worcestershire
countycouncil

Audit and Governance Committee
12 December 2014

5. DISASTER RECOVERY

Recommendation

1. The Head of Systems and Customer Access recommends that:

a) The update to the draft Disaster Recovery Internal Audit Report be noted;

b) The update to the position with Frameworki be noted; and

c) The proposals to manage the current operational environment for FWi at minimal cost, and to commission the new service provider for ICT infrastructure to cost a scheme to re-host FWi and provide a disaster recovery service, in line with the suggested service improvement plan, at the earliest opportunity be noted.

(a) Disaster Recovery for Frameworki Application

Introduction

2. At the meeting of the Committee on 12 September 2014, members considered the draft Disaster Recovery Internal Audit Report. The Committee requested that van update on Disaster Recovery be brought to this Committee. In addition, the Committee requested that the Head of Systems and Customer Access (S&CA) write to members outlining: whether all options had been considered to address the risks associated with the Frameworki system; what mitigation measures had been undertaken to address the risks in the short term; and the costs associated with addressing these risks.

3. Having consulted the Chairman and Vice-Chairman, it was determined that the issues highlighted by the Committee in relation to Frameworki would be addressed in this Committee report rather than by letter.

Background Information

4. Frameworki (FWi) is a shared application between the Directorate for Adult Services and Health (DASH) and Children's Services (ChS).

5. It is the key ICT system used by Social Workers for storing case histories for both Adults and Children. The ICT Owner for FWi is DASH, with funding for the service coming jointly from DASH and ChS in proportion to their usage (agreed between them).

6. FWi was purchased in 2004 from Corelogic and became operational in 2006, augmenting CLIX at that time. It served social workers operating within business working hours only and had an operational availability set at 98%. The business created a FWi Support team capable of maintaining the FWi application, development and business support.

7. The computer architecture for FWi originally comprised a number of dedicated servers sited in the Councils main ICT Server room. It provided a single production system with Test and Training facilities. No disaster recovery (DR) opportunity was designed or provided. There was no provision for any dedicated ICT service, either capable of instantly taking over from the failed service, nor was there provision for spare ICT hardware to be used in an emergency.

8. Current FWi ICT environment has changed little over the period and still retains the single environment design. By default, DR was (and continues to be) provided by the ICT Section, on the basis of a restore on an 'acquire hardware', 'rebuild the ICT systems' basis. This is the standard approach taken for all ICT systems that have not identified any special arrangements.

9. The DR Service Level offered by the ICT Section was 48 hours, from time of failure to restore, given hardware was available.
The design of the FWi service has what is referred to as a 'Reports' server. This reports server holds a copy of the FWi database as it was at the end of the previous day's activity. The Reports server is used to run information retrievals that would otherwise impact production users if performed on the on-line FWi database. For situations where the production FWi database becomes unavailable, the Reports server can be made available to users for enquiry purposes. This offers some business continuity opportunity in the interim.

10. The operating hours for the service was 8.30am to 5pm as specified by the business when Frameworki was installed.

11. In order to access FWi a number of Corporate Applications and Network connections also need to be available and resilient. Any point in the chain could look to the user as meaning FWi is not available but it actually may not be FWi that is not available or has a problem it may be one of the Corporate applications themselves which are unavailable or a Corporate network link may be down. Therefore finding a solution that balances business criticality with cost is part of the overall decision criteria moving forward.

Formal Review in 2012

12. In August 2012 the FWi Support team became part of a central for ICT responsibilities as part of the formation of Systems & Customer Access. This transfer enabled the FWi activity to become part of the ICT single operating model, with customer contact provided by the ICT ServiceDesk and technical support integrated.

13. At that time S&CA undertook a review of the FWi service and concluded that there were a number of underlying issues that were affecting operational running of the service that could in a short timescale affect availability to users. These were documented and discussed with the Directorate sponsor.

What were the fundamental issues?

14. The fundamental issues are:

- over-run of the overnight batch processing affecting availability of the Reports database
- Over-run of the data back-up process that could affect the ability

of the service to be restored if there were a significant failure of the system

- The database size continues to grow and it was estimated it would fill within 6 months (estimated early 2013)
- Access to FWi data was moving to a 7 * 24 service, which is not part of the application design, and consequently there was more pressure on the availability and use of the FWi Report service for access to data overnight by the WHASCAS service
- Disaster recovery arrangements appeared to be out of step with the new business requirements
- The ICT hardware used to provide the service was old and in need of replacement
- The database software used for FWi (SQL 2005) is out of mainstream support and extended support by Microsoft will end on12 April 2016 which will mean no further security patches
- There was no formal out of hours support for the application of underlying infrastructure. The external maintenance support providers operated on a 9:00 to 17:00 business working day service level.

Short term actions - work started

15. Work on FWi infrastructure was prioritised to address the operational needs of the service to ensure its availability was maintained. The business were very supportive of this work, but evidence pointed to a longer term re-design of the production environment at which point the design could include appropriate DR arrangements. Interim measures were put in place to address the data back-up; disk space and batch schedule issues.

16. A failure of the FWi service on Sunday 23 December 2012 highlighted the inconvenience felt by users, with the level of support offered out of working hours.

17. A document describing the opportunities for FWi disaster recovery was discussed at the DASH DLT on 09/01/2013. It was decided to change the recovery target for FWi to enable a restore of service for loss of FWi in 2 hours post completion of the refresh implementation.

18. An Immediate review of the current DR capability proved that the FWi service could be restored should the service be lost. This was tested in the background in the first quarter of 2013, using spare ICT equipment and working interspersed with normal staff tasks. A significant amount of knowledge was obtained by going through this process, but resulted in a successful test.

19. Given that the time to restore a FWi production database takes between 5 to 7 hours. It was estimated that a full restore of the service with dedicated resource could be completed within 5 days, or 3 days if equipment was to hand immediately. However the process to rebuild and restore FWi was proven, and can be repeated if necessary to cater for loss of the production environment should it happen in the future.

Options going forward for further Business resilience

20. A proposal was created from which a number of scenarios for recovery could be explored that would meet the enhanced business criticality. The scenarios included a new production and DR solution hosted internally (with varying configurations balancing FWi and wider business opportunities that infrastructure could have provided) or an

external hosting service taken from the supplier of the software, Corelogic.

21. An interim version of this paper was discussed with DASH management in July 2013, to explore whether the opportunities put forward were appropriate. The paper was formally delivered to DASH management in October 2013. The business requirements for disaster recovery were as follows:

Restore within 2hrs or 24hrs
System Availability 24x7x365
5 year operational window
Cater for growing data requirements
Batch Processing to be completed overnight

22. The options ranged in cost from £86,000 to £425,000. The paper was approved by DASH on 9 April 2014 and a new project established to implement those recommendations, which included establishing a new set of financial projections.

23. Meanwhile, as S&CA were in the process of commissioning the ICT service, a decision was taken with the business in August 2014 to have the FWi DR project delivered by the new service provider in such a manner that it would be a catalyst for improving the operational and Disaster Recovery options for other systems. This would minimise cost and the solution implemented in a manner appropriate to the opportunities a new service provider could bring.

Summary

24. Over the last three years, the measured availability of the FWi service is greater than the 98% originally assigned to it, operating at 99.99% with only three failures since 2012. None of these instances was actually due to a failure of the application itself, but of the FWi hardware and underlying network. However, having said this as a mission critical system the service does need a more robust design that assures business continuity going forward. This is scheduled for the mid part of 2015. Detailed plans are being formulated as part of the ICT managed services commissioning process.

Conclusion

25. The FWi system is not designed to operate in a high availability configuration and has single points of failure. It is only recoverable through the use of business continuity and disaster recovery from a 'cold' start. If the service is lost, it may take up to five days to recover.

26. The current production environment for FWi is at the end of its operational life and needs to be replaced. Short term actions have been implemented to improve the current situation at no financial cost, including testing all the procedures associated with a full restore.

27. The current operational environment for FWi will be managed at minimal cost, and the new service provider for ICT infrastructure will be commissioned to cost a scheme to re-host FWi and provide a disaster recovery service, in line with the suggested service improvement plan,

at the earliest opportunity.

(b) Update to the Draft Disaster Recovery Internal Audit report

28. The Draft Disaster Recovery Internal Audit report dated 7 August 2014 has the following Detailed Audit Findings.

Ref 5.1

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.

Update
29. This is now complete and instruction included in the 'S&CA Main ITDR Plan' Document.

Ref 5.2
30. No actions required. Acknowledges that: "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."

Ref 5.3
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.**

Update
31. The premise in this recommendation revolves around the continued use of the current ICT infrastructure and especially the two computer rooms at County Hall and Wildwood. Both the Commissioning work, engaging with HP to deliver operational support for the Council systems, and the Digital by Default strategy, will see substantial change in the way systems are designed and delivered to the Council.

32. The limitations of the two existing computer rooms, specifically, the lack of fire suppressant, is well understood and can be built into the arrangements for recovery of systems, such that the risk of loss of service through fire can be tolerated.

33. The Digital by Design is making greater use of services provided externally in the Cloud, reducing the risk of loss from disruption to central resources. Similarly, opportunity exists to seek hosting services external to the Council via the contract for support with HP.

34. Deployment of services away from the Council through current and developing technologies will reduce the risk of loss on the Council to a point where the Council can accept the risk as in option 5.3(a) opposite.

Ref 5.4
Prioritise the delivery of the project to enhance resilience of FWi to ensure it is delivered as soon as practicable.

Update
35. The HP proposal (for ICT Service commissioning) includes a complete refresh of the server and storage estate and the introduction of resilience across our 2 data rooms in County Hall and Wildwood. 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.

36. The current configuration of our two datacentres is centred around G1 (as illustrated in the Appendix). Assuming a failure within G1 the current restore times would be as follows:

- Day 1: Purchase new kit
- Day 3-4: New kit onsite at Wildwood and CH. Begin configuration of new kit
- Day 5: Start rebuild of Internet, Email, Frameworki and Talis
- Day 7: Internet and basic email available
- Day 7: Start rebuild of business apps in priority order
- Day 8-10: Frameworki and Talis available
- Day 10-18: Other business applications available in priority order
- The above schedule would require additional resources and a 24x7 shift pattern established within the team. We currently have no arrangements with third parties to provide kit on standby.

37. The new configuration, which was built into the commissioning strategy, will be finalised once the contract with HP Enterprise Services Ltd is signed and will take our disaster recovery capability onto a new level of performance more consistent with an organisation who see technology as critical to its operation. The Network and Server estate will be split across both sites rather than just primarily one. Commissioning the Service and accessing the skills and knowledge of a mature ICT services provider has provided the opportunity to deliver this improved disaster recovery capability which we would have been very difficult to achieve on our own. It is anticipated that the following is the improved restore times for the major applications involved:

- 2 hours: Mission critical applications in the infrastructure are re-designed in a failover mode (internet, email, Frameworki, Talis)
- 48 hours: Other key applications available.
- Day 5: remaining business applications restored to failed over/new equipment. Some apps may be sooner if they have been configured for application failover as above
- Getting to this new configuration is a major piece of work and will take a substantial amount on 2015 to achieve.

38. A 'Mission critical application' is, by definition, an application that is essential to the continued business of the enterprise. It is usual for Mission Critical Applications to be built with a 99.9% availability over a designated period e.g. 7*24*365 or 5*24*365. Even 99.9% availability however means that an application that is supposed to be available 7*24*365 can actually be 'down' for 61.5 hours per annum. Obviously this does not include planned maintenance.

39. For Mission Critical applications it is therefore usual to have both Application and Infrastructure resilience i.e. should a problem occur then the application can instantly recover to its secondary copy, usually held in a separate location in case of site emergencies.

40. A discussion with Corelogic confirmed that our current Frameworki application does support high level availability using application server clustering. However there are two areas of the system that do not support instant failover; these being forms manager and finance code. In these cases a node failure would result in the user being presented with the login screen and automatically redirected to the next node in the cluster. Data loss in this case would be minimal and only for users connected to the failed node.

41. Although an upgrade of Frameworki is not required to utilise the failover features it would mean a complete reconfiguration and redeployment of the product in line with an infrastructure upgrade as we do not have our instance of Frameworki configured for this at present. In addition to the proposed resilient infrastructure included within the HP proposal we would also purchase and configure load balancers for this application level failover to be implemented.

42. Mosaic has been developed further and has seamless failover for all areas of the application. We have requested supporting documentation to this effect from Corelogic.

Ref 5.5
Implement an ITDR testing strategy and programme that provides the required realism and benefits to validate plans will work when enacted, weighed against potential disruption to the Council.

Update
43. 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.

44. S&CA will arrange for this to be revisited at the earliest appropriate time in the BAB meeting agenda, where S&CA and Directorates can agree a way forward with performing DR tests mission and business critical systems.

Supporting information

Appendix - Current architecture for services In County Hall

Contact Points

County Council Contact Points

Worcester (01905) 763763, Kidderminster (01562) 822511 or Minicom: Worcester (01905) 766399

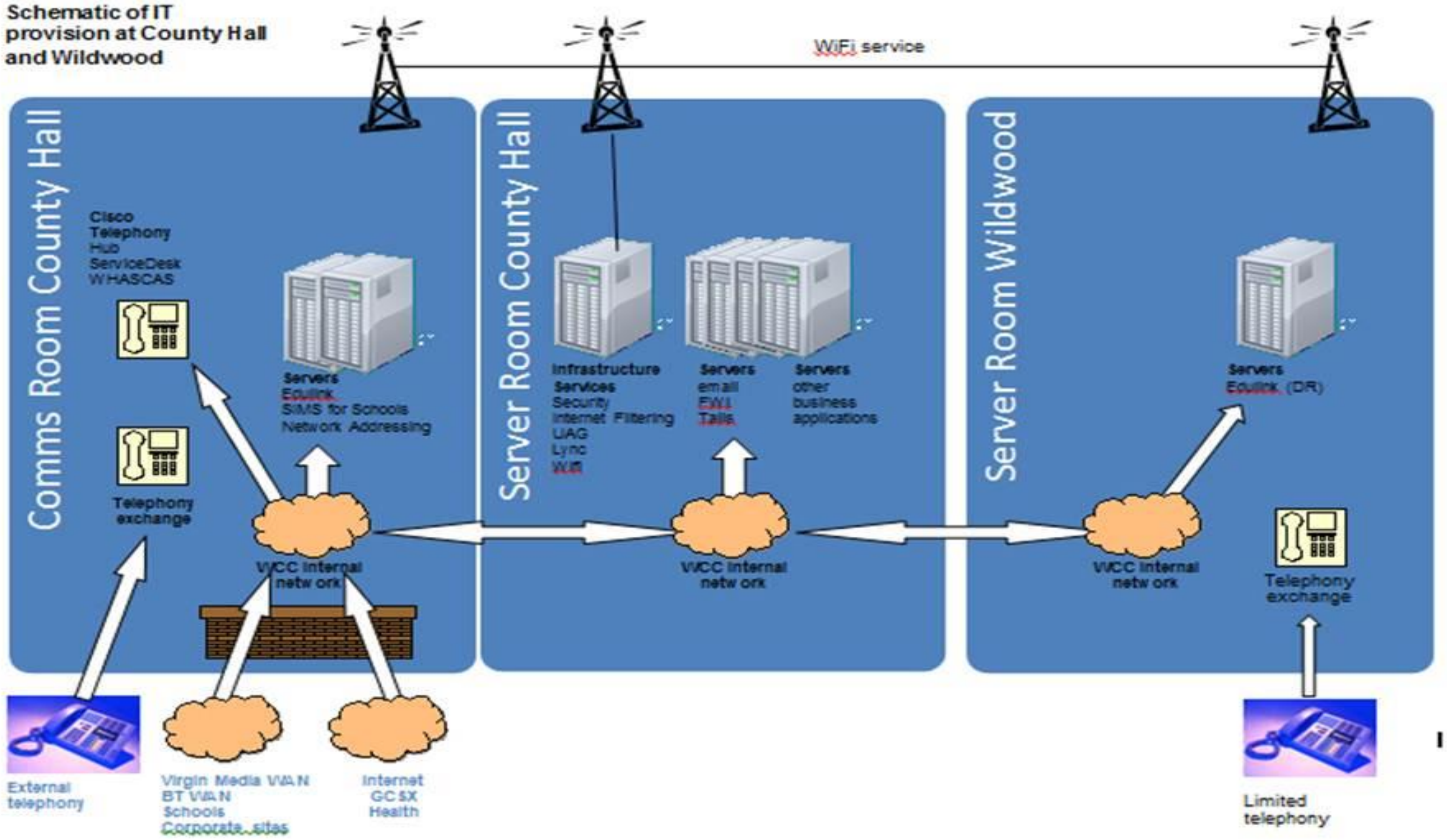
Specific Contact Points
Peter Bishop, Head of Systems & Customer Access
Email: pbishop@worcestershire.gov.uk
(01905) 766020

Background papers

In the opinion of the proper officer (in this case, the Head of S&CA) the following are the background papers relating to this report:

The agenda papers and Minutes of the meeting of the Audit and Governance Committee held on 12 September 2014

Appendix – Current architecture for services In County Hall


Schematic of IT provision at County Hall and Wildwood
WiFi service
Comms Room County Hall
Cisco Telephony Hub ServiceDesk WHASCAS
Servers Edulink SIMS for Schools Network Addressing
Telephony exchange
WCC Internal netw ork
External telephony
Virgin Media WAN BT WAN Schools Corporate sites
Internet GCSX Health
Server Room County Hall
Infrastructure Services Security Internet Filtering UAG Lync Wifi
Servers email EWI Tails
Servers other business applications
WCC Internal netw ork
Server Room Wildwood
Servers Edulink (DR)
WCC Internal netw ork
Telephony exchange
Limited telephony