LONDON BOROUGH OF BRENT

CORPORATE RISK GUIDANCE

CONTENTS

This guidance and additional guidance on assessing impact and likelihood of risks is available on the Procurement and Risk Management section of the Brent Intranet.

1. THE RISK MANAGEMENT STRUCTURE

1.1 Scope of this guidance

This guidance sets out the process by which it is intended to monitor and manage corporate and service area risks.

Monitoring and management of risk will be linked as far as possible into the service planning and monitoring framework. The service plans require services to identify risks, which should be done by following this guidance, and cross referenced to the Corporate Risk Register.

The most important thing for service managers to bear in mind is that risk management is an integral part of good management. It should be done in a proportionate way by ensuring that focus is on those risks which are most relevant to the service area, have most impact and are most likely to happen.

1.2 Definition of Risk

Risk is the potential for events (e.g. change in legislation, reduction in funding, staff recruitment problems) and their consequences that constitute either an opportunity for benefit (positive risk) or threats to success (negative risk) in delivering our corporate strategy goals and/or services.

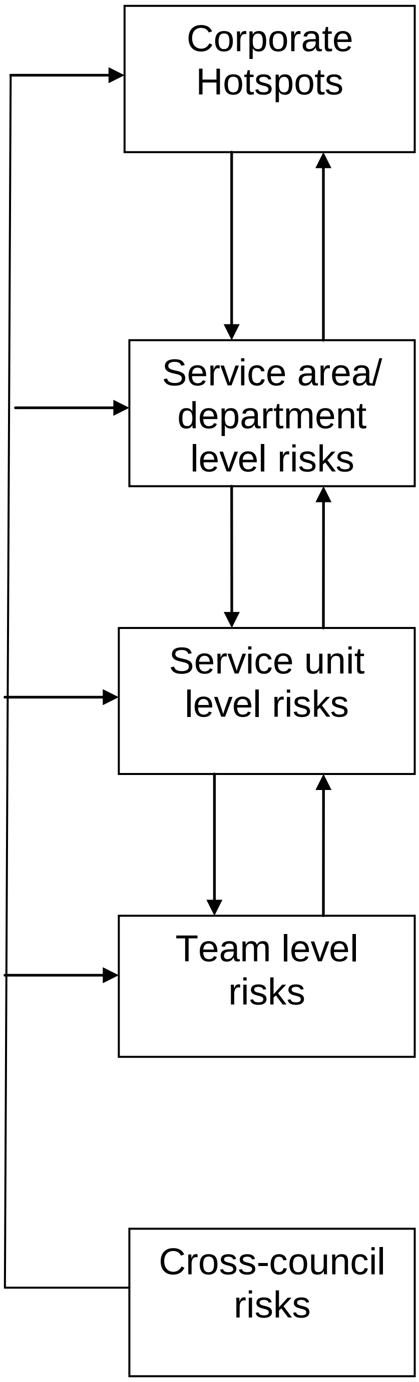
Risk evaluation is the combination of the probability or likelihood of an event and the impact of its consequences. The focus of good risk management is the identification and treatment of these risks. Good risk management increases the likelihood of success and reduces uncertainty in achieving our corporate goals.

1.3 Definition of Risk Management

Risk management is the process by which the council seeks to achieve its objectives by identifying risks to the achievement of these objectives and reducing the likelihood of the event occurring and minimising the impact of the event should it occur.

1.4 Risk Hierarchy

Risks are recorded at various levels of the council's business activity. This can be viewed as a hierarchy which maps to service planning:



These are the highest level council risks which are reported to the Policy Co-ordination Group on a quarterly basis. They include the highest category – likelihood and impact - of cross-council level and service area level risks eg significant risks to the achievement of key strategic objectives, to the finances of the authority, to the health and well-being of residents and/or staff, or to the reputation of the authority.

These are the highest level services area/departmental risks. They are discussed with the Lead Member and monitored at service area/departmental management teams. They include cross-council risks that apply at service area level and service area level risks. They will include the highest service unit risks. Some of the risks at may also be on corporate hotspots.

These are recorded in service plans. They include cross-council risks that apply at service unit level and specific service unit risks. These are risks that would impede service delivery. They will include the highest level team risks. The highest service unit level risks will be treated as service area/department level risks.

These are recorded in team plans. These are local level risks for the team. The highest level team risks will be included in service level risks and could be included in corporate hotspots. They may include corporate level risks that apply to an individual team.

These risks are identified by corporate groups, such as the strategic finance group and the corporate information governance group. The groups are responsible for ensuring the risks are being managed at the appropriate level within the organisation. Some of the risks will be managed at a corporate level – eg procedures to prevent unencrypted data being removed from council premises – and others at local level – eg control of information on children at risk.

The levels defined above do not relate to who owns the risk. They relate to its severity to the council as a whole.

Each risk is assigned a risk owner who has responsibility for mitigating or controlling the risk. This risk owner is not affected by the hierarchy and should be the most responsible person for that risk regardless of their position within the organisation. For example a corporate level risk could be owned by someone within an individual team.

Risk Identification

It is the responsibility of all council employees to identify risks relevant to their work.

It is the responsibility of all team leaders to identify risks relevant to their teams.

It is the responsibility of all service unit heads to identify risks relevant to their service.

1.5 Project Risks

Project level risks will be recorded in the system as a risk for the project as a whole. Individual project level risks will then be maintained in a separate register for that project which should be held in the Brent Projects Database:

http://content.brent.gov.uk/project1.nsf/WebMain?OpenNavigator

The owner of the project risk in the risk register should be the project manager – A staff member of Brent Council who is authorised to update projects on the Project Web system.

1.6 Corporate Level Risk Categories

The corporate Risk Management Group has identified the following corporate level risk categories.

Risk Category	**Corporate Group**
Budget, fraud and corruption	Strategic Finance Group
Health and safety	Strategic HR Group
Human resources	Strategic HR Group
Information and communications technology	IT Steering Group
Information Governance	Information Governance Group
Partnership	Strategic Performance Group
Performance and CAA	Strategic Performance Group
Procurement	Procurement Forum
Property	Asset Management Board
Sustainability	Carbon Management Steering Group

Risks at all levels will be assigned a corporate level risk category. The expectation is that the vast majority of risks in service areas fit within these categories. By identifying the corporate risk areas we intend to achieve consistency in the way in which risk is addressed across the council. Where more than one category applies, select the primary category which applies.

1.7 Links to the Council Objectives

Each risk will be associated with a Corporate Objective. These will be the key objectives agreed in the Corporate Strategy.

In the case of a generic risk which does not fall under any of the specific objectives, the objective “Improving our Capacity” should be used.[1]

1.8 Risks in Service Plans

The information required in service plans on individual risks is as follows:

- Service plan objective
- Risk title
- Description of risk
- Gross risk score:[2]
  - Likelihood – low/medium/high
  - Severity/impact – medium/high[3]
- Controls in place
- Controlled risk score:
  - Likelihood – low/medium/high
  - Severity/impact – medium/high
- Further action required
- Lead officer
- Corporate risk register code
- Risk area
- Source of assurance (eg Internal or External Audit, Inspection etc)

1.9 Monitoring and Managing Risks

Each service area needs to carry out regular monitoring of risks included in the risk register and service plans. The focus should be on identifying those risks which are most likely to have a damaging impact on the council’s finances, services, residents and customers, employees and reputation and reviewing the effectiveness of measures to control both the likelihood and impact of those risks. It needs to be a targeted approach, with time spent assessing the risk linked to likelihood and impact.

1.10 Links between Risk Management and Business Continuity

The Business Continuity Protocol states that:

- Directors and Assistant Directors will ensure that a Business Impact Analysis for each service is completed and reviewed at least annually. Departments will create and maintain business continuity plans, which will include arrangements for Priority 1 services. Business continuity review is to be included in the annual service plan for each service.
- Each Business Continuity plan is to be agreed by the Assistant Director and the Emergency Planning & Business Continuity Unit (EPBCU) to ensure the content is consistent with corporate arrangements. The Assistant Director will review assessments of the prioritisation of services and agree the classifications with the EPBCU. In the event of agreement not being reached, the matter will be referred to the appropriate Director for final decision

[1] When recording a risk within the corporate risk management system, links to appropriate material will be allowed. This may include operational procedures, web pages etc.

[2] Gross, controlled and target risk are defined in section 2.

[3] Low severity risks can be recorded on the risk management system. They would not however be included in service plans. Low likelihood risks would be included if they had high impact.

- Service / Unit Heads will review the business continuity plan for their service at least annually and following any exercise or disruptive event and prepare and maintain the BC plan and supporting arrangements.

Risks to processes that are determined to be a Priority 1 or 2 service by this Business Impact Analysis as identified in the Business Continuity Protocol should have appropriate controls in place to mitigate the risk.

These controls should be prefixed as “BC-“ in the risk management system to highlight that they are a Business Continuity consideration.

1.11 Overall Framework

Annex 1 to this guidance illustrates the overall framework.

2. RISK SCORING

2.1 Responsibility for Scoring

It is the responsibility of the risk owner to score the risk.

2.2 Types of Risk Scoring

There are three main types of risk score – gross risk, controlled (net) risk, and target risk. These are described below:

Gross Risk

Initially risks will be recorded in the system as a Gross Risk. This is the level of the risk if left unmanaged.

Controlled (Net) Risk

The Controlled Risk score is the level of risk when controls are put in place. Controls are permanent measures to mitigate the risk. The Controlled Risk score will be lower than the Gross Risk score, recognising the controls that are in place.

Target Risk

The Target Risk is the score that it is hoped will be achieved once actions aimed at strengthening the controls and further reducing the risk have been taken. The Target Risk score will be less than the Gross Risk and Controlled Risk score, recognising that actions will be targeted to reduce risk.

2.3 Controls and Actions

Controls and actions will be recorded on the system along with the risk, together with the name of the person responsible for the control. The owner of each control and action may be different from the owner of the risk

Controls are measures that are already in place to mitigate the risk. Current controls should lower the Gross Risk to the Controlled Risk. However, if it is considered that the Controlled Risk is still too high, then a Target Risk is set and actions to increase controls are identified in order to achieve this. This is illustrated in the table below:

Risk	**Gross Risk (impact and likelihood)**	**Current Controls**	**Controlled Risk (impact and likelihood)**	**Target Risk (impact and likelihood)**	**Further Controls needed**
	High x High		High x Medium	High x Low	

2.4 Reporting Schedule

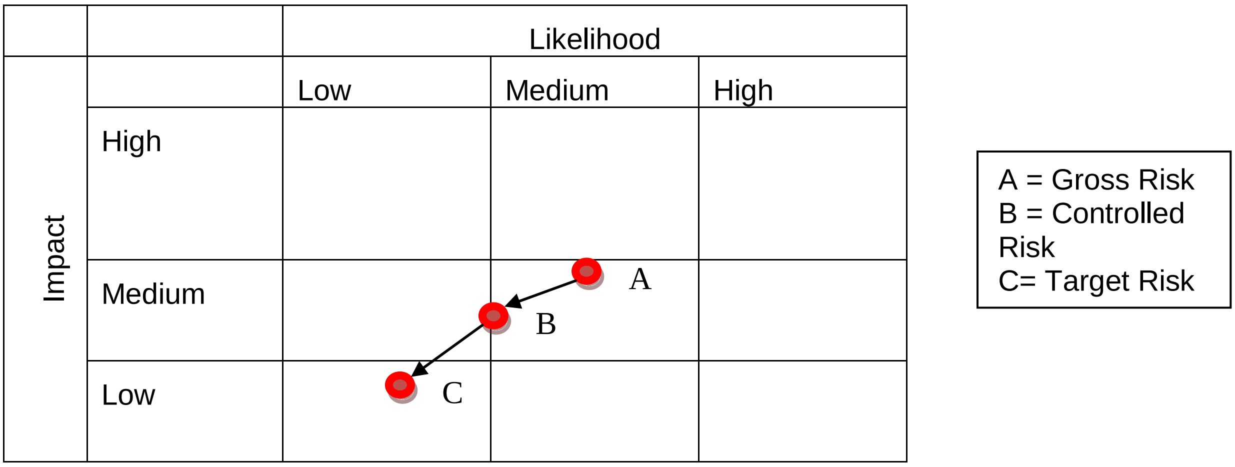
Each risk should be associated with a reporting schedule to ensure that the risks, controls, and actions are periodically reviewed.[4]

2.5 Scoring Matrix

All 3 types of score (Gross; Controlled; and Target) are derived using a single scoring table:

		Likelihood		
Impact		Low	Medium	High
	High			
	Medium			
	Low			

Risks are entered on the scoring matrix as follows, where A is the Gross Risk, B is the Controlled Risk (ie Gross Risk after controls are in place) and C is the Target Risk (ie where the risk is expected to be after planned actions to further manage the risk – over and above controls already in place – have been taken):



Note that there is a scoring range on each square of the grid so position A (Gross Risk) above will score higher than position B (Controlled Risk)

Controlled Risks should always be lower than Gross Risk, and Target Risk should always be lower than Gross Risk and Controlled Risk.

[4] Schedules may not be the same for review of risks, controls and actions.

All three risks are recorded on the risk system. However, when recording risk scores in service plans, record your Gross Risks and Controlled Risks only[5]. Do this by recording the position in the grid as Likelihood: Low; Medium; or High, and Impact: Medium; or High.

2.6 Defining Likelihood and Impact

For all risks, the general definition of the different categories of likelihood is shown below.

Likelihood	Definition
Low	Chance of happening is between 0%-33%
Medium	Chance of happening is between 33%-67%
High	Chance of happening is between over 67%

Impact should be rated as in the table below. For each risk area, Appendix 2 sets out more specific definitions to be used for that risk area.

Impact	Definition
Low	Impact would be unlikely to have a significant impact on achievement of objectives, residents or staff, finances, reputation etc
Medium	Impact would have a relatively significant impact on achievement of objectives, residents or staff, finances, reputation etc
High	Impact would have a very significant impact on achievement of objectives, residents or staff, finances, reputation and could, for example, lead to service failure

2.7 Risk Allocation

Risks may be identified at any level within the organisation – individual, team, service unit, department, corporate steering group or CMT.

However most risks will be scored and managed at team or unit level. Higher level risks will then be reported at service area, corporate steering group, or CMT where appropriate.

2.8 Team Level Risks

Where the risk is managed at team level and does not need to be reported at a higher level, the bottom left hand section of the scoring grid should be used.

To record team or unit level Controlled Risks in the system, use only the bottom left box of the table:

[5] If you have a risk that has no controls in place, this will be the same value as for your Gross Risk.

		Likelihood		
Impact		Low	Medium	High
	High			
	Medium			
	Low	▨		

As the scoring is a range within this box, this is the equivalent of the larger table:

<table>
<tr><td></td><td></td><td colspan="3">Likelihood</td></tr>
<tr><td rowspan="4">Impact</td><td></td><td>Low</td><td>Medium</td><td>High</td></tr>
<tr><td>High</td><td></td><td></td><td></td></tr>
<tr><td>Medium</td><td></td><td></td><td></td></tr>
<tr><td>Low</td><td><table><tr><td>▨</td><td>Low</td><td>Med</td><td>High</td></tr><tr><td>High</td><td>▨</td><td>▨</td><td>▨</td></tr><tr><td>Med</td><td>▨</td><td>▨</td><td>▨</td></tr><tr><td>Low</td><td>▨</td><td>▨</td><td>▨</td></tr></table></td><td></td><td></td></tr>
</table>

2.9 Service Unit Level Risks

To record service level risks in the system, use only the section of the table indicated by the shading below:

		Likelihood		
Impact		Low	Medium	High
	High			
	Medium	▨	▨	
	Low	▨	▨	

As the scoring is a range within this box (see Example 1), this is the equivalent of the larger table:

		Likelihood				
Impact		Low		Medium		High
	High					
	Medium		Low	Medium	High	
		High				
	Low	Medium				
		Low				

It is the responsibility of the Service Unit Head to ensure that all service level risks are recorded and included in the service plan.

To record the risk score in the Service Plan, record the score based on the position in the smaller grid:

- Likelihood: Low; Medium; or High
- Impact: Low; Medium; or High.

When recording these risks in the risk management system Service Unit Heads should be aware that the only Controlled Risks which are considered to be of Service Area (Department) significance should feature beyond the bottom left square of the main grid.

2.10 Service Area (Department) Level Risks

Where, despite controls in place, the risk is one which needs to be reported at service area (department) level (because even though likelihood is low, the impact for the organisation as a whole is high or the likelihood is medium to high and the impact on the organisation as a whole is medium to high), this will become a service area (department) level risk which will be reported at departmental management team level. In this case additional boxes in the scoring grid can be used to score the Controlled Risks.

It should be noted that, whilst Gross Risks may be in the boxes on the right hand top side of the matrix, very few Controlled Risks will be included in this part of the matrix because controls in place will have reduced the likelihood of the event happening and its impact.

		Likelihood		
Impact		Low	Medium	High
	High			

	Medium	▨	▨	▨
	Low			

2.11 Corporate Hotspots

These are the highest level cross- council risks which are reported to the Policy Co-ordination Group on a quarterly basis. They are also monitored by CMT at its regular fortnightly meetings under the CMT Action Plan. They include the highest category – likelihood and impact - of corporate level and service level risks.

In most cases these will be identified by either departmental management teams or by corporate steering groups. They will include Controlled Risks that are in the higher boxes. It should be noted that a judgement will have to be made about whether all risks in the medium likelihood, medium impact box or the low likelihood, high impact box should be included on the corporate hotspots list.

		Likelihood		
Impact		Low	Medium	High
	High	▨	▨	▨
	Medium		▨	▨
	Low			

2.12 Cross-Council Risks

These are risks which cut across the council's activities such as finance, IT, information management, health and safety.

These risks can either be treated as team/unit risks, or may be service area risks, or may be on Corporate Hotspots.

It is the responsibility of the appropriate corporate strategic group for the risk area to ensure that all corporate level risks are recorded and included in the risk management system and service plans at the appropriate level. Corporate steering groups for each risk area are defined in section 1.7.

Cross-council risks fall into 2 main types:

- Cross-council risks which need to be managed by all service areas – e.g. control of data leaving the authority – will be identified by the relevant corporate steering group, in this case the Information Governance Group. They will then be entered on the risk management system by the lead unit for the level corporate steering group – in this case ITU.
- Cross-council risks which need to be managed within specific areas – e.g. data on children at risk. These will be entered on the risk management system by the relevant service unit – in this case, Children's Social Care.

3. CROSS-COUNCIL RISKS - GUIDANCE

3.1 Budget, Fraud and Corruption

Main categories of corporate budget risk

Corporately Managed Risks – these do not need to be included in individual service plans

A. pay related, where general pay increases may be more than provided within budget (does not apply to local settlements);
B. major disasters;

All Services – these risks need to be included in all service plans

C. failure of internal financial control;

Specific Services – these risks will only be included in service plans where the risk to that service is significant

D. demand, where level of service provision depends on projections of need;

E. new legislation, where the council faces uncertainty about the costs of implementing new legislation;

F. legal challenges, where the council may have to make a settlement or be unable to collect income;

G. partnership, where there is a risk that a partner may not be able to meet their share of costs or will pass on costs;

H. interest rate, where fluctuations would have an impact on the estimated costs of borrowing;

I. procurement, where market conditions could mean that costs could increase where services are being re-tendered;

J. government grant, where there is uncertainty about the amount that will be allocated;

K. non-achievement of high risk savings or income targets in the budget;

L. overspend on major capital schemes;

M. other budget risks.

Controls and actions in place for budget risks are as follows:

Controls:

i. Nature and extent of risk identified in risk register;

ii. Clear accountability and responsibility for budget at service level;

iii. Intensive monitoring arrangements of spend and activity put in place (more intensive than for other areas);

iv. Processes put in place for reducing risk of event occurring (eg forecasting demand, demand management etc).

Actions:

i. Where budget overspend occurs, service area puts in place measures to address it;

ii. Overspends reported in monthly budget monitoring reports to corporate finance;

iii. Reasons for budget overspend identified and addressed.

Fraud and Corruption

Corporately Managed Risks – these do not need to be included in individual service plans

A. Unit wide deception

All Services – these risks need to be included in all service plans

None

Specific Services – these risks will only be included in service plans where the risk to that service is significant

B. Theft (basic) - removal of council property (can also include intellectual) or cash. Usually third party but can be internal. Includes property held on behalf of others i.e. clients.

C. Theft (complex) – removal of funds / assets through computer misuse. For example external hack or infiltration into any system controlling funds.

D. Fraudulent Applications for benefits, grants, financial assistance, services or property. Usually by third party by means of giving false information on some form of application. Obvious examples are Housing Benefits, Renovation Grants, Homelessness Applications. Less obvious but equally expensive are Direct Payment Care Packages, Section 17 payments.

E. Internal Fraud has a myriad of forms and ranges from simple over claiming of expenses/overtime to manipulation of computer data to generate false payments i.e. creditors, benefit claims, payroll, overtime etc. There will be an element of clear financial gain in all these cases. However, there are also frauds involving false information on job applications, working whilst off sick, falsifying attendance records / time sheets, misuse of council equipment/information technology and conducting private business in council time where there may be no financial gain but a clear pecuniary advantage. Low value fraud risks should not be included in the register.

F. Corruption can occur in the letting of contracts, payments to third parties or in any role where a permission, benefit, grant, funding agreement or award is given, where the officer has some influence over the decision. Can also include voluntary sector and regeneration initiatives. Can also occur in passing or selling of sensitive information.

Controls and actions in place for fraud and corruption risks are as follows:

Controls:

1. Budgetary and other financial controls
2. Physical security
3. Organisational security

Actions:

1. Supervision and checking of outputs
2. Monitoring (provision and review of management information)

3. Audit trail
4. Deterrent statements
5. Application of contract standing orders

3.2 Health and Safety

Corporately Managed Risks – these do not need to be included in individual service plans

A. All health and safety risks arise from delivery of services or ownership of assets. Whilst the legal duty to ensure health and safety falls to the Corporate entity, all health and risks are delegated to service areas to manage. For example property H&S risks are managed corporately in respect of the main offices (Muniport) but each of the other service area has properties which it manages itself. None of the most significant H&S risks are, therefore, able to be excluded from service area plans. The Corporate systems in place to assist services manage these H&S risks are outlined below.

All Services – these risks need to be included in all service plans

B. All services need to include in their plans a review of their general risk assessment which will identify which health and safety risks need priority action in their service plans. All services will need to include the following risks in their general risk assessment (although some may be able to conclude that risks are very low):

- Aggression and violence to staff and lone working issues
- Workplace hazards (housekeeping, slips trips and falls, work environment)
- Manual Handling
- Stress and working time issues
- Equipment use, including electrical and gas appliances
- First Aid arrangements
- Control of Contractors

Specific Services – these risks will be included in service plans where the general risk assessment identifies that more action is needed to control it

C. Building related issues – fire, asbestos, legionnaires disease, vehicle and pedestrian safety, building and services maintenance, construction and building operations etc

D. Activity related issues – safe systems of work, driving, working on building sites, musculo-skeletal disorders, work at heights

E. Customer related issues – violence from client or member of the public, care issues, educational or recreational visits

Controls and actions in place for health and safety risks are as follows:

The controls and actions are outlined in some detail in the Council's Health and Safety Policy statement which outlines the Corporate H&S Management system and proposes a model service area H&S management system for use by Service Areas.

The Corporate H&S Management system comprises:

- Policy e.g. Council's H&S Policy Statement
- Organisational Arrangements for control and communication of risks as well as arrangements for ensuring competence and promoting co-operation e.g. management competencies, Corporate H&S Committee.
- Planning and Implementation arrangements including risk assessment and workplace precautions e.g. Corporate H&S standards,
- Monitoring and Performance Measurement arrangements e.g. Accident statistics, Annual Performance report
- Audit arrangements e.g. H&S Audits

Service Area H&S Management systems will include the above with the possible exception of policy and Audit which are primarily a Corporate responsibility.

3.3 Human Resources

Corporately Managed Risks – these do not need to be included in individual service plans

A. Single Status

B. Employee Relations

All Services – these risks need to be included in all service plans

C. Failure to comply with employment legislation

D. Failure to comply with HR policies and procedures

E. Failure to recruit and retain staff

Specific Services – these risks will only be included in service plans where the risk to that service is significant

F. Inability to recruit to key posts and as such unable to deliver service

Controls and actions in place for human resources risks are as follows:

Controls:

1. Comprehensive HR policies and procedures with clear levels of responsibility and accountability
2. Monitoring of HR data in relation to employee relation issues and workforce data to highlight potential issues
3. Nature and extent of risk identified in risk register
4. Training for staff and managers
5. Consultation framework with unions
6. Environmental scanning

Actions:

1. Application of relevant HR policy and procedure, seeking advice from HR as appropriate.
2. Review circumstances and introduce measures to minimise reoccurrence
3. Consult with unions
4. Implementation of recruitment and retention initiatives using temporary workers to meet immediate need

3.4 Information and Communications Technology

Main categories of corporate information and communications technology risk:

Corporately Managed Risks – these do not need to be included in individual service plans

A. Failure of ICT infrastructure

All Services – these risks need to be included in all service plans

B. Failure to comply with ICT corporate standards

Specific Services – these risks will only be included in service plans where the risk to that service is significant

C. Loss of service specific data

Controls and actions in place for information and communications technology risks are as follows:

Controls:

1. Adherence to ICT corporate standards
2. Consult with ITU.
3. Understand nature and extent of risk identified in risk register;
4. Understand and adhere to ICT corporate standards

Actions:

1. Ensure procedures / policies in operation are reviewed.
2. Regularly review all documentation and working practices
3. ITU to be advised immediately of events

3.5 Information Governance

3.6 Partnership

Corporately Managed Risks – these do not need to be included in individual service plans

None

All Services – these risks need to be included in all service plans

None

Specific Services – these risks will only be included in service plans where the risk to that service is significant

A. Specific service not being delivered/budget overspends

Controls and actions in place for partnership risks are as follows:

Controls:

1. Nature and extent of risk identified in risk register
2. Clear levels of accountability and responsibility for budget and services by partnerships and at service level.
3. Intensive monitoring arrangements of spend and activity put in place (more intensive than for other areas);
4. Processes put in place for reducing risk of event occurring (e.g. forecasting demand, demand management etc).

Actions:

1. Where budget overspend occurs, partnership where relevant and service area puts in place measures to address it;
2. Where performance fails, partnership where relevant and service area puts in place measures to address it;
3. Overspends reported in monthly budget monitoring reports to corporate finance;
4. Performance reported through performance plus, subject to agreed monitoring timeframes.
5. Reasons for budget overspend and failure of performance identified and addressed.

3.7 Performance and CAA

Main categories of corporate performance risk

Corporately Managed Risks – these do not need to be included in individual service plans

None

All Services – these risks need to be included in all service plans

A. Failure to comply with corporate performance management arrangements

Specific Services – these risks will only be included in service plans where the risk to that service is significant

B. Failure to achieve corporate performance targets required to achieve targeted CPA category and/or Local Area Agreement stretch target

Controls and actions in place for performance risks are as follows:

Controls:

i. Nature and extent of risk identified in risk register/service plan

ii. Clear levels of accountability and responsibility for performance at service level

iii. Adhere to roles of performance officers across council as set out in Performance Management Group Terms of Reference

iv. Intensive monitoring and review arrangements put in place

v. Processes put in place for reducing risk of event occurring (e.g. forecasting performance and adjusting activity)

Actions:

i. Where poor performance occurs, service area puts in place measures to address it

ii. Poor performance should be reported monthly to departmental management team

iii. Poor performance reported in quarterly vital signs reports to CMT, Executive and performance and Finance select committee

iv. Performance reported through performance plus, subject to agreed monitoring timeframes.

v. Reasons for failure of performance are identified and address

3.8 Procurement

Main categories of procurement risk

Corporately Managed Risks – these do not need to be included in individual service plans

A. Commercial risk. This would include under performance by the supplier or collapse of the supplier's business

B. Partnership risk. Partners not able to successfully perform the contract, Partner actions could result in additional contract costs to the council

C. Law and Regulatory. New legislation, loss of intellectual property rights

D. Economic/Financial /Market. Inflation, shortage of working capital, business failure of key market leader

E. Political risk. Change in policy, adverse media reporting

All Services – these risks need to be included in all service plans

None

Specific Services – these risks will only be included in service plans where the risk to that service is significant

F. Organisational/Management/Human Factors. Specification poorly drafted, subsequent contract insufficiently managed, supplier performance not adequately monitored

Controls and actions in place for procurement risks are as follows:

Controls:

1. Clear accountability and responsibility for procurement risk and procurement activity at service level
2. Quarterly monitoring of risk and procurement activity by management teams
3. Adherence by managers and staff to contract management guidance and procurement procedures

4. Appropriate training on contract letting and contract management

Actions:

1. Service areas should utilise procurement project methodology on major contract work, assigning project owners and project managers to drive regular gateway reviews of risk and procurement progress
2. Staff involved in procurement work should be signed up to the appropriate level of corporate training in risk and procurement

3.9 Property

Main categories of corporate property risk

Corporately Managed Risks – these do not need to be included in individual service plans

A. Property ownership records

B. Accommodation strategy

All Services – these risks need to be included in all service plans

C. Non compliance with legislation and/or procedures

Specific Services – these risks will only be included in service plans where the risk to that service is significant

D. Working environment non compliance with legislation and/or procedures

E. Asset maintenance

F. Property project failure

G. Unplanned running costs

H. Access to property

Controls and actions in place for property risks are as follows:

Controls:

1. Understand and follow property procedures.
2. Comply with health and safety legislation
3. Consult with property and asset management

Actions:

1. Head of property to be advised immediately
2. If Health & Safety issue contact HSL immediately
3. Ensure procedures/ policies in operation are reviewed
4. Regularly review all documentation and working methods

3.10 Sustainability

Consider the following impact types:

a) emissions to air,

b) releases to water,

c) releases to land,
d) use of raw materials and natural resources, use of energy,
e) energy emitted, e.g. heat, radiation, vibration,
f) waste and by-products, and
g) physical attributes, e.g. size, shape, colour, appearance.
h) cultural heritage
i) effect on the community

Corporate Level Risks

- Council carbon reduction strategy and targets (energy; gas; fuel use)
- Council waste strategy and targets
- Council Travel Plan
- Potential environmental emergencies on a borough-wide or local scale
- Climate change mitigation and adaptation

Service Level Risks

- Processes which, if disrupted, would seriously impede the delivery of Priority 1 and 2 services – MUST have an associated control.
- Non compliance with legislation and/or procedures
- Non compliance with Policy

  Full list of Corporate Environmental Policies available on the intranet: http://content.brent.gov.uk/goinggreen.nsf/Environmental%20Management/LBB-8

Team Level Risks

- Non compliance with legislation and/or procedures
- Non compliance with Policy

  Full list of Corporate Environmental Policies available on the intranet:

  http://content.brent.gov.uk/goinggreen.nsf/Environmental%20Management/LBB-8
- Operations resulting in a measurable or observable change in the environment or community
- Environmental performance issue where there is significant public concern
- Environmental performance issue where there is significant cost if left unmanaged
  - Financial
  - Reputation
  - Resources (e.g. staff or equipment)
  - Environmental or social
- Activities with the potential to result in an emergency

○ Processes which, if disrupted, would seriously impede the delivery of services

For those Services with certification to ISO14001, this is the level where you will record and score your potential environmental impacts

Controls:

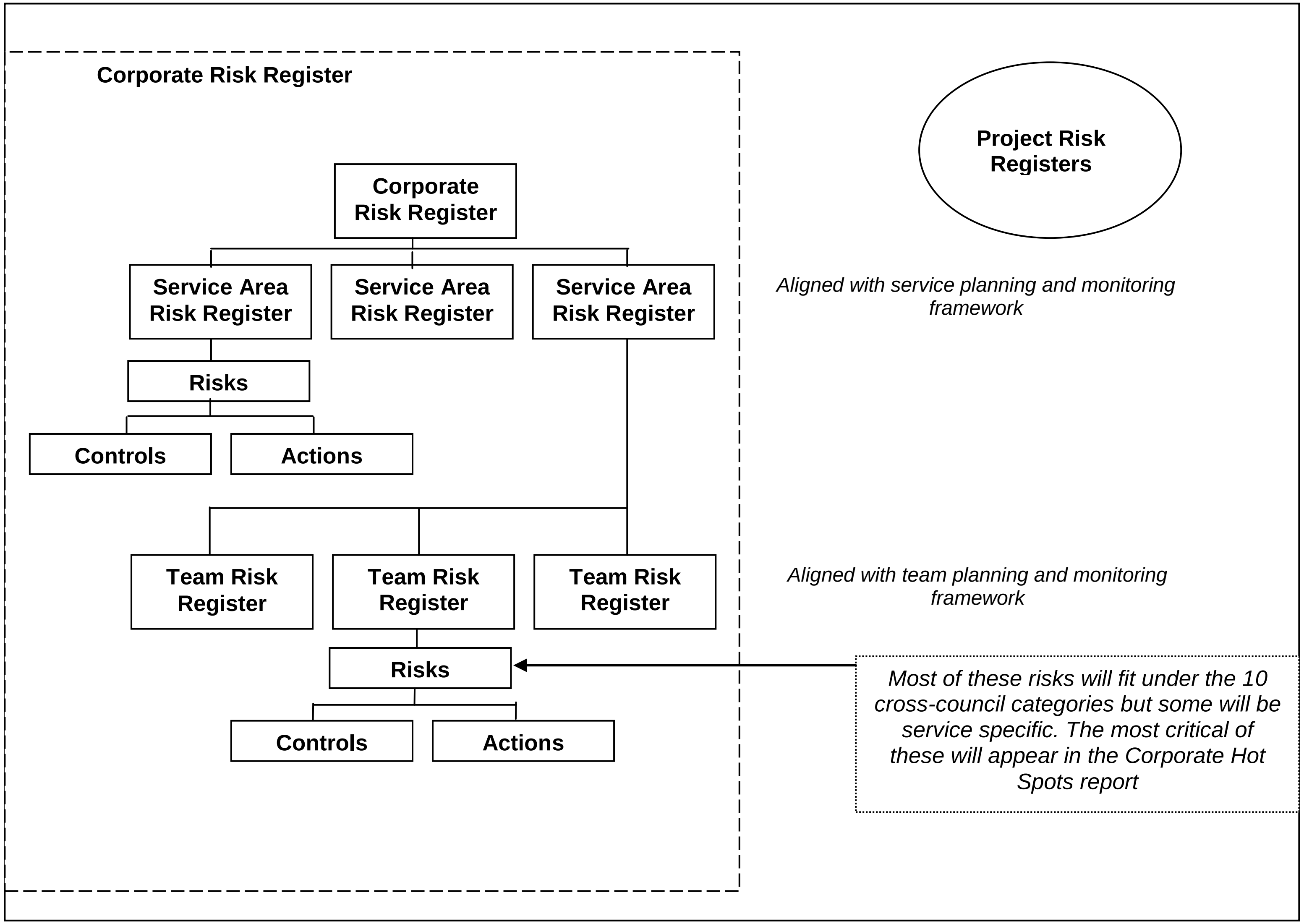
1. Defined procedure
2. Contract
3. Enforcement
4. Legal Consents

Actions:

1. Objective for improvement
2. Target or Performance Indicator

a. Action Plan
b. Environmental Improvement Programme

ANNEX A



Aligned with service planning and monitoring framework

Aligned with team planning and monitoring framework

Most of these risks will fit under the 10 cross-council categories but some will be service specific. The most critical of these will appear in the Corporate Hot Spots report