising lifespan	Negligible loss (£<1k)	Minor loss (£1k - £10k) Minor impact on service/ security / reputation	Significant loss (£10k - £100k) Moderate Service / Reputation impact	Major loss (£100k-£1m) Significant impact on service and/or reputation	Severe loss (£>1m) Severe impact on customer, services and reputation
Change	Failure to recognise, plan for, and manage significant change, both internally and externally.	Barely noticeable in scope / quality / schedule of objectives. Negligible impact on reputation.	Minor reduction in scope/ quality/ schedule of objectives. Possible adverse local media attention.	Reduction in scope or quality, project objectives or schedule. Some missed opportunities and potential for bad PR.	Significant reduction in ability to meet change objectives. Significant missed opportunity(s) and likelihood of bad PR.	Inability to meet change objectives. Significant financial loss/ missed opportunity; and/or reputation severly damaged.
Governance	Failures in governance, leadership, accountability or decision making.	Barely noticeable impact on reputation / compliance / service delivery. Unlikely to damage relations with a legislative or regulatory body.	Minor impact on reputation / compliance / service delivery. Possible adverse local media attention.	Significant impact on reputation / compliance / service delivery. It may also damage relations with a legislative or regulatory body.	Major impact on reputation / compliance / service delivery The event may affect our standing with a legislative or regulatory body.	High likelihood or actual formal censure by a legislative or regulatory body. Severe impact on reputation / compliance / service delivery.
Partnerships	Failures in partnerships or contracts with external bodies.	Deteriorating performance of a non-critical 3rd party supplier or partner. Negligible impact on service or reputation	Partial Failure of a non-critical 3rd party supplier or partner Unlikely to impact on customer, service, or reputation	Partial Failure of a major 3rd party supplier or partner. Possible impact on customers and adverse local media	Significant Failure of a major 3rd party supplier or partner Significant impact on service, customers and reputation	Total Failure of a major supplier or partner Severe impact on customer, services and reputation