FOR RESOLUTION

SUBJECT **Risk Register, Risk Management Strategy & Business Continuity Management Policy.**

REPORT OF **The Lead Officer on behalf of the Advisory Board**

PURPOSE OF THE REPORT

To report to Members on the current evaluation of risk and to seek approval of a Risk Management Strategy which will underpin the future management, monitoring and reporting of risk to the Joint Committee.

RECOMMENDATIONS

The Joint Committee is recommended to:

[i] Review the current evaluation of risk (Appendix 1)
[ii] Approve the Risk Management Strategy and summary of the Joint Committee's Risk Appetite (Appendix 2)
[iii] Report any Member training needs in relation to Risk Management
[iv] Receive a Risk Report at each meeting.
[v] Approve the Business Continuity Management Policy (Appendix 3)

FINANCIAL CONSEQUENCES

Financial risk management is identified within the report.

CONTACT OFFICERS

Louise Hutchinson, PATROL Headquarters, Barlow House, Minshull Street, Manchester, M1 3DZ Tel: 0161 242 5270

1. BACKGROUND

1.1 The enclosed risk register responds to the auditors' recommendations and suggestions made by the Joint Committee at their meetings.

1.2 Follow-up work on risk management was undertaken by Internal Audit as part of their annual audit plan for 2010/11. A recommendation from Internal Audit was for the Joint Committee to approve a Risk Management Strategy upon which future risk management and reporting will be undertaken.

1.3 The Joint Committee approved the following summary of its risk appetite:

We will avoid risks that threaten our ability to undertake our principal objectives in a way which provides quality and value. We will maintain a sufficient level of reserves to support liquidity and absorb short term fluctuations in income and expenditure beyond our control.

2. RECOMMENDATIONS

The Joint Committee is recommended to:

[i] Review the current evaluation of risk (Appendix 1)
[ii] Approve the Risk Management Strategy and summary of the Joint Committee's Risk Appetite (Appendix 2)
[iii] Report any Member training needs in relation to Risk Management
[iv] Receive a Risk Report at each meeting.
[v] Approve the Business Continuity Management Policy (Appendix 3)

APPENDIX 1 LATEST EVALUATION OF RISK

Rank	Risk Description	Consequence Description	Risk Impact	Liklihood	Score	Key Controls In Place	Assurances	Response	Previously Reported Status	Current Status	Further Actions to be taken to Manage Risk Better	Lead
1.	Unforeseen significant fluctuations in income and assurance on service charge income	Inability to meet financial obligations	5	2	10	Audit figures on which to base forecasts. Historical data on which to base forecasts. Reserve policy in place	Internal & External Audit Reports Committee Reports	Treat			Continued forecasting, budget monitoring and cashflow analysis.	HOS
2.	Inability of IT to support needs of organisation and technology users	Reduced effectiveness and efficiency for tribunal, councils and appellants.	4	3	12	Formal tender procedure undertaken Initial project planning undertaken.	Business Process and IT Review	Treat			Contract for new web portal and case management system Separation of tribunal's domain	HOS
3.	Loss of key members of management and staff	Disruption to operations Management of vacancies Project and operational targets affected	2	5	10	Clearly defined roles with flexibility to provide cover. Documented procedures Arrangements for temporary cover Arrangements in place to extend cover. Appointment Sub Committee & Working Group	Committee Reports	Treat			Review of existing vacancies and risk based approach to planning for future vacancies. Recruitment process agreed for Chief Adjudicator. Support arrangements for transfer to new host authority.	HOS
4	Insufficient adjudicator/staff resources to meet demand	Inability to meet targets Pressure to reach decisions may result in increased number of judicial reviews	3	4	12	Monitoring of demand and performance Staff recruitment, induction, training and appraisal. Contingency Planning	Committee Reports	Treat			Adjudicator Recruitment 2012	CA

5	Achievement of Key Objectives	Failure to achieve key objectives	4	3	12	Performance Management Strategy and Reporting	Internal & External Audit Reports Committee Reports	Treat			Multiple project planning required for 2012/13 (new host authority, new IT system, recruitment of adjudicators)	HOS

CA = Chief Adjudicator
HOS = Head of Service Note 1 The Risk Register is underpinned by the Risk Management Strategy and should be read in conjunction with business continuity planning arrangements.

Risks that have been downgraded in accordance with the Risk Management Strategy

	Effective Financial and Resource Management including spending within agreed budgets	Financial instability	2	2	4	Historical data on which to base forecasts. Specified role for budget holders in budget monitoring. Recommendations from Internal Audit	Internal & External Audit Reports Committee Reports	Treat			Impact of revisions to budget management Internal Audit Annual Plan for 2011/12.
	Change in government policy	Change in direction for traffic regulations/adjudication	5	1	5	Establishing and maintaining dialogue with relevant government departments, responding to consultation, participation in working groups	Committee Reports	Tolerate			None at this time
	Health and Safety Breach	Risk to welfare of adjudicators, appellant, staff Disruption to tribunal operation	3	1	3	Health and Safety policy in place. Procedures in place for monitoring risk/handling incidents which may be a threat to health and security. Business Continuity Plan in place.	Reporting requirements for Health and Safety Matters	Treat			None at this time

Risk Impact Details

Name		Description
1	Immaterial	Loss of up to £10k; examples include little effect on service delivery; no health and safety impact; no damage to reputation.
2	Minor	Loss of £10k to £50k; examples include minor disruption to effective service delivery i.e. staff in unplanned absence for up to one week; minor injury; no requirement for professional medical treatment; slight damage to reputation.
3	Moderate	Loss of £50k to £250k; examples include delays in effective service delivery i.e. adjustments to work programmes in up to one week or staff long term absence; injury to an individual(s) requiring professional medical treatments; reputation damage is localised and minor.
4	Significant	Loss of £250k to £500k; examples include effective service delivery is disrupted in specific areas of the business; multiple serious injuries requiring professional medical treatment; reputation damage occurs with key stakeholders.
5	Major	Loss of £500k +; examples include effective service delivery is no longer achievable, fatality of staff, visitor or public; reputation damage is irrecoverable i.e. regulatory body intervention.

Likelihood

Description	Probability	Indicators
5. Highly Probable	> 80%	• Is expected to occur in most circumstances • Circumstances frequently encountered – daily/weekly/monthly/annually • Imminent/near miss
4. Probable/ Likely	60% - 80%	• Will probably occur in many circumstances • Circumstances occasionally encountered but not a persistent issue (e.g. once every couple/few years) • Has happened in the past or elsewhere
3. Possible	40% - 60%	• Not expected to happen, but is possible (once in 3 or more years) • Not known in this activity
2. Unlikely	20% - 40%	• May occur only in exceptional circumstances • Has rarely / never happened before • Force majeure
1. Remote	20%	• The risk will not emerge in any foreseeable circumstance

The evaluation process will highlight the key risks that require urgent attention. However, all the risks need to be considered and action agreed, even if this is to take no action at the current time. The options are either to: Tolerate, Treat, Terminate or Transfer each risk.

- **Tolerate the risk (accept it)** – some low scoring risks may be considered as acceptable, but these need to be reviewed on a regular basis to confirm that the circumstances have not changed.

- **Treat the risk (reduce by control procedures)** – the risk can be considered acceptable provided the control mechanisms work.
- **Terminate the risk (cease or modify the method of delivery)** – where risks are unacceptable and control mechanisms will not provide adequate security, the activity or the method of delivery must be modified.
- **Transfer the risk** – through insurance of financial contingency provision.

MEASUREMENT OF RISK AND REPORTING

Risk Matrix

		Consequence				
		5	4	3	2	1
Likelihood	5	25	20	15	10	5
	4	20	16	12	8	4
	3	15	12	9	6	3
	2	10	8	6	4	2
	1	5	4	3	2	1

Legend:

Score of 25 equates to **Extreme Risk**: Immediate escalation to Head of Service for urgent consideration by Joint Committee.
Scores of 20-15 **High Risk:** Risk to be escalated to the Joint Committee/Executive Sub Committee with mitigating action plan. Risk to be actively managed by Head of Service and Advisory Board.
Scores of 12-6 **Medium Risk:** Risk to be captured on Risk Register and progress with mitigation to be tracked by Head of Service and Advisory Board/Joint Committee/Executive Sub Committee.
Scores of 5 and below **Low Risk**: Risk to be removed from register and managed within appropriate services.

APPENDIX 2
BUS LANE ADJUDICATION SERVICE JOINT COMMITTEE
RISK MANAGEMENT STRATEGY
DRAFT JUNE 2012

1. PURPOSE

The Joint Committee recognises that effective risk management is an important element of a robust corporate governance framework and is therefore committed to:

- Developing and maintaining a systematic approach for the identification, evaluation and cost effective control of the risks that threaten the achievement of corporate objectives.
- Ensuring that effective risk management is embedded in the business processes

2. OBJECTIVES

The objectives of this strategy are to:

- Ensure that risks to the achievement of the corporate objectives are eliminated or reduced to an acceptable level.
- Ensure other risks to reputation, assets, finances and people are appropriately managed.
- Raise awareness of, and integrate risk management into the culture of the organisation.
- Manage risk in accordance with best practice by identifying roles and responsibilities.
- Maintain effective stewardship of funds and demonstrate good corporate governance.

3. IMPLEMENTATION

The Joint Committee will achieve these objectives by:

- Approving this strategy
- The Head of Service establishing and maintaining the risk management review framework identified within this strategy.
- Including risk management as a standing agenda item at each Joint Committee/Executive Sub Committee and Advisory Board meeting supported by reports from Officers.

- Continuing to demonstrate the application of risk management principles in practice.
- Establishing the training requirements of Members and Officers
- Maintaining documented procedures for the control of risk.
- Monitoring risk management arrangements on an ongoing basis and periodically reviewing risk.
- Embedding risk management into business processes.

4. DEFINITIONS AND CATEGORIES

a. DEFINITIONS

RISK is a combination of the **LIKELIHOOD** of something happening and the **CONSEQUENCE** for business objectives.

RISK MANAGEMENT is the process by which risks and potential opportunities are identified, evaluated and controlled.

b. CATEGORIES OF RISK

The Audit Commission and CIPFA identify two categories of risk namely strategic and operational. Strategic are those risks to the medium and long term goals and objectives of the organisation. Operational are those risks and hazards encountered in the daily course of work affecting managers and staff.

c. RISK APPETITE

In defining the risk appetite, consideration should be given to:

- The level of risk which an organisation or individual is prepared to tolerate without introducing further risk mitigation measures or controls.
- Identifying the point where the Joint Committee accepts that a risk exists and that to put in place further measures aimed at reducing the risk to a more acceptable level is not possible, practical or not cost effective.
- The wider context of risk and tolerance levels of other parties who may be affected by the risk, including members of the public and other stakeholders.

The Joint Committee summarises its risk appetite as follows:

We will avoid risks that threaten our ability to undertake our principal objectives in a way which provides quality and value. We will maintain a sufficient level of reserves to support liquidity and absorb short term fluctuations in income and expenditure beyond our control.

5. RISK MANAGEMENT PROCESS

Key questions in risk management include:

- What can go wrong?
- What is the likelihood of it going wrong?
- What is the impact should it go wrong?
- What can be done to eliminate the threat?
- What should be done to reduce the threat's likelihood or impact?

The risk management cycle involves

a) Identifying Risk
b) Analysing and Evaluating
c) Prioritising
d) Taking Action
e) Monitoring and Review

6. MEASUREMENT OF RISK AND REPORTING

Risk Matrix

		Consequence				
		5	4	3	2	1
Likelihood	5	25	20	15	10	5
	4	20	16	12	8	4
	3	15	12	9	6	3
	2	10	8	6	4	2
	1	5	4	3	2	1

Legend:

Score of 25 equates to **Extreme Risk**: Immediate escalation to Head of

Service for urgent consideration by Joint Committee.
Scores of 20-15 **High Risk:** Risk to be escalated to the Joint Committee/Executive Sub Committee with mitigating action plan. Risk to be actively managed by Head of Service and Advisory Board.
Scores of 12-6 **Medium Risk:** Risk to be captured on Risk Register and progress with mitigation to be tracked by Head of Service and Advisory Board/Joint Committee/Executive Sub Committee.
Scores of 5 and below **Low Risk**: Risk to be removed from register and managed within appropriate services.

Risk Impact Details

Name	Description
Immaterial	Loss of up to £10k; examples include little effect on service delivery; no health and safety impact; no damage to reputation.
Minor	Loss of £10k to £50k; examples include minor disruption to effective service delivery i.e. staff in unplanned absence for up to one week; minor injury; no requirement for professional medical treatment; slight damage to reputation.
Moderate	Loss of £50k to £250k; examples include delays in effective service delivery i.e. adjustments to work programmes in up to one week or staff long term absence; injury to an individual(s) requiring professional medical treatments; reputation damage is localised and minor.
Significant	Loss of £250k to £500k; examples include effective service delivery is disrupted in specific areas of the business; multiple serious injuries requiring professional medical treatment; reputation damage occurs with key stakeholders.
Major	Loss of £500k +; examples include effective service delivery is no longer achievable, fatality of staff, visitor or public; reputation damage is irrecoverable i.e. regulatory body intervention.

Likelihood

Description	Probability	Indicators
5. Highly Probable	> 80%	• Is expected to occur in most circumstances • Circumstances frequently encountered – daily/weekly/monthly/annually • Imminent/near miss
4. Probable/ Likely	60% - 80%	• Will probably occur in many circumstances • Circumstances occasionally encountered but not a persistent issue (e.g. once every couple/few years) • Has happened in the past or elsewhere
3. Possible	40% - 60%	• Not expected to happen, but is possible (once in 3 or more years) • Not known in this activity
2. Unlikely	20% - 40%	• May occur only in exceptional circumstances • Has rarely / never happened before • Force majeure
1. Remote	< 20%	• The risk will not emerge in any foreseeable circumstance

5.4 The evaluation process will highlight the key risks that require urgent attention. However, all the risks need to be considered and action agreed, even if this is to take no action at the current time. The options are either to: Tolerate, Treat, Terminate or Transfer each risk.

- **Tolerate the risk (accept it)** – some low scoring risks may be considered as acceptable, but these need to be reviewed on a regular basis to confirm that the circumstances have not changed.
- **Treat the risk (reduce by control procedures)** – the risk can be considered acceptable provided the control mechanisms work.
- **Terminate the risk (cease or modify the method of delivery)** – where risks are unacceptable and control mechanisms will not provide adequate security, the activity or the method of delivery must be modified.
- **Transfer the risk** – through insurance of financial contingency provision.

5.5 The risk register will be monitored and reviewed by a Risk Management Group and reported to Members and the Advisory Board. New risks will be added to the register where appropriate and assigned an individual risk owner. An updated risk register will be provided as a standard report to the Joint Committee.

RISK MANAGEMENT ROLES AND RESPONSIBILITIES

6.1 The Joint Committee

The roles and responsibilities of the Joint Committee are:

- to ensure that a comprehensive approach to risk management is developed and implemented
- to oversee and obtain assurance over the effective management of the risks by the Head of Service.

6.2 The Head of Service

- To support and develop the risk management culture of the Risk Management Group which helps support the Joint Committee's strategic leadership and corporate governance roles.
- To develop and maintain a risk management framework.
- To maintain effective links with stakeholders on risk management issues and to report as appropriate to the Joint Committee or Executive Sub Committee and the Advisory Board.

6.3 Risk Management Group

The risk management framework established by the Head of Service allocates the following responsibilities to the Risk Management Group:

- Initial identification and evaluation of risks.

- Registration of risks.
- Evaluation of effectiveness of controls.
- Action planning to mitigate the impact of risks on the achievement of the Joint Committee's objectives.
- Reporting to Joint Committee and/or Executive Sub Committee and Advisory Board.
- Preparing changes to this policy.
- Providing guidance and training for staff on risk awareness.

7. MONITORING AND REVIEW

The Joint Committee will monitor the effectiveness of this policy and will receive a copy of the latest risk register and a report from the Head of Service at each Joint Committee meeting.

8. APPROVALS

Approved Joint Committee June 2011

APPENDIX 3

DRAFT BUSINESS CONTINUITY MANAGEMENT POLICY

1. PURPOSE

The purpose of this policy is to formalise the Business Continuity program and to provide guidelines for developing, maintaining and exercising Business Continuity Plans (BCPs). This policy establishes the basic principles and framework necessary to ensure emergency response, resumption and recovery, restoration and permanent recovery of operations and business activities during a business interruption event.

2. SCOPE

This policy applies to staff, facilities and IT systems and preparation for scenarios including, but not limited to, natural disaster, power outage, hardware/telecommunications failures, data corruption and terrorism. These events may be local in nature, or could have regional impact, with multiple facilities in a geographic region becoming inaccessible. This policy provides guidance for the resumption and recovery of time sensitive business operations in accordance with pre-established timeframes as well as ensuring that adequate plans are in place for the less time sensitive business operations.

3. POLICY

The Joint Committee recognises the potential strategic, operational, financial, reputational and stakeholder risks associated with service interruptions and the importance of maintaining viable capability to continue business processes with minimum impact in the event of an emergency.

DEFINITIONS
- **BCG** – Business Continuity Group
- **BCP** – Business Continuity Plan
- **BIA** – Business Impact Analysis

4. PROCEDURES:

Statement of Policy
Business continuity policy and planning are fundamental to reduce the impact of business interruption and should be read in conjunction with the Joint Committee's Risk Management Statement.

The Joint Committee recognises the importance of developing, exercising and testing and maintaining plans for the resumption and recovery of business functions and processing resources. The resumption and recovery plans must be based on a risk assessment that considers potential losses due to unavailability of service versus the cost of resumption. These plans shall anticipate a variety of probable scenarios at local, regional and national level.

Responsibilities

Joint Committee and Advisory Board: Responsible for ensuring that Business Continuity Management policy and procedures are in place and reviewed by Officers on a regular basis.

Head of Service: Responsible for the documented development, maintenance and review of the Business Continuity Management policy and procedures and identifying key staff to have specific responsibility for business continuity in terms of premises, Adjudicators, staff, tribunal services, IT and finance. These Officers will comprise the Business Continuity Group.

Business Impact Analysis (BIA) and Risk Assessment

The BCG shall undertake a BIA on an annual basis to identify and prioritise the critical business processes and costs of downtime. The BIA shall cover the major business processes that cut across the multiple sections or teams. It shall identify the business process availability, recovery time objectives and associated risks if these processes were not available.

The Business Continuity Plan

The BCG shall develop the BCP to recover from an incident and provide, at the very minimum, the ability to recover critical processes in line with the findings of the BIA. The recovery plans for an incident shall be developed by the BCG. The BCG shall have oversight as to the creation of plans to provide leadership and guidance, and ensure appropriate consistency and coordination among the various business dependencies, as well as compliance/consistency with standards.

During an incident, the Head of Service and Officers identified in the Business Continuity Plan *shall* activate the Business Continuity Plan. The BCG shall work with the affected sections/teams to ensure smooth execution of the BCP. Where relocation is required, consideration will be given to alternative ways of working to ensure a swift resumption of services.

The Business Continuity Plan will be reviewed every six months and updated as changes occur. All incidents will be documented and records maintained.

Develop Resumption and Recovery Plans for People Assets

Adjudicators and staff shall be provided with communication approaches and tools to ensure communication among themselves and with the staff for emergency response and business continuity.

The BCG shall implement and maintain a basic communication plan for all sections/teams for emergency response and business continuity. Confidentiality of staff personal contact information for this purpose shall be managed in compliance with the Information Security and HR policies and practices.

Business continuity plans shall identify the designated primary staff member (from the business operation) and an alternate who can perform functional responsibilities in the absence of the primary staff member.

The BCG shall work to develop clear guidance on how the staff shall report their time during crisis. These staff may be directed to suspend their regular duties until the operations are restored at a permanent site or some alternate direction is provided.

Develop Resumption and Recovery Plans for Facilities and Office Space

In order to successfully resume critical business operations during an incident/crisis, the BCG must identify a safe, easily accessible and fully operational location with adequate resources (IT and others) for staff to report to and initiate operations from during the period of crisis. Any decisions regarding alterative facilities must provide adequate office space and alternate communication links.

Develop IT Systems Resumption and Recovery Plans

The BCP shall develop a coordinated strategy involving plans, policies, procedures, and technical measures that enable the recovery of IT systems, operations, and data that is identified as critical. The BCG shall also work with other companies that are responsible for development and maintenance of the technology and information that support critical business processes. The network architecture and telecommunications shall help ensure there is the ability to withstand local/regional crisis/national crisis.

BC policy and planning shall be integrated in IT policy, budget and implementation decisions. IT budget guidelines shall take into account good practices concerning business continuity planning and preparedness.

For new application development, BC planning should be integrated in all phases of the IT project life cycle, starting from Business Requirements, System Architecture, Design, Construction, Testing, Implementation, Maintenance and Retirement.

Testing

In order to validate the Business Continuity Plan and ensure strategies are capable of providing response and recovery results within agreed timeframes, planned testing will be conducted training provided to all staff on an annual basis and or as needs arise. The IT core system will be disaster recovery tested at an off site location annually. Test results shall be shared with the Advisory Board.

Communications

The BCP shall include mandatory instructions, advice, process, procedure or guidance concerning internal and external communications.

External communication during an incident/crisis is a critical business process. The BCG shall develop the process and messages that will be communicated to staff and stakeholders in the event of an incident or business interruption.

Training

Business Continuity training for the BCG (and other relevant staff) is essential for effective resumption and recovery of operations. BCG staff shall be supported with training to keep current in the business continuity best practice, latest technologies, tools, international standards and regulations that guide the development of BC plans. Training must include details regarding business resumption and recovery roles in coordination with the BCG.

BCP Maintenance and Management Reporting

The BCPs shall be updated on a bi-annual basis, or as often as changes require, using agreed templates. Most importantly all major updates should be incorporated as soon as possible and not held to satisfy a pre-arranged schedule.

The BCG shall consider the use of automated tools to support business continuity planning. Reporting business continuity planning status and progress is a key element of creating an effective BC program. The BCG shall report the status and progress of the BC program to the Advisory Board on an annual basis or after every BC test.

5. POLICY COMPLIANCE

Consistent compliance with this policy is essential to its effectiveness and therefore adherence to this policy is expected. The BCG will assess the preparedness of all the sections/teams. The assessment will include the quantification and qualification of exposures including, but not limited to, the resumption of time-sensitive operations and the recovery of other operations.

Internal Audit, as part of its work program, will review the business continuity plans periodically to ensure, as appropriate, alignment of the overall Business Continuity Program with Standards such as BS25999.

Policy Agreed:
Planned Review Date:
Actual Review Date: