TfL's RESILIENCE MANAGEMENT POLICY FRAMEWORK

1. Purpose of the Resilience Management Policy Framework

The TfL Resilience Management Policy Framework sets out TfL's approach to minimising the likelihood of harmful or disruptive events and maintaining adequate capability to prepare for, manage and recover from such events whether malicious, accidental or natural.

This Policy applies to all TfL employees, all TfL Group companies and all those not directly employed by TfL who when working on behalf of TfL might have an impact on TfL's Resilience.

2 Policy statement

TfL is committed to ensuring that it has processes to assess, and controls to minimise, the likelihood and potential impact of any operational or non-operational harmful or disruptive events. We will ensure the security of staff, customers and contractors, assets, including information, and service delivery. We will prepare for and be able to efficiently recover from harmful or disruptive events from whatever cause. We will have effective and tested plans and procedures to minimise harm to people and the environment, damage to property, financial impacts and damage to reputation following a harmful or disruptive event. All resilience planning and responses will be based on the principle of 'prudent over-reaction'.

3. Resilience Management Policy Framework

TfL will fulfil the Policy requirements by ensuring that all areas of TfL have the capability to:

- reduce the risk of harmful or disruptive events to an acceptable level by structured review of existing processes, changes and new projects;
- manage immediate impacts; and,
- recover effectively from a harmful or disruptive event.

TfL will achieve this by having systems to identify and reduce risks and maintaining emergency, contingency and recovery plans that staff are trained to use, that are tested and are regularly reviewed and updated.

Each business area has responsibility for ensuring that its activities are adequately resilient by assessing and controlling risks and by developing and maintaining emergency, contingency and business recovery plans.

In line with the requirements placed on it as a Category 2 responder under the Civil Contingencies Act 2004, and as a transport provider, TfL will contribute to the resilience of London and be prepared to support post-incident recovery in London by providing transport services. These requirements and processes

for their delivery will be maintained in conjunction with partner organisations involved in maintaining London's resilience capability.

4. Assessing and controlling risks

Resilience is a risk recognised in TfL's Strategic Risk Management Framework. TfL will ensure that resilience is considered and addressed through routine risk management and when projects are planned or changes introduced, including during procurement processes.

The appropriateness and adequacy of proposals to address resilience in projects will be addressed during Business Case Development, Business Planning processes and project and programme approvals.

TfL will establish standards and procedures for the security of staff, customers and contractors and assets, including information and service delivery. TfL will have the capability to receive and respond to security information through planned and documented processes.

5. Emergency, Contingency and Business Recovery Planning

TfL will maintain Emergency Management, Contingency Management and Recovery Management plans supporting the resilience objectives of TfL which are reviewed and updated as appropriate.

6. Assurance

Assurance of the TfL Resilience Management Policy Framework will be provided via four principal mechanisms. These are Management, the TfL Risk Management processes, Internal Audit and Resilience Assurance Letters.

The Risk Management process identifies significant business risks, including resilience risks and captures the mitigations in place and additional mitigations that are planned.

Internal Audits are planned and conducted in accordance with a structured risk based plan that identifies the significant risks to TfL and then audits and reports against those.

The Resilience Assurance Letter process requires each Managing Director to report annually on compliance with the Resilience Management Policy Framework.

7. Review and Amendments

This Policy is owned by General Counsel and this version was agreed by the Safety, Health and Environment Assurance Committee on 2 August 2011. It will be reviewed every three years and changes will be reported to the Safety, Health and Environment Assurance Committee. The TfL Group Resilience Adviser can be contacted for advice and guidance on the content and implementation of this Policy.

8. Glossary

Resilience Management - the process of minimising the likelihood of, and impact from, operational and/or non-operational harmful or disruptive events, whether malicious, accidental or natural, and minimising harm to people and the environment, damage to property, financial impacts and damage to reputation. Providing security for employees, contractors, customers, assets, including information and service delivery is an integral part of resilience management.

Risk Management - understanding the threats to a business or elements of it, assessing the likelihood of these threats being realised and identifying mechanisms for reducing the threats, or their likelihood, to an acceptable level.

Incident - an unplanned, natural or malicious event or accident that threatens or disrupts normal operations, services or other aspects of the ability to do business.

Emergency Management - managing the response to, and containment of, the impact of an incident upon normal operations or services.

Contingency Management - maintaining critical operations or services during a disruption with significant impact on the organisation.

Recovery Management - managing business recovery to return to normal operations or services following an incident.

Emergency, Contingency and Business Recovery Planning - management of the development, maintenance and implementation of emergency, contingency and business recovery plans.

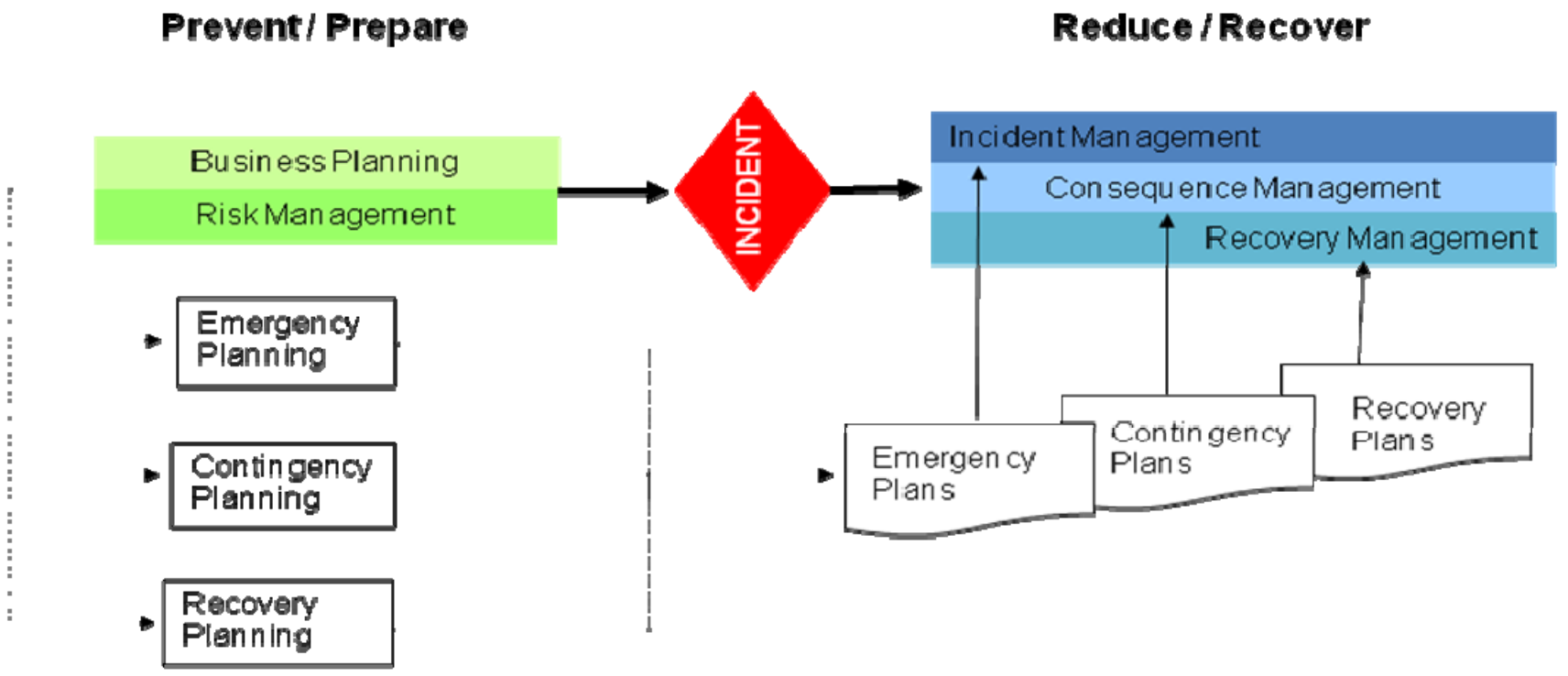
Emergency and Contingency Plans - procedures and information used at the time of an incident to minimise harm to people, the environment, damage to property and to contain the impact of the incident.

Recovery Plans - procedures and information for managing the recovery of normal operations or services which have been significantly impacted by an incident.

Security Management – minimising threats to employees, contactors, customers, assets, including information, and service delivery.

Relationship of the key resilience related processes
The following diagram shows these relationships.

Resilience Management Process*



* Operational & non-operational