IT Audit Services

Durham County Council

IT Audit Review – 2014/2015

Limited IT system review - 31st March 2015
Durham County Council

Engagement Summary

Engagement Summary

International Standards on Auditing require us to obtain an understanding of the control environment in place at Durham County Council ('the Council'), including the risks arising from its use of IT. This report summarises the work we have undertaken and conclusions reached in respect of our work on the general IT control environment as part of our work on the 2014/15 financial statements.

The principal objectives of our work were to:

- update our understanding of the Council's IT environment;
- undertake a review of the general IT controls in place; and
- make recommendations as to how the general IT controls could be improved.

Scope of our work

We have undertaken work in the following areas:

IT mapping and data flow

We have updated our understanding of the IT applications relevant to the Council's financial statements.

IT Oracle transition project understanding

We obtained an understanding of the project by documenting the project overview and completing data migration testing.

IT general controls

We have carried out walked-through and evaluated the internal controls within the Council's IT environment (local applications and infrastructure) in relation to:

- physical security;
- back-up and disaster recovery plan;
- access management and logical security;
- strategy and internal control; and
- change management.

IT general controls testing

We have assessed the operating effectiveness of controls relating to:

- physical access;
- access management;
    - granting access;
    - terminating access; and
    - changing access.
- application access;
- anti-virus system;
- daily checks;
- data protection; and
- change management.

We have not undertaken any testing of application specific controls and this report should not be considered a comprehensive record of all potential weaknesses that exist within the Council's IT systems.

Limitations of use

This report is designed to provide an analysis of our findings for IT officers and is not a public report. The contents of this report are confidential and are not for distribution to anyone other than Durham County Council. Third parties cannot be made aware of this document without the prior written consent of Mazars. Mazars declines all responsibilities regarding third parties who may choose to use or rely on the information contained within this document.

Engagement summary

As part of our review, we conducted a series of interviews with Council officers and would like to thank them for the time they committed to our work and the positive manner that they approached the review. A list of officers involved in this work is provided below.

Name	Role
Bernard Haston	IT Project Manager
Steve Hodgson	Technical Services Manager
Norman Maccoy	ICT Project Leader Internal Applications
Keith Munroe	Finance Manager – Systems Development
Michael Ross	Financial Systems Support Manager

Summary of our findings – IT General Controls (1/7)

Domain	Weaknesses	Identified Risks	Recommendations
Disaster Recovery Plan	No formalised Disaster Recovery Plan (DRP) was identified at the time of our review. Nevertheless the DRP was under development and a Business Continuity Place was formalised and is annually reviewed and tested.	Loss of data Impossibility of data recovery and business continuity	To ensure proper and timely support of the Council's operational activity in the event of a major incident or disaster, we recommend: ▪ documenting a formalised Disaster Recovery Plan suitable for the Council's systems and operations; ▪ ensuring the Disaster Recovery Plan is acknowledged by all relevant staff; and ▪ periodically testing the Disaster Recovery Plan; business users should also be included in the testing, and a formalised test report should be documented for monitoring and audit purposes. **Client comments:** The DRP is made up from elements of the ICT Business Continuity Plan and the Backup/Restore Policies. These documents have been developed and reviewed recently (in line with the review policy). A test plan is being developed in conjunction with the Corporate Business Continuity Board and will take place by the end of November 2015.
Logical Security (network)	From a total number of 19,842 users, 762 generic accounts were identified at domain level (including 1 account with administrative privileges).	Unauthorised access Lack of traceability and accountability for network operations	In order to avoid unauthorised access to the Council's network and data we recommend disabling generic accounts when they are inactive. Also, in order to ensure proper traceability and accountability for operations, we recommend replacing all internal generic accounts with privileged rights to nominal accounts. **Client comments:** Generic accounts are now reviewed regularly and any activity by accounts with administrator privileges is logged using the corporate logging system (Logpoint).

High | Medium | Low

Risk Level

Durham County Council

MAZARS

Summary of our findings – IT General Controls (2/7)

Domain	Weaknesses	Identified Risks	Recommendations
Logical Security (network)	No regular user review is in place at domain level.	Unauthorised access	To ensure access to the Council's network is appropriately restricted, we recommend disabling generic accounts when they are inactive . We also recommend implementing a periodic review aiming to determine if their accounts are still required, covering: • users that have not logged on for more than 30-90 days; • generic accounts; and • administrative accounts. **Client comments:** This recommendation will be implemented by the end of November 2015
Logical Security (network and applications)	During our user access management testing, from the 40 selected leavers, we were not provided with evidence supporting the process for 36.	Unauthorised access Lack of a unitary performance of the process Lack of audit and monitoring	In order to avoid unauthorised access, and to enforce proper monitoring and compliance with the user access management processes, we recommend ensuring that: • disabling access for leavers is requested on a timely basis; • all leavers have disabling requests; and • access is restricted to a need-to-have basis. **Client comments:** The 'leavers process' has been reviewed recently and Senior Managers have disabled and deleted accounts to ensure that inappropriate access is no longer available. This activity is now being carried out on a regular (monthly) basis.

Summary of our findings – IT General Controls (3/7)

Domain	Weaknesses	Identified Risks	Recommendations
Logical Security (applications)	No formalised periodic review is in place at applications level.	Unauthorised access	In order to avoid unauthorised access to the Council's programs and data, we recommend implementing a periodic review of the following, to determine if the accounts are still needed: • users that have not logged on for more than 30-90 days; • generic accounts; and • administrative accounts. **Client comments:** This recommendation will be implemented by the end of August 2015.

Durham County Council

High Medium Low

Risk Level

MAZARS

Summary of our findings – IT General Controls (4/7)

Domain	Weaknesses	Identified Risks	Recommendations
Logical Security (applications)	Generic accounts were identified at application level during our review, as follows: • **Oracle EBS**: From 2,200 users, we identified 143 generic accounts; • **Northgate**: From 486 users, we identified 69 generic accounts; • **ResourceLink_Bureau**: From 158 users, we identified 7 generic accounts; • **ResourceLink_Salaries**: From 357 users, we identified 9 generic accounts; • **ICON**: From 1,862 users, we identified 7 generic accounts (including 1 administrator). • **IPF:** From 165 users, 4 generic accounts were identified (including 2 with administrative rights). Also, 35 users have not logged on to IPF for more than one year (including one generic account); No information was provided for Financial Director, Civica Revenues & Benefits, Orchard, Civica Housing.	Unauthorised access Lack of traceability and accountability	To ensure access to the Council's programs and data is appropriately restricted, we recommend disabling generic accounts when not used. We also recommend implementing a periodic review aiming to determine if their accounts are still required, covering: • users that have not logged on for more than 30-90 days; • generic accounts; and • administrative accounts. **Client comments:** Generic accounts have been reviewed and disabled/deleted as appropriate. Generic accounts will be reviewed on a quarterly basis.

High Medium Low

Risk Level

Summary of our findings – IT General Controls (5/7)

Domain	Weaknesses	Identified Risks	Recommendations
Logical Security (applications)	No formalised policy/procedure was documented for governing the user access management at application level.	Lack of a unitary understanding and performance of the process	To ensure formal responsibility and commitment, we recommend implementing a formalised procedure/policy governing user access management. This should cover all process steps, including: • access request initiation; • access request authorisation; • access granting/disabling; • review and monitoring. **Client comments:** This process is now managed through the ICT Service Desk with periodic reviews in line with the recommendations above.
Logical Security (applications)	Deficiencies were identified with application password settings, as follows: • **minimum length**: the system default credentials are used for Resource Link, 7 characters (complexity enforced) are used for IPF and Northgate Housing; • **no information** regarding password settings was provided for Financial Director, Civica Benefits & Revenues, Orchard, Civica Housing; and • **no information** regarding the account lockout settings was provided for SSID.	Unauthorised access	In order to ensure access to the Council's programs and data is appropriately restricted, we recommend considering the best practices for password settings: • **minimum length**: 8 characters, complexity enabled; • **Account lockout**: user account should be automatically locked after several unsuccessful logon attempts. **Client comments:** Agreed.

High Medium Low

Risk Level

Summary of our findings – IT General Controls (6/7)

Domain	Weaknesses	Identified Risks	Recommendations
Change Management (network and infrastructure)	It was noted that no standardised change management procedure is in place for registering, classifying and tracking the network change requests; however monitoring is performed through the Network Configuration Management Systems program, keeping logs for changes performed, including historical configuration and user who performed the change.	Unauthorised access Lack of traceability and accountability	To ensure no unauthorised changes are implemented affecting the Council's network and infrastructure, we recommend implementing a standardised process. This should be managed through a dedicated system that would allow categorising, tracing and monitoring changes. The process should be formalised under dedicated procedures/policies and acknowledged by all relevant staff. **Client comments:** The ICT Management Team is reviewing change management. Given the scale, complexity and interdependency of the ICT systems, networks and service platforms, it is likely that it will take some time to develop a fully coordinated change management procedure. This recommendation is agreed and will be completed by the end of March 2016.
Change Management (applications)	No proper segregation of duties is enforced for change management processes, as the same team (applications super users) perform both development and migration into production of changes.	Unauthorised changes	To avoid unauthorised changes being deployed on the Council's systems, we recommend ensuring proper segregation of duties between development and migration into production of changes. If the limitation or allocation of resources does not allow full segregation of duties, we recommend ensuring close monitoring of changes being deployed on the Council's systems. **Client comments:** This separation of duties is difficult when budgets and staff numbers are reducing. However, by maintaining separation of operational activities and higher level system administrative functions, logging can be used to track and monitor changes in system state. This separation and logging is in place.

High | Medium | Low

Risk Level

Summary of our findings – IT General Controls (7/7)

<table>
<tr><th>Domain</th><th>Weaknesses</th><th>Identified Risks</th><th>Recommendations</th></tr>
<tr>
<td>Oracle Migration Project</td>
<td>
Although the project has been performed to a good standard of quality, the data reconciliation strategy was not identified at the beginning of the project, leading to data reconciliation during live migration has not fully covered completeness and accuracy of transactions. The number of transaction has not been reconciled and the deficiencies identified needed further detailed investigation.

Detailed testing was performed by the financial audit team. The risk level was assessed as low.

<u>Accounts Receivables</u>
<table>
<tr><th>Op Unit</th><th>Report</th><th>Pre Upgrade</th><th>Post Upgrade</th><th>Difference</th></tr>
<tr><td>DUR</td><td>Receipts Register</td><td>51,069,333.66</td><td>51,064,382.76</td><td>4,950.90</td></tr>
<tr><td>DUR</td><td>Tax Rec - Gross</td><td>50,756,529.67</td><td>50,733,493.58</td><td>23,036.09</td></tr>
<tr><td>FRA</td><td>Receipts Register</td><td>2,963,291.10</td><td>3,564,660.61</td><td>-601,369.51</td></tr>
<tr><td colspan="5"><u>Accounts Payables</u></td></tr>
<tr><th>Op Unit</th><th></th><th>Pre Upgrade</th><th>Post Upgrade</th><th>Difference</th></tr>
<tr><td>DCC</td><td>Posted Payments Register</td><td>106,532,374.83</td><td>106,573,520.42</td><td>-41,145.59</td></tr>
<tr><td>DCCT</td><td>Tax Audit Trail</td><td>1,315.74</td><td>1,425.74</td><td>-110.00</td></tr>
<tr><td>DCC</td><td>Tax Audit Trail</td><td>51,905,632.73</td><td>51,412,672.20</td><td>492,960.53</td></tr>
<tr><td>DVH</td><td>Tax Audit Trail</td><td>146,557.27</td><td>146,111.42</td><td>445.85</td></tr>
<tr><td>FRA</td><td>Tax Audit Trail</td><td>1,872,494.59</td><td>1,875,607.79</td><td>-3,113.20</td></tr>
<tr><td colspan="5"><u>CM Report Comparison - LIVE</u></td></tr>
<tr><th>Op Unit</th><th>Bank Account</th><th>Pre Upgrade</th><th>Post Upgrade</th><th>Difference</th></tr>
<tr><td>DUR</td><td>County Fund</td><td>- 520,503,775.09</td><td>-519,338,649.06</td><td>- 1,165,126.03</td></tr>
</table>
</td>
<td>Compromising the data integrity through migration process</td>
<td>
To ensure data is correctly and completely migrated between systems/ versions, we recommend ensuring proper testing/reconciliation is performed. This should include:
• Cross-checking the number of transactions between the systems;
• Cross-checking amounts per detailed category (e.g. per account), not limited to totals.

<u>Client comments:</u>

Agreed. Clear testing and reconciliation procedures will be included in the scope of future system migrations/upgrades.
</td>
</tr>
</table>

Durham County Council

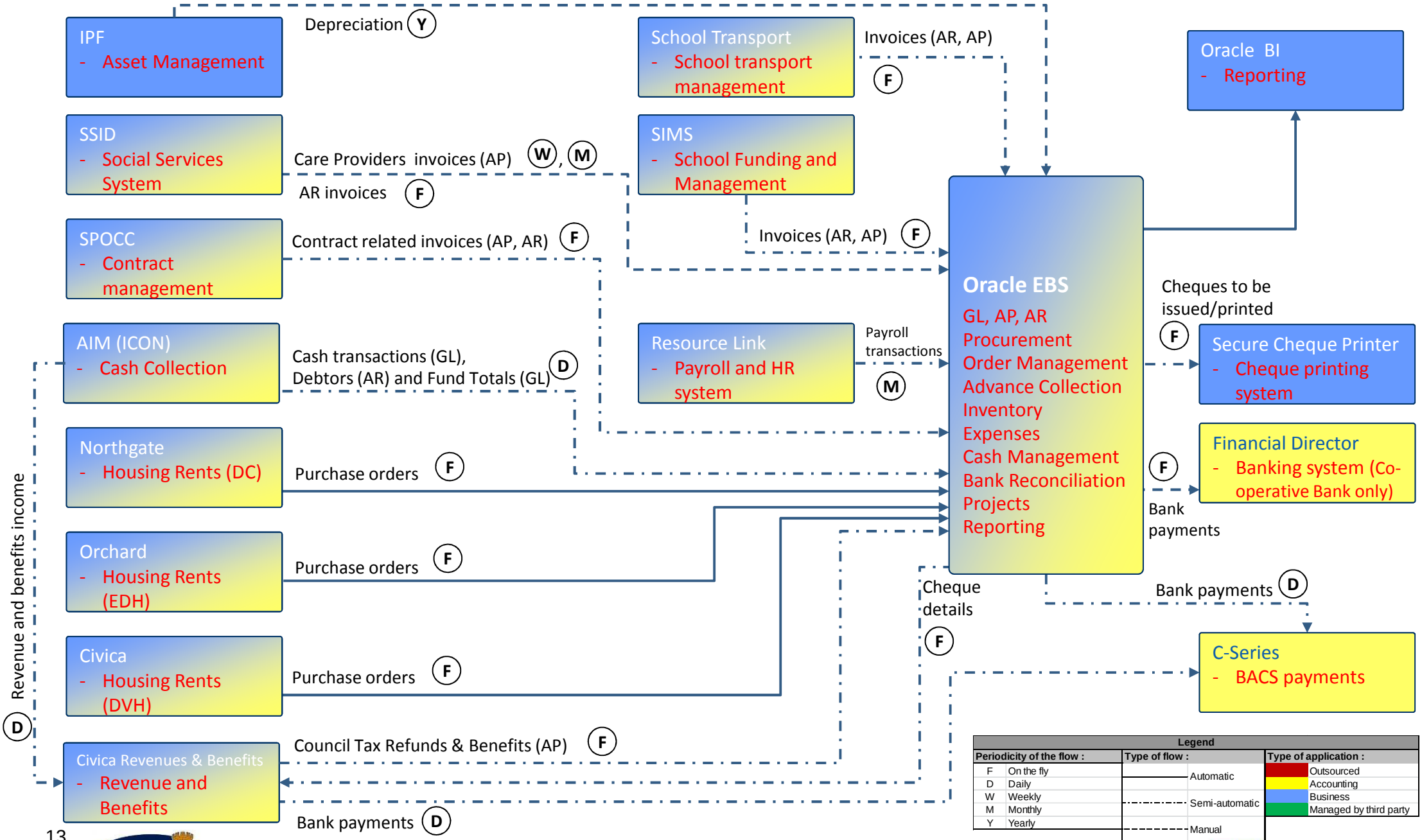
High Medium Low

Risk Level

MAZARS

I. IT Systems Mapping

I. IT SYSTEMS MAPPING – Durham County Council, 2nd April 2015



Durham County Council

MAZARS

I. IT SYSTEMS MAPPING – Details (1/3)

Application	Functionalities	Users	Maintenance contract
Oracle EBS Editor: Oracle Database: Oracle	Enterprise Resource Planning (ERP) system, managing: • GL, AP, AR; • Procurement; • Order Management; • Advance Collection; • Inventory; • Expenses; • Cash Management; • Bank Reconciliation; • Projects; • Reporting.	2 466 users	• Software contracts: Oracle; • Hardware contracts: Dell.
Civica Revenues & Benefits Editor: Civica	Revenues & Benefits system, managing: • Council Tax (CTAX) contributors; • National Non-Domestic Rates (NNRD) contributors; • Payments and rates for CTAX and NNDR.		• Software contracts: Civica; • Hardware contracts: Dell.
ICON (AIM) Editor: Capita	System used for cash collection, fed from: • Paye.net – on-line payments from individuals; • Capita – pay point cash payments from individuals (ACR – Cash Receipting).	1 005 users	• Software contracts: Capita; • Hardware contracts: Dell.

I. IT SYSTEMS MAPPING – Details (2/3)

Application	Functionalities	Users	Maintenance contract
Northgate Editor: Northgate	Pre LSVT - Housing system used covering **Durham City** area. The system manages: • Housing rents; • Properties; • Applicants.	492 users	• Software contracts: Northgate; • Hardware contracts: Dell.
Orchard Editor: Orchard	Pre LSVT - Housing system used covering **East Durham** area. The system manages: • Housing rents; • Properties; • Applicants.		• Software contracts: Orchard; • Hardware contracts: Dell.
Civica Housing Editor: Civica	Pre LSVT - Housing system used covering **Dale & Valley** area. The system manages: • Housing rents; • Properties; • Applicants.		• Software contracts: Civica; • Hardware contracts: Dell.

I. IT SYSTEMS MAPPING – Details (3/3)

Application	Functionalities	Users	Maintenance contract
IPF Editor: CIPFA	Fixed Assets Management system. The system does not feed directly into the GL, and issues no journal entries. The only impact upon the Council's accounts is the yearly depreciation manually transferred into the GL.	165 users	• Software contracts: CIPFA; • Hardware contracts: Dell.
SSID	Adult and Children Social Care Management System , managing: • Contracts and referrals; • Assessment plans; • Care commissioning; • Personal budgets; • Adult social care payments; • Foster care payments;	2 837 users	• Software contracts: No information provided; • Hardware contracts: Dell.
Resource Link Editor: Northgate	Integrated HR and Payroll system, managing: • Recruitment process; • Human resources information (jobs, employees details, pay scale, etc.); • Payroll; • Pensions and absence information;	357 users	• Software contracts: Northgate; • Hardware contracts: Dell.
Financial Director Editor: Co-op Bank	Banking system used for Co-operative Bank transactions. The system will be out of use in the next financial year.	N/A	• Software contracts: Co-operative Bank; • Hardware contracts: Dell.

I. IT SYSTEMS MAPPING – Details (3/3)

Application	Functionalities	Users	Maintenance contract
SPOCC	Contract Management system.		• Software contracts: No information provided; • Hardware contracts: Dell.
School Transport	School Transport Management system, managing funds and costs for school transportation.	N/A	• Software contracts: N/A; • Hardware contracts: N/A.
SIMS	System used by schools in order to manage allocated budget and related expenses. Feeds expenses and invoices information into Council's accounts.	N/A	• Software contracts: N/A; • Hardware contracts: N/A.
C-Series Editor: Xpress Software Solutions	Banking system used for BACS transactions.		• Software contracts: Xpress Software Solutions; • Hardware contracts: Dell.
Secure Cheque Printer	System used for cheque printing. Cheques information is received from Oracle EBS, and the system is used for automatically arranging the information in a cheque printable format.	N/A	• Software contracts: N/A; • Hardware contracts: Dell.

I. IT SYSTEMS MAPPING – Interfaces description (1/3)

Outgoing application	Incoming application	Data stream type	Flow periodicity	Data stream and monitoring description	Control manager
IPF	**Oracle**	Manual	Yearly	Fixed assets depreciation is manually input into Oracle based on IPF calculations.	N/A
School Transport	**Oracle**	Semi-automated	Ad-hoc	Schools transport invoices (AP, AR) data is transferred towards Oracle.	N/A
SIMS	**Oracle**	Semi-automated	Ad-hoc	Schools expenses and invoices are transferred into the Schools costs (GL accounts).	N/A
AIM	**Civica Benefits & Revenues**	Semi-automated	Daily	Collection data regarding Council Tax and National Non-Domestic Rates is transferred to the Revenues & Benefits system.	N/A

I. IT SYSTEMS MAPPING – Interfaces description (1/3)

Outgoing application	Incoming application	Data stream type	Flow periodicity	Data stream and monitoring description	Control manager
SSID	**Oracle**	Manual	Weekly, Monthly	Care providers AP invoices information is fed into GL.	N/A
SSID	**Oracle**	Semi-automated	Ad-hoc	Care providers AR invoices information is fed into GL.	N/A
SPOCC	**Oracle**	Semi-automated	Ad-hoc	Contract related invoices information is fed into GL semi-automated.	N/A
AIM	**Oracle**	Semi-automated	Daily	Cash transactions information (amount, debtors, fund totals) is fed into Oracle on a daily basis.	N/A

I. IT SYSTEMS MAPPING – Interfaces description (1/3)

Outgoing application	Incoming application	Data stream type	Flow periodicity	Data stream and monitoring description	Control manager
Resource Link	**Oracle**	Semi-automated	Monthly	Payroll transactions generated in Resource Link are transferred monthly into GL.	N/A
Northgate	**Oracle**	Automated	Ad-hoc	Housing purchase orders for Durham City area are automatically fed into Oracle.	N/A
Orchard	**Oracle**	Automated	Ad-hoc	Housing purchase orders for East Durham area are automatically fed into Oracle.	N/A
Civica Housing	**Oracle**	Automated	Ad-hoc	Housing purchase orders for Dale & Valley area are automatically fed into Oracle.	N/A

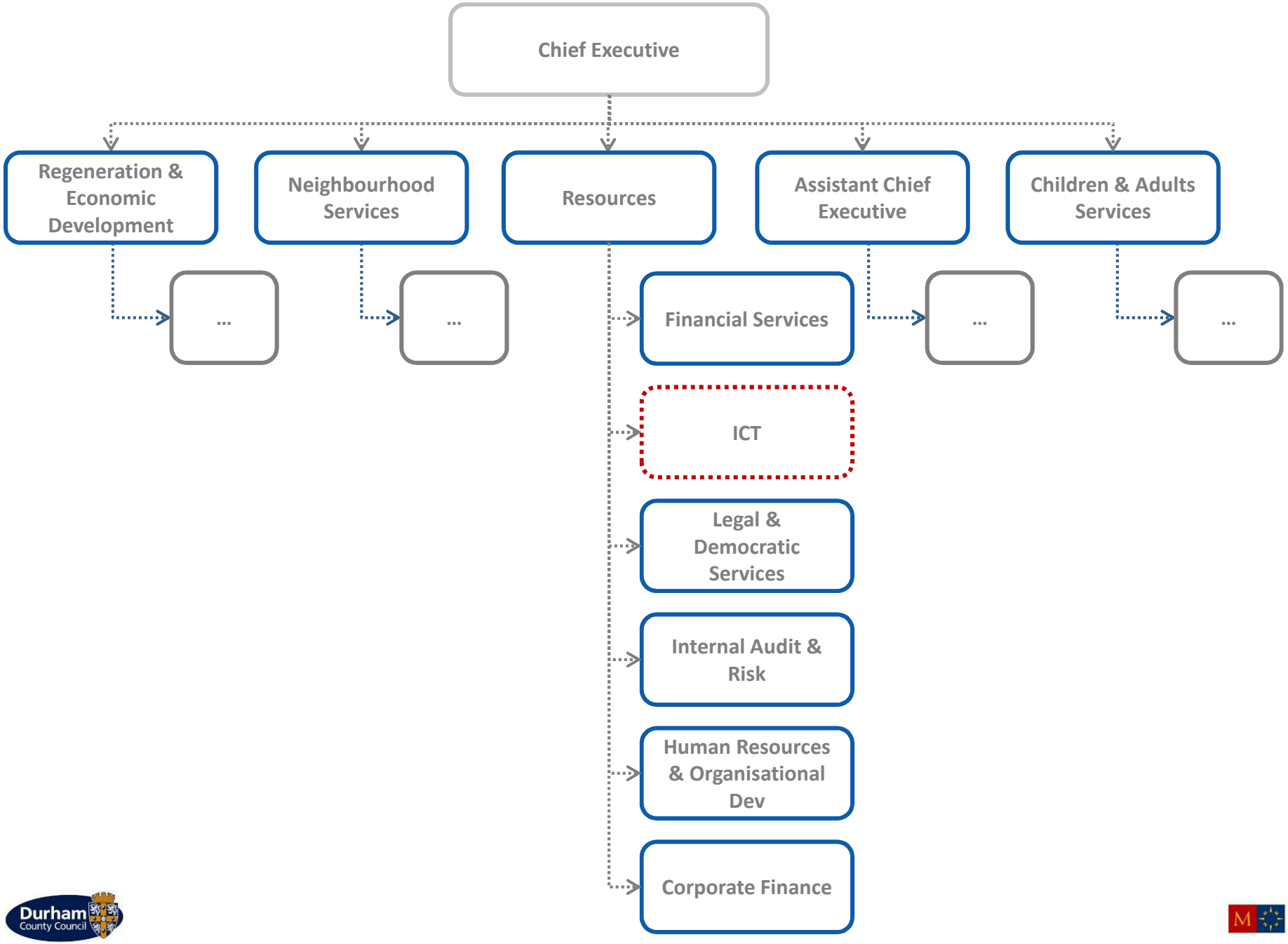
I. IT SYSTEMS MAPPING – Interfaces description (1/3)

Outgoing application	Incoming application	Data stream type	Flow periodicity	Data stream and monitoring description	Control manager
Civica Revenues & Benefits	**Oracle**	Semi-automated	Ad-hoc	Council Tax and Non-Domestic Rates refunds are fed into Oracle.	N/A
Oracle	**Civica Revenues & Benefits**	Semi-automated	Ad-hoc	Cheque details are transferred from Oracle to the Revenues & Benefits system.	N/A
Civica Revenues & Benefits	**C-Series**	Semi-automated	Daily	Bacs transactions to the Co-operative Bank are generated in Civica Revenues & Benefits and sent to C-Series for bank transfer.	N/A
Oracle	**C-Series**	Semi-automated	Daily	Bacs transactions to the Co-operative Bank are generated in Oracle and sent to C-Series for bank transfer.	N/A

I. IT SYSTEMS MAPPING – Interfaces description (1/3)

Outgoing application	Incoming application	Data stream type	Flow periodicity	Data stream and monitoring description	Control manager
Oracle	**Financial Director**	Semi-automated	Daily	Bacs transactions to the Co-operative Bank are generated in Oracle and sent to Financial Director for bank transfer.	N/A
Oracle	**Secure Cheque Printer**	Semi-automated	Daily	Cheques information is generated in Oracle and sent to Secure Cheque Printer, where it is formatted in order for the cheque to be printed. No data alteration is possible in Secure Cheque Printer – only formatting and printing functions. **Control**: Cheques amounts are reconciled with Oracle transactions.	Finance Department

I. Organisation chart



II. Oracle migration Project Overview

Durham County Council

MAZARS

Oracle Migration Project Overview

Control Objective

To ensure that migration project has been appropriately planned, managed and performed.

Risks/Possible implications

- Business risks: profitability, reputation , regulation;
- IT Risks: data loss, application stability, cut-over aborts, extended downtime, budget overruns, delays; and
- Data Migration Risks: completeness risk, semantic risks, corruption risks, stability risks, execution time risks.

Work detail

Migration background

Until 2014 the Council had been using Oracle EBS version 11.5.10. Extended support for 11.5.10 ended in December 2013. Oracle had provided exceptional extended support to it's clients until December 2014. The need to migrate to version 12.1.3 was considered by the Council in 2013. The actual migration occurred in November 2014.

Project Review

We obtained and reviewed the project documentation supporting the main stages of the project, namely:

- **Planning:** A project plan was designed at the beginning of the project, clearly stating all activities to be undertaken, assigning an owner and estimated time for completion - the plan was regularly reviewed and updated as required;
- **Project meetings:** Regular project meetings were conducted with all relevant teams, including Pension Fund team members;
- **Testing:** two test iterations were performed and documented; during both test phases the Council performed test migration of data;
- **Go-live and project monitoring:** A fault register was issued and permanently monitored in order to ensure issues and risks are timely identified and appropriately addressed; and
- **Reconciliation of transferred data:** The Council has reconciled the transferred data by totals in divisions by operational units and accounting areas. There were several differences found during the reconciliation, which the Council has addressed but not documented the solution process and results.

Please refer to the following slide for the testing details and the main conclusions.

Oracle Migration Project Overview

Work detail

Reconciliation of Accounts Payables, Accounts Receivables, Inventory, Transaction log and Projects:

Accounts Receivables

Op Unit	Report	Pre Upgrade	Post Upgrade	Comments
CDDC	Aging 7 Buckets - By Account	-2.22	-2.22	OK
CDDC	Transaction Register	No Data	No Data	OK
CDDC	Receipts Register	-5869.51	-5,869.51	OK
CDDC	Tax Rec - Gross	-4,997.42	-4,997.42	OK
CDDC	Tax Rec - Tax	-872.09	-872.09	OK
DCCT	Aging 7 Buckets - By Account	0	0	OK
DCCT	Transaction Register	No Data	No Data	OK
DCCT	Receipts Register	1,178.74	1,178.74	OK
DCCT	Tax Rec - Gross	1,178.74	1,178.74	OK
DCCT	Tax Rec - Tax	0.00	0.00	OK
DDC	Aging 7 Buckets - By Account	Not run	Not run	OK
DDC	Transaction Register	Not run	Not run	OK
DDC	Receipts Register	Not run	Not run	OK
DDC	Tax Reconciliation	Not run	Not run	OK
DUR	Aging 7 Buckets - By Account	18,020,809.70	18,020,809.70	OK
DUR	Transaction Register	6,712,355.88	6,712,355.88	OK
DUR	Receipts Register	51,069,333.66	51,064,382.76	4,950.90
DUR	Tax Rec - Gross	50,756,529.67	50,733,493.58	23,036.09
DUR	Tax Rec - Tax	135,124.77	135,124.77	OK
DVH	Aging 7 Buckets - By Account	321,471.29	321,471.29	OK
DVH	Transaction Register	1,907,761.20	1,907,761.20	OK
DVH	Receipts Register	1,401,929.94	1,401,929.94	OK
DVH	Tax Rec - Gross	1,033,786.14	1,033,786.14	OK
DVH	Tax Rec - Tax	312,331.44	312,331.44	OK
FRA	Aging 7 Buckets - By Account	770,136.28	770,136.28	OK
FRA	Transaction Register	287,170.10	287,170.10	OK
FRA	Receipts Register	2,963,291.10	3,564,660.61	-601,369.51
FRA	Tax Rec - Gross	3,182,237.23	3,182,237.23	OK
FRA	Tax Rec - Tax	47,744.52	47,744.52	OK
PEN	Aging 7 Buckets - By Account	218,822.43	218,822.43	OK
PEN	Transaction Register	440,391.56	440,391.56	OK
PEN	Receipts Register	7,937,825.06	7,937,825.06	OK
PEN	Tax Rec - Gross	7,911,084.54	7,911,084.54	OK
PEN	Tax Rec - Tax	2,864.31	2,864.31	OK
SDC	Aging 7 Buckets - By Account	8,543.67	8,543.67	OK
SDC	Transaction Register	101,778.06	101,778.06	OK
SDC	Receipts Register	119,144.72	119,144.72	OK
SDC	Tax Rec - Gross	124,356.93	124,356.93	OK
SDC	Tax Rec - Tax	16,899.69	16,899.69	OK

Accounts Payables

Op Unit		Pre Upgrade	Post Upgrade	Difference
CDDC	Accounts Payable Trial Balance	-6	-6.00	0.00
DCCT	Accounts Payable Trial Balance	0	0.00	0.00
DCC	Accounts Payable Trial Balance	3,339,365.13	**3,339,365.13**	0.00
DVH	Accounts Payable Trial Balance	1,175.36	**1,175.36**	0.00
FRA	Accounts Payable Trial Balance	95,434.43	**95,434.43**	0.00
PEN	Accounts Payable Trial Balance	0.00	0.00	0.00
SDC	Accounts Payable Trial Balance	0.00	0.00	0.00
CDDC	Posted Invoice Register	0	0.00	0.00
DCCT	Posted Invoice Register	14,104.53	14,104.53	0.00
DCC	Posted Invoice Register	106,454,217.23	-106,454,217.23	0.00
DVH	Posted Invoice Register	992,082.36	-992,082.36	0.00
FRA	Posted Invoice Register	4,921,410.62	-4,921,410.62	0.00
PEN	Posted Invoice Register	6,695,051.59	-6,695,051.59	0.00
SDC	Posted Invoice Register	118,737.61	-118,737.61	0.00
CDDC	Posted Payments Register	0.00	0.00	0.00
DCCT	Posted Payments Register	15,548.45	15,548.45	0.00
DCC	Posted Payments Register	106,532,374.83	106,573,520.42	-41,145.59
DVH	Posted Payments Register	1,044,200.77	1,044,200.77	0.00
FRA	Posted Payments Register	4,855,973.55	4,855,973.55	0.00
PEN	Posted Payments Register	6,695,051.59	6,695,051.59	0.00
SDC	Posted Payments Register	141,302.62	141,302.62	0.00
CDDC	Invoice Aging Report	-6	-6.00	0.00
DCCT	Invoice Aging Report	405.14	405.14	0.00
DCC	Invoice Aging Report	8,162,388.04	8,162,388.04	0.00
DVH	Invoice Aging Report	-11,169.76	-11,169.76	0.00
FRA	Invoice Aging Report	154,428.86	154,428.86	0.00
PEN	Invoice Aging Report	27,253.19	27,253.19	0.00
SDC	Invoice Aging Report	22,372.06	22,372.06	0.00
CDDC	Tax Audit Trail	0.00	0.00	0.00
DCCT	Tax Audit Trail	1,315.74	1,425.74	-110.00
DCC	Tax Audit Trail	51,905,632.73	51,412,672.20	492,960.53
DVH	Tax Audit Trail	146,557.27	146,111.42	445.85
FRA	Tax Audit Trail	1,872,494.59	1,875,607.79	-3,113.20
PEN	Tax Audit Trail	1,263,974.62	1,263,974.62	0.00
SDC	Tax Audit Trail	44,490.34	44,490.34	0.00

CM Report Comparison - LIVE

Op Unit	Bank Account	Pre Upgrade	Post Upgrade	Comments
CDDC	CDDC	87,051.41	87,051.41	OK
DCCT	DCCT	85,793.43	85,793.43	OK
DDC	DDC	Not Run	Not Run	OK
DUR	County Fund	- 520,503,775.09	-519,338,649.06	- 1,165,126.03
DUR	Income Account	426,699,451.08	426,699,451.08	OK
DVH	DVH	3,807.05	3,807.05	OK
FRA	Co-op	115,062.13	115,062.13	OK
FRA	HSBC	878,460.44	878,460.44	OK
PEN	PEN	86,131,296.72	86,131,296.72	OK
SDC	SDC	677,361.10	677,361.10	OK

Inventory Checks

Op Unit		Pre Upgrade	Post Upgrade	Difference
FRA		514,187.49	514,187.49	0.00
ICT		149,820.61	149,820.61	0.00
ITS		124,458.84	124,458.84	0.00
SDI		1,769,068.19	1,769,068.19	0.00

Transaction Register

Op Unit	Month	Pre Upgrade	Post Upgrade	Difference
FRA	June	12,337.19	12,337.19	0.00
FRA	July	-25,616.61	-25,616.61	0.00
ICT	June	-13,169.76	-13,169.76	0.00
ICT	July	23,484.28	23,484.28	0.00
ITS	June	22,866.83	22,866.83	0.00
ITS	July	49,791.82	49,791.82	0.00
SDI	June	-139,911.74	-139,911.74	0.00
SDI	July	26,097.94	26,097.94	0.00

Projects

Category	Formula	Pre Upgrade	Post Upgrade	Difference
Count of Open Projects		92,583.00	92,583.00	0.00
count and sum of project expenditures	count (expenditure_item_id)	4,401,911.00	4,401,911.00	0.00
count and sum of project expenditures	sum(raw_cost)	793,688,422.62	793,688,422.62	0.00
count and sum of project expenditures	sum(burden_cost)	811,431,182.11	811,431,182.11	0.00
count and sum of events	count(event_id)	137,377.00	137,377.00	0.00
count and sum of events	sum(bill_amount)	49,773,349.04	49,773,349.04	0.00
count and sum of events	sum(revenue_amount)	45,982,213.14	45,982,213.14	0.00
count and sum of revenue	count(project_id)	28,710.00	28,710.00	0.00
count and sum of revenue	sum(unbilled_receivable_dr)	49,349,125.47	49,349,125.47	0.00
count and sum of revenue	sum(unearned_revenue_cr)	3,357,404.54	3,357,404.54	0.00
count and sum of invoices	count(project_id)	25,143.00	25,143.00	0.00
count and sum of invoices	sum(unearned_revenue_cr)	-3,350,911.08	-3,350,911.08	0.00
count and sum of invoices	sum(unbilled_receivable_dr)	-47,991,623.92	-47,991,623.92	0.00

Conclusion and recommendations

Low

Although the project has been performed with a good standard of quality, the data reconciliation strategy was not identified at the beginning of the project, leading to data reconciliation during live migration which has not fully covered completeness and accuracy of transactions. The number of transactions has not been reconciled and the deficiencies identified needed further detailed investigation.

We recommend that substantive testing over data migration process is performed – this has been performed already by the financial audit team.

III. IT General Controls

Physical Security (1/3)

#	Sub-Domain	Question		Comments
PS1	Access to the data center	There is a room dedicated to servers	Yes	Servers are located in a dedicated room in one of the Council's buildings.
PS2		The Data Centre is not vulnerable in any way	Yes	No windows, inflammable materials or other aspects that would make the Data Centre vulnerable were identified at the time of our review.
PS3		The doors to the Data Centre are always locked	Yes	The access is restricted via a swipe card system.
PS4		There is a protection system able to detect intruders (alarms, camera...)	Yes	Alarms and CCTV systems are in place throughout the building, including the Data Centre. Alarms are linked to the police and a security guard who would be alerted in case of intruders.
PS5		There is a procedure for granting and revoking physical access to the data centre	Yes	Physical access is granted/restricted by Facilities Management based on the authorisation of the IT Department representatives.
PS6		Only authorised personnel have access to the Data Centre	Yes	Access is restricted to 8 members of the Facilities team and 42 members of the IT Department.

Physical Security (2/3)

#	Sub-Domain	Question		Comments
PS7	Access to the data centre (cont'd)	The IT department manages visitor authorisations (people who are temporarily authorised to access these rooms)	Yes	The IT department authorises temporary access, which is granted by the Facilities Team. Visitors are escorted by a member of the IT Department.
PS8	Fire alarm devices	A fire detector is installed inside the Data Centre	Yes	Smoke and fire detection sensors are placed under the raised floor and on the ceiling of the Data Centre.
PS9		There is a fire extinguisher inside the Data Centre	Yes	An automatic fire extinguishing system is installed in the Data Centre, and manual fire extinguishers are place throughout the building.
PS10		The Data Centre is equipped with an automatic fire-extinguishing device	Yes	Cf. PS9.
PS11		Specialised companies audit the devices at regular intervals	Yes	Annual testing and recertification is performed for all Data Centre equipment and controls.
PS12	Devices protecting against power surges and power cuts	A device protects (servers and workstations) against power surges and power cuts (uninterruptible power supply)	Yes	One Gamatronic UPS is in place for the data centre, that would keep the equipment running for ~10 minutes. Also, 3 generators are installed: 2 of them supporting the entire building, including the Data Centre equipment, and one on stand-by for back-up purposes. The generators could run continuously for 7 days (based on the fuel reserve the Council has installed).

Physical Security (3/3)

#	Sub-Domain	Question		Comments
PS13	Devices protecting against power surges and power cuts (cont'd)	Tests are conducted regularly	Yes	Annual testing and recertification is performed for all Data Centre equipment and controls.
PS14	Other security devices	The Data Center is always kept clean (there are no papers near the servers)	Yes	The Data Centre is kept clean. No papers or other inflammable materials were found in the Data Centre at the time of our review.
PS15		The room where the servers are located is well ventilated and has air conditioning	Yes	2 air conditioning systems are in place for the Data Centre.
PS16		Servers are installed in such a way that they do not come into contact with the ground	Yes	Servers are placed on dedicated racks, that prevent them from taking direct contact with the ground.
PS17		Servers are not located inside the Council building but are located inside the offices of an outside service provider (e.g.: ISO27001 certified or acknowledged structure)	N/A	
PS18		The Data Center is not located in a potential flood-risk area (basement, attic, water main above the servers etc.)	Yes	The Data Centre is located at the ground floor of the building.
PS19		The Data Center has a raised flooring	Yes	The Data Centre has a raised flooring.

Back-up and Disaster Recovery Plan (1/5)

#	Sub-Domain	Question		Comments
BD1	Back up management	There is a procedure defining back up management	Yes	A daily back up is in place for Durham County Council's programs and data. • **Oracle**: incremental back-up is performed daily using Oracle Recovery Manager for disk back-up, and TSM for tapes back-up; • **SQL Servers**: incremental back-up is performed daily on tapes. Tapes are taken on a daily basis off-site, to Sunderland (more than 5 miles away from the primary location), and retained for 100 days and for tapes and disk data.
BD2		The procedure is formalised	Yes	The back up policy was formalised.
BD3		The procedure specifies the type of data that must be backed up	Yes	Cf. BD1.
BD4		There is a back up procedure for laptops	No	No business/operational data is stored on the users' local drives.

Back-up and Disaster Recovery Plan (2/5)

#	Sub-Domain	Question		Comments
BD5	Back up management (cont'd)	Back ups are automated	Yes	Scheduled jobs are setup for performing daily back-up.
BD6		Back up logs are systematically monitored	Yes	The back-up job issues history logs, including the results (failure, success).
BD7		All back up failures are documented	Yes	Besides the back-up logs, in case of back-up failure the IT Department representatives are automatically notified via e-mail .
BD8		Back ups are kept in a separate room from the servers	Yes	Back-ups are kept in a locked safe in a dedicated room, separate from the servers, until picked up as for transfer to a locked safe in the secondary site (Sunderland).
BD9		Back ups are kept in a protected environment (such as a fire-proof vault)	Yes	Cf. BD8.

Back-up and Disaster Recovery Plan (3/5)

#	Sub-Domain	Question		Comments
BD10	Back up management (cont'd)	A spare copy of the Back ups is kept outside Council walls	Yes	Cf. BD8.
BD11		Complete data restoration is tested regularly	Yes	Production data restoration tests are performed every 2 months.
BD12		Restoration tests will include operational users	Yes	Operational users are involved in testing.
BD13		In case back-ups are externalised, the contract has defined the service provider's agreement to all of the preceding points (back-up plan, number of generations and their life cycles, media stored in a secure place, restoration procedures, back-up plan update procedure, periodic test of full data restoration in test environment for critical applications and/or servers, reporting procedure)	N/A	

Back-up and Disaster Recovery Plan (4/5)

#	Sub-Domain	Question		Comments
BD14	Back up management (cont'd)	Does the Back up strategy guarantee a limited loss of data acceptable to the Council?	Yes	1 day.
BD15	Financial obligations	Back ups are archived long enough to answer to obligations linked to tax investigations	Yes	100 days.
BD16	Disaster recovery plan	There is a formalised Disaster Recovery Plan	No	No formalised Disaster Recovery Plan (DRP) was identified at the time of our review. Nevertheless, the DRP was under development, and a Business Continuity Plan was formalised and is annually reviewed and tested.
BD17		Rescue equipment is available	No	Cf. BD16.
BD18		There is a rescue site (Relocation arrangements have been made if need be)	No	Cf. BD16.

Back-up and Disaster Recovery Plan (5/5)

#	Sub-Domain	Question		Comments
BD19	Disaster recovery plan (cont'd)	The Disaster Recovery Plan is tested at least once every year	No	Nevertheless, the business continuity plan is tested yearly.
BD20		A formal report of the test is made	No	Cf. BD20.
BD21		The Council has an insurance policy which covers the hardware	Yes	The insurance policy covers the hardware equipment.
BD22		The Council has a maintenance contract for the servers	Yes	Hardware support and maintenance contract in place with DELL.

Logical Security (1/17)

#	Sub-Domain	Question		Comments
LS1	Network security	There is a user management procedure (user profile, creating a user, modifying a user, deleting a user)	Yes	The user access management process is performed as follows: • **Starters/ Access change**: For network access, a dedicated form is filled in by the line manager for the new/changed user through a dedicated Service Desk ticketing tool. The IT Department analyses the request and proceeds to access granting/changing; • **Leavers**: The HR Department provides the IT Department with a list of leavers on a monthly basis, and the IT representatives proceed to disable the accounts.
LS2		The procedure is formalised	Yes	A dedicated procedure was formalised as for governing the user access management process.
LS3		Access to the network is protected by a password	Yes	Active Directory.
LS4		Passwords contain at least 8 complex characters	Yes	8 characters, complexity enabled.
LS5		The first password will be attributed individually to each user by IT services (random password)	Yes	A random password is assigned individually to the user when joining the Council.
LS6		The first password must be modified by the user upon the user's first connection	Yes	Users are prompted to change their password at first logon.
LS7		Passwords are renewed regularly	Yes	Every 60 days.
LS8		Users are not allowed to use the same password several times in a row	Yes	24 passwords remembered.

Logical Security (2/17)

#	Sub-Domain	Question		Comments
LS9	Network security (cont'd)	After several unsuccessful access attempts, the user account is locked out	Yes	3 unsuccessful attempts.
LS10		After a pre-determined time of inactivity, the workstation goes into sleep mode (automatic disconnection and/or password protection)	Yes	30 minutes.
LS11		There are different profiles for each type of user	Yes	Profiles are assigned according to the required access, and administrative privileges are segregated from operational users.
LS12		There are no generic accounts (traceability breach)	No	From a total number of 19,842 users, 762 generic accounts were identified at domain level (including 1 account with administrative privileges).
LS13		A regular review of user access rights is made and formalised	No	No regular review is in place at network level.
LS14		Remote access is secured and protected by a password (VPN...)	Yes	Juniper SSL VPN is used for secure remote access.
LS15		WIFI access and data transfer are encrypted	Yes	Wifi connections are used; data transfer is encrypted. Public Wifi is password restricted, and corporate Wifi is certificate-based and password restricted.
LS16		Laptop hard-drives are encrypted	Yes	Safend is used for laptop hard-drives encryption.

Logical Security (3/17)

#	Sub-Domain	Question		Comments
LS17	Outside links	Network access is protected from outside intrusions: e.g.: Internet by a proxy, local network by a firewall	Yes	Network controls (e.g. firewalls, etc.) are in place.
LS18	Security measures concerning applications with financial impact	There is a user management procedure (user profile, creating a user, modifying a user, deleting a user)	Yes	• **Starters/ Access change**: A dedicated form is filled in by the line manager for the new/changed user through a dedicated Service Desk ticketing tool. The IT Department/system administrator analyses the request and proceeds to access granting/changing; • **Leavers**: The HR Department provides the IT Department and system administrators with a list of leavers on a monthly basis, and the IT representatives proceed to disabling the accounts.
LS19		The procedure is formalised	No	No formalised procedure was identified during our review.
LS20		Access to applications is protected by password	No	• **Oracle:** Yes; • **Resource Link:** Yes; • **IPF:** Yes; • **Financial Director:** No – no evidence was provided; • **CIVICA Revenues & Benefits:** No – no evidence was provided; • **ICON (AIM):** No – no evidence was provided; • **SSID:** Yes; • **Orchard:** No – no evidence was provided; • **Northgate:** Yes; • **Civica Housing:** No – no evidence was provided.

Logical Security (4/17)

#	Sub-Domain	Question		Comments
LS21	Security measures concerning applications with financial impact (cont'd)	Passwords contain at least 8 complex characters	No	• **Oracle:** Yes – 8 characters, complexity enabled; • **Resource Link:** No – system default credentials are used; • **IPF:** No – no evidence provided; • **Financial Director:** No – no evidence was provided; • **CIVICA Revenues & Benefits:** No – no evidence provided; • **ICON (AIM):** No – no evidence provided; • **SSID:** Yes – 8 characters, standard Oracle password verify function script is used; • **Orchard:** No – no evidence was provided; • **Northgate**: No – 7 characters, complexity enforced; • **Civica Housing:** No – no evidence was provided.

Logical Security (5/17)

#	Sub-Domain	Question		Comments
LS22	Security measures concerning applications with financial impact (cont'd)	The first password will be attributed individually to each user by IT services (random password)	No	• **Oracle:** Yes; • **Resource Link:** Yes; • **IPF:** Yes; • **Financial Director:** No – no evidence was provided; • **CIVICA Revenues & Benefits:** No – no evidence was provided; • **ICON (AIM):** No – no evidence was provided; • **SSID:** Yes; • **Orchard:** No – no evidence was provided; • **Northgate:** Yes; • **Civica Housing:** No – no evidence was provided.

Logical Security (6/17)

#	Sub-Domain	Question		Comments
LS23	Security measures concerning applications with financial impact (cont'd)	The first password must be modified by the user upon user's first connection	No	• **Oracle:** Yes; • **Resource Link:** Yes; • **IPF:** Yes; • **Financial Director:** No – no evidence was provided; • **CIVICA Revenues & Benefits:** No – no evidence was provided; • **ICON (AIM):** No – no evidence was provided; • **SSID:** Yes; • **Orchard:** No – no evidence was provided; • **Northgate:** Yes; • **Civica Housing:** No – no evidence was provided.

Logical Security (7/17)

#	Sub-Domain	Question		Comments
LS24	Security measures concerning applications with financial impact (cont'd)	Passwords are renewed regularly	No	• **Oracle:** Yes – 60 days; • **Resource Link:** Yes – 90 days; • **IPF:** Yes – 90 days; • **Financial Director:** No – no evidence was provided; • **CIVICA Revenues & Benefits:** No – no evidence was provided; • **ICON (AIM):** No – no evidence was provided; • **SSID:** Yes – 63 days; • **Orchard:** No – no evidence was provided; • **Northgate:** Yes – 28 days; • **Civica Housing:** No – no evidence was provided.

Logical Security (8/17)

#	Sub-Domain	Question		Comments
LS25	Security measures concerning applications with financial impact (cont'd)	Users are not allowed to use the same password several times in a row.	No	• **Oracle:** Yes – 380 passwords remembered; • **Resource Link:** Yes – 10 passwords remembered; • **IPF:** No – no history enforced; • **Financial Director:** No – no evidence was provided; • **CIVICA Revenues & Benefits:** No – no evidence was provided; • **ICON (AIM):** No – no evidence was provided; • **SSID:** Yes – 5 passwords remembered; • **Orchard:** No – no evidence was provided; • **Northgate:** Yes – 8 passwords remembered; • **Civica Housing:** No – no evidence was provided.

Logical Security (9/17)

#	Sub-Domain	Question		Comments
LS26	Security measures concerning applications with financial impact (cont'd)	After several unsuccessful access attempts, the user account is locked out	No	• **Oracle:** Yes – 3 unsuccessful attempts; • **Resource Link:** Yes – 3 unsuccessful attempts; • **IPF:** Yes – 3 unsuccessful attempts; • **Financial Director:** No – no evidence was provided; • **CIVICA Revenues & Benefits:** No – no evidence was provided; • **ICON (AIM):** No – no evidence was provided; • **SSID:** No – no evidence was provided; • **Orchard:** No – no evidence was provided; • **Northgate:** Yes – 4 unsuccessful attempts; • **Civica Housing:** No – no evidence was provided.

Logical Security (10/17)

#	Sub-Domain	Question		Comments
LS27	Security measures concerning applications with financial impact (cont'd)	The application will automatically disconnect users after a predetermined time of inactivity	Yes	• **Oracle:** Yes – session timeout set to 30 minutes; • **Resource Link:** Yes – session timeout set to 30 minutes; • **IPF:** Yes – session timeout set to 30 minutes; • **Financial Director:** Yes – compensating control: screensaver; • **CIVICA Revenues & Benefits:** Yes – compensating control: screensaver; • **ICON (AIM):** Yes – compensating control: screensaver; • **SSID:** Yes – compensating control: screensaver; • **Orchard:** Yes – compensating control: screensaver; • **Northgate:** Yes – compensating control: screensaver; • **Civica Housing:** Yes – compensating control: screensaver.

Logical Security (11/17)

#	Sub-Domain	Question		Comments
LS28	Security measures concerning applications with financial impact (cont'd)	There are different profiles for each type of user	Yes	• **Oracle:** Yes; • **Resource Link:** Yes; • **IPF:** Yes; • **Financial Director:** No – no evidence was provided; • **CIVICA Revenues & Benefits:** No – no evidence was provided; • **ICON (AIM):** No – no evidence was provided; • **SSID:** Yes; • **Orchard:** No – no evidence was provided; • **Northgate:** Yes; • **Civica Housing:** No – no evidence was provided.

Logical Security (12/17)

#	Sub-Domain	Question		Comments
LS29	Security measures concerning applications with financial impact (cont'd)	Administrator rights on application level are granted only to a limited number of application managers	No	• **Oracle:** Yes – 4 administrators; • **Resource Link:** No – no evidence provided; • **IPF:** Yes - 16 administrators; • **Financial Director:** No – no evidence provided; • **CIVICA Revenues & Benefits:** No – no evidence provided; • **ICON (AIM):** No – 20 admin accounts; • **SSID:** No – no evidence provided; • **Orchard:** No – no evidence provided; • **Northgate:** Yes - 95 administrators; • **Civica Housing:** No – no evidence provided;

Logical Security (13/17)

#	Sub-Domain	Question		Comments
LS30	Security measures concerning applications with financial impact (cont'd)	There are no generic accounts (traceability breach)	No	• **Oracle:** No – 144 generic accounts; • **Resource Link:** No – 7 generic accounts; • **IPF:** No – 4 generic accounts (including 2 with administrative rights); • **Financial Director:** No – no information provided; • **CIVICA Revenues & Benefits:** No –no information provided; • **ICON (AIM):** No – 7 generic accounts (including 1 with administrative rights); • **SSID:** Yes; • **Orchard:** No – no evidence was provided; • **Northgate:** No – 69 generic accounts; • **Civica Housing:** No – no evidence was provided.

Logical Security (14/17)

#	Sub-Domain	Question		Comments
LS31	Security measures concerning applications with financial impact (cont'd)	The Council has conducted a study concerning the segregation of duties leading to user profiles identifying their associated rights, which are formalised in a document that has obtained head office approval	Yes	• **Oracle:** Access rights are granted according to the user's job description; • **Resource Link:** Access rights are granted according to the user's job description; • **IPF:** Access rights are granted according to the user's job description; • **Financial Director:** Access rights are granted according to the user's job description; • **CIVICA Revenues & Benefits:** Access rights are granted according to the user's job description; • **ICON (AIM):** Access rights are granted according to the user's job description; • **SSID:** Access rights are granted according to the user's job description; • **Orchard:** Access rights are granted according to the user's job description; • **Northgate:** Access rights are granted according to the user's job description; • **Civica Housing:** Access rights are granted according to the user's job description.

Logical Security (15/17)

#	Sub-Domain	Question		Comments
LS32	Security measures concerning applications with financial impact (cont'd)	A regular review of user access rights is made and formalised	No	• **Oracle:** Yes – monthly review of access rights is performed, focusing on leavers and access rights. • **Resource Link:** No; • **IPF:** No; • **Financial Director:** No; • **CIVICA Revenues & Benefits:** No; • **ICON (AIM):** No; • **SSID:** No; • **Orchard:** No; • **Northgate:** No; • **Civica Housing:** No;
LS33	Extra	Workstations and servers are equipped with antivirus software that is updated regularly	Yes	Kaspersky anti-virus program is used for workstations and servers.

Logical Security (16/17)

#	Sub-Domain	Question		Comments
LS34	Extra (cont'd)	Antivirus software is activated on all workstations and cannot be deactivated by users	Yes	Regular users are not able to disable/change the settings.
LS35		Messages and attached files are also decontaminated	Yes	Messages and attached files are also scanned.
LS36		Anti-spam software is installed	Yes	Kaspersky software is used for anti-spam.
LS37		Users do not have administrator rights on their workstation	Yes	Administrative privileges are restricted to 9 users within the IT Department.

Logical Security (17/17)

#	Sub-Domain	Question		Comments
LS38	Extra (cont'd)	Administrator rights are granted to a limited number of IT staff	Yes	There are 8 users with domain administration rights and one generic Administrator account.
LS39		Database access is only permitted for database administrators	Yes	IT Department.
L40		The server has the latest Service Packs and relevant security updates installed	Yes	MS SCM is used. Critical security updates are installed at all Windows servers.
L41		An information security policy is adopted and formalised	Yes	Information security policy is in place.

Strategy and Internal Control (1/4)

#	Sub-Domain	Question		Comments
SI1	IT Master Plan	An Information System Master Plan has been formalised	Yes	IT Strategy is elaborated using a 3-year perspective.
SI2		The Information System Master Plan is coherent with Council strategy. It is regularly updated	Yes	The IT Strategy is elaborated as for supporting the operational business, and reviewed/updated annually, or in case of major changes.
SI3		The Information System Master Plan is budgeted over a several year time span. A budget comparative is made and presented at least once a year	Yes	The IT Strategy has a perspective of 3 years, and is reviewed annually or in case of major changes.
SI4		Operational managers are involved in the elaboration process and updating of the Information System Master Plan	Yes	Operational managers are responsible for elaborating the project plans and business cases also reflecting the need of IT services/projects.
SI5	Internal control of IT processing	The IT department does not carry out operational tasks (e.g.: invoicing entry, etc.)	Yes	IT Department's tasks are limited to administration and support.

Strategy and Internal Control (2/4)

#	Sub-Domain	Question		Comments
SI6	Internal control of IT processing (cont'd)	The IT department's prerogatives are limited in terms of investment and strategy	Yes	The Strategic Board perform analysis and prioritisation of the projects, with limited participation of IT Department representatives.
SI7		There is a procedure log book describing the main process operations, acknowledged practices and operating mode	No	Nevertheless, all users that require information call Service Desk, who further direct them towards the key representatives.
SI8		Expertise is shared and documented within the IT department	Yes	
SI9		There is a training plan for the IT department	Yes	The IT Manager is in charge of planning the training for the IT Department. Both internal and external training is performed, depending on the needs and requirements of the IT Team.
SI10		The procedure managing incidents allows to categorise, trace, analyse and follow-up solutions (e.g. incident registration tool)	Yes	An Incident management procedure is in place, also including categorisation, tracing and monitoring of incidents. The process is managed through the IT Service Desk.
SI11		The procedure is formalised	Yes	Incident Management procedure was formalised for governing the process.

Strategy and Internal Control (3/4)

#	Sub-Domain	Question		Comments
SI12	IT Charter	There is an Information Technology Charter signed by the users, legally validated and appended to the Council's rules and regulations	Yes	When joining the Council, employees sign the Acceptable Use Policy, committing to understanding and respecting the Council's policies, including data privacy.
SI13		The Information Technology Charter defines the rules concerning IT use (applications, data), workstations and/or servers, email, and the internet	Yes	
SI14		The Information Technology Charter is approved by the works council / staff committee	Yes	
SI15	Financial obligations	Data is stored for a period of time in adequacy with regulation concerning tax investigations (e.g.: 3 years + current year excluding fiscal year showing deficit - in France)	Yes	100 days.
SI16	Data privacy	The data stored complies with instructions given by the agency for Information Technology and the defense of files and liberties (France: CNIL / UK: Information Commissioner's Office / Canada: Privacy Commission…)	N/A	

Strategy and Internal Control (4/4)

#	Sub-Domain	Question		Comments
SI17	Managing license agreements	All the software installed on the computers have registered licensed products	Yes	Regular audits are performed for licenses checks by Microsoft. The software installation process is managed by the IT Department, and regular users are not allowed to install software on their workstations.
SI18	Managing maintenance contracts	All critical hardwares have a maintenance contract with a guaranteed recovery time or a guaranteed intervention time	Yes	Hardware support and maintenance contract in place with DELL.
SI19		Applications have corrective and upgrading maintenance contracts	Yes	A dedicated contract library is in place for ensuring proper monitoring of software contracts. All in scope systems are covered by valid maintenance and support contracts.
SI20		As far as hosting is concerned, there is a service contract defining: the kind of provision of service, service quality monitored by adequate indicators, prices, delays, end of contract conditions, management and security procedures, and responsibilities incumbent upon both parties	N/A	

Change Management (1/3)

#	Sub-Domain	Question		Comments
CM1	Change Management	There is a procedure managing changes (developments)	No	**Infrastructure**: the IT Department is in charge of the Infrastructure Change Management process. The process is deficient in terms of registering and tracking the change requests, however the monitoring is performed through Network Configuration Management Systems program, keeping a log for changes performed, including historical configuration and the users who performed the change); **Applications**: changes may occur as a result of planned development or bugs/faults requiring fixing. The process is managed through a dedicated ticketing tool, as below: • **Change request** is initiated by business users; major changes are supported by more detailed business cases; The change requests/business cases are collected and centralised throughout the year into an Enhancement Register; • **Authorisation** is performed through annual meetings of managers, IT Department and members of the Board, in order to analyse and prioritise the projects/change requests that would be implemented throughout the next year; • **Development** and **testing** is performed externally (if third party development is required) and internally (by developers and business users); • **Go-live approval** is offered by the users who requested the change once the test results are satisfactory.
CM2		The procedure is formalised	No	No formalised procedure was identified during our review.

Change Management (2/3)

#	Sub-Domain	Question		Comments
CM3	Change Management (cont'd)	Management validates demands for functional developments	No	**Infrastructure**: No; **Applications**: Yes - Management representatives analyse all change requests and prioritise/approve the changes to be developed throughout the year.
CM4		The procedure includes registering and formalising the change requests	No	**Infrastructure**: No; **Applications**: A dedicated ticketing tool is used.
CM5		The formalised change request is validated by the requestor	No	**Infrastructure**: No; nevertheless, network change history logs are kept by the Network Configuration Management System, enforcing traceability and accountability of changes; **Applications**: Yes - A dedicated ticketing tool is used.
CM6		Changes are documented	Yes	Cf. CM5.
CM7		Changes are tested by developers and are submitted to regression tests	Yes	**Infrastructure**: Changes are tested, however no documentation or evidence is retained; **Applications**: Changes are tested by developers and business users.
CM8		The requestor conducts a series of tests, reports and validation before the implementation of the development in production environment	Yes	Cf. CM7.

Change Management (3/3)

#	Sub-Domain	Question		Comments
CM9	Change Management (cont'd)	The procedure includes the special case of upgrades to superior versions of applications and/or basic software that must be managed like a development project	Yes	Application upgrades and bug fixing are covered by the contract with the software providers.
CM10		There is a special procedure for emergency changes	No	Cf. CM2.
CM11		The application software environment for development and production are segregated	Yes	Development, testing and production environments are segregated.
CM12		Privileges to migrate changes to the production environment are strictly restricted	Yes	Migration of changes into production is restricted to database administrators and applications super users.
CM13		The segregation of duties is respected within the IT department: developers do not have access to the production environment	No	The same team (applications super users) can perform both development and migration to production of changes.

CONTACTS

Roch Caumon, Director of IT Audit & Advisory
Mob. : +44 (0)7881 283451 / Mob. : +33 (0)6 68 54 61 45

Mazars LLP
Tower Bridge House, St Katharine's Way, London E1W 1DD

Praxity MEMBER GLOBAL ALLIANCE OF INDEPENDENT FIRMS

Durham County Council

MAZARS