REPORT TO THE TRANSFORMATION PROGRAMME BOARD

Date:	20 July 2016
Subject:	**RISK MANAGEMENT STRATEGY**
Author/Service:	David Bailey, Head of Transformation

Recommendations:

(1) To adopt the Transformation Programme Risk Management Strategy.

Reasons for Proposed Decision:

The management of risk is essential to the successful delivery of the Transformation Programme. The purpose of this strategy is to define the approach to identify, assess, plan, implement and communicate the management of risks within the Transformation Programme.

Other Options for Action:

Board could amend the strategy.

Report:

1. The Risk Management Strategy for the Transformation Programme is given below, which is fundamentally based on the Corporate Risk Management Strategy.

2. The key risk categories for the Transformation Programme are identified. The risks identified will be profiled in detail through the completion of risk records following approval of this strategy.

RISK MANAGEMENT STRATEGY

1. Introduction

Making changes to the way we deliver services is not without risk. Research shows that 70% of all changes in organisations fail (Kotter, 1997). It is therefore essential that the authority acts in a way that mitigates hazards and gives us the best chance of delivering successful change. The Transformation Programme is more likely to be successful because it:

- Analyses the organisation and understands the need for change;
- Creates a shared vision and a common direction;
- Makes a clear break with the past;
- Creates a sense of urgency;
- Supports a strong leader role;
- Has political sponsorship;
- Crafts an implementation plan;
- Establishes enabling structures;
- Honestly communicates and involves people; and
- Reinforces and institutionalises change.

This Risk Management Strategy is to be applied to transformation projects and programmes to help control the risks to programme and project objectives. It covers the strategy and procedure to be followed for all risks – both threats and opportunities – relating to both the work during projects and the services in operational use.

- The Transformation Programme Board is ultimately responsible for this strategy; and
- The Head of Transformation will be responsible for maintaining the strategy.

2. Risk management procedure

The following steps should apply to the Transformation Programme's risk management procedure:

Identify step

Risks – both threats and opportunities – should be identified and added to the Risk Register. The tools and techniques mentioned below will aid this. Risks should be clearly described in unambiguous terms and include the risk cause, risk event and risk effect on the programme's objectives.

Assess step

Each risk should be assessed for its probability (the likelihood of it occurring), its impact (how it will affect the programme's objectives should it occur) and its proximity (when it's likely to occur), using the guides outlined below.

Plan step

Identify and evaluate a range of options for responding to threats and opportunities. Prepare specific risk management responses to the threats and opportunities to ideally remove or reduce the threats and maximise the opportunities. See risk response category section below.

Implement step

Programme Plans, Project Plans and other plans should be updated where appropriate, to include any relevant risk response actions. Any fallback plans should be included within the relevant plan and triggered if the related risk occurs.

Communicate step

The following management reports are used to communicate risks both within projects and programmes, the Transformation Programme Board, and externally to key stakeholders as indicated in the Communication Management Strategy.

- Highlight Report – for the Transformation Programme Board regarding Programme, Project and Stage-level risks;
- Checkpoint Report – for Project Managers regarding Work Package risks;
- End Stage Report – for Transformation Programme Board regarding risk status at the end of each stage;
- End Project Report – for the Transformation Programme Board regarding risk status at the end of a project; and
- Exception Report – in the case of a risk tolerance being exceeded.

3. Tools and techniques

The following risk techniques and tools should be used to help with the identification and assessment of risks:

- Reviewing lessons from previous projects and programmes;
- Risk Checklists – using the corporate risk checklist;

- Risk Potential Assessments – to assess the complexity and potential risks of projects and recommend an appropriate level of project management;
- Risk Brainstorms – involving appropriate programme and project team members or users;
- Risk Breakdown Structure – using our chosen risk categories from the Corporate Risk Management Strategy as described below;
- Expected Monetary Value to help with assessing the ‘financial value’ of the overall impact of all risks on the programmes’ viability;
- Summary risk profile should be used to summarise risks and their estimations – to be include in Highlight Reports; and
- Probability impact matrix should be used to rank and summarise risks qualitatively, using the matrix from the Corporate Risk Management Strategy.

Document templates can be found in the Transformation Programme ‘project management’ folder on the Corporate Intranet.

4. Records

A Risk Register is to be used which will give documented evidence that risks have been identified. It should contain the following details on each identified risk:

- Risk reference or identifier (Rnnn);
- Risk title;
- Risk author – the person who raised the risk;
- Date registered;
- Risk categories: Strategic, Political, Environmental, Legislative, Organisational, Financial and Technical;
- Risk description – to include risk cause and event;
- Risk consequences – to include effect on the project’s objectives;
- Probability, impact and expected values – for inherent risk (pre-response action) and residual risks (post-response action);
- Proximity;
- Risk response categories – for threats and opportunities, see response categories section of this strategy for further guidance;
- Risk response – the action(s) chosen to resolve the risk;
- Risk status;
- Risk owner – the person who will own and manage all aspects of the risk; and
- Risk actionee – the person who will carry out the risk response actions.

5. Reporting

The following management reports should include information on the project's risks:

- Highlight Reports*;
- Checkpoint Reports;
- End Stage Reports;
- Lessons Reports; and
- End Project Report.

*A Summary Risk Profile should be used to summarise / communicate risks and be included as part of each Highlight Report. This should include a 'RAG' colour coding status where:

- Green would represent 'No risk action applied and/or actions applied and risk currently stable';
- Amber represents 'formal risk actions applied, risk increasing but within tolerance'; and
- Red represents 'formal risk actions applied, but risk currently beyond tolerance'.

The templates for the Risk Register and Summary Risk Profile can be found in the Transformation Programme page on the Corporate Intranet.

6. Risk management activity timings

Key risk management activities (e.g. Identification, Assessment, Plan and Implement) should be undertaken at the following points of the project:

- 'Minimally' at the end of each stage, as part of reviewing all risks and 'during' each management stage on a monthly basis;
- Each time a Plan is produced and authorised (Project, Stage and Team level plans);
- On creation of any Exception Plans;
- Each time a Work Package is authorised (via discussions with the Team Manager); and
- When carrying out impact analysis on issues or assessment of any risk.

7. Scales

In line with the Corporate Risk Management Strategy, the following scales should be used for assessing the probability (or likelihood) of each risk:

	Level	*Descriptor*	*Probability*
A	Very High	Expected to occur in most circumstances	>75%
B	High	More likely than not	61% – 75%
C	Medium	Fairly likely to occur	31% – 60%
D	Low or Very Low	Low but not impossible	1% – 30%

Table 1: Risk probability or likelihood.

The following scales should be used for assessing the (negative) impact of each risk on a project's objectives. Descriptors for these levels are given in the table below:

Impact levels and descriptors for projects

	Insignificant 4	Minor 3	Moderate 2	Major 1
Impact on people and resources	Minor injuries or stress with no workdays lost or minimal medical treatment. No impact on staff moral	Injuries or stress level requiring some medical treatment, potentially some workdays lost. Potential impact on moral and performance on teams rather than by individual case (i.e. not isolated)	Serious injuries or stressful experience requiring medical treatment, many workdays lost, Major impact on moral and performance of more than 50 staff	Life threatening or multiple serious injuries or prolonged work place stress. Severe impact on moral and service performance. Mass strike actions, etc.
Legal, statutory compliance and reputation	Internal review, unlikely to have impact on corporate image	Scrutiny required by internal committees or internal audit to prevent escalation. Probable limited unfavourable media coverage.	Scrutiny required by external agencies, external audit etc. Unfavourable external media coverage. Noticeable impact on public opinion	Intense political and media scrutiny i.e. front page headlines, TV. Possible criminal or high profile, civil action against the Council, members or officers
Service delivery and processes	Minor errors in systems / operations or processes requiring action or minor delay without impact on overall schedule. Handled within normal day to day routines.	Significant short-term disruption of non-core activities. Standing Orders occasionally not complied with, or services do not fully meet needs. Service action will be required	Significant disruption of core activities. Key targets missed, some services compromised. Management action required to overcome medium term difficulties. Escalation to Management Board for action	Cessation of core activities. Strategies not consistent with government agenda, trends show service is degraded. Failure of major projects. Escalation to the Cabinet
Financial and budgetary impacts (costs and funding)	Minimal financial loss – minimal effect on budget/cost: Less than £10k	Medium financial loss – small increase on budget/cost: Between £10k and £250k	High financial loss – significant increase on budget/cost: Between £250k and £1m	Major financial loss – large increase on budget/cost: Greater than £1m Statutory intervention triggered. Impact the whole Council
Projects	Time: Negligible delays Cost: <5% of project spend/scope Quality: Minor deviations from project specification; does not affect final benefits	Time: Minor delays with some uncertainties; potential to cause more major impacts. Cost: <10% of project spend/scope Quality: Notable change to project specification, handled within the change control process	Time: Significant delays in project implementation and benefits realisation Cost >10% of project spend/scope Quality: Potential for reduced quality of end product/service. Impacts on other delivery vehicles/ interdependencies	Time: Project benefits will not be realised Cost: Punitive costs that require financial re-planning and service cuts elsewhere or project no longer sustainable Quality: Product/service not fit for purpose. Impacts on other delivery vehicles/ interdependencies

Table 2: Impact levels and descriptors for projects.

The Probability score should be combined with the Impact score to provide an overall assessment of the risk's severity (or threat level), as shown in the risk matrix below.

			Impact (Negative)			
			4	**3**	**2**	**1**
			Insignificant	**Minor**	**Moderate**	**Major**
Probability	**A**	**Very High** >75%	Low (A4)	Medium (A3)	High (A2)	High (A1)
	B	**High** 61%-75%	Low (B4)	Medium (B3)	High (B2)	High (B1)
	C	**Medium** 31%-60%	Low (C4)	Medium (C3)	Medium (C2)	Medium (C1)
	D	**Low or Very Low** 1%-30%	Low (D4)	Low (D3)	Low (D2)	Low (D1)

Table 3: Risk Matrix (Threats).

Ensuring that all risks are assessed and managed through the corporate risk management methodology drives consistency through the risk management framework and enables risks to be compared and reported on against a like-for-like basis. It also provides the authority with the ability to map its collective risk exposure of a particular activity, objective, outcome, function(s) or indeed whole Council operation.

8. Risk tolerance

The Transformation Programme Board have stressed that any risk which has a probability value greater than 60% (i.e. B High), must have an appropriate risk response action(s) applied. Based on the overall risk assessment values of a risk (e.g. the probability and impact combined) the risk should be managed as follows:

Level of risk	Consequences	Actions required
Red High	Severe (negative) impact. Considerable threat	Treatment / mitigation action(s). Required to minimise threat(s)
Amber Medium	Medium (negative) impact. Manageable threat	Managed via contingency plans. Treatment / mitigation action(s). Required to minimise threat(s)
Green Low	Relatively light (negative) impact. Acceptable threat	The Council is content to accept this risk, but threat(s) should be reviewed regularly

Table 4: Risk Appetite (Threats).

9. Proximity

Risk proximity (i.e. when the risk is expected to materialise) scales to be used for projects are as follows:

- Imminent (e.g. within 1-2 weeks);
- Within the current project stage;
- Within the project; and
- Beyond the project.

10. Key risk categories

Within the Transformation Programme, the following key risk categories should be used to help identify specific areas at risk:

- Strategic – regarding the Business Case / benefits;
- Political – regarding local, national or international politics;
- Environmental – relating to our impact on the natural world;
- Legislative – rules, regulations, standards, etc;
- Organisational – regarding performance, capability, availability of all project human resources;
- Communications – including engagement;
- Customers – regarding our external customers and residents;
- Partners – regarding our external partners and stakeholders;
- Financial – regarding costs of materials, inflation, etc; and
- Technical – regarding all specialist work and related specifications or criteria.

11. Risk response categories

The following are valid response categories to be used for the Transformation Programme.

For Threats:

- Avoid – to stop the risk from occurring or to prevent any impact;
- Reduce – to treat the risk in order to reduce the impact and/or probability;
- Fallback – a plan of action to be used if the risk happens;
- Transfer – a third party takes on responsibility for some or all of the impact;
- Share – via procurement, the negative impact of the threat can be shared with the supplier; or

- Accept – A conscious decision to retain the threat usually due to it being more economical to do nothing than to attempt to take action. The opportunity should still be monitored to ensure it remains tolerable.

For Opportunities:

- Exploit – seize the opportunity to ensure it **will** happen and the impact **will** be realised;
- Enhance – take action to enhance the probability of the event occurring and enhance the impact of the event should it occur;
- Share – via procurement, the positive impact of the opportunity can be shared with the supplier; or
- Reject – a deliberate decision may be made to not exploit or enhance an opportunity due to it being more economical to not attempt an opportunity response action. The opportunity should still be monitored.

12. Early Warning Indicators

- If specialist team resources fall below 70% availability (for any work areas);
- If any project schedule is ahead by 4 weeks, or behind schedule by 4 weeks (linked to project time tolerances);
- 50% of issues remaining unresolved; or
- If the average number of days for resolving critical or major issues exceeds 10 working days.

13. Risk budget

Each project budget should include 5% of the total sum set aside in the Transformation Programme budget to deal with risks. This budget should only be used to pay for risk management activities. The Head of Transformation must agree access to this budget via the Programme Management Office. Its use will be as follows:

- Funding all agreed risk management actions to the project's threats and opportunities, e.g. for funding specific fallback plans, actions that will reduce the risk threat, avoidance actions, or for exploiting or enhancing any recognised opportunities; and
- The risk budget will be divided over each stage of the project, the amount of which to be agreed with the Programme Management Office at each stage end.

14. Risk roles and responsibilities for projects

Role	Responsibility
Transformation Programme Board	Ensure risks related to the Business Case are identified, assessed and controlled. Monitor and where appropriate manage / own risks at a business / strategic level. Approve the Risk Management Strategy
Senior User	Ensure risks to the users are identified, assessed and controlled
Senior Supplier	Ensure risks relating to the supplier aspects are identified, assessed and controlled
Project Manager	Create and maintain the Risk Register. Ensure all risks are identified, recorded in the Risk Register and regularly reviewed. Manage specific risks assigned to them. Approve risk response actions at Work Package level
Team Manager	Participate in the identification, assessment and control of risks
Programme Lead	Review risk management procedures to ensure they are performed in line with this Risk Management Strategy
Project Support	Assist the Project Manager with the maintenance of the Risk Register. Protect the Risk Management Strategy under configuration management

Table 5: Risk Management Strategy: Roles and responsibilities.

15. References

Kotter, J. P., 1997. Leading Change: Why Transformation Efforts Fail. *Harvard Business Review,* 2007(1), pp. 34-40.

SPOCE Project Management 2011.