Public Document Pack

Business Overview and Scrutiny Committee

Date:	**Tuesday, 12 July 2016**
Time:	**6.00 pm**
Venue:	Committee Room 1 - Wallasey Town Hall

Contact Officer:	Andrew Mossop
Tel:	0151 691 8501
e-mail:	andrewmossop@wirral.gov.uk
Website:	http://www.wirral.gov.uk

AGENDA SUPPLEMENT

7. DISASTER RECOVERY SCRUTINY REVIEW (Pages 1 - 28)

This page is intentionally left blank

WIRRAL

BUSINESS OVERVIEW & SCRUTINY COMMITTEE
TUESDAY 12TH July 2016

REPORT TITLE:	**IT DISASTER RECOVERY**
REPORT OF:	**MEMBERS OF THE IT DISASTER RECOVERY SCRUTINY REVIEW PANEL**

REPORT SUMMARY

This report (included as Appendix 1) provides the findings and recommendations emanating from the IT Disaster Recovery Scrutiny Review.

Members of the Business Overview and Scrutiny Committee are requested to consider the contents of this report and support the recommendations arising from this review.

RECOMMENDATION/S

1. Members of the Committee are requested to support the contents and recommendations of the Scrutiny Report, 'IT Disaster Recovery';

2. The report be referred to the next appropriate Cabinet meeting;

SUPPORTING INFORMATION

1.0 REASON/S FOR RECOMMENDATION/S

The Scrutiny Review report is subject to review by Members of the Committee and is required to be referred to Cabinet for consideration.

2.0 OTHER OPTIONS CONSIDERED

Not Applicable

2.0 BACKGROUND INFORMATION

3.1 A Report to the Transformation & Resources Policy & Performance Committee on 21 September 2015 revealed that Wirral Council's IT infrastructure had suffered from underinvestment for a number of years. It emerged that there was some uncertainty regarding the existence of a comprehensive and up to date IT disaster recovery plan for Wirral Council. Disaster Recovery had also been identified as a significant risk in the Council's risk register.

3.2 Committee Members agreed to carry out a task & finish review of the Council's IT disaster recovery arrangements. Five Members of the Committee volunteered to undertake this work; Cllr Chris Carubia, Cllr Steve Foulkes, Cllr Leah Fraser, Cllr John Salter and Cllr Adam Sykes.

3.3 At the first meeting of the Review Panel, it was agreed Cllr Adam Sykes would be the Chair of the Panel. The review was conducted over a small number of meetings held with appropriate officers and information was provided as requested by the Review Panel to allow detailed question and answer sessions to be carried out.

3.4 The Panel's objectives in doing this work were to receive assurances that the Council establishes effective IT disaster recovery arrangements and takes steps to mitigate risks relating to IT disaster recovery highlighted in the Council's risk register. It was also an aim of the Panel to raise the profile of IT disaster recovery across the Council.

3.5 The Review Panel commended the Council on a number of projects undertaken to increase IT resilience and reduce risks of IT failure via the data centre project and other associated work. The Review Panel believes that it is important to ensure progress continues with these projects in order to enhance and update the Council's IT infrastructure following a period of underinvestment.

3.6 This report provides a number of recommendations which the Review Panel believes will assist the Council in providing a suitable IT platform to support delivery of the Wirral Plan pledges.

4.0 FINANCIAL IMPLICATIONS

Not Applicable

5.0 LEGAL IMPLICATIONS

Not Applicable

6.0 RESOURCE IMPLICATIONS: ICT, STAFFING AND ASSETS

Not Applicable.

7.0 RELEVANT RISKS

Not Applicable

8.0 ENGAGEMENT/CONSULTATION

Not Applicable

9.0 EQUALITY IMPLICATIONS

This report is for information to Members and there are no direct equality implications.

REPORT AUTHOR: **Patrick Torpey**
Scrutiny Support
0151 691 8381
email: patricktorpey@wirral.gov.uk

APPENDICES:
Appendix 1: IT Disaster Recovery Scrutiny Review Report

REFERENCE MATERIAL
SUBJECT HISTORY (last 3 years)

Council Meeting	Date

This page is intentionally left blank

IT Disaster Recovery
Scrutiny Review

A report produced by

The Transformation and Resources Policy & Performance Committee

FINAL REPORT
June 2016

WIRRAL BOROUGH COUNCIL

IT Disaster Recovery Scrutiny Review

FINAL REPORT

1 EXECUTIVE SUMMARY

1.1 It is good practice for large organisations to have in place effective and up to date IT disaster recovery plans. These plans are designed to provide a detailed overview of an organisation's key IT systems and an assessment of risks and potential threats to its IT infrastructure. IT Disaster recovery plans should also provide step-by step procedures for recovering and restoring key systems to full operation, minimising disruption to services in the event of an IT failure. Plans should be reviewed and tested annually and key system owners across an organisation should have a good understanding of the impact an IT disaster would have on their systems and the effect this would have on service delivery. The Review Panel considered a number of IT disaster recovery documents from other local authorities as part of this review.

1.2 In reviewing the data, it was clear to the Panel that Wirral does not have a current, fit for purpose IT disaster recovery plan. In comparison with industry good practice and other local authorities, Wirral performs poorly in this regard. The IT disaster recovery plan presented to the Review Panel was out of date and did not provide a comprehensive overview of the Council's IT infrastructure. The plan did not outline steps to take to recover key systems in the event of an IT disaster and it was clear to the Review Panel that this plan had not been reviewed or tested for a number of years. It was reported that Wirral Council's IT infrastructure had suffered from underinvestment for a number of years. The Council's Corporate Risk Register (2015) stated that there was a risk of a sustained catastrophic failure in the Council's IT systems and improvements to Council's IT disaster recovery arrangements were required, alongside a programme of IT improvements.

1.3 A number of projects in progress are expected to greatly increase the IT resilience of the Council and mitigate risks associated with a catastrophic IT failure. The Review Panel were informed of the Data Centre Project. This project aims to source a suitable partner and location to house one of the Council's two data centres. Wirral Council currently houses its primary and back-up data centres in the same location and this co-location is not considered to be good practice. It is recommended that an organisation's primary and back-up data centres are located at different geographical sites to reduce the risk of IT failure in the event of loss of power or communications at one location. A suitable partner and site have been identified which would provide a clear geographical divide between data centres. Discussions with the partner are ongoing and further testing and preparation is required to ensure that the migration of one of the data centres can take place. If the partnership goes ahead it is expected that the data centre will be set up by April 2017.

1.4 Industry good practice suggests that IT disaster recovery plans should be created using business impact assessments from around an organisation. A business impact assessment evaluates the effect an IT disaster would have on critical IT systems and service delivery. A business impact exercise carried out by the Review Panel attempted to gauge the level of staff understanding of IT systems around the Council

and the consequences an IT failure would have on services. The responses revealed a need for training to take place to raise awareness of and improve the general understanding of the effects of IT disaster around the Council.

1.5 The review panel were concerned that the IT disaster recovery arrangements of partners with linked IT systems, or who delivered services on behalf of the council was not known. It was agreed that the Council should seek assurances from all partners of their IT disaster recovery arrangements and incorporate this into discussions with future partners.

1.6 Overall the Panel were impressed with a number projects underway or completed which will increase IT resilience and reduce the risks of IT disaster. The Review Panel believes that it is important to ensure progress continues with these projects in order to enhance and update the Council's IT infrastructure following a period of underinvestment. However, it was felt that there is a need for this work to be consolidated into a comprehensive IT DR plan for the, to provide clarity in the steps required to recover key systems as quickly as possible in the event of a disaster. More could be done through training to raise staff awareness of IT disaster recovery and the impact on services across the Council. Additionally, consideration should be given to the disaster recovery arrangements of current and potential partners, particularly if their systems are linked to the Council, or if they are providing an IT related service on behalf of the Council. A number of recommendations to this effect are set out below.

Recommendations

1) IT Services should develop and document a comprehensive IT Disaster Recovery Plan in conjunction with key officers from the Council. It should be ensured that:

   i) The plan is consistent with industry best practice;
   ii) Roles and responsibilities of those involved in implementing the plan are fully detailed;
   iii) All critical IT systems are documented and include appropriate recovery time objectives;
   iv) A full test of the plan is carried out to ensure its effectiveness and to ensure that key staff are aware of their responsibilities and actions in a disaster recovery situation; and
   v) A copy of the plan is held in more than one secure place (including off-site) for resilience purposes.

2) To provide ongoing assurance that the IT Disaster Recovery Plan remains current and fit for purpose, IT Services should ensure that the plan is reviewed, tested and updated annually or immediately following the installation of key IT systems.

3) A report should be presented to the Business Overview and Scrutiny Committee to update Members on the progress towards delivery of the Council's data centres within the next six months.

4) The provision of appropriate training for senior officers should be explored as part of a drive to increase understanding and awareness of the impact of IT system failure and business continuity management. As part of the training, consideration should be given to developing appropriate scenario based exercises which could be carried out without a disaster recovery plan in place.

5) Where partners provide and administer IT systems on behalf of the council, assurance should be obtained that effective disaster recovery plans are in place which meet the council's defined standards.

2. INTRODUCTION

At the meeting of the Transformation and Resources Policy & Performance Committee on 21 September 2015, Members proposed a review of the Council's IT Disaster Recovery Arrangements. A Scrutiny Review Panel consisting of five Members of the Committee was established and a single evidence gathering session was planned. The purpose of the review was for the Review Panel to receive assurances that the Council is taking the appropriate steps to ensure that effective IT Disaster Recovery arrangements are put in place.

3. ORIGINAL SCOPE AND METHODOLOGY

3.1 Scope

A scoping meeting was convened with the Review Panel and the Information Technology Infrastructure Manager in October 2015. The agreed scoping document is included as Appendix 1. It was agreed that the focus of the review would concentrate on the following key areas:

1. To understand what constitutes a disaster for the Council.
2. To provide assurance that the Council establishes effective disaster recovery arrangements.

3.2 Methodology

To provide the Review Panel with a comprehensive overview of the principles of disaster recovery, a briefing paper was prepared by the Scrutiny Support Officer. This briefing paper provided a definition of IT disaster recovery to assist in developing the scope of the Task & Finish scrutiny review.

It was determined that the scrutiny review would be held over a single evidence session with the focus being maintained on the Council's progress in implementing a number of projects which would greatly increase the ICT resilience of the organisation. To support Members in these sessions, the Review Panel requested or it was suggested by officers that further information and specific data analysis should be considered as part of the review. Information / analysis included:

- Examples of ICT Disaster Recovery Plans from other authorities
- The existing Wirral Council IT Disaster Recovery Plan
- Results of an internal impact analysis exercise

4. FINDINGS AND RECOMMENDATIONS

4.1 What is an IT Disaster?

IT disasters are rare but when they do occur they can have devastating consequences for an organisation. Key services will quickly come to a standstill in the event of a prolonged computer breakdown. As local authorities increasingly rely on computerised systems to manage services and store information, their vulnerability to the effects of catastrophic IT failure has also increased. An IT disaster can be defined as the loss or damage of part of, or an authority's entire IT infrastructure, which would have a significant business impact on the authority.

What is an IT Disaster Recovery Plan?

An information technology (IT) disaster recovery (DR) plan provides a structured approach for responding to unplanned incidents that threaten an IT infrastructure, which includes hardware, software, networks, processes and people. Protecting an organisation's investment in its technology infrastructure, and protecting an organisation's ability to conduct business are the key reasons for implementing an IT disaster recovery plan.

IT disaster recovery plans provide step-by-step procedures for recovering disrupted systems and networks, and help an organisation resume normal operations. The goal of these processes is to minimise any negative impacts to operations. An effective IT disaster recovery plan identifies critical IT systems and networks; prioritises their recovery time; and outlines the steps needed to restart, reconfigure, and recover them. A comprehensive IT disaster recovery plan also includes all the relevant supplier contacts, sources of expertise for recovering disrupted systems and a logical sequence of action steps to take for a smooth recovery.

Assuming organisations have completed risk assessments and have identified potential threats to IT infrastructure, the next step is to determine which infrastructure elements are most important to the performance of the organisation's business.

According to industry good practice, the following summarises the ideal structure for an IT disaster recovery plan:

Develop the contingency planning policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
Conduct the business impact analysis (BIA). The business impact analysis helps to identify and prioritise critical IT systems and components.
Identify preventive controls. These are measures that reduce the effects of system disruptions and can increase system availability and reduce costs for contingencies.
Develop recovery strategies. Thorough recovery strategies ensure that the system can be recovered quickly and effectively following a disruption.
Develop an IT contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system.

Plan testing, training and exercising. Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.
Plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements

Evidence of IT Disaster Recovery plans in other Local Authorities
In preparation for this review, officers researched other local authorities' approaches to IT disaster recovery. A number of IT disaster recovery plans and reports from other authorities were examined. The Review Panel was impressed by a number of features of these plans, such as: Thurrock Council's disaster recovery plan which nominated Disaster Management and Service Delivery Teams with defined responsibilities. The Thurrock plan also included a step by step description of disaster recovery arrangements including command centre & backup centre locations and requirements. An IT Disaster Recovery Internal Audit Report by Aberdeen City Council in 2015 recommended that an annual walkthrough of disaster recovery plans by those involved in their operation should take place to identify any weaknesses and to ensure that key people are aware of their responsibilities and actions in a disaster recovery situation.
A table summarising the main features of each document reviewed is included in Appendix 2.

In reviewing these plans, the Review Panel identified a number of features which could be included in an IT disaster recovery plan for Wirral Council, including:

- An overview of IT infrastructure and identification of key services.
- Identification of key staff and their roles and responsibilities in a disaster recovery situation.
- Annual testing of systems and plans.

4.2 Current IT Disaster Recovery Arrangements in Wirral

During a report on IT Services Business Continuity and Disaster Recovery to the Transformation and Resources Policy & Performance Committee on 21 September 2015, it was reported that Wirral Council's IT infrastructure had suffered from underinvestment for a number of years. A number of risks and issues related to IT reliability, resilience and availability needed to be addressed. Committee Members were informed that a series of projects designed to deliver a fit for purpose IT infrastructure were underway.

Despite this it emerged that there was some uncertainty regarding the existence of a comprehensive and current IT disaster recovery plan for Wirral Council. In preparation for this review, a set of documents were presented to the Review Panel by IT services as the Council's IT disaster recovery plan. The majority of the documents were dated 2004 or 2005. The documents included an overview of the Council's machine rooms including risks and controls, lists of IT applications, site security information and building power down arrangements. A Business Resilience Model document contained a number of system maps and described the process, impact and response in the event of different IT failure scenarios. Finally, the plan was also comprised of a

series of emails which provided names, contact details and roles and responsibilities of key staff. It was noted by the Review Panel that many of the named staff were no longer working at the Council. Although the plan contained some features expected in a disaster recovery plan, the documents were at least ten years old and were therefore unlikely to be relevant to much of today's IT infrastructure. In its presented format, the plan did not provide a comprehensive picture of the Council's IT estate and did not provide clarity regarding the actions to be taken in the event of an IT disaster. The Review Panel concluded that the IT disaster recovery plan presented could not be considered as a current or fit for purpose disaster recovery plan for the Council.

An extract from the Council's Corporate Risk Register from November 2015 (below) highlights the importance of having in place effective disaster recovery arrangements in order to ensure that the Council is suitably prepared in the event of an IT failure. A number of projects are underway which will improve the Council's IT resilience and greatly mitigate the risks and impact of an IT disaster. These projects are described in more detail later in this report. However, the absence of an overarching Council wide IT disaster recovery plan clearly presents a significant risk to the Council in terms of its ability to co-ordinate and implement an effective response and recovery in the event of a major IT disaster.

Risk Description	Lead Officer	Potential Impact	Principal Controls (Existing)	Current Risk Scores			Principal Controls (Planned)	Responsibility and Date
				Impact	Likelihood	Total		
A sustained catastrophic failure in the Council's ICT systems ***(PH3)***	Strategic Director Trans & Resources	Huge impact on service delivery, possibly affecting the public (especially the vulnerable) damage to reputation, breach of contracts, inability to share data with partners and government	• Second machine room • Fire suppressant system in rooms • Additional backup /security based at Cheshire Lines implemented	**5**	**2**	**10**	• Implement programme of ICT improvements • Improve IT disaster recovery arrangements	• Strategic Director – Transformation & Resources • Strategic Director – Transformation & Resources (ongoing)

After reviewing details of IT disaster recovery plans in other authorities and considering the Council's own risk rating concerning its existing disaster recovery arrangements, the Review Panel was concerned that no clear and up to date IT disaster recovery plan is in place. The Review Panel concluded that the Council should prioritise the development of a comprehensive IT disaster recovery plan. Learning from industry best practice and existing examples of IT disaster recovery plans, the Review Panel further concluded that Wirral's IT disaster recovery plan should contain a number of features which, it is hoped, would ensure clarity across the organisation regarding responsibilities of key staff and raise awareness of key IT systems. It is also the conclusion of the Review Panel that the plan should be tested for effectiveness prior to its implementation.

Recommendation 1. IT Services should develop and document a comprehensive IT Disaster Recovery Plan in conjunction with key officers from the Council. It should be ensured that:

- ***i) The plan is consistent with industry best practice;***
- ***ii) Roles and responsibilities of those involved in implementing the plan are fully detailed;***
- ***iii) All critical IT systems are documented and include appropriate recovery time objectives;***
- ***iv) A full test of the plan is carried out to ensure its effectiveness and to ensure that key staff are aware of their responsibilities and actions in a disaster recovery situation; and***
- ***v) A copy of the plan is held in more than one secure place (including off-site) for resilience purposes.***

A key feature of all IT disaster recovery plans viewed by the Review Panel was annual testing. As Wirral's IT disaster recovery plan had been allowed to become obsolete due to a lack of testing and review, and in line with the pace of change in the area of IT, the Review Panel concluded that for Wirral to have an effective and up to date IT disaster recovery Plan, it should be tested and reviewed on an annual basis.

Recommendation 2. To provide ongoing assurance that the IT Disaster Recovery Plan remains current and fit for purpose, IT Services should ensure that the plan is reviewed, tested and updated annually or immediately following the installation of key IT systems.

4.3 IT Projects

The Review Panel was informed of a number of significant IT projects underway designed to remove risks associated with historical underinvestment in the IT infrastructure.

Data Centre Project

The most significant project currently underway is the data centre project.

Data centres are facilities used to house an organisation's physical IT infrastructure assets, such as hardware, servers, network and communications equipment. Data centres are designed to protect IT systems and ensure high levels of availability of those systems. Industry best practice suggests that there should be a primary data centre and a secondary or back-up data centre, which replicates the primary data centre. Both centres should have sufficient capacity, storage, data and communications services to run all live Council IT services independently in the event of a data centre loss. Wirral Council currently houses both data centres in the Treasury Building (one in each computer room). It was explained to the Review Panel that co-location of data centres in close proximity on the same site is not considered to be good practice and represents a business risk. A geographical divide between data centres is recommended, to provide increased IT resilience and mitigate the risk of IT

failure in the event of a major incident involving the loss of power or communications at one site.

The project is exploring options to relocate one of the council data centres to an off-site location. Discussions with a local public sector organisation are at an advanced stage. It is proposed to relocate one of Wirral's data centres to a building in Liverpool which currently houses this organisation's server rooms. Further testing is to take place and some enhancements and modifications would be required at the proposed site to increase capacity and functionality to ensure that there is sufficient capability to run all of the Council's computing facilities out of one data centre.

Officers are confident that the proposed site, subject to minor modifications, is an appropriate environment to host one of Wirral's data centres. The physical security of the site is already superior to existing arrangements in the Treasury Building and Wirral's equipment would have an additional layer of security. Staff access control protocols would also be agreed as part of the contract, which would allow Wirral staff to access the site at any time.

Should the proposal go ahead, Wirral's two data centres would be separated by the River Mersey providing a good geographical divide. The data centres would run from different power and communications supplies, representing good risk management in case of full loss of power on either side of the river.

This project will require some initial set-up costs (associated with physical and IT preparations at the new and existing sites) and will involve an annual running cost. Officers are confident however that this would be financially prudent for the council as other commercial options explored to date would involve significantly higher set up and annual running costs.
The proposed contract length of five years with an option to renew, works well for Wirral Council as it provides some years of stability whilst allowing a break after five years if technological changes provide other opportunities, such as a cloud based solutions.

There is cautious optimism over this partnership as it is believed to represent a good deal for both parties and in line with moves towards shared services.

Once contracts have been signed the Council will enter into a tendering and procurement phase to appoint IT specialists with experience and expertise in this field. Moving infrastructure on this scale creates a number of risks, both known and unknown. Consequently specialist IT support will be required to ensure that the migration of services to the new data centre is appropriately planned, risk assessed and delivered.

Assuming that the project continues according to plan, completion is expected by April 2017. If the project is delivered successfully, IT officers believe the project is of significant importance in terms of increasing IT resilience and reduction of risk, that

the risk rating attached to this issue in the corporate risk register would be downgraded.

Target Operated Environment
A project to refresh the Council's back office Windows infrastructure (Targeted Operating Environment) is currently running. There are up to 600 virtual/physical servers running on an end of life Microsoft operating system. These servers are currently in an extended support period for security updates from Microsoft which is due to expire in July 2016. The project will involve a migration of these systems to the most up to date version of the Microsoft Windows Server which has a longer life span and will require fewer annual upgrades than the existing version.

The Chief Information Officer explained that IT in local government is more complex than similar sized commercial sector organisations due to the high number of separate applications running. There would be very few commercial organisations with 375 separate IT applications running. This project will identify each application and then map processes and system requirements from servers to the user screen. Once this is understood and documented, this will allow some rationalisation of systems and may reduce duplication and costs. Suppliers can also be approached regarding running applications in a virtual environment.

Office 365 Project
Another project underway is the Office 365 project. There are 5000 email accounts at the council containing 20tb of data. This will remove the Council's reliance on a legacy email infrastructure and provide a more agile and robust email system.

The Review Panel was reassured that these projects, when complete, will significantly increase the Council's resilience against IT disaster. In particular, it was agreed that the delivery of the data centre project alone would remove a considerable risk associated with housing the Council's data in a single location. Consequently, the Review Panel request to be kept informed of progress regarding the data centre project at regular intervals until its successful completion.

Recommendation 3. A report should be presented to the Business Overview and Scrutiny Committee to update Members on the progress towards delivery of the Council's data centres within the next six months.

4.4 Officer Awareness of IT Disaster Recovery

Industry good practice suggests that IT disaster recovery plans should be informed by business impact analysis exercises, usually carried out at department or service level. Business impact analysis is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster.

In order for the Review Panel to appreciate the extent to which officers around the Council are aware of the impact an IT failure would have on their ability to deliver

services, an impact analysis exercise was carried out in advance of the evidence session. Key officers from services around the Council were contacted and asked to provide details of the IT systems / applications that they used and to provide a summary of the business processes that would be affected through short and prolonged IT systems failure. They were also asked to describe the impact this would have on service delivery. The Review Panel received responses from 18 service areas around the Council. A full table of responses was collated and presented to the Review Panel and officers.

In relation to the responses from managers across the Council on the impact of IT failure for their service, the Chief Information Officer agreed that there is a clear need to work with colleagues to improve understanding of business impact. In particular it was suggested that colleagues should have a clearer understanding of how long their services could operate without key systems. In IT disaster recovery terminology, there are two key issues to understand:
Recovery Time Objective: The length of time a service can operate without a key system before major disruption to service is caused.
Recovery Point Objective: The amount of data a service can afford to lose without causing a major disruption to service.

The Review Panel queried if this was the first time that the issue of business impact analysis had been explored widely at Wirral. Officers acknowledged that they had not previously conducted exercises like this to measure colleagues understanding of business impact. It was further acknowledged that in conducting this research, the Review Panel has identified a gap in current practices and a need to work with and educate colleagues to better understand the business impact a major IT disruption would have on their services. Only after this could valuable business impact analyses take place around the organisation.

When asked if the council possessed the resources and expertise to train colleagues on the area of business impact, officers acknowledged that the expertise does not currently exist to conduct this and training would need to be procured.

The Review Panel concluded that the Council may wish to explore the possibility of utilising the expertise of specialist IT providers to provide training to raise awareness and understanding of business impact. The exploration and negotiation of free Business Impact Analysis training / workshops with specialist IT providers could be built in to the tender and procurement process for the infrastructure transfer to the new data centre.

The Review Panel also suggested that in line with good practice and other IT disaster recovery plans, and to ensure that business continuity and impact is given sufficient prominence around the Council, annual scenario training for managers should take place. The use of scenario training as a means to regularly test managers' response to a range of different IT failure scenarios should be explored by the Council. It is the Review Panel's opinion that annual scenario training could be implemented quickly

and the outputs of these sessions could be used to inform the development of the Council IT disaster recovery plan.

Recommendation 4. The provision of appropriate training for senior officers should be explored as part of a drive to increase understanding and awareness of the impact of IT system failure and business continuity management. As part of the training, consideration should be given to developing appropriate scenario based exercises which could be carried out without a disaster recovery plan in place.

As the Council moves more towards partnership working and commissioning of services, it can be expected that more partner IT systems will be linked to the Council's infrastructure. It can also be expected that partners may use IT systems to deliver services on the Council's behalf.

The Review Panel queried the extent to which the disaster recovery arrangements of partner organisations were documented internally. The Review Panel also asked if the risks associated with linked IT systems were routinely assessed. It was acknowledged by officers that any such arrangements would reside at department / service level and there was no central log of such information. It was further explained that officers were not aware of the disaster recovery arrangements of other organisations.

It was agreed that a serious IT system failure of a partner organisation had the potential to affect services delivered to Wirral residents on behalf of the Council. This also represented a reputational risk to the Council. The Panel concluded that assurances over IT disaster recovery arrangements should be sought from all partners engaged in the delivery of services using IT systems. This consideration should also form part of the tender process for future partnerships which involve shared, or linked IT systems.

Recommendation 5. Where partners provide and administer IT systems on behalf of the council, assurance should be obtained that effective disaster recovery plans are in place which meet the council's defined standards.

5. CONCLUSION

It is clear to the Review Panel that it would be unacceptable for the Council to continue without a comprehensive IT disaster recovery plan in place. A plan should be implemented and should contain amongst its contents a comprehensive list of key IT systems, an assessment of risk and the arrangements in place both to mitigate risks and to recover IT systems in the event of an IT failure.

There needs to be wider staff understanding of the impact of IT disaster on key systems and the effect this would have on services across the Council. It is important that key system owners have an understanding of disaster recover principles, including business impact analysis as a Council wide disaster recovery plan must be informed by business impact assessments from around the organisation. Staff training to raise awareness of disaster recovery and business impact is therefore important.

The Review Panel congratulates the Council's on steps taken to increase IT resilience and reduce risks of IT failure via the data centre project and other associated work. The Review Panel believes that it is important to ensure progress continues with these projects in order to enhance and update the Council's IT infrastructure following a period of underinvestment. The Review Panel also believes that by implementing these proposed recommendations, it will assist the Council in providing a suitable IT platform to support delivery of the Wirral Plan pledges.

6. MEMBERS OF THE REVIEW PANEL

Chair's Statement:

"As we began this Review, Wirral Borough Council had experienced some incidents of down-time due to IT systems failure. The reliance of the organisation on IT, as any other today, can cause a significant operational risk, as outlined by both internal and external audits. Whilst the council's IT departments have been taking steps to update the overall infrastructure of the organisation's systems, the need for highlighting disaster recovery as a priority had become clear.

This Scrutiny Panel has investigated the current disaster recovery position of the Council, and I would like to thank the officers involved for their engagement in this process.

The recommendations that have come out of this investigation aim to help to improve the Council's response to disaster recovery, through implementation of a full disaster recovery planning and testing regime. Secondly, it was found to be important that the potential impact was outlined to staff across the council, with better training and clear accountability. Finally, with increased partner working by the Council, it was recommended that serious thought be given to disaster recovery, when working with outside organisations, ensuring that they meet with the standards that the council would expect."

Review Panel Membership

Councillor Adam Sykes (Chair)

Councillor Chris Carubia

Councillor Steve Foulkes

Former Councillor Leah Fraser

Former Councillor John Salter

This Report was produced by the ICT Disaster Recovery Scrutiny Review Panel
(which reports to the Transformation and Resources Policy & Performance Committee)

Appendix 1:

Draft Scope Document

Review Title: Disaster Recovery
Date: 29th October 2015

1. Contact Information:	
Scrutiny Panel Chair: Councillor Adam Sykes adamsykes@wirral.gov.uk **Panel members:** Councillor Steve Foulkes Stevefoulkes@wirral.gov.uk Councillor Chris Carubia Christophercarubia@wirral.gov.uk Councillor Leah Fraser leahfraser@wirral.gov.uk Councillor John Salter johnsalter@wirral.gov.uk	**Scrutiny Officer(s):** Michael Lester Scrutiny Support Officer michaellester@wirral.gov.uk 691-8628 **Departmental Link Officers:** Mike Zammit Chief Information Officer mikezammit@wirral.gov.uk 666-3029 Phil Moss IT Infrastructure Manager philipmoss@wirral.gov.uk 666-3868
Other Key Contacts: Appropriate IT Officers (To be determined)	

2. Review Aims:

Which Wirral Plan Pledge does this review relate to?
Scrutiny Review is linked to enabling projects as disaster recovery underpins the delivery of the Wirral Plan.

What are the main issues?

- There is a Disaster Recovery Plan but this has not been updated for ten years resulting in all or parts of it being ineffective.
- Disaster Recovery has been identified as a significant risk in the Council's risk register.
- It is not clear what business continuity plans are in place to ensure services can continue in the event of a disaster. There is a legal requirement to have business continuity plans.

The Panel's objectives in doing this work:

- To understand what constitutes a disaster for the Council
- To provide assurance that the Council establishes effective disaster recovery arrangements

The desired outputs/outcomes:

- The profile of disaster recovery is increased across the Council.
- Risks relating to disaster recovery in the Council's risk register can be mitigated further.

3. Review Approach

How will the Panel engage with the Executive?

- The findings and recommendations arising from the review will be discussed with the Portfolio Holder.
- The final report will be referred to Cabinet for consideration of the recommendations

Who will the Panel be trying to influence as part of its work?

- Senior Managers
- Cabinet

Duration of review?
It is anticipated that this will be short review conducted over a single evidence session. An additional session can be scheduled if required.

Extra resources needed? Would the investigation benefit from the co-operation of an expert witness?
Not identified at this stage

4. Sources of Evidence:

Secondary information (background information, existing reports, legislation, central government documents, etc.).

- Disaster Recovery Committee Report
- Copy of the existing Disaster Recovery Plan
- Information around the legal requirements for DR and business continuity.
- Copy of the risk register (risk relating to the review)
- Details of off-site storage and all other mitigations in place.
- Background information on Public Services Network

Primary/new evidence/information

- Feedback from Senior Managers on impact of IT going down and details on what services would be affected (including what business continuity arrangements are in place to mitigate this).
- Details of security breaches relevant to disaster recovery.
- Details of off-site storage and all other mitigations in place.

Who can provide us with further relevant evidence? (Cabinet portfolio holder, officer, service user, general public, expert witness, etc.).
council officers to include:
Council officers (See Section 4)

What specific areas do we want them to cover when they give evidence?
See Section 4

What processes can we use to feed into the review? (site visits/observations, face-to-face questioning, telephone survey, written questionnaire, etc.).

- Face to face questioning
- Written questionnaire

In what ways can we involve the public and at what stages? (consider whole range of consultative mechanisms, local committees and local ward mechanisms).
Not applicable at this stage

Should we involve the Press & Public Relations Team at any stage of the review? (Homepage news release, press releases etc.)
Not applicable

Appendix 2:

Existing Disaster Recovery Arrangements

Authority	Disaster Recovery Arrangements	Features	Date
Merton	Strategic Business Continuity Plan merton strategic business continuity plan 2014.pdf	• Section on Disaster Recovery with DR Plan as Appendix. • DR Plan written using departments Business Impact Assessments (BIA). • Stated aim of DR Plan is to have all critical IT services restored within 24 hours.	April 2014
Dartmoor	Disaster Recovery & Business Continuity Plan for ICT Services Dartmoor ICT-Disaster-Recovery-Plan-Rev-0810.pdf	• Overview of ICT infrastructure and key services • Detailed risk assessment and recovery plan. • Section on testing of systems.	August 2010 (reviewed annually)
Thurrock	ICT Service Disaster Recovery Plan for Serco Contract Thurrock Disaster Recovery Plans for IT.pdf	• Nomination of Disaster Management and Service Delivery Teams with defined responsibilities. • Step by step description of DR arrangements including Command Centre & Backup Centre locations and requirements • List of critical business services • Key vendor and supplier contacts.	Jan 2015

Recommendations / Findings from Review and Audit of Disaster Recovery Arrangements

Authority	Source	Main Findings / Recommendations	Date
Worcestershire	Internal audit to evaluate the effectiveness of the processes and controls surrounding the councils ITDR management. Worcestershire Disaster Recovery.pdf	The audit returned the following findings: • The current ITDR arrangements are limited in capability should an event such as fire cause damage to the IT infrastructure • There is no formal agreement in place to procure replacement servers in a disaster situation beyond standard Council procurement processes. • It is noted that with the outsourcing of IT Services completing next calendar year, it is important for the County Council to consider risks for ITDR in the current state, and future state once the outsourcing has migrated to the new provider. Recommendations included: • Develop a recovery sequence for a major incident occurring at either of the main server rooms to coordinate recovery of IT systems against worst case scenarios. • Senior Management to consider options for ITDR including: (a) Whether to accept the current limited ITDR capability; (b) Further invest in ITDR capability to enhance recovery times. Options for consideration could potentially include: - Upgrade of County Hall server room to install fire suppression system; - Upgrade of Wildwood server room to act as a ITDR site; - 3rd party contract for disaster recovery, potentially including data centre space and infrastructure	Aug 2014
Rochdale	Report to Overview & Scrutiny Committee outlining current ICT DR provision, recommending a course of actions to meet audit requirements.	The report delivered the following finding: • The current level of IT DR maturity is level 1 (level 5 being highest). “Many systems and processes are undocumented and uncontrolled. Documentation about system resilience is	Oct 2011

	Rochdale Disaster Recovery Report.pdf	also limited" Recommended actions to rectify this included: • Creation of an IT Disaster Recovery plan which will meet minimum requirements • A risk assessment detailing all remaining risks and mitigating actions • A report making recommendations for longer term improvements including an options appraisal based on service requirements, cost and acceptable risk.	
Aberdeen	IT Disaster Recovery Internal Audit Report Aberdeen City Council DRIT Report FINAL.pdf	The audit identified four low-risk findings: • There has been no formal review, of the ICT Disaster Recovery Plan, to ensure that plans are an accurate representation of current practice and considers all critical systems; • Staff involved in disaster recovery are not provided with any specific training; • There are variations in the robustness of Disaster recovery testing across outsourced IT systems and DR responsibilities are not reflected in the DR Plan. • Not all departments provide staff to assist with the data centre DR testing. The following remedial actions were recommended: • Future updates of the ICT Disaster Recovery Plan will be scheduled annually and after any significant changes to systems, and will incorporate changes to current practice, levels of system criticality and lessons learned from any Disaster Recovery exercises. • ICT will undertake an annual walkthrough of the plans by those involved in their operation to try and identify any weaknesses and to ensure that key people are aware of their responsibilities and actions in a disaster recovery situation (a table top review). • DR processes will be updated and tested for outsourced IT systems where they are not robust and with the support of	Jan 2015

		the providers, as per their contractual arrangements. • System Owners should consider and document the risk of not testing their systems during disaster recovery testing of the data centre. IT will ensure that they request and retain copies of risk assessments prior to all future IT Disaster Recovery exercises.	

This page is intentionally left blank