Audit and Governance Committee

Dorset County Council

Date of Meeting	20 September 2016
Cabinet Member Cllr Robin Cook – Cabinet Member for Organisational Development and Transformation Local Members All Members Lead Director Debbie Ward – Chief Executive	
Subject of Report	**DES Business Continuity Update**
Executive Summary	In November 2015 the former Audit and Scrutiny Committee considered a report on the ICT General Control Environment following on from the annual report from the External Auditors, KPMG. It was noted that we had only undertaken limited service continuity test of DES and the Committee asked for a further report following planned tests in summer 2016. Tests in July of DES, the new Smarter Computing (desktop and mobile) infrastructure and a number of critical business applications were undertaken. This exercise has provided assurance that DES can be recovered in the event of a major incident. The annual major test of all business critical systems is planned for October 2016. A recent risk to business continuity is 'cyber security'; an attack by individuals or software designed to deny access to data and systems or steal information. The county council has experienced two such attacks in 2016 and has been able to contain them and recover without significant impact. The risk of a major attack severely disrupting service remains very real and an audit of our preparedness has been commissioned from the South West Audit

	Partnership and will start in September 2016.
Impact Assessment:	Equalities Impact Assessment: N/A
	Use of Evidence: This report draws upon the Internal Audit report DES ICT General Controls 2014/15 and the Post Exercise Report July 2016.
	Budget/ Risk Assessment: None
Recommendation	That the Committee notes and comments on the outcome of the July 2016 ICT Service Continuity Exercise.
Reason for Recommendation	To provide the Committee assurance over the controls relating to the operation of DES and our ability to recover the system in the event of a major incident.
Appendices	Appendix 1: ICT service continuity test objectives and outcome – July 2016
Background Papers	Audit and Scrutiny Report – ICT General Control Environment November 2015
Report Originator and Contact	Name: Richard Pascoe Tel: 01305 224204 Email: r.j.pascoe@dorsetcc.gov.uk

1. Background

1.1. In November 2015 the former Audit and Scrutiny Committee considered a report on the ICT General Control Environment following on from the annual report from the External Auditors, KPMG.

1.2. The General Controls Environment relates to the controls for the council's core financial ICT application, DES, and KPMG's report draws upon the Internal Auditor's annual review. The 2015 South West Audit Partnership report provided 'reasonable' assurance, with no priority 5 recommendations and one priority 4.

1.3. The November officer report provided commentary on the key risks from the Internal Audit report and noted that we had upgraded the technology underpinning DES and had refreshed the 'disaster recovery' systems for DES that are sited at Hampshire CC.

1.4. However, whilst we had tested the DES system in isolation at Hampshire, we had not yet been able to conduct a full service continuity test where we simulate the data centre at Dorchester being unavailable and evaluate how well and quickly we could start up and operate from Hampshire.

1.5. This was because the new desktop computing infrastructure being introduced by the Smarter Computing Project had to be in place before a meaningful full test could be completed.

1.6. Our ICT Service Continuity Policy sets out an intention to conduct a full test exercise in October and a more limited one in April each year. The Committee noted the plan to conduct a full test of a small number of systems, including DES and the new Smarter Computing infrastructure, in summer 2016 and asked for a report on the findings.

2. Scope and outcome of the July 2016 ICT service continuity test

2.1. Note that the term 'service continuity' is used rather than 'business continuity' as this was a test of our ability to recover our ICT systems and not how the broader organisation's plans to maintain service in the event of a major incident.

2.2. The purpose of the July test was to provide assurance that DES, the Smarter Computing infrastructure and a limited number of applications supporting critical business functions, could be recovered following the (theoretical) loss of the data centre at County Hall. The test largely met its objectives and the high-level test results are provided in Appendix 1. A detailed test report was produced.

2.3. The tests demonstrated that the core technology solutions can be restored and perform largely as expected. The test successfully demonstrated the readiness of the service continuity infrastructure supporting DES and provides assurance that this system can be recovered in the event of a major incident.

2.4. There were some minor issues reported in the detailed test report, including the need to ensure all test scripts are completely up to date and that these are followed step by step. Occasionally technical staff who are familiar with the systems and don't need the instructions do not always follow them exactly. It's important we have tested the instructions, as well as the systems, as we may have to rely on support staff who are not normally responsible for the systems in a real emergency.

2.5. The major test being planned for October 2016 will seek to provide assurance that these minor issues have been addressed and also ensure we have accommodated a number of upgrades to DES that are currently being implemented.

3. Annual major continuity test

3.1. The major annual test in October 2016 will take the County Hall data centre offline to simulate an outage and will run a full test to demonstrate the readiness of all continuity arrangements for critical infrastructure services and applications supporting critical business functions. This test will provide a full picture of ICT service continuity readiness, following recent changes to the ICT infrastructure and also ensure we have addressed the issues which the July test highlighted in the sub-set of the other critical business applications tested.

3.2. We rigorously plan the ICT continuity tests, with clear communication to the wider organisation. The test processes require business user engagement to conduct user testing to provide the necessary assurance that systems perform as expected, and are not simply ‘switched on’. Testing plans and results are monitored by the corporate Resilience Group.

3.3. It is worth noting that, whilst not related to DES, we have a key weakness relating to our telephony services in that the loss of the data centre would, over a period of a week, see telephones gradually stop working. This is due to a network constraint that we have been unable to resolve with KCOM, our current network provider. Work is underway to migrate to a new network to replace the KCOM network and this issue with the telephony service continuity arrangements will be resolved as soon as possible and before the end of the financial year.

4. Cyber security and the risk to business continuity

4.1. Whilst disaster recovery conjures thoughts of flood or fire, the more likely scenarios have been a major electrical power outage (as we had in 2008) or hardware failure. Today, the threat of a ‘cyber attack’ has grown and become a key risk.

4.2. Such an attack refers to actions of individuals or computer software that seek to deny access to data and systems or steal information. The attacks may be specifically targeting the organisation; the majority operate over the internet seeking to infect whichever organisations or individuals they come across.

4.3. We are automatically at risk by having a connection to the internet.

4.4. A prevalent form of attack is known as ‘ransomware’ – this uses a computer program to encrypt data files such that they cannot be accessed unless a ransom is paid.

4.5. The effects of a malicious cyber-attack can be limited to the short-term productivity of an individual, or extend to affecting the ability of the whole organisation to access its ICT systems and data, such that we would need to implement full business continuity arrangements, with all the impacts on service provision this brings.

5. The county council has been subject to two such infections, both in 2016, though we were able to quickly identify, contain and eradicate the malicious program and restore data files from back-up with limited loss of service or work. Lincolnshire County Council shut down their entire computing infrastructure following a similar attack in January 2016.

5.1. We employ a range of defence tools, including anti-virus software and firewalls, to protect our internal networks and engage with other organisations, including regional and national information sharing schemes and, Zephyr, the regional organised crime unit specialising in cyber crime in order to share intelligence.

5.2. However, it is not possible for technical measures to stop all attacks and we rely on the vigilance of individuals as often such attacks are triggered by opening a link or attachment in an email.

5.3. In September 2016, the South West Audit Partnership will conduct an audit of our cyber-security provisions. It is proposed that the audit scope will cover:

- Information Security Policy and processes
- Recovery planning and procedures in the event of a cyber-attack (auto-response)
- Staff training and awareness
- Information asset identification and classification (to ensure critical assets are identified and prioritised to maximise security in these areas)
- Monitoring and preventative measures (hardware and software monitoring, stress testing) including mechanisms for monitoring the cyber threat landscape and implementing appropriate response measures
- Identification, capture, reporting, application and dissemination of lessons learnt from cyber-attacks.

Richard Pascoe

Head of ICT and Customer Services

Appendix 1: ICT service continuity test objectives and outcome – July 2016

Objective	Additional Information	Overall Result
Disconnect the Primary data centre from the WAN, Telephone Exchange and Internet.	This work completed although a little later than anticipated as there was a delay on KCom's side.	SUCCESS
Rehearse a documented recovery of the core ICT services and systems	As with previous exercises the presence and use of documentation was not consistent.	PARTIAL
Provide assurance that the recovery methods for our core services (DHCP, DNS, Active Directory, Network Drives, App-V, Internet Link and Canon Print Solution) are still fit for purpose.		SUCCESS
Ensure that Service Continuity Plans (SCPs) are up to date for core services.	Continuity Plans are in varying states of completeness, this exercise has provided the opportunity to identify gaps in the documentation.	PARTIAL
Prove that the DES continuity solution and documentation is fit for purpose.	This was the first formal recovery of DES since 2012.	SUCCESS
Provide a limited test of line of business applications.	Additional information is in section 8 of the test report (see Appendix 3).	SUCCESS