Worcestershire County Council

Agenda

Audit and Governance Committee

Friday, 12 September 2014, 10.00 am
County Hall, Worcester

This document can be made available in other formats (large print, audio tape, computer disk and Braille) on request from Democratic Services on telephone number 01905 728713 or by emailing democraticServices@worcestershire.gov.uk

If you can not understand the contents of this document and do not have access to anyone who can translate it for you, please contact 01905 765765 for help.

বাংলা। আপনি যদি এই দলিলের বিষয়বস্তু বুঝতে না পারেন এবং আপনার জন্য অনুবাদ করার মত পরিচিত কেউ না থাকলে,অনুগ্রহ করে সাহায্যের জন্য 01905 765765 নম্বরে যোগাযোগ করুন। *(Bengali)*

廣東話。如果您對本文檔內容有任何不解之處並且沒有人能夠對此問題做出解釋，請撥打 01905 765765 尋求幫助。*(Cantonese)*

普通话。如果您对本文件内容有任何不解之处并且没有人能够对此问题做出解释，请拨打 01905 765765 寻求帮助。*(Mandarin)*

Polski eżeli nie rozumieją Państwo treści tego dokumentu i nie znają nikogo, kto mógłby go dla Państwa przetłumaczyć, proszę zadzwonić pod numer 01905 765765 w celu uzyskania pomocy. *(Polish)*

Português. Se não conseguir compreender o conteúdo deste documento e não conhecer ninguém que lho possa traduzir, contacte o 01905 765765 para obter assistência. *(Portuguese)*

Español. Si no comprende el contenido de este documento ni conoce a nadie que pueda traducírselo, puede solicitar ayuda llamando al teléfono 01905 765765. *(Spanish)*

Türkçe. Bu dokümanın içeriğini anlayamazsanız veya dokümanı sizin için tercüme edebilecek birisine ulaşamıyorsanız, lütfen yardım için 01905 765765 numaralı telefonu arayınız. *(Turkish)*

اردو. اگر آپ اس دستاویز کی مشمولات کو سمجھنے سے قاصر ہیں اور کسی ایسے شخص تک آپ کی رسائی نہیں ہے جو آپ کے لئے اس کا ترجمہ کرسکے تو، براہ کرم مدد کے لئے 01905 765765 پر رابطہ کریں۔ *(Urdu)*

کوردی سۆرانی. ئەگەر ناتوانی تێبگەی لە ناوەرۆکی ئەم بڵگەیە و دەستت بە هیچ کەس ناگات کە وەیگێڕێتەوە بۆت، تکایە تەلەفۆن بکە بۆ ژمارەی 01905 765765 و داوای ڕێنوێنی بکە. *(Kurdish)*

ਪੰਜਾਬੀ। ਜੇ ਤੁਸੀਂ ਇਸ ਦਸਤਾਵੇਜ਼ ਦਾ ਮਜ਼ਮੂਨ ਸਮਝ ਨਹੀਂ ਸਕਦੇ ਅਤੇ ਕਿਸੇ ਅਜਿਹੇ ਵਿਅਕਤੀ ਤੱਕ ਪਹੁੰਚ ਨਹੀਂ ਹੈ, ਜੋ ਇਸਦਾ ਤੁਹਾਡੇ ਲਈ ਅਨੁਵਾਦ ਕਰ ਸਕੇ, ਤਾਂ ਕਿਰਪਾ ਕਰਕੇ ਮਦਦ ਲਈ 01905 765765 'ਤੇ ਫ਼ੋਨ ਕਰੋ। *(Punjabi)*

Find out more online:
www.worcestershire.gov.uk

worcestershire county council

DISCLOSING INTERESTS

There are now 2 types of interests:
'Disclosable pecuniary interests' and 'other disclosable interests'

WHAT IS A 'DISCLOSABLE PECUNIARY INTEREST' (DPI)?

- Any **employment**, office, trade or vocation carried on for profit or gain
- **Sponsorship** by a 3rd party of your member or election expenses
- Any **contract** for goods, services or works between the Council and you, a firm where you are a partner/director, or company in which you hold shares
- Interests in **land** in Worcestershire (including licence to occupy for a month or longer)
- **Shares** etc (with either a total nominal value above £25,000 or 1% of the total issued share capital) in companies with a place of business or land in Worcestershire.

NB Your DPIs include the interests of your spouse/partner as well as you

WHAT MUST I DO WITH A DPI?

- **Register** it within 28 days and
- **Declare** it where you have a DPI in a matter at a particular meeting
  - you must **not participate** and you **must withdraw**.

NB It is a criminal offence to participate in matters in which you have a DPI

WHAT ABOUT 'OTHER DISCLOSABLE INTERESTS'?

- No need to register them but
- You must **declare** them at a particular meeting where:
  You/your family/person or body with whom you are associated have a **pecuniary interest** in or **close connection** with the matter under discussion.

WHAT ABOUT MEMBERSHIP OF ANOTHER AUTHORITY OR PUBLIC BODY?

You will not normally even need to declare this as an interest. The only exception is where the conflict of interest is so significant it is seen as likely to prejudice your judgement of the public interest.

DO I HAVE TO WITHDRAW IF I HAVE A DISCLOSABLE INTEREST WHICH ISN'T A DPI?

Not normally. You must withdraw only if it:

- affects your **pecuniary interests OR**
  relates to a **planning or regulatory** matter
- **AND** it is seen as likely to **prejudice your judgement** of the public interest.

DON'T FORGET

- If you have a disclosable interest at a meeting you must **disclose both its existence and nature** – 'as noted/recorded' is insufficient
- **Declarations must relate to specific business** on the agenda
  - General scattergun declarations are not needed and achieve little
- Breaches of most of the **DPI provisions** are now **criminal offences** which may be referred to the police which can on conviction by a court lead to fines up to £5,000 and disqualification up to 5 years
- Formal **dispensation** in respect of interests can be sought in appropriate cases.

Simon Mallinson Head of Legal and Democratic Services July 2012 WCC/SPM summary/f

worcestershire
countycouncil

Audit and Governance Committee
Friday, 12 September 2014, 10.00 am, County Hall, Worcester

Membership: Mr W P Gretton (Chairman), Mrs S Askin, Mr S J M Clee, Mr N Desmond, Mr L C R Mallett, Mr R J Sutton and Mr P A Tuthill

Agenda

Item No	Subject	Page No
9	**Disaster Recovery Procedures**	53 - 68

Agenda produced and published by Patrick Birch, Director of Resources, County Hall, Spetchley Road, Worcester WR5 2NP

To obtain further information or a copy of this agenda contact Simon Lewis, Committee Officer on 01905 766621, slewis@worcestershire.gov.uk

All the above reports and supporting information can be accessed via the Council's website at http://www.worcestershire.gov.uk/cms/democratic-services/minutes-and-agenda.aspx

Date of Issue: Wednesday, 3 September 2014

This page is intentionally left blank

worcestershire countycouncil

Audit and Governance Committee
12 September 2014

9. DISASTER RECOVERY PROCEDURES

Recommendation

1. **The Chief Financial Officer recommends that the content of the Draft Disaster Recovery Internal Audit report (attached as an Appendix) be noted.**

Introduction

2. The Committee has requested that a report be brought to Audit and Governance Committee following concerns raised by its Members regarding disaster recovery procedures.

3. As part of the 2014/15 Internal Audit Plan an audit of IT Disaster Recovery (ITDR) was carried out.

4. The objective of this review is to evaluate the effectiveness of the processes and controls surrounding ITDR Management. The draft Disaster Recovery Internal Audit report is attached and members are asked to consider and note its content.

Supporting Information

- Appendix - Draft Disaster Recovery Internal Audit report

Contact Points

County Council Contact Points
Worcester (01905) 763763, Kidderminster (01562) 822511 or Minicom: Worcester (01905) 766399

Specific Contact Points for this Report
Dave Jenkins, Senior Manager - Internal Audit and Assurance
01905 766567, DJenkins@worcestershire.gov.uk

Background Papers

In the opinion of the proper officer (in this case the Chief Financial Officer) the following are the background papers relating to this report:

Previous agenda papers and minutes of the Audit and Governance Committee.

This page is intentionally left blank

worcestershire county council

DRAFT

Protected

Internal Audit Report

IT Disaster Recovery

Document Details:

Reference:	Report nos from monitoring spreadsheet/2013.14
Senior Manager, Internal Audit & Assurance:	David Jenkins ext. xxxx
Engagement Manager:	Chris Dickens, PwC
Auditor:	Scott Hughes, PwC

Date: 07 August 2014

1. EXECUTIVE SUMMARY

1.1 INTRODUCTION

As part of the 2014/15 Internal Audit Plan an audit of IT Disaster Recovery (ITDR) was carried out.

The objective of this review is to evaluate the effectiveness of the processes and controls surrounding ITDR Management.

Our report will provide a risk rating based upon how effective we assess these arrangements to be, including:

- Whether complete and relevant ITDR plan(s) are in place;
- How the ITDR Plan is invoked and how technical recovery teams are coordinated after invocation of the plan(s);
- Whether inclusion of end-to-end recovery processes and the identification of interfaces between dependent and feeder systems are understood within the ITDR Plan(s);
- What testing is performed to validate ITDR, how the outcomes are reported and corrective actions implemented; and,
- The approach for data backup.

1.2 OVERALL OPINION

The overall opinion of this review is limited assurance.

There are areas of ITDR good practice evident within the Council including:

- Investment in virtualisation and Storage Area Network (SAN) has provided advantages for the recovery of some IT systems;
- There is a formally documented and communicated ITDR command and control structure in place to manage IT outages.
- Good links between the Corporate Risk Management approach and the ITDR programme, with business driven recovery requirements.

However, the main finding and cause of the rating for this review is that the current ITDR arrangements are limited in capability should an event such as fire cause damage to the IT infrastructure hosted in the County Hall server room. In the event of a disruption requiring a full invocation of the ITDR plan for this server room, the County Council would have to potentially operate with a significant loss of priority 1 and 2, and other IT Systems and probable significant impact on the business and customers for weeks until new servers can be sourced, and systems and data recovered effectively. It is noted that SAP has additional ITDR arrangements and may be recovered within about 5 working days from a major incident leading to loss of the server room.

Testing of IT recovery has been limited over the past few years, with the notable exception of SAP and Civica Icon systems.

ITDR Documentation is in place for individual IT system recovery; however we would typically expect an ITDR recovery sequence to also be in place defining a logical technical recovery order of IT systems in priority order taking account of dependencies and feeder systems. This forms the basis to coordinate recovery in a disaster scenario across several IT recovery teams to ensure it is effective and efficient.

This review found that 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. The current ITDR arrangement may be in place for the initial 12 months of the new outsourced contract for IT, however this is to be determined as part of the ongoing contract award.

	Overall Audit Opinion	
	Full assurance	Full assurance that the system of internal control meets the organisation's objectives and controls are consistently applied.
	Significant assurance	Significant assurance that there is a generally sound system of control designed to meet the organisation's objectives. However, some weaknesses in the design or inconsistent application of controls put the achievement of some objectives at some risk.
➔	**Limited assurance**	**Limited assurance as weaknesses in the design or inconsistent application of controls put the achievement of the organisation's objectives at risk in some of the areas reviewed.**
	No assurance	No assurance can be given on the system of internal control as weaknesses in the design and/or operation of key control could result or have resulted in failure(s) to achieve the organisation's objectives in the area(s) reviewed.

2. SUMMARY OF CONCLUSIONS

2.1 The conclusion for each control objective evaluated as part of this audit was as follows:

Control Objective	**Assurance**			
	Full	**Significant**	**Limited**	**None**
CO1: Whether complete and relevant ITDR plan(s) are in place.		✓		
CO2: How the ITDR Plan is invoked and how technical recovery teams are coordinated after	✓			

invocation of the plan(s).				
CO3: Whether inclusion of end-to-end recovery processes and the identification of interfaces between dependent and feeder systems are understood within the ITDR Plan(s).			✓	
CO4: What testing is performed to validate ITDR, how the outcomes are reported and corrective actions implemented.		✓		
CO5: The approach for data backup.	✓			

2.2 The recommendations arising from the review are ranked according to their level of priority as detailed at the end of the report within the detailed audit findings. Recommendations are also colour coded according to their level of priority with the highest priorities highlighted in red, medium priorities in amber and lower priorities in green. In addition, the detailed audit findings include columns for the management response, the responsible officer and the time scale for implementation of all agreed recommendations.

2.3 Where high recommendations are made within this report it would be expected that they should be implemented within three months from the date of the report to ensure that the major areas of risk have either been resolved or that mitigating controls have been put in place and that medium and low recommendations will be implemented within six and nine months respectively.

3. LIMITATIONS REGARDING THE SCOPE OF THE AUDIT

The following areas did not form part of this audit:

- Business continuity management programme

4. ACKNOWLEDGEMENTS

Audit would like to thank all involved for their assistance during this review.

5. DETAILED AUDIT FINDINGS

Ref.	Priority	Findings	Risk Arising/ Consequence	Recommendation	Management Response	Responsibility and Timescale	Recommendation Implemented (Officer & Date)
CO1: Whether complete and relevant IT Disaster Recovery plan(s) are in place.							
1	Medium	IT Disaster Recovery (ITDR) documentation is in place, including a high level ITDR Plan (*entitled Main DR Document*) and supporting detailed technical work instructions for use by the IT recovery teams. These documents are available for recovery of individual IT systems. However, there is no coordinated ITDR documentation for effective response to major incidents, such as large scale damage to the infrastructure hosted within the County Hall server room (known internally as G1). We would typically expect a recovery sequence to be in place defining a logical technical recovery order of IT systems in priority order taking account of dependencies and feeder	Without a clearly defined plan for plausible worst case scenarios the correct ITDR recovery sequence may not be carried out leading to failure in recovery of priority IT systems which the County Council and partners rely upon to deliver key business activities.	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.	Section 12 of the main DR Document describes a high level plan for the recovery of services through the use of the Recovery Teams. This plan is used to demonstrate the recovery pattern for the underlying infrastructure ahead of any application recovery after a major incident. The second table of Section 11, "Analysis of Critical Systems (Priorities 1 and 2) with DR" then describes the priorities of individual business applications. Both these section used together paint the recovery priorities. It is true that section 12 does not include actions that could result in the move to an alternate computer room or similar accommodation issues. The DR plan will be revised to include those elements. Individual recovery documents for each business application gives reference to dependencies of that	S&CA Service Operations manager. 31/09/2014.	

Ref.	Priority	Findings	Risk Arising/ Consequence	Recommendation	Management Response	Responsibility and Timescale	Recommendation Implemented (Officer & Date)
		systems. This may include interfaces to other applications and IT infrastructure services such as active directory.			application on others. In addition the ICT Managed Services Contract has included a detailed section regarding the requirement for a detailed DR plan mapping into the county's Business continuity plan. This is also enhanced by the requirement of the new MSP to annual DR testing.		
CO2: How the ITDR Plan is invoked and how technical recovery teams are coordinated after invocation of the plan(s).							
2	N/a	There is a formally documented and communicated ITDR command and control structure in place to manage IT outages, set out within the Main ITDR Plan.	N/a	N/a	N/a	N/a	N/a
CO3: Whether inclusion of end-to-end recovery processes and the identification of interfaces between dependent and feeder systems are understood within the ITDR Plan(s).							
3	High	The current ITDR arrangements are limited in capability should an event such as fire damage to the infrastructure hosted in the County Hall server room, known as G1. There is no fire suppression system for G1 server room, and only a single Security	In the event of a disruption requiring a full invocation of the ITDR plan for G1 server room in County Hall, the Council would have to potentially operate with a significant loss of priority 1 and 2, and other IT	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.	The commissioning of ICT Infrastructure will paint a different picture of the capabilities of the ICT provider for normal operation and disaster recovery of business systems. All shortlisted prospective service providers will offer enhanced DR arrangements as part of their standard service. Hence DR	S&CA Service Operations manager, in conjunction with the new commissioned service provide.. 31/03/2015.	

Ref.	Priority	Findings	Risk Arising/ Consequence	Recommendation	Management Response	Responsibility and Timescale	Recommendation Implemented (Officer & Date)
		Guard on site during out of hours at County Hall. Alarms connected to sensors in this server room would alert the Property or Facility Teams, however they would not be on site to respond to the incident. There is no formal agreement in place to procure replacement servers in a disaster situation beyond standard procurement processes. It is our understanding that current ITDR arrangement may be in place for the initial 12 months of the new outsourced contract for IT, however this is to be determined as part of the ongoing contract award.	Systems and probable significant impact on the business and customers for weeks.	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	opportunity will improve. Currently there is no fire suppressant in the computer room, save fire extinguishers to help provide a safe means of escape for staff caught in a fire in the computer room. This has already been discussed at S&CA Management team this year. Given that the computer rooms are not environmentally sealed, fire suppressant outside of the use of traditional fire extinguishers is ineffective, and costly to implement. The facility at Wildwood has the capability of being used as a small scale computer room and features the same environmental characteristics as that in G1, including lack of fire suppressant (but does include UPS and power generation). What is lacking is the network and server focal point to give a true 'failover' service. This will be addressed as part of the new service provider's solution in relation to critical applications and functions. Again as detailed above, the contract for the ICT		

Ref.	Priority	Findings	Risk Arising/ Consequence	Recommendation	Management Response	Responsibility and Timescale	Recommendation Implemented (Officer & Date)
					managed Service requires a detailed DR plan mapped into the BC plan and also annual DR testing. Commissioning of the ICT service will determine if there is longevity in the use of the G1 computer room and that of Wildwood, and if appropriate, a formal review of costs will be done, that will need to take into consideration having a 3rd party provided DR opportunity. In addition the OJEU for the ICT Managed Service allows for the procurement of any further ICT related assets. The scale of the organisations concerned means that there will be no concerns about sourcing replacement hardware in extremely short timescales (typically overnight) should it be required. However improvements to systems resilience through the design and architecture, and continued virtualisation of the environment will remove the dependency on individual hardware items. The overall approach to DR, and any enhancements to the plans		

Ref.	Priority	Findings	Risk Arising/ Consequence	Recommendation	Management Response	Responsibility and Timescale	Recommendation Implemented (Officer & Date)
					will be discussed with the service provider during service transition (the first 3 months of the contract).		
4	High	Framework i (FWi) is considered a high priority system to the County Council, used by internal and external parties including Social Workers and Police in the field. However, all system related infrastructure is hosted within the G1 server room in County Hall which is a single point of failure should the hardware hosted within be damaged during a major incident such as fire.	It is estimated that recovery (system *rebuild and recovery of data from tape*) would take in excess of 5 working days, and so will not meet current expectations for recovery. There is a project underway to rectify these issues for the resilience and recovery of FWi, however the new solution is not expected to be in place until Autumn 2014. The new solution will include virtualisation of the live environment, with secondary DR environment to be	Prioritise the delivery of the project to enhance resilience of FWi to ensure it is delivered as soon as practicable.	The current DR arrangements for FWi do provide a working solution to recover from the loss of the service. The proposal put forward by S&CA and accepted by DASH leadership team was to include replacement of the production infrastructure and to provide a new DR arrangement that will provide longevity to the service and reduce recovery time to within desired limits (less than 2 hours). The implementation of such an arrangement was seen by S&CA as setting the pattern for future DR infrastructure for other business systems. This is a high cost option and considered to be a strategic way forward for other DR opportunities. As such, given the imminent commissioning of ICT infrastructure, it is considered	S&CA Service Operations manager, in conjunction with the new commissioned service provider to review opportunities available through that new service provider. 31/12/2014.	

Ref.	Priority	Findings	Risk Arising/ Consequence	Recommendation	Management Response	Responsibility and Timescale	Recommendation Implemented (Officer & Date)
			located in Wildwood server room. This review did not include a detailed examination of project documentation for the delivery of FWi resilience.		appropriate to delay the implementation of the S&CA recommendation, as the recommended service partner will implement enhanced levels of resiliency across the infrastructure and it is important to achieve the correct fit in terms of the FWi solution and the future architecture. It is also likely that the required levels of resilience will be delivered as part of the proposed changes at a much lower cost than implementing a point solution. The changes proposed by the solution provider should be in place within 12 months of contract start date and the FWi element will be prioritised to address this concern. As a mission critical application FWi will be prioritised in terms of both the aforementioned hardware refresh and resilience but also contractually in terms of the DR planning and DR testing.		
CO4: What testing is performed to validate IT Disaster Recovery, how the outcomes are reported and corrective actions implemented.							
5	Medium	Evidence of testing is captured within the Main ITDR document; however it	There is a risk that if they are not realistically tested,	Implement an ITDR testing strategy and	Agreed, there is little appetite for directorates to test DR arrangements for systems. This is	S&CA Service Operations manager to	

Ref.	Priority	Findings	Risk Arising/ Consequence	Recommendation	Management Response	Responsibility and Timescale	Recommendation Implemented (Officer & Date)
		has been several years since recovery of a large proportion of systems has been tested. It is noted that SAP and Icon system recovery solutions have been tested. However, Test Reports were not available for the SAP test upon request.	ITDR solutions may not be fit for purpose, leading to delays to system recoveries.	programme that provides the required realism and benefits to validate plans will work when enacted, weighed against potential disruption to the Council.	seen as a cost that derives little immediate benefit. There is opportunity to review a document sent to BAB in February 2014 that gives an overview of the current DR arrangements for business systems priorities as 1 and 2 (critical systems). This document was aimed at raising awareness of the last of formal DR arrangements that included a formal test. We have included the requirement for DR testing within the ICT managed Service Contract and as such, alongside the business the new provider will proactively manage DR testing in the new environment.	review and update the BAB document and present the revised version that will include a recommendation for directorates to undertake a DR review to include formal testing of the plan. 31/03/2015.	
CO5: The approach for data backup.							
	N/a	A formal backup policy has been documented and there is a common understanding of backup and restore standards and capability using tape based recovery.	N/a	N/a	N/a	N/a	N/a

Key to Priorities:

High	This is essential to provide satisfactory control of serious risk(s)
Medium	This is important to provide satisfactory control of risk
Low	This will improve internal control

Limitations relating to the Internal Auditor's work

The matters raised in this report are limited to those that came to our attention, from the relevant sample selected, during the course of our audit and to the extent that every system is subject to inherent weaknesses such as human error or the deliberate circumvention of controls. Our assessment of the controls which are developed and maintained by management is also limited to the time of the audit work and cannot take account of future changes in the control environment.

Tracking:

	Name	**Date**
Management Responses completed by:	Terence Hancox	03/09/2014
Issued to Head of Service on:	Xxxxxx Xxxxx	Xx/xx/xx
Agreement received from Head of Service:	Xxxxxx Xxxxx	Xx/xx/xx
Issued to Director on:	Xxxxxx Xxxxx	Xx/xx/xx

This page is intentionally left blank