Governance, Risk and Best Value Committee

10.00am, Tuesday 3 November 2020

Operational Risk Management Framework

Item number	
Executive/routine	**Executive**
Wards	
Council Commitments	

1. Recommendations

It is recommended that the Committee:

1.1 approves the proposals set out in this paper for improving the Council's operational risk management framework on a phased basis across the next three years, enabling more effective alignment with the 'three lines of defence' model and implementing good practice.

1.2 notes the response from the Chief Executive to the actions agreed at the August 2020 meeting of the Committee in relation to the Risk Management internal audit report.

Stephen S. Moir

Executive Director of Resources

Contact: Nick Smith, Head of Legal and Risk and Council Monitoring Officer

Legal and Risk Division, Resources Directorate

E-mail: nick.smith@edinburgh.gov.uk | Tel: 0131 529 4377

Report

Operational Risk Management Framework

2. Executive Summary

2.1 The purpose of this paper is to recommend a refresh of the Council's current operational risk management arrangements over the next three years in response to the Council's changing risk profile, ensuring that is more effectively aligned with the 'three lines of defence' model and good practice. The proposals have been discussed with external audit; professional risk management consultants; and risk managers in other public sector organisations to validate the proposed design, and subsequently with first line operational managers, Heads of Service, Executive Directors and the Chief Executive.

2.2 To ensure the ongoing effectiveness of the Council's risk management framework, it will be important for Executive Directors and Heads of Service to ensure that their first line divisional and risk managers and coordinators have sufficient capacity together with the relevant skills and experience to support the proposed changes.

2.3 An independent Risk Management audit has recently been completed by Scott Moncrieff (now Azets) to support the 2019/20 Internal Audit annual opinion, and was scrutinised by the Committee at their meeting in August 2020. The proposals outlined in this paper should also address the outcomes from this audit.

3. Background

Risk Management and the Three Lines of Defence

3.1 The Three Lines of Defence model is widely used to help organisations to clearly define and delineate the roles and responsibilities between their first line service delivery and operational teams (the doers), second line governance and support teams (the helpers), and also independent third line assurance provided by Internal Audit (the checkers). This model can be applied to support effective risk management within the Council.

The Council's Risk Management Journey

3.2 Previously, the second line corporate risk management team assumed responsibility for coordinating and chairing directorate and first line corporate

leadership team risk and assurance committees; and coordinating maintenance of directorate and corporate leadership team risk registers.

3.3 The Pentana risk management system was gradually introduced across the Council from July 2018 to support electronic maintenance and consolidation of risk registers, with a number of users and services across the Council currently using the system.

3.4 In January 2020, the Executive Director of Resources approved that ongoing responsibility for risk management and management of the corporate risk team should be transferred to the Council's Chief Internal Auditor (CIA) with effect from 1 April 2020, reporting through the Head of Legal and Risk to the Executive Director of Resources. This enabled the deletion of the vacant post of Chief Risk Officer allowing the funding for this post to be removed to contribute to the Council's overall savings targets. This has, however, restricted the capacity of the second line Risk Management team and, following discussions with the Chief Executive and at CLT in late 2019 it has been recognised and agreed that risk management and assurance responsibility should sit within the first line, i.e. service managers/teams, rather than with the second line risk management team.

3.5 This proposed reporting structure is permitted by Public Sector Internal Audit Standards (PSIAS) but will require implementation of clear lines of delineation between the IA and risk management teams to ensure that IA independence is effectively maintained.

3.6 Any future audits of corporate risk management (usually completed once every three years) will continue to be performed by an external third party assurance provider to ensure that the CIA's independence is maintained in line with PSIAS requirements.

3.7 In September 2020, the Policy and Sustainability Committee approved the Council's refreshed risk management policy and risk appetite statement. These documents outline the roles and responsibilities of Council employees to ensure the effective ongoing identification and management of risks, and states the amount of risk the Council, or a part of it, is willing to accept in relation to service delivery; infrastructure; compliance and financial risks.

3.8 Risk appetite is defined as 'the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives', whilst target risk is defined as 'the maximum level of risk that an organisation is prepared to accept in pursuit of a specific business objective'.

3.9 Assurance mapping results in a visual representation (or mapping) of assurance activities performed by each of the three lines of defence and external assurance providers across an organisation, detailing how they provide assurance on the ongoing management of the organisation's risks, and in particular the most significant risks.

3.10 A strong and effective risk management and assurance framework will improve the accuracy and insightfulness of the Council's assurance statements and should, over time, reduce the amount of time spent by teams on internal audit activities.

Governance, Risk and Best Value Committee (GRBV) Meeting Action – August 2020

3.11 Following review of the 2019/20 Internal Audit annual opinion and the Scott Moncrieff Risk Management internal audit outcomes at their August 2020 meeting, the Committee requested inclusion of a response in this report that confirms how the Council plans to respond to the risk highlighted in the report concerning the matter of independent challenge for key operational and strategic decisions taken by the Corporate Leadership Team.

4. Main report

Current Risk Management Operational Processes

4.1 The risk management audit recently performed by Scott Moncrieff has concluded that, whilst the Council's risk management policy and risk appetite statement are fit for purpose, further work is required to ensure that the operational risk management processes and procedures are defined and consistently and effectively applied in practice by and across service areas.

4.2 A review of the processes applied to identify; assess; record; and consolidate risks across the Council was performed by Risk Management in June 2020, and confirmed that there was no consistent approach applied. Specifically:

4.2.1 not all risk registers inspected were complete and up to date;

4.2.2 there was no clearly established and consistent flow of thematic risks identified by specialist working groups (for example in relation to information governance, health and safety, Brexit or serious and organised crime) into divisional; directorate; and CLT risk registers;

4.2.3 there was limited inclusion of risks highlighted by internal and external assurance providers in divisional; directorate; and CLT risk registers;

4.2.4 whilst the risks associated with major projects were included in reports provided to the Change Board, the associated risks are not consistently recorded in divisional; directorate; and CLT risk registers;

4.2.5 there is currently no clearly defined process supporting the consolidation of divisional risks into risks for inclusion in directorate risk registers, and accordingly this impacts the accuracy of the consolidation of directorate risks into the CLT risk register; and

4.2.6 the full population of Council risks were not consistently reported through the CLT risk committee and included in the Corporate risk register, but were instead reviewed by other governance forums such as the Brexit Resilience Group and the Change Board.

Proposed changes to the Council's risk management framework

4.3 It is recommended that the Council's operational risk management methodology and processes are further refined over a three year period to support more effective identification; assessment; recording; and management of the Council's risks, and to align more closely with the three lines of defence model. This will involve:

Year one – 2020/21

4.3.1 Implementing a revised operational risk management approach to ensure that all relevant strategic; operational; and thematic risks flow effectively and consistently through relevant risk registers and into the CLT risk register.

4.3.2 Revising the Council's existing risk governance structures to ensure that the CLT Risk and Assurance Committee, and the Governance, Risk, and Best Value Committee are the principal management and executive committees that review and scrutinise risk across the Council.

4.3.3 Implementing a refreshed thematic risk hierarchy that supports assessment of the Council's most significant original (inherent) and current (residual) risks based on assessment and consolidation of lower level sub-risks across directorates and divisions. This process will combine use of the established risk heat map to determine the significance of lower level sub-risks with a simple scoring methodology then applied to consolidate them and assess their significance across the Council.

4.3.4 This risk hierarchy and consolidation process has already been developed to support identification of Adaptation and Renewal programme risks and is currently being further developed to support divisional and directorate risk management processes. Further information on the Adaptation and Renewal Programme risk management approach is included at Appendix 2.

4.3.5 Agreement on revised risk management roles and responsibilities in line with the three lines of defence models for relevant first; second; and third line teams across the Council (refer Appendix 1: slide 6). It is crucial that each director understands and agrees to what will be required of their teams in this regard.

4.3.6 Delivery of ongoing risk management training for first line senior managers; heads of divisions; and directors (where required); and first line risk managers, with learning and development to be designed and delivered by Corporate Risk Management.

4.3.7 Corporate Risk Management has already established a first line 'risk management forum' comprising representatives from directorates to facilitate discussions in relation to new and emerging risks identified from ongoing horizon scanning; current challenges; and sharing best practice. The membership of this group needs to be considered and refined to ensure appropriate representation of first line colleagues.

Year 2 – 2021/22

4.3.8 Full implementation of the Three Lines of Defence model across first line divisional and directorate teams and the second line Corporate Risk Management Team.

4.3.9 Introduction of sample based assurance reviews performed by Corporate Risk Management Team to confirm the ongoing completeness and accuracy of risk flows and risk assessments through divisions and directorates and into the CLT risk register, with feedback and outcomes shared at Directorate and CLT risk and assurance committees.

4.3.10 Further embedding the Council's risk appetite by adopting the assessing of target risk as a proxy for setting risk appetite at a more granular level; discussing and assessing target risk at divisional, directorate and CLT risk and assurance committees; and recording target risks (where possible) in risk registers. It is proposed that this approach is piloted through the Adaptation and Renewal programme in 20/21, with lessons learned incorporated into the approach to be applied across Council divisions; directorates; and CLT. Identifying target risk levels for the most significant risks and seeking to ensure that any risk remains within that target risk level will assist the Council to achieve its objectives. Where current levels of downside risk exceed the target risk, action can be taken to establish appropriate controls to ensure that the risks are effectively managed to be within the target risk (in effect risk appetite) levels

4.3.11 Ongoing consideration of possible alternative risk management systems, recognising the limitations associated with the Pentana risk management system and the need to rationalise the number of systems currently used across the Council. Anecdotal evidence indicates that other authorities are using a variety of risk reporting tools and software, and it appears that there is no one system that is better than any other.

Year 3 – 2022/23

4.3.12 It was noted at the December 2019 Governance, Risk and Best Value Committee meeting that the CLT had agreed to implement a Council wide accountability and assurance framework, in response to a specific Chartered Institute of Public Finance and Accountancy (CIPFA) recommendation, which confirms the range and quality of internal and external assurance provided across the Council by 31 March 2022. It is now proposed that the assurance mapping exercise required to support the design and implementation of the framework is completed by Corporate Risk Management in financial year 2022/23. This timeframe extension reflects the impacts of Covid-19 on the Council and provides sufficient time to fully and effectively embed the refreshed operational risk management arrangements proposed above.

4.3.13 Implementation of an alternative risk management system where this is considered necessary.

Staffing impact

4.4 Implementation of these changes will enable the second line Corporate Risk Management Team of two Principal Risk Advisers managed by the Chief Internal Auditor as the Council's Senior Manager for Audit and Risk, to change their operating model to align more effectively with the second line risk management responsibilities detailed above.

4.5 The Chief Executive is presently examining options for a review of the Council's Chief Officer and senior management structure. He is also reviewing survey responses received from other councils which indicate that there are a number of potential risk, governance, and assurance models in operation. This review will consider the most appropriate structure to support the first line risk management responsibilities as outlined at 4.3.5 above and detailed in Appendix 1. These revised structures will be co-ordinated through the Adaptation and Renewal programme.

Response to the GRBV August 2020 Committee Meeting Action

4.6 It is proposed that the Council's approach to the issues identified in the Risk Management audit concerning the matter of independent challenge for key operational and strategic decisions taken by the Corporate Leadership Team (CLT) will be resolved through the review of the Council's Chief Officer and senior management structure, which will consider the operation of CLT; good governance; and assurance.

5. Next Steps

5.1 Implementation of approved recommendations across the Council with support from the corporate risk management team across the next three financial years.

6. Financial impact

6.1 It is understood that there will be no new funding available for any replacement risk management system. Any new system will be looked at in this context at the relevant time.

7. Stakeholder/Community Impact

7.1 Implementation of these recommendations should further enhance the Council's governance, risk management and control frameworks, with an indirect positive impact on services delivered to citizens, stakeholders, and communities.

8. Background reading/external references

8.1 October 2020 Enterprise Risk Management Policy – item 7.11

8.2 October 2020 Risk Appetite Statement – item 7.12

8.3 The Role of the Head of Internal Audit and Leading Internal Audit in the Public Sector – item 13

9. Appendices

Appendix 1 – Council Risk Flows and Governance.

Appendix 2 – Adaptation and Renewal Proposed Risk Management Framework

Appendix 1

Operational Risk Management Framework
Council risk flows and governance

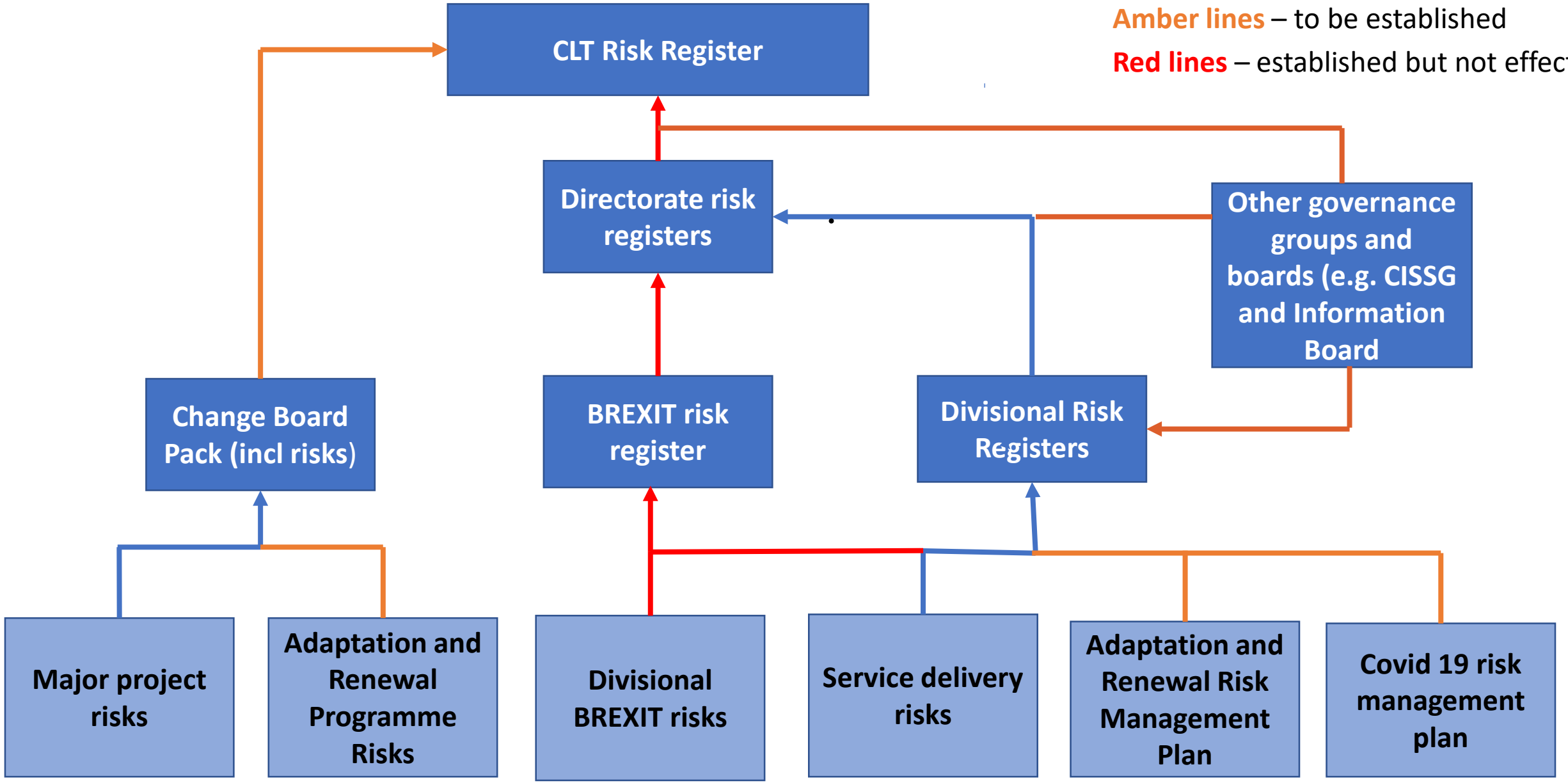
Flow of current Council risks as at June 2020

Key:

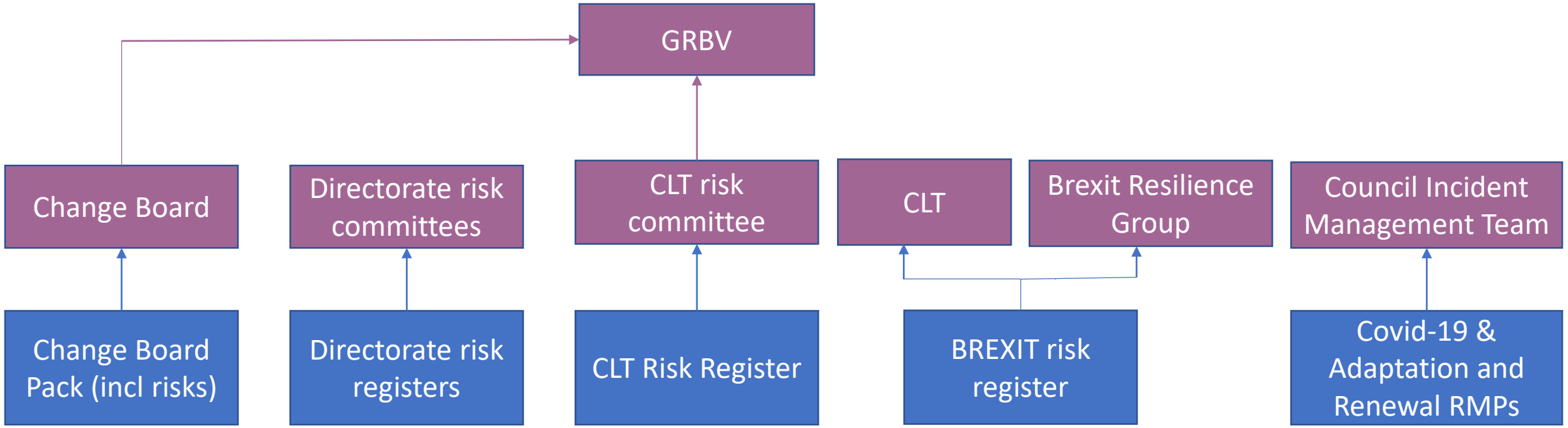
Blue lines – established and effective

Amber lines – to be established

Red lines – established but not effective



Council Risk Governance Structure as at June 2020



Proposed flow of Council risks

Key corporate risks and themes

- Council Health and Safety Group
- Other Corporate risk groups
  RM, CISSG, SOC, etc
- BREXIT risk register
- Covid-19 RMP

CLT Risk Register

Directorate Risk Registers

Divisional Risk Registers

Service delivery, strategic and 1st line change / project risks

Adaptation and Renewal Board

Adaptation and Renewal Programme Risks

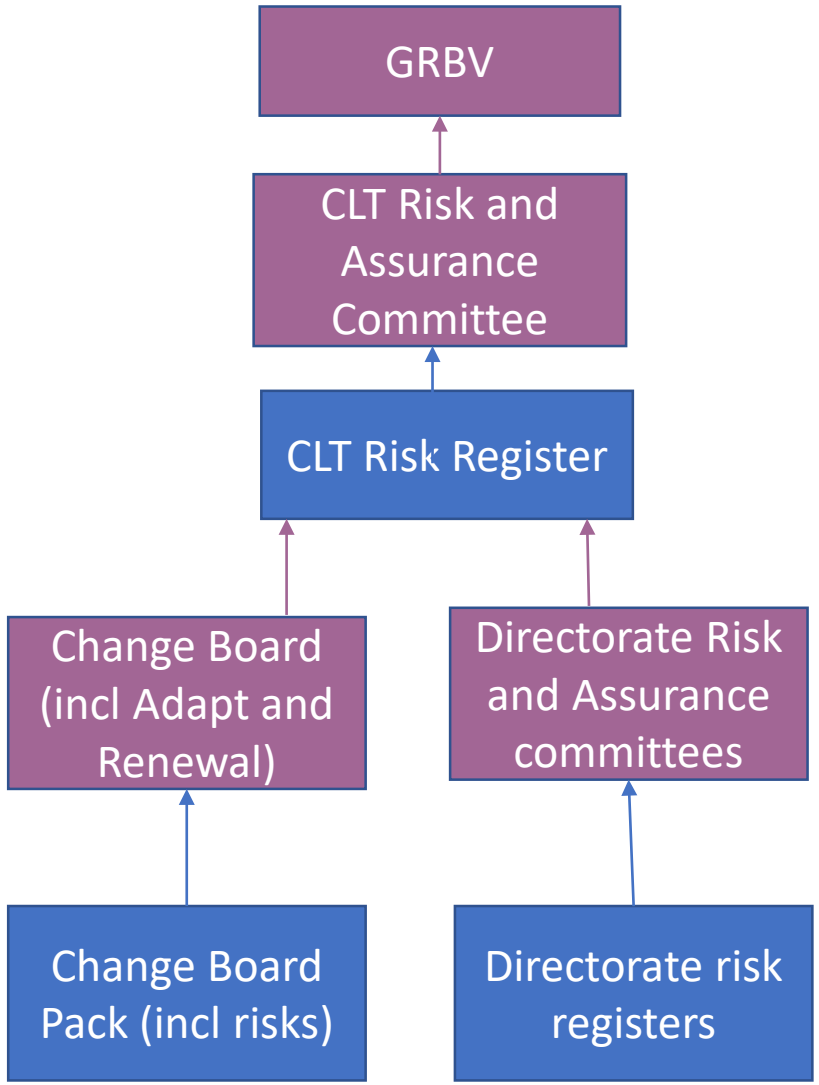
Adaptation and Renewal Risk Management Plan

Project and change risks and themes

Key risks associated with assurance findings raised by internal and external assurance providers

- **3rd Line:**
  Internal Audit, External Audit, Care Inspectorate, Education Scotland, Scottish Govt etc
- **2nd Line:**
  Health and Safety Audits, Information Governance etc
- **1st Line:**
  Self-Assurance Outcomes

Proposed Council Risk Governance Structure



Roles and Responsibilities

1st Line – Divisions and Directorates who own and manage risks should implement and consistently apply the Council's risk management framework by:

- Chairing and leading first line divisional and directorate risk and assurance committees and maintaining risk registers, and

ensuring that directorate risk registers include the risks associated with:

- All significant divisional operational service delivery risks
- All significant risks associated with strategic decisions.
- All thematic risks (e.g Brexit; Covid; technology; security; and health and safety)
- All relevant project management risks (including adaptation and renewal)
- Risks associated with 1st; 2nd; and 3rd line assurance outcomes
- An assessment of the original (pre controls) risks based on their likelihood and impact
- Details of controls established to manage these risks and assessment of their effectiveness supporting the current risk assessment
- Details of actions and implementation timeframes to achieve target risk.

2nd Line – Teams that design frameworks to support risk management and provide assurance

- Risk Management – design and maintain a clear risk management framework and support processes for application by 1st line teams, including appropriate technology solutions
- Risk Management – confirm 1st line awareness of all first, second, and third line assurance outcomes to confirm that risks associated with findings are included in relevant risk registers.
- Risk Management – attend all directorate and corporate leadership team risk and assurance committees as a 'critical friend' to support identification of significant thematic risks.
- Risk management – attend Change Board and other Board and Corporate Risk Groups as a 'critical friend' to support identification of significant thematic project / change management risks for inclusion in the CLT risk register.
- Risk Management – share the outcomes of horizon scanning to identify and communicate any potential new and emerging risks.
- Risk Management – complete ongoing assurance reviews to confirm the completeness and accuracy of risk flows into the CLT risk register.
- Boards and other Corporate Risk Groups (e.g. Serious Organised Crime; Health and Safety; Cyber and Information Security etc)- will maintain risk registers and support the flow of these risks through Risk Management for inclusion in first line divisional and directorate risk registers.
- Strategy and Communications Programme Management Office – ensure that thematic major project risks are identified and recorded in Programme Board packs.

3rd Line – Internal (and external) teams that provide independent assurance

- Internal Audit - attend all directorate and corporate leadership team risk and assurance committees as a 'critical friend' to support discussions on controls and their effectiveness
- Internal Audit – attend Change Board as a 'critical friend' to support discussions on the effectiveness of controls to address thematic project / programme risks.
- Internal Audit – attend Boards and other Corporate Risk Groups as a 'critical friend' to support discussions on effectiveness of controls to address thematic risks.
- Independent external audit - completed at least once every three years to assess the design adequacy and operating effectiveness of the Council's risk management framework,

Appendix 2 - Adaptation and Renewal Programme

Proposed Risk Management Framework

Objective

The main objective is:

To embed a Risk Management Framework consistently across all Programme workstreams

Where:

- Workstream risks are consistently described, assessed, and record in workstream risk registers, and consolidated to identify thematic Programme risks
- Thematic risks and their mitigating actions are discussed at the main Programme Board and included in the programme risk register
- Thematic programme risks are then escalated to the Corporate Leadership Team Risk and Assurance Committee for inclusion in the Corporate Risk Register - which is provided quarterly to the Governance Risk and Best Value Committee for their review and scrutiny

Approach

The proposed approach involves the following:

1) Identifying key strategic risks that are supported by a number of sub risks – this approach has been applied in the Covid 19 Risk Management Plan and works well

2) Strategic and sub risks will have standard descriptions that are applied consistently across the Programme workstreams

3) Sub risks will be assessed on the basis of original (inherent); current (residual); and target risk using the impact and likelihood risk matrix used across the Council – refer slide 5.

4) Sub risk assessment outcomes will either be Critical (black), High (red), Medium (amber) or Low (green) – definitions for each of these categories is included at slide 6

5) Sub risks will then be consolidated (using a simple scoring mechanism based on best practice methodology) to determine the overall original; current; and target strategic risks for each workstream - refer Slide 7

Proposed strategic risks and sub risks

1. Project and programme governance

a) Governance - oversight of progress and key decisions by project and programme governance forums and relevant Council executive committees, including project status reporting.

b) Decision making - Terms of reference and clearly established decision making authorities, and recording and approval of all key decisions and their supporting rationale.

c) Business case - clearly defined business case

d) Project plans - development and regular review and refresh of project plans

e) Risk appetite - clearly defined risk appetite

f) RAIDS management - risks; assumptions; issues; and dependencies (RAIDS) identification, assessment, recording and management

g) Benefits - identification, recording and tracking of quantitative and qualitative benefits, including completion of post implementation reviews

h) Financial - budget monitoring and management

i) Post implementation review/

2. Stakeholder engagement and communication

a) Stakeholder identification - identification of all key internal and external stakeholders

b) Political engagement – engagement with all political parties and support for project / programme objectives

c) Communication strategy - clearly defined engagement and communication strategy

Proposed strategic risks and sub risks (cont)

3. Service / system design and implementation

a) Service / system design - design specification and requirements including design of systems and process controls

b) Regulatory, legislative, and contractual requirements – have all been identified and incorporated in the service / system design

c) Testing – clearly defined testing plans that include all required types pre implementation and user acceptance testing, with evidence of testing recorded and significant weaknesses addressed prior to implementation

d) Implementation process – clearly defined implementation process that includes contingency time and back out options.

e) Go live decisioning - clearly documented rationale that supports go live decisioning, including consideration of any outstanding design and testing issues to be addressed post implementation.

4. Project delivery

a) Project timeframes at risk (including design, testing and implementation timelines)

b) Adequacy of budget to support project delivery

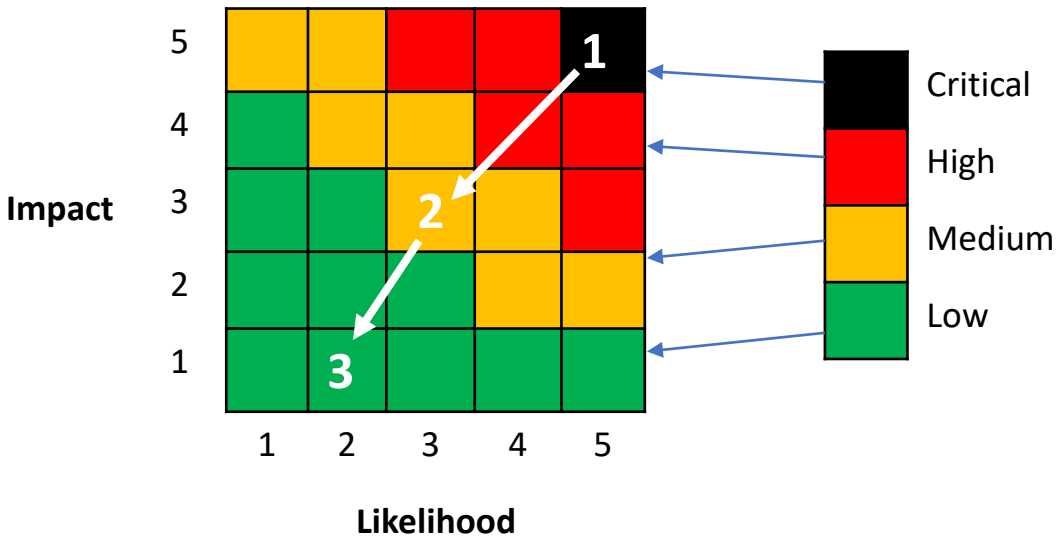
c) Adequacy of resources and their capacity

d) Dependencies (including third party deliverables) not achieved

e) Regulatory, legislative and contractual requirements delaying delivery

Risk assessment

Summary risk scoring heatmap



3 stages of risk assessment

1. **Original or inherent risk -** the level of risk before controls are implemented
2. **Current or residual risk -** the current level risk with controls in place
3. **Target risk -** the acceptable level of risk that we are aiming for

Description of risk assessment outcomes

Critical	It is extremely likely that this risk will become an issue that will have a significant adverse impact on the project. Appropriate mitigating actions should be implemented immediately to ensure that this risk is addressed.
High	There is a strong likelihood that this risk will become an issue that it will have a significant and potentially adverse impact on the project. Appropriate mitigating actions should be implemented as soon as possible to ensure that the risk is addressed.
Medium	There is a moderate likelihood that this risk will become an issue. If the risk does become an issue, it is likely that it will have a moderate impact on the project. Consequently, appropriate mitigating actions should be implemented prior to project completion.
Low	It is unlikely that this risk will become an issue. If the risk does become an issue it is likely that it will only have a minor impact on the project. Consequently, the risk can either be accepted with no action required, or actions implemented either close to or after project completion to address the risk.

Rating strategic risk by consolidating sub risk assessments

Sub risk assessment per heatmap	Score based on sub risk assessment
Nil	0
Low	1
Medium	3
High	10
Critical	40

Consolidated sub risk scores	Strategic risk rating
0 - 6	Low
7 - 15	Medium
16 - 39	High
40+	Critical

Example: Calculating assessment of an original strategic risk: Project Delivery

Sub risks		Assessments	Scores	Resulting strategic risk score	
1	Project timeframes	High	10	27	High
2	Adequacy of budget	High	10		
3	Resources and capacity	Medium	3		
4	Dependencies	Low	1		
5	Regulatory	Medium	3		

The above process should be repeated to determine the consolidated original, current and target rating for each strategic risk.