

Isle of Wight Council

Internal Audit Report 2015/16

Business Continuity and IT Disaster Recovery

April 2016

FINAL

Contents



1. Executive summary	2
2. Detailed current year findings	4
Appendix A: Basis of our classifications	7
Appendix B: Terms of Reference	10
Appendix C: Limitations and responsibilities	14

Distribution List

For action	Gavin Muncaster, Head of IT Darren Steed, Head of Emergency Management Iain Lawrie, Resilience Co-ordinator(BC) Kieran Tarrant, Facilities Management Officer Debbie Downer, Business Support Manager
For information	Jo Thistlewood, Technical Finance Manager

The report has been prepared solely for the Isle of Wight Council, this report should not be disclosed to any third party, quoted or referred to without prior approval from internal audit.

1. Executive summary

Report classification  High Risk	Trend  Increase in risk rating since business continuity and IT Disaster Recovery were last reviewed	Total number of findings					
			Critical	High	Medium	Low	Advisory
		Control design	0	1	2	0	0
		Operating effectiveness	0	0	0	0	0
		Total	0	1	2	0	0

Summary of findings:

This review was undertaken as part of the 2015/16 Internal Audit Plan, agreed by the Audit Committee. The purpose of this audit was to review the Council's Business Continuity and IT Disaster Recovery arrangements; under IT disaster recovery we also carried out a high level review of the controls in place over the Council's Data Centre.

The Council invested heavily in the Data Centre a number of years ago and we are pleased to report that enhanced arrangements are still effective, these include:

- Strong controls over access management; an outer door secured by a swipe card lock, with access requiring authorisation by IT and an inner door requiring a PIN code.
- Centrally managed air conditioning and UPS (Uninterruptible Power Supply), backed by a power generator onsite.
- Multiple redundant systems; dual links to key Council offices and redundancy in servers, for example mirrored hard disks.
- Regular backups, stored remotely from the Data Centre.
- A current contract with a third party supplier for replacement hardware, if required in the event of a continuity incident.

Ultimately it is better to avoid a continuity incident - a well-managed, resilient Data Centre maximises availability and helps to support continuous, uninterrupted service by all areas of the Council reliant on systems hosted in the County Hall Data Centre.

Regarding wider Business Continuity and IT Disaster Recovery, while overarching documentation does need updating, substantively it is still fit for purpose. The main recent development in this area is refocussing effort on the most critical areas of the Council's work – this is sensible, in light of the reduced resources the Council has available. A new business continuity plan template has been developed and is being trialled by Adult Services and Premises Management, prior to rollout to the most critical areas, once these have been confirmed as part of the 2016/17 planning cycle.

The highest risk issue we identified is limited recent testing of arrangements, both regarding wider business continuity and specific IT arrangements. While this is understandable, with reduced resources available, testing plans for critical services should be prioritised in 2016; this will help to ensure that plans will be effective in the event of a continuity incident. We also identified that business continuity plans are out of date in Adult Social Care and are not reflective of current practice; while plans will be updated once the new Paris system is implemented until this time there is a risk that, in the event of a continuity incident, plans would not bit fit for purpose – primarily due to this issue this report has been rated as high risk overall. We have raised three detailed findings, as summarised below:

- *Business Continuity Framework/Business Impact Analysis (BIA)*: a new framework is in the process of being implemented, refocussing business continuity effort on the Council's most critical services, responding to the reduced resources now available; while we did note that an exercise to confirm the Council's critical services has

not been carried out for a number of years implicitly these are known, for example Adult and Children's Services – essentially services classified as 'public protection'. A revised template is currently being trialled by Adult Social Care and Premises Management. As part of the 2016/17 planning cycle the most critical Council services will be identified, these areas will then be required to complete copies of the revised business continuity plan template, with the support of Emergency Management – this process should continue as planned.

We also identified that the overarching Business Continuity Strategy has not been substantively updated since 2013. As business continuity effort is refocussed this document should be revised, to remove redundant content and ensure it is reflective of changed expectations. We have raised this area as a **medium risk** finding.

- *Adult Social Care Business Continuity*: through our fieldwork for this review we identified that business continuity plans for Adult Social Care have not been revised for a number of years, predating the Service's relocation to Enterprise House. Adult Social Care is one of the Council's most critical services; with the pending implementation of Paris revising plans in the short term would be of limited value, however once Paris is in place they should be revised as a matter of priority and included in the scheduled table top test of plans for critical services in September 2016. We have raised this area as a **high risk** finding.
- *IT Disaster Recovery*: while overarching IT Disaster Recovery documentation is broadly fit for purpose, it has not been substantively revised since 2013. Our review did identify a number of errors; for example staff who are no longer with the Council and properties which are no longer occupied by the Council. To ensure that the Plans are fit for purpose, if and when required, all IT Disaster Recovery documentation should be reviewed and updated. We also noted that the copy of the Server Recovery Contract provided for our review while current is not signed by the provider; a signed copy of this document should be requested from the provider.

One of the issues with business continuity historically at the Council is service areas making unrealistic assumptions about the response they will receive from IT. To help confirm this issue has been addressed we reviewed the Business Continuity Plan for the Civic Centre in Sandown, where a number of key Council services are located, for example Revenue and Benefit service and the Business Continuity Plan for the Contact Centre. Both documents are up to date and set out high level plans for alternative processing in the event of a continuity incident. However we did note that all systems used at Sandown, for example SAP and Northgate, are categorised as 'priority 3', with restoration identified in the main IT Disaster Recovery Plan as taking up to four weeks; this would have a significant impact on the Council's ability to effectively process payments and revenue. The criticality categorisation for all systems should be revisited, to ensure that it is in line with the needs of service areas and the Council as a whole.

We also noted that while a contract is in place for the provision of replacement hardware in the event of a continuity incident, as above, the annual rehearsal clause has not been exercised since 2014. A rehearsal should be scheduled in 2016, focussing on the most critical systems, once this list has been revised. We have raised this area as a **medium risk** finding.

We would like to take this opportunity to thank Isle of Wight Council staff for their help and assistance with this review.

2. Detailed current year findings

1. Business Continuity Framework/Business Impact Analysis (BIA) – control design

Finding

The Emergency Management Team (three FTEs) is responsible for coordinating the Council's business continuity arrangements and for supporting activity in wider service areas. In addition, the Team are responsible for covering a number of other areas under the umbrella of Emergency Management, for example ensuring compliance with the Civil Contingencies Act 2004 – our review is solely of the Team's business continuity responsibilities. The current overarching Business Continuity Strategy was last updated in 2013, predating significant reductions in staffing and the reorganisations of last three years. While at a high level much of the content is still valid, there are elements, for example resilience champions, which are no longer correct – the Business Continuity Strategy needs to be revised, primarily to remove redundant content but also to align with new business continuity expectations, as below.

The key foundation of Business Continuity is identifying an organisation's critical services and ensuring these continue running in all situations; this is referred to as Business Impact Analysis (BIA). While implicitly the Council know its critical services (essentially these are services flagged as 'public protection', such as social care, followed by statutory services and core support services, such as IT on which all services rely), a formal BIA process has not taken place for at least five years - in our view, 12 months would be a good practice interval for this to be refreshed.

This issue is well understood by the Emergency Management Team and we were informed that critical services will be confirmed through the 2016/17 planning cycle, as below. Critical areas will then be required to complete a new business continuity plan template, which is currently being trialled by Adult Social Care and Premises Management – associated with this, these services need to ensure they provide feedback in time to inform wider rollout, by April 2016.

Planning for 2016/17 will start in the next few months, although this has been delayed until the Council has confirmation of its final grant settlement from central government; the Head of Emergency Management has confirmed that service planning will include all areas of the Council identifying their 'critical' services. Once this process is complete the list of critical services will need to be moderated by Emergency Management (supported by IT, to confirm critical systems) and approved by the CMT (Corporate Management Team). Areas agreed as 'critical' will then be required to complete the new template business continuity plan, with copies of updated plans to be held by Emergency Management (both within the command and control centre in County Hall and offsite, at Ryde Fire Station), to ensure they are available when needed and to support Emergency Management in exercising their oversight role. Once a thorough BIA has been carried out this should be confirmed as correct annually via CMT, with a more comprehensive exercise carried out at a suitable interval, for example every three years.

Untested plans will be reliant on assumptions, which may prove to be incorrect in the event of a continuity incident. Once critical areas have been agreed a sample of plans should be table top tested on an annual basis to validate that assumptions are correct - in light of the new processes and importance of the Service, Adult Social Care should be included in 2016 table top testing.

Risks

If the overarching Strategy is not reflective of expectations then responsibilities may be unclear and will be less likely to be exercised effectively in the event of a serious incident. If feedback from areas trialling new business continuity plans is not received in a timely manner then feedback will not be available to inform revision, prior to wider rollout; any issues will be less likely to be identified and addressed.

If critical services are not correctly identified, with appropriate plans put in place and tested, then in the event of a continuity incident the response is more likely to be poor, potentially leading to an unacceptable interruption to service, for example to vulnerable adults.

Finding rating	Agreed actions	Responsible person / title
<p style="text-align: center;">Medium</p>	<p>1. The Facilities Management Officer and Business Support Manager will provide feedback on the new business continuity plan template, in time to inform its wider rollout.</p>	<p>1. Kieran Tarrant, Facilities Management Officer and Debbie Downer, Business Support Manager 2. Darren Steed, Head of Emergency Management</p>
	<p>The Head of Emergency Management, delegating as necessary, will:</p>	<p>Target Date</p>
	<ul style="list-style-type: none"> 2. Revise the overarching Business Continuity Strategy, to remove redundant content and align with the focus of future business continuity effort. 2. Review the areas identified as critical through the 2016/17 service planning cycle, gaining confirmation that this is correct from CMT. 2. Support areas identified as critical in completing the new template; specifically Adult Social Care. 2. Schedule an annual refresh of BIA, with a more comprehensive exercise to be carried out at a suitable interval, for example every three years. 	<ul style="list-style-type: none"> 1. April 2016 2. July 2016 3. October 2016
	<ul style="list-style-type: none"> 3. Schedule a table top test of new plans, specifically to include Adult Social Care in October 2016. 	<p>Report reference:</p> <p>IOW- 21-01</p>

2. Adult Social Care Business Continuity – control design

Finding		
<p>As identified in finding one above, we queried the current position with the two services trialling the new business continuity plan template, Adult Social Care and Premises Management. Both services are in the process of reviewing these templates and have agreed to provide feedback, in time to inform wider rollout of the template.</p> <p>Regarding Adult Social Care, we noted that the current business continuity plans are over three years' old, predating the Service's move to its current location in Enterprise House and their previous location, at the Civic Centre in Sandown. We have been informed that overall responsibility for business continuity in the Service will sit with the new Commissioning Manager for the Service, this post currently being filled on an interim basis.</p> <p>In the short term the Service is reliant on shared drives (Swift, the current system, is supplemented by MS Word Templates, completed and moved between shared drive locations to manage workflow) and would find it difficult to continue an effective service in the event of a system outage lasting more than a few days. However business continuity requirements will be significantly impacted by the implementation of the new Paris system and associated Care Act compliant processes. This is scheduled to be completed by April/May 2016 and any work on updating business continuity plans prior to this will be of limited value and in the short term the best approach is potentially to accept this risk – once Paris has been implemented and the new Commissioning Manager post holder is in place, plans should be revised as a matter of high priority, with a particular focus on identifying alternative processing arrangements if Paris is not available. Revised plans should then be table top tested, to validate that they are fit for purpose to cover any continuity incidents.</p>		
Risks		
<p>If Adult Services do not have appropriate plans put in place and tested, then in the event of a continuity incident the quality of the service is likely to be significantly degraded, potentially leading to an unacceptable interruption to service, for example to vulnerable adults, specifically correctly responding to safeguarding alerts.</p>		
Finding rating	Agreed actions	Responsible person / title
High	<p>The Interim Head of Adult Social Care will:</p> <ul style="list-style-type: none"> Ensure that service plans are produced in line with corporate expectations, specifically including identification of critical business activities and maximum tolerable periods of disruption. <p>Once in post the new Head of Adult Social Care, delegating as necessary will once Paris has been implemented ensure:</p> <ul style="list-style-type: none"> Business continuity plans are revised, with a particular focus on identifying alternative processing arrangements and table top testing, to ensure they will be sufficient if Paris is not available. 	Phillip Sharpe, Interim head of Adult Social Care
		Target Date
		July 2016
		Report reference:
		IOW- 21-02

3. IT Disaster Recovery – control design

Finding

The Emergency Management Team meet with senior management from IT biannually, to review whether IT Disaster Recovery arrangements are correctly aligned with the Council's wider business continuity arrangements; meetings are formally managed, with agendas agreed in advance and agreed minutes produced to ensure discussions and actions are recorded and tracked. At the last meeting, held on the 14th January 2016, a table top rehearsal was agreed, to be scheduled in March 2016, focusing on loss of internet connectivity – particularly salient as the Council considers making greater use of Cloud technology, hosted off Island.

We were provided with four documents, setting out IT's plans regarding managing a continuity incident:

4. Core IT Disaster Recovery Plan.
5. Detailed list of systems, ordered by criticality.
6. List of key applications, with business and technical ownership identified.
7. Server recovery contract with Adam Continuity.

The last revision to the main IT Disaster Recovery Plan is identified as 2013, while our review of all documentation identified a number of elements which are out of date, for example:

- References to staff who are no longer with the Council, both in the main IT Disaster Recovery Plan and the list of system owners.
- References to buildings which are no longer occupied by the Council, in both the main IT Disaster Recovery Plan and detailed list of systems by criticality.

We also noted that while the Server Recovery Contract is current the version provided for our review was not signed by a representative from Adam – the provider should be contacted to source an appropriately signed copy. While the wider documentation is still broadly fit for purpose it should be reviewed and updated, specifically to address the areas identified above.

One of the areas which has been an issue historically is service areas having unrealistic expectation of what they can expect from IT, in the event of a continuity incident. To validate that service areas expectations are realistic we reviewed business continuity plans for the Civic Centre in Sandown, where a number of key Council services are located, for example Revenues and Benefits, Payments and Car Parking and the business continuity plan for the Contact Centre.

The Civic Centre Business Continuity Plan is up to date, last reviewed in April 2015. It also identifies alternative processing arrangements and potentially working in partnership with Portsmouth Council (who use substantively the same systems in most areas), if systems are down for in excess of two weeks. However we did note that all systems used at Sandown are 'priority 3', identified as taking up to four weeks to restore in the main IT Disaster Recovery Plan. The whole area of system criticality would benefit from being revisited to confirm that systems are correctly categorised – if, for example, the Council could not process payments or revenue effectively for four weeks this could have a significant adverse impact on claimants and the whole Council.

The Contact Centre Plan identifies alternative processing sites, with a monthly offline extract of key data, for example contact numbers, sufficient to cover agreed downtime until the core Council systems, for example CRM are restored.

The majority of systems are hosted in the main Data Centre in County Hall; we confirmed:

- Centralised UPS (Uninterruptable Power Supplies) are in place for all systems, further backed by a diesel power generator on site.
- Centralised air conditioning is in place.
- Multiple redundancy, for example mirrored disks and multiple connections to branch offices are in place.

- Systems are backed up on daily and weekly cycles, with backups stored remotely in Enterprise House or, for Unix based systems, in a local bank vault.
- Access is limited to IT and premises management staff, with authorisation to be added to the access list required from IT.

To ensure the availability of replacement hardware in the event of a continuity incident we note that the Council has a contract in place with a third party provider and the Contract includes the provision of an annual disaster recovery rehearsal. However this was not carried out in 2015; this should be exercised in 2016, focusing on the most critical systems once this list has been reviewed and updated, as covered above.

As an advisory point, while we didn't identify any issues, the backup log provided for our review is difficult to follow. Consideration should be given to extracting information regarding key systems/servers into a separate spreadsheet, noting the dates of last successful backups. This would help to ensure that, in the event of restoration being required, that a sufficiently recent backup is available.

Risks

Out of date documentation may lead to plans not being fit for purpose if/when required. For example unclear roles/responsibilities and delays in implementing plans due to confusion with incorrect location specified.

Incorrectly prioritised system could lead to poorly focussed restoration effort and an unacceptable impact on services if their restoration does not happen in a sufficiently timely manner.

Delayed/non provision of vital services/money to Island residents.

If disaster recovery is not rehearsed assumptions may prove to be incorrect, ultimately restoration may be delayed, leading to an unacceptable interruption to services.





Finding rating	Agreed actions	Responsible person / title
Medium	The Head of IT, delegating as necessary, will: <ol style="list-style-type: none"> 1. Update the main IT Disaster Recovery Plan and supporting documentation. 2. In collaboration with service areas review and revise the criticality categorisation of systems, to ensure this in in line with the Council's and service needs. 3. Source a signed copy of the Server Recovery Contract. 4. Schedule a disaster recovery rehearsal, focussing on the most critical systems, once this list has been revised, as above. 5. Consider enhancing the recording of backup outcomes, to ensure that sufficiently recent backups are available in the event that restoration is required. 	Gavin Muncaster, Head of IT
		Target Date
		1, 2 & 3. May 2016
		4 & 5. September 2016
		Report reference:
IOW- 21-03		

-Finding rating	Effect on Service	Embarrassment / reputation	Personal Safety	Personal privacy infringement	Failure to provide statutory duties/meet legal obligations	Financial	Effect on Project Objectives/ Schedule Deadlines
Critical	<p>A finding that could result in a:</p> <ul style="list-style-type: none"> Major loss of service, including several important areas of service and /or protracted period. Service Disruption 5+ Days 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Adverse and persistent national media coverage Adverse central government response, involving (threat of) removal of delegated powers Officer(s) and/or Members forced to resign 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Death of an individual or several people 	<p>A finding that could result in:</p> <p>All personal details compromised/ revealed</p>	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Litigation/claims/ fines from Department £250k + Corporate £500k + 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Costs over £500,000 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Complete failure of project/ extreme delay – 3 months or more
High	<p>A finding that could result in a:</p> <ul style="list-style-type: none"> Complete loss of an important service area for a short period Major effect to services in one or more areas for a period of weeks Service Disruption 3-5 Days 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Adverse publicity in professional/municipal press, affecting perception/standing in professional/local government community Adverse local publicity of a major and persistent nature 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Major injury to an individual or several people 	<p>A finding that could result in:</p> <p>Many individual personal details compromised/ revealed</p>	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Litigation/claims/fines from Department £50k to £125k Corporate £100k to £250k 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Costs between £50,000 and £500,000 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Significant impact on project or most of expected benefits fail/ major delay – 2-3 months

-Finding rating	Effect on Service	Embarrassment / reputation	Personal Safety	Personal privacy infringement	Failure to provide statutory duties/meet legal obligations	Financial	Effect on Project Objectives/ Schedule Deadlines
Medium	<p>A finding that could result in a:</p> <ul style="list-style-type: none"> Major effect to an important service area for a short period Adverse effect to services in one or more areas for a period of weeks Service Disruption 2-3 Days 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Adverse local publicity /local public opinion aware Statutory prosecution of a non-serious nature 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Severe injury to an individual or several people 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Some individual personal details compromised/ revealed 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Litigation/claims/fines from Department £25k to £50k Corporate £50k to £100k 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Costs between £5,000 and £50,000 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Adverse effect on project/ significant slippage – 3 weeks–2 months
Low	<p>A finding that could result in a:</p> <ul style="list-style-type: none"> Brief disruption of important service area Significant effect to non-crucial service area Service Disruption 1 Day 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Contained within section/Unit or Directorate Complaint from individual/small group, of arguable merit 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Minor injury or discomfort to an individual or several people 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Isolated individual personal detail compromised/ revealed 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Litigation/claims/fines from Department £12k to £25k Corporate £25k to £50k 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Costs less than £5,000 	<p>A finding that could result in:</p> <ul style="list-style-type: none"> Minimal impact to project/ slight delay less than 2 weeks
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.						

Report classifications

Findings rating	Points
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

Report classification	Points
 Low risk	6 points or less
 Medium risk	7– 15 points
 High risk	16– 39 points
 Critical risk	40 points and over

Appendix B: Terms of Reference

Background and Scope

Three related auditable units are scheduled for review in 2015/16:

- Business Continuity.
- IT Disaster Recovery.
- The Council’s Data Centre.

To make best use of available audit resource we have combined three areas into a single, cross cutting review. This audit will review overall business continuity arrangements, with a focus on ensuring that arrangements are risk focussed, realistic and sufficiently flexible to accommodate ongoing changes to the Council while continuing to be effective. As part of our sample testing we will review a subset of services’ expectations of IT, to ensure that these have been confirmed as realistic with IT, specifically regarding agreed data loss and system resumption timeframes.

Specific to the Data Centre we will review overall arrangements covering resilience, physical and environmental controls to ensure that availability is maximised and the Data Centre is physically secure.

The control objectives and potential related risks included in this review are:

	Control objective	Potential risks
1	<p>Business Continuity</p> <ul style="list-style-type: none"> • A Business Impact Analysis (BIA) has been carried out in the last 12 months, which categorises services by criticality and has been approved by senior management. • The Emergency Management Team hold plans for the most critical areas (service areas where any interruption to service is unacceptable); arrangements for these areas are tested annually. • Corporate expectations are documented for non-critical areas; these have been approved by senior management and communicated to service areas. Requirements are pragmatic and flexible, to accommodate ongoing changes at the Council. • A sustainable level of quality assurance is in place for non-critical areas. 	<p>If a BIA has not been used to identify the most critical functions, effort may be wasted on areas which are not critical, or areas which should have been identified as critical may not have appropriate arrangements in place.</p> <p>If copies of business continuity plans for critical areas are not held centrally they may not be available in the event of a continuity incident.</p> <p>If plans have not been reviewed/quality assured and tested (for critical areas) they may not be in line with the needs of the Council.</p>
2	<p>IT Disaster Recovery</p> <ul style="list-style-type: none"> • There is ongoing liaison between IT and Emergency Management, to ensure that IT arrangements are in line with corporate need. • There is an up to date, approved IT Disaster Recovery Plan. • The order in which systems will be restored is categorised according to criticality, as agreed between business areas and IT. • Expectations of IT from service areas have been confirmed with IT as realistic. • All data necessary to support resumed service in line with the IT Disaster Recovery plan has been identified and is included as required in 	<p>Without ongoing liaison between IT and the team responsible for overall continuity, IT Disaster Recovery may not be in line with the Council’s requirements; IT Disaster Recovery may be insufficiently focussed on maintaining service delivery by the wider Council.</p> <p>If an up to date IT Disaster Recovery plan is not available IT service resumption may be delayed leading to unnecessary interruption to service delivery in the wider Council.</p>

	Control objective	Potential risks
	<p>backup arrangements. Backups are carried out through daily, weekly and monthly cycles and stored offsite.</p> <ul style="list-style-type: none"> • Arrangements have been made to ensure the availability of replacement hardware, sufficient to resume service in line with agreed service levels. • The IT Disaster Recovery plans are table top tested by IT management at least annually; resumption of systems are tested in a rolling programme, in line with business need. 	<p>If systems are not categorised in order of business criticality, IT effort may not be focussed in line with the needs of the wider Council.</p> <p>If accurate, complete and timely backups are not available, in the event of a continuity incident, service resumption may be delayed or data may be lost.</p> <p>If recovery plans have not been tested they may prove to be unrealistic in the event of a continuity incident.</p>
3	<p>The Council's Data Centre</p> <ul style="list-style-type: none"> • Access to the Data Centre is restricted to staff authorised by IT. • Multiple redundant, error tolerant hardware and parallel processing have been implemented, including connectivity to branch offices, where justified by business need and any single points of failure have been identified and appropriately mitigated. • The Council's Data Centre incorporates environmental controls and technology to ensure the continuous availability of power, as justified by business need. 	<p>If unauthorised personnel can gain access then data security will be more likely to be compromised.</p> <p>If redundancy is not implemented, as justified by business need, then there may be unnecessary interruptions to service delivery by the wider Council.</p> <p>If appropriate environmental controls are not in place there could be an unacceptable interruption to service, for example as a result of servers overheating.</p>

Audit approach

Our audit approach is as follows:

- Obtain an understanding of Business Continuity, IT Disaster Recovery and Data Centre oversight arrangements, reporting processes and financial and risk management controls through discussions with key personnel and review of systems documentation.
- Identify the key risks to the effective management and oversight of Business Continuity, IT Disaster Recovery and Data Centre.
- Evaluate the design of the controls in place to address the key risks.
- Test the operating effectiveness of the key controls.

Internal audit team

Name	Title	Role	Contact details
Emma Butler	Director	Engagement Leader	emma.butler@uk.pwc.com
Dan Deacon	Manager	Engagement Manager	daniel.r.deacon@uk.pwc.com
Geraint Newton	Senior Associate	Auditor	geraint.newton@uk.pwc.com

Key contacts – Isle of Wight Council

Name	Title	Contact details
Gavin Muncaster	Head of IT	gavin.muncaster@iow.gov.uk
Darren Steed	Head of Emergency Management	darren.steed@iow.gov.uk

Timetable

Fieldwork start	4th January 2016
Fieldwork completed	18th March 2016
Draft report issued to Head of Internal Audit	The draft report will be issued to the Head of Internal Audit within 10 working days of the completion of fieldwork.
Head of Internal Audit response due by	The Head of Internal Audit will provide comments on draft report within 2 working days of receiving the report.
Draft report issued to Audit Sponsor	The draft report will be issued to the Audit Sponsor within 10 working days of the completion of fieldwork.
Management response due by	The Audit Sponsor will provide the Head of Internal Audit with a complete written response to the internal audit report within 10 days of receipt of the draft report. Where there is disagreement over the report or recommendations, these must be resolved within 10 working days of the problem being highlighted.
Final report issued by	Final report will be issued to the Head of Internal Audit for issue to the Audit Sponsor 5 working days of receiving the management response.
Client satisfaction survey	A client satisfaction survey will be issued following each audit. You may wish to consider this throughout the audit.

Agreed timescales are subject to the following assumptions:

- All relevant documentation, including source data, reports and procedures, will be made available to us promptly on request
- Staff and management will make reasonable time available for interviews and will respond promptly to follow-up questions or requests for documentation

Information requested

Below is a list of information we expect to have available on the first day of the audit:

- Copy of most recent Business Impact Assessment and evidence of approval.
- Plans for areas identified as critical and evidence of testing.
- Expectations of non-critical areas, evidence of communication and quality assurance.
- IT Continuity Plan.
- Inventory of systems including information necessary for resumption, evidencing categorisation by criticality, based on business need.
- Any relevant policies which relate to continuity, for example Backup Policy.
- Backup schedule and/or process notes.
- Outputs from backups, showing that backups are verified.
- Copies of any relevant support contracts, for example server replacement, including agreed response times in line with the requirements of the IT Disaster Recovery Plan.
- Details of testing carried out in last 12 months.
- Details regarding how the Data Centre is secured and list of staff with access.
- Documentation relating to key infrastructure items identifying where redundancy is deployed and any single points of failure along with mitigation.
- Documentation relating to the Council's Data Centre, evidencing deployment of environmental controls and uninterruptable power supplies.

Appendix C: Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken the review of the Business Continuity and IT Disaster Recovery arrangements subject to the limitations outlined below.

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

Our assessment of controls relating to the Business Continuity and IT Disaster Recovery arrangements is for controls effective from April 2015 to February 2016. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- the degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.

