

IT Disaster Recovery 2012/13**Recommendation R1:**

A Disaster Recovery Plan should be developed and approved. As a minimum, this should include;

- the identification and prioritisation of key IT systems
- the roles and responsibilities of relevant officers and third party suppliers
- a set of IT procedures which should be executed initially to react to crises/disaster
- escalation procedures
- salvage procedures that deal with retrieval of items from affected sites
- the recovery and reconfiguration of all IT and communication systems
- details of additional accounts where monies may be sourced to aid recovery efforts
- a schedule in respect of the testing of the plan

Rationale for Recommendation:

During 2009/10, there was no Disaster Recovery Plan. Recovery from the server

Failures in February 2010 gave highest priority to restoration of the IT infrastructure. Meetings and telephone conversations with Heads of Services and Directors were held to agree the recovery plan / priorities and time scales. No IT Disaster Recovery

Strategy was found to be documented to describe the role and development of a Disaster Recovery Plan and to improve the recovery options of IT systems

Detailed Tracking of recommendation by activity

Recommendation	Current Position and Explanation for Slippage:	Target Dates:
<p>A Disaster Recovery Plan should be developed and approved. As a minimum, this should include:</p>	<p>A Disaster Recovery Plan has been developed and approved by Information Technology's Senior Management Team.</p> <p>There are a number of areas that require further work as detailed below.</p>	<p>Complete</p>
<ul style="list-style-type: none"> • the identification and prioritisation of key IT systems 	<p>Information Technology's assessment of Business critical locations, operations and/or systems should be informed by Business Continuity Plans. Senior Management approved Business Continuity Plans should be used to define the agreed services and systems within Information Technology's Disaster Recovery Plan.</p> <p>Emergency Planning to work with Directorates on Business Continuity Plans and</p>	<p>Once Service area/Directorates have agreed and approved Business Continuity Plans</p>

Recommendation	Current Position and Explanation for Slippage:	Target Dates:
	<p>those agreed Business Continuity Plans should inform Information Technology's Disaster Recovery Plan. A Disaster Recovery Plan to reflect Business Continuity Plan priorities as agreed by Senior Management. Information Technology will meet with Emergency Planning and work with them to drive this forward.</p> <p>A recovery matrix will be developed and included in the Disaster Recovery Plan with prioritisation and categorisation columns. This will be presented to Senior Management for agreement and sign off.</p> <p>Update since January Committee Meeting held with Emergency Planning. Emergency Planning are working on this and are actively developing process and templates. Information Technology have helped with this activity by providing a Business Impact Assessment template, and will be helping with further templates including the Business Continuity Plan.</p> <p>Update June – Further work on this required. Information Technology and Emergency Planning to meet on a regular basis to progress</p> <p>Completion of this recommendation is reliant on Service area/Directorates.</p>	
<ul style="list-style-type: none"> the roles and responsibilities of relevant officers and third party suppliers 	<p>Engage Emergency Planning Team in development of Information Technology's Disaster Recovery Plan. Ensure that roles and responsibilities are clearly identified and agreed. Information Technology to agree with Emergency Planning Team roles and responsibilities and update Information Technology's Disaster Recovery Plan with details of individuals to be contacted should disaster recovery be invoked. This is subject to the outcome of the meeting above.</p> <p>Update since January Committee Information Technology's Management Team is working on this as part of the Disaster Recovery procedures, once the list complete it will be reviewed with Emergency Planning.</p> <p>Update June – Roles and responsibilities updated in Information Technology's Disaster Recovery Plan</p>	<p>March 2014</p> <p>Complete</p>
<ul style="list-style-type: none"> a set of IT procedures which 	<p>Detailed operational Disaster Recovery procedures to be developed and included</p>	<p>March 2014</p>

Recommendation	Current Position and Explanation for Slippage:	Target Dates:
<p>should be executed initially to react to crises/disaster</p>	<p>in the Disaster Recovery Plan. Decision tree to be developed by Information Technology's Management Team to enable a structured and clear response to a Disaster Recovery event. Resolution of the recent system performance issues has contributed towards the minor delay.</p> <p>Update since January Committee A Decision tree has been developed for Information Technology and agreed by the Information Technology's Management Team, detailed operational procedures are being finalised and will be signed off by Information Technology's Management Team at end of March.</p> <p>Update June – Disaster Recovery Process has now been inserted into Information Technology's Disaster Recovery Plan. New Head of Service for Operational Delivery will take ownership of this for on-going management and updates.</p>	<p>Complete</p>
<ul style="list-style-type: none"> escalation procedures 	<p>Escalation procedures will be developed in-line with Information Technology Structure and will be aligned with capabilities, knowledge and skill sets. See above.</p> <p>Update since January Committee The escalation procedure is part of the wider Disaster Recovery procedures, see above</p> <p>Escalation processes with Service areas/Directorates will be developed in conjunction with Emergency Planning and will incorporate Business Continuity Plans.</p> <p>Update June – Further work required with Emergency Planning to finalise these procedures.</p>	<p>March 2014</p> <p>Once Service areas/Directorates will have agreed and approved Directorate Business Continuity Plans</p>
<ul style="list-style-type: none"> salvage procedures that deal with retrieval of items from affected sites 	<p>Salvage process and procedures to be devised, working in partnership with ONI the co-location service provider, and included within Disaster Recovery Plan.</p> <p>The proposed procedure will be developed and included in the Disaster Recovery Plan.</p>	<p>March 2014</p>

Recommendation	Current Position and Explanation for Slippage:	Target Dates:
	<p>Update since January Committee The Salvage processes are currently being devised and will be presented to Information Technology's Management Team at the end of March.</p> <p>Update June – Salvage procedure completed, on-going day to day management of operational Disaster Recovery will become responsibility of new Head of Service for Operational Delivery.</p>	<p>Complete</p>
<ul style="list-style-type: none"> the recovery and reconfiguration of all IT and communication systems 	<p>Information Technology's Disaster Recovery Plan should detail the prioritisation of the Council services and systems in-line with the agreed Corporate Business Continuity Plan. Categorisation of those services should be identified within Information Technology's Disaster Recovery Plan and the recovery order agreed with the Corporate Management Team.</p> <p>Business Continuity Plans should identify critical recovery time periods for their services before material losses. These time periods should be included in the recovery matrix of Information Technology's Disaster Recovery Plan. Recovery Time Objectives to be developed and included within the Disaster Recovery Plan.</p> <p>Recovery matrix to be developed and included in Disaster Recovery Plan with prioritisation, categorisation columns. It shall also include recovery time periods within Information Technology. Signed off by Information Technology's Management Team.</p> <p>Recovery Time Objectives to be developed and included in Information Technology's Disaster Recovery Plan once recovery matrix is signed off and included.</p> <p>Update since January Committee Recovery Time Objectives have been included as a section within the Business Impact Assessments, the Service Area's need to complete these in order for Information Technology to include in its Disaster Recovery Plan.</p> <p>Update June – Further work required with Emergency Planning.</p> <p>Completion of this recommendation is reliant on Service areas/Directorates.</p>	<p>Once Service areas/Directorates have agreed and approved Business Continuity Plans</p>

Recommendation	Current Position and Explanation for Slippage:	Target Dates:
<ul style="list-style-type: none"> details of additional accounts where monies may be sourced to aid recovery efforts 	<p>An agreed fund for Disaster Recovery should be identified and held available to support recovery of services in the event of an emergency. Secure confirmation from section 151 officer concerning source of funding.</p> <p>Update since January Committee Emergency Planning have confirmed that there is no funding for Disaster Recovery, and should Disaster Recovery be invoked the funds will be found corporately. Need to confirm this with the Chief Finance Officer.</p> <p>Update June – Chief Information Officer and Chief Finance Officer have confirmed there are no central funds for Disaster Recovery and that any event will be funded corporately</p>	<p>Once Service areas/Directorates have agreed additional funds</p> <p>Complete</p>
<ul style="list-style-type: none"> a schedule in respect of the testing of the plan 	<p>An agreed Disaster Recovery test plan to be developed in-line with the Recovery Matrix and Disaster Recovery testing to be undertaken on an annual basis. Disaster Recovery Tests already underway, and are continuing to be performed as part of the incremental programme of Disaster Recovery capability enhancement.</p> <p>Back-up testing has commenced as part of annual Disaster Recovery test plan and included with the Disaster Recovery Plan. Backup tests already underway, and will be performed as part of the incremental programme of Disaster Recovery capability enhancement. The SAN (Storage Area Network) backup process has been reviewed and Citrix 6.5 fail over testing has been undertaken.</p> <p>Update since January Committee Detailed test plan is being produced and will be signed of by Information Technology Management Team at the end of March.</p> <p>Internal data centres have moved to externally hosted sites which are in-line with SAS-70 and/or BS-25999. The final data centre move was able to be moved forward.</p>	<p>March 2014</p> <p>March 2014</p> <p>Complete</p>