Buckinghamshire & Milton Keynes Fire Authority

MEETING	Executive Committee
DATE OF MEETING	23 November 2016
OFFICER	Julian Parsons, Head of Service Development
LEAD MEMBER	Councillor Adrian Busby
SUBJECT OF THE REPORT	**ICT Disaster Recovery Plan**
EXECUTIVE SUMMARY	Currently the Service holds a significant operating risk in that the disaster recovery (DR) servers and the business as usual servers for our ICT systems are in the same server room at BHQ. A fire, air conditioning failure or significant power outage could cause a total failure of the ICT systems across the Service, having a serious impact on both critical and business as usual functions. It was agreed at the Strategic Management Board (SMB) meeting on 25 October 2016 that rather than have our own DR servers, the data is replicated into a cloud based, hosted solution, with further supporting ancillary works. This is in accordance with the revised ICT Mission Statement. **"The KIS department will deliver integrated solutions on robust, resilient and secure platforms. Wherever prudent, solutions should be remotely hosted or cloud-based..."** This revision was agreed by this Committee during the meeting on 2 December 2015. This project is completely compliant with current HM Government policy to migrate solutions to the cloud, including most recently a major migration of the Ministry of Defence systems to Microsoft cloud solutions. A further risk is the emerging and growing threat of cyber-attacks. Due to recent experience and an ICT Health Check, a number of weaknesses have been identified which are in the process of being rectified based on the risk levels presented. The purpose of this paper is to inform the Executive Committee of the actions that are being taken to manage these risks. Appendix A is a copy of the report presented to SMB.

ACTION	Information/Decision.
RECOMMENDATIONS	1. That the decision to move to cloud based technology to provide the basis of the Service's ICT disaster recovery plan is noted. 2. That the Executive Committee agree that the progress in delivering this project is reported to the Overview & Audit Committee.
RISK MANAGEMENT	Currently the Service has a significant business continuity risk with regard to ICT. Loss of the main and disaster recovery servers at the same time is possible. This loss would result in the complete disruption to the Service's ICT network and therefore significant disruption to critical and usual business for a significant period of time. The proposals will all but eliminate this risk to the Service. The Service is also undertaking a number of actions to reduce our vulnerability from cyber-attacks and also improve our recovery time should one be effective in breaching our defences.
FINANCIAL IMPLICATIONS	The saving to the Authority for the first six years is £32k. One-off costs of £32k (plus 25% contingency) are to be funded by a one-off transfer from the contingency budget in 2016/17. The on-going revenue costs will be funded by reducing the revenue contribution to capital by £8k permanently (as less capital money will be required as transferring to the cloud removes the need to purchase a new server every six years). The savings in future six-year cycles will be even higher (c£72k) as implementation costs will not need to be paid again.
LEGAL IMPLICATIONS	Under the Civil Contingencies Act 2004, Fire and Rescue Services are categorised as Category 1 responders and are therefore expected to be highly robust and able to maintain operations at all times. The business continuity and disaster recovery plan for the Service must be robust enough to deal with and maintain its statutory obligations throughout all reasonably foreseeable events. Many aspects of our ICT systems manages information that would be subject to the Data Protection act 1998. The security of our systems is paramount and the management of our data is intrinsically linked to our ICT business continuity arrangements.
CONSISTENCY WITH THE PRINCIPLES OF	In 2015 Buckinghamshire Fire and Rescue Service (BFRS) and Royal Berkshire Fire and Rescue Service (RBFRS) explored opportunities to potential

COLLABORATION	collaborate in providing mutual resilience in relation to disaster recovery servers. This would effectively mean that each service would host the others back-up server arrays. Though technically very feasible and the geographical remoteness of the two services HQ was attractive, the costs of replicating the server arrays in each other's server rooms was cost prohibitive.
HEALTH AND SAFETY	There are no health, safety or well-being matters arising from this report.
EQUALITY AND DIVERSITY	There are no equality or diversity matters arising from this report.
USE OF RESOURCES	**Contribution to the achievement of strategic objectives;** The ICT Strategy 2014-19 (revised 2/12/2015) is designed to modernise our ICT infrastructure to take in the latest technology and thinking. It is key in supporting the ICT strategic objective to move applications to the cloud and support initiatives such as the BASI project. **Communication with stakeholders;** Part of the plan for increasing the resilience of our ICT system and recovery from any future cyber-attacks is through education of our staff to minimise the data stored on our systems and also use email and the internet more safely and from a greater position of understanding and recognising cyber threats. **The system of internal control;** Agreed projects and initiatives will be captured in the ICT 2014-2019 project portfolio. Progress will be monitored at a departmental level and reported corporately through to Overview & Audit Committee. **The medium term financial strategy;** The projects required to improve our ICT business continuity and disaster planning will be financially supported through realignment of existing budgets.
PROVENANCE SECTION & BACKGROUND PAPERS	**Background** As part of the revision of the ICT Strategy 2014-2019 it was identified that current HM Government policy is to encourage public sector organisations to explore the benefits of cloud hosting and reduce the public spend on internal ICT infrastructure. **Background Papers** • [O&A Meeting 2 December 2015 Minutes](#) • [ICT Strategy Review](#)
APPENDICES	Appendix A: ICT Systems Disaster Recovery Review

TIME REQUIRED	10 Minutes.
REPORT ORIGINATOR AND CONTACT	Dave Thexton dthexton@bucksfire.gov.uk 07876 448 744