worcestershire
county council

FINAL

Internal Audit Report

Information Technology Risk Diagnostic

This report is not for reproduction publication or disclosure by any means to unauthorised persons.

Contents

1. Introduction

Background

We facilitated a self-assessment of ICT risks and controls at your Information and Computer Technology (ICT) services based at Worcestershire County Council, using our ICT risk diagnostic tool (ITRD). This tool provides valuable insight into the current performance and quality of ICT control activities in the Council.

Approach

We facilitated workshops with your senior ICT team (see Appendix D) to gather the scores needed to populate the tool. Our role was to challenge management's responses through a series of questions regarding the current and future desired performance of ICT processes and controls in the following seven areas:

- ICT strategic decision making;
- ICT governance;
- ICT management;
- System quality;
- System support and change;
- ICT operations; and
- Information security.

Output results

This report presents the results of this diagnostic and will provide a base upon which any future improvements can be measured.

Three benchmarking exercises were performed:

- Current controls against good practice (rating of 3 represents good practice;)
- Current controls against desired control; and
- Current and desired controls against those from 23 similar organisations.

All the ratings are ***subjective*** and based on facilitated discussions during the workshop rather than on audited evidence. The scores presented in this document are averages of a number of scored questions contained within the subject area. The detailed scores were not retained by WCC staff but the scores to the detailed questions were agreed with management in the workshop and the detailed feedback included in this report has been discussed with management. As with all benchmarks, this analysis should be treated as indicative rather than comprehensive. Desired controls will represent where the ICT Management aspire to be, taking into account budget and resource restrictions.

Limitation of Scope

The audit did not constitute an assurance engagement. This review was a high level health check of the way in which you manage certain risks associated with your IT function. We did not test any of the controls in place but merely highlight areas of high risk.

2. Executive summary

The results produced by the diagnostic enable you to consider:

- The current and future operating effectiveness of the ICT control environment;
- areas where ICT controls could be further strengthened; and
- where you might be over controlled when considering lower areas of risk and might redirect resource.

Summarised below are our key observations following this review.

Key observations of good practice are:

Benchmarking results are very positive	• Average scores across the seven areas assessed show two were operating at good practice. Average scores across the remaining five areas were close to good practice. • When compared to 23 similar organisations, you are within the top quartile for two areas and upper second quartile for the remaining five areas. • These results are a positive reflection on control maturity within ICT.
Strong controls in the area of Systems Support & Change and Information Security	• Strong controls were noted across the area of Systems Support & Change, in particular the Change Management process. • Information security controls exceeded good practice over Security Awareness and Training, Threat and vulnerability management.

Key areas where further improvements could be made:

Centralisation and Standardisation	• Centralisation of all applications. • Some attention required on the age of equipment and hardware. • Standardisation of all ICT controls and processes is required.
ICT Performance Management	• Formalisation and Council wide agreement of some internal service level agreements required. • Improved control in measuring and monitoring of some ICT performance management required. • Some attention to capacity management planning is needed.
People Management	• Attention to detail of job description to align with role responsibilities is required. • Consideration of ICT staff member succession planning. • Potential requirement of a talent management scheme.

These observations are explored in further detail in the pages which follow.

3. Detail observations

Expanding on the points raised in the executive summary, below are detailed observations and recommendations arising from the diagnostic:

Theme	Areas that are currently under-controlled		
Risk area	Centralisation and Standardisation	ICT Performance Management	People Management
Observation	The current ICT strategy is to have all ICT services centralised. It was noted that services and support for some Directorates are not adhering to the ICT strategy for centralisation, resulting in these applications not being managed by ICT. Some ICT equipment being used is very old and out of date. Not all ICT processes and controls have been standardised across the Council.	ICT Service level agreements (SLAs) with the rest of the Council are not formalised or up to date. ICT infrastructure SLAs have been agreed with the business and are to be reported against. Measuring and monitoring of ICT performance is well defined in some areas but the approach is not consistent in all aspects of ICT performance (e.g. Power usage). With regards to capacity management, alerts are in place for storage capacity and network usage, but there is no formalised forecasting/planning for future capacity requirements. Issues have been noted by ICT in respect of capacity constraints for application requirements and WIFI connectivity.	Members of ICT do have job descriptions. Job descriptions are not up to date for all members against current responsibilities. There is a well defined process for hiring staff, knowledge sharing is in place but there is no staff succession planning for members of ICT. Training is supplied for members of staff against training requirements, but there is no skills management scheme in place at the Council.
Recommendation	In December 2013 as part of the Resources Commissioning Strategy, ICT Infrastructure and Service Management has been identified as a key capability that could be delivered by an external organisation. We recommend the Council standardise and centralise application support and ICT processes and controls as required by the documented ICT strategy. Upon completion this will aid the transition of outsourced services (commissioning) to preferred suppliers.	The Council plans to update SLAs and agree with key stakeholders by October 2014, we would encourage this deadline is met. We recommend Measuring/Monitoring of ICT performance and Capacity management controls are enhanced before ICT services are outsourced. This will aid in the transition of support processes and controls to the third party(s).	ICT management feel the above issues will be addressed as part of the preparations in readiness for outsourcing (commissioning) to third parties. We recommend effort is made to standardise and fully define staff responsibilities as part of their job description, introduce succession plans for key members of ICT and consider the implementation of a skills management programme. Such efforts will aid in a smooth transition towards commissioning of services.

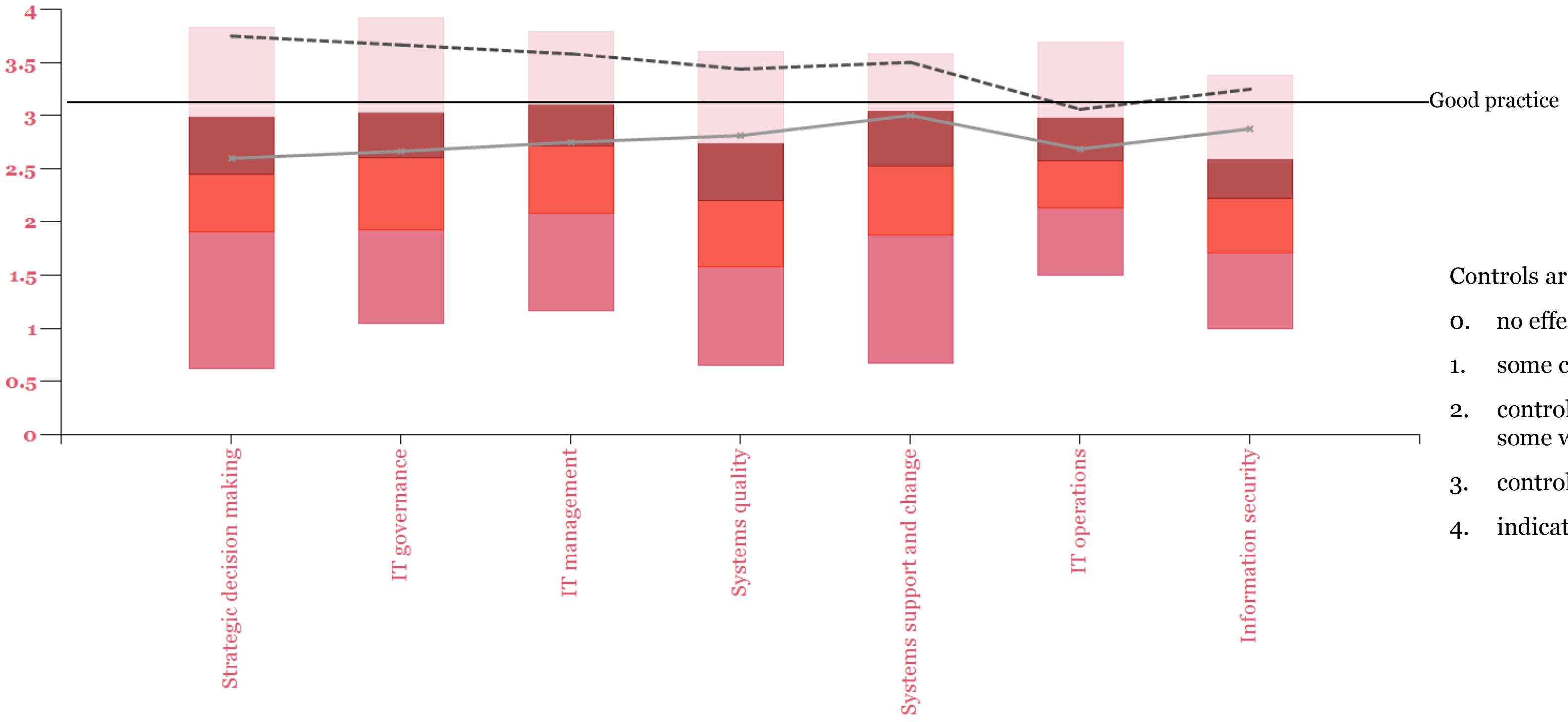
4. ICT controls benchmarking results

ICT controls benchmarking results against similar organisations

- ▬ ▬ Desired
- ▬ Worcestershire County Council IT Risk Diagnostic
- ▨ Top Quartile
- ▨ Second Quartile
- ▨ Third Quartile
- ▨ Bottom Quartile

Benchmarking against similar organisations – Overview

The bar chart below shows, for the seven domains, current control scores against management's desired levels. It also presents your position relative to the database group selected to benchmark against – this group being 23 Social work/security, Educational, Public and Governmental Institutes.



Controls are rated as defined below:

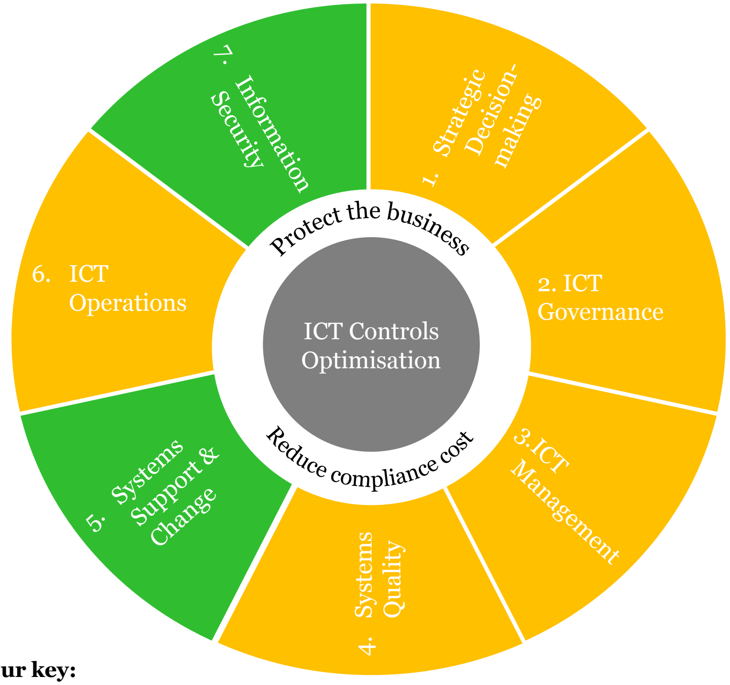
0. no effective controls in the area;
1. some controls, but they are largely inadequate;
2. controls are mostly adequate, but there are still some weaknesses;
3. controls are at good practice level; and
4. indicates controls are very strong.

4. ICT controls benchmarking results

ICT control benchmarking results against good practice

Qualitative Review

The wheel below presents a comparison of current controls against good practice. An average score has been taken for each and therefore this calculation might disguise poorer scoring controls.



Colour key:

🟥 Significant areas for control improvement compared to good practice (>1.00)

🟧 Some areas for improvement compared to good practice (< 1.0)

🟩 Controls meet or exceed good practice level

1. Strategic Decision-making
Current 2.50 (Target 3.75)

Controls over ICT Strategy exceed good practice. Controls over Decision Making are close to good practice. Across the domain controls over Emerging technology, Sustainability/Green IT, Centralisation and standardisation are only adequate and require improvement.

2. ICT Governance
Current 2.75 (Target 3.75)

Controls over ICT Compliance exceed good practice. Governance Structure controls meet good practice. Controls over ICT Risk Management are close to good practice. Controls over ICT Policies and standards, Cost and Charge back, are only adequate and require improvement. Controls for ICT Performance Management are largely inadequate.

3. ICT Management
Current 2.75 (Target 3.50)

Strong controls noted for Hardware Asset Management.

Controls over ICT Management exceed good practice.

Software Licensing controls meet good practice.

Controls over Application Portfolio/Program Management and Third Party Management are only adequate and require improvement. People Management controls are largely inadequate.

4. Systems Quality
Current 2.75 (Target 3.50)

Strong controls noted for Project Management and Benefits Realisation. Data Quality controls are close to good practice. Controls over Systems quality & business intelligence, End User Computing (EUC) controls are only adequate and require improvement.

5. Systems Support & Change
Current 3.00 (Target 3.50)

Controls over the Change Management process exceed good practice. System Support Capability controls meet good practice. Promotion (and access) to live environment controls are only adequate and require improvement.

6. ICT Operations
Current 2.75 (Target 3.00)

Controls over Data Retention exceed good practice (note that archiving was not included within the scope of data retention and is currently an ICT concern).

Service Delivery and Problem Management controls meet good practice. Physical data centre security, Disaster recovery and business continuity planning controls are only adequate and require improvement.

7. Information Security
Current 3.00 (Target 3.25)

Controls over Security Awareness and Training, Threat and vulnerability management exceed good practice. Identity and Access Management controls meet good practice. Across the domain controls over Security Management, Monitoring Unusual & Privileged Access and Data Loss Prevention are only adequate and require improvement.

Appendix
ICT controls benchmarking results

Appendix A:
Current control strength versus impact grid

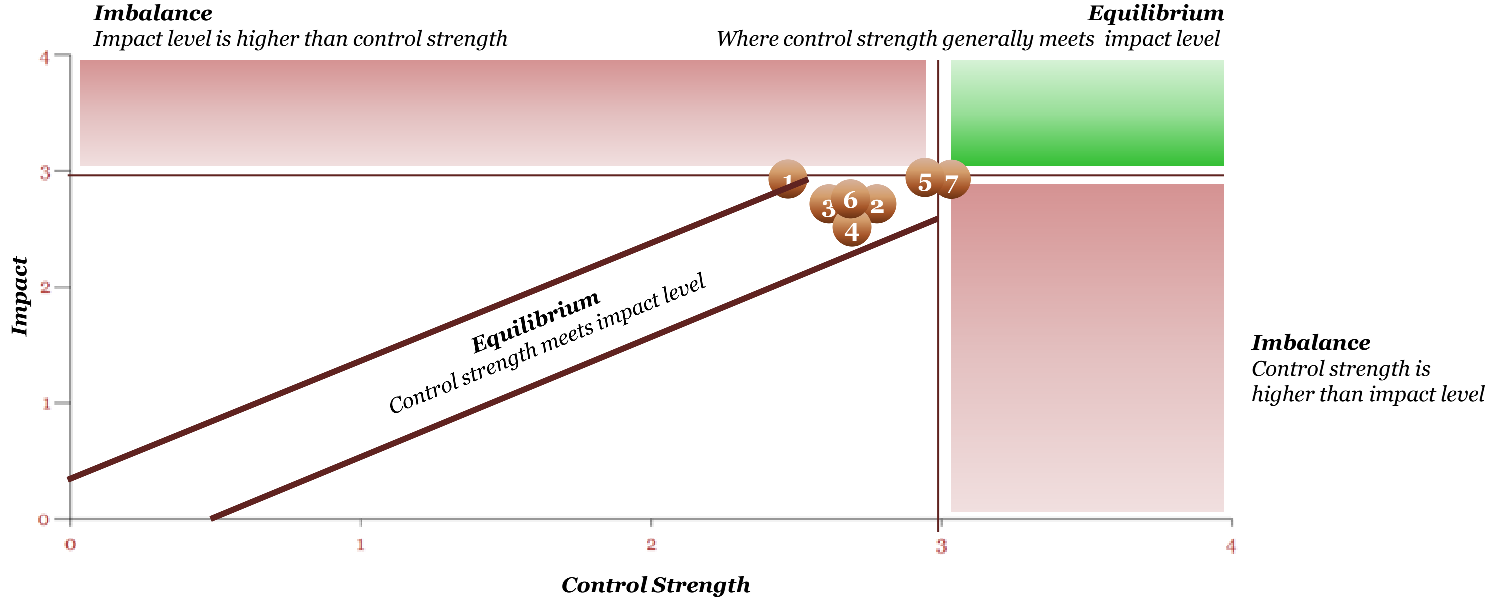
This grid demonstrates where current controls strength aligns to impact levels. Key observations are as follows:

- ICT Governance, ICT Management, Systems Quality, Systems Support, ICT Operations and Information Security have control strengths broadly in-line with their impact level.
- Strategic decisions controls are slightly weaker than that demanded of the impact level.

Impact scores

Area	1 – Strategic Decisions	2 – ICT Governance	3 – ICT Management	4 – Systems Quality	5 – Systems Support	6 – ICT Operations	7 – Info Security
Impact	3.00	2.75	2.75	2.50	3.00	2.75	3.00
Control Strength	2.50	2.75	2.75	2.75	3.00	2.75	3.00

Very High 4, High 3, Medium 2, low 1, very low 0 (an average was taken to score each section)

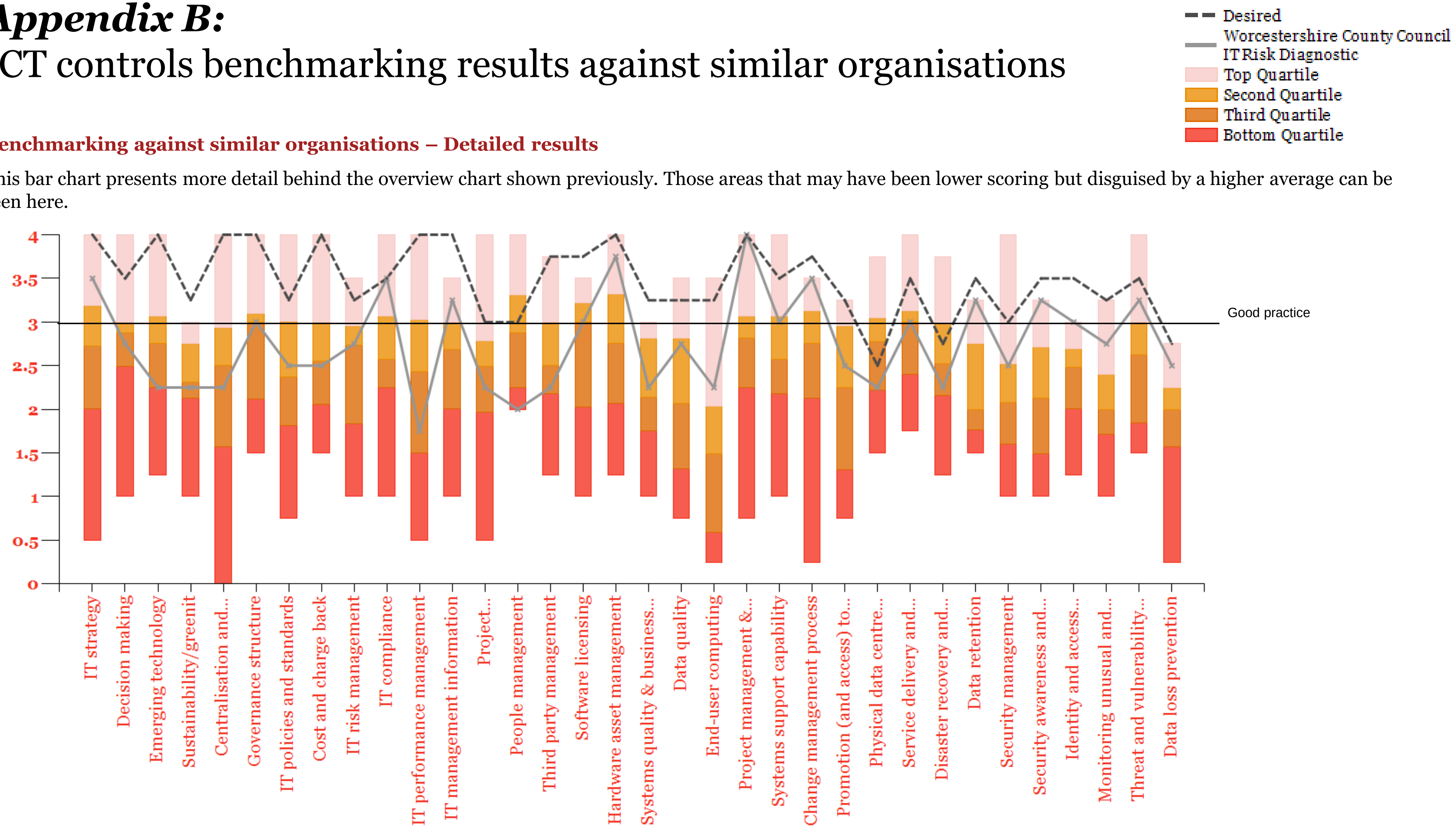


Appendix B:

ICT controls benchmarking results against similar organisations

Benchmarking against similar organisations – Detailed results

This bar chart presents more detail behind the overview chart shown previously. Those areas that may have been lower scoring but disguised by a higher average can be seen here.



Appendix C:
Detailed questions and scores

- **Strategic decision-making**
- **ICT Governance**
- **ICT Management**
- **Systems Quality**
- **Systems support and change**
- **ICT operations**
- **Information Security**

Question	Potential Impact Rating	Desired Control Strength	Current Control Strength
1.1 ICT Strategy - Has the ICT strategy been aligned with the business strategy?	High	4.00	3.50
1.2 Decision making - To what extent has strategic ICT decision making been mandated and aligned?	High	3.50	2.75
1.3 Emerging technology - To what extent does the organisation understand and monitor the impact of new trends and technologies?	High	4.00	2.25
1.4 Sustainability/Green IT - How effective is the organisation at managing its environmental and social impacts through ICT?	High	3.25	2.25
1.6 Centralisation and standardisation - To what extent has the business centralised and standardised technology, ICT processes and controls?	High	4.00	2.25

Appendix C:
Detailed questions and scores

Strategic decision-making

ICT Governance

ICT Management

Systems Quality

Systems support and change

ICT operations

Information Security

Question	Potential Impact Rating	Desired Control Strength	Current Control Strength
2.1 Governance structure - To what extent has formal governance structures been identified and formulated?	High	4.00	3.00
2.2 ICT policies and standards - To what extent do policies and standards exist and operate in the organisation?	Medium	3.25	2.50
2.3 Cost and charge back - To what extent does the ICT organisation manage and recover ICT costs from the business domain?	Very High	4.00	2.50
2.4 ICT risk management - To what extent has ICT risk management functions been identified?	Medium	3.25	2.75
2.5 ICT compliance - To what extent does the organisation ensure that ICT processes and systems are in compliance with relevant statutory, regulatory and contractual requirements?	High	3.50	3.50
2.6 ICT performance management - To what extent is the performance of the ICT function monitored and managed?	Medium	4.00	1.75

Appendix C:
Detailed questions and scores

Strategic decision-making | ICT Governance | **ICT Management** | Systems Quality | Systems support and change | ICT operations | Information Security

Question	Potential Impact Rating	Desired Control Strength	Current Control Strength
3.1 ICT management information - To what extent does ICT management have good quality management information (MI) on the performance of ICT?	Medium	4.00	3.25
3.2 Project portfolio/programme management - To what extent is the portfolio of information systems and future projects been optimised?	High	3.00	2.25
3.3 People management - How are job responsibilities defined and resourced across the ICT Function?	High	3.00	2.00
3.4 Third party management - To what extent are ICT services provided by third parties (e.g. under outsourcing arrangements) controlled?	High	3.75	2.25
3.5 Software licensing - How effective are controls to ensure that unlicensed software is not in use?	High	3.75	3.00
3.6 Hardware asset management - How effective are controls to ensure that hardware assets are retained and that unauthorised devices are not connected to the network?	Medium	4.00	3.75

Appendix C:
Detailed questions and scores

Strategic decision-making

ICT Governance

ICT Management

Systems Quality

Systems support and change

ICT operations

Information Security

Question	Potential Impact Rating	Desired Control Strength	Current Control Strength
4.1 Systems quality and business intelligence - How effective are the systems at supporting the business, including the quality of information used to support decision-making?	Medium	3.25	2.25
4.2 Data quality - How well does the organisation understand and manage the data it uses to run its business?	High	3.25	2.75
4.3 End-user computing - How effective are controls over end-user computing models (EUCs)?	Medium	3.25	2.25
4.4 Project management and benefits realisation - To what extent are IT projects appropriately authorised, managed and delivered?	High	4.00	4.00

Appendix C:
Detailed questions and scores

Strategic decision-making | ICT Governance | ICT Management | Systems Quality | **Systems support and change** | ICT operations | Information Security

Question	Potential Impact Rating	Desired Control Strength	Current Control Strength
5.1 Systems support capability - How effective is the support for key systems (such as ERP and major operational systems)?	High	3.50	3.00
5.2 Changes management process - To what extent are business-as-usual or changes to existing systems appropriately authorised, tracked and tested?	High	3.75	3.50
5.3 Promotion (and access) to live environment - Is there segregation of duties within ICT between those that can change code or systems configuration and those that can implement changes into the live environment?	High	3.25	2.50

Appendix C:
Detailed questions and scores

Strategic decision-making

ICT Governance

ICT Management

Systems Quality

Systems support and change

ICT operations

Information Security

Question	Potential Impact Rating	Desired Control Strength	Current Control Strength
6.1 Physical data centre security - How effective are the physical and environmental controls in place over the data centre or computer room?	High	2.50	2.25
6.2 Service delivery and problem management - How effective are the processes for identifying and fixing ICT problems?	Medium	3.50	3.00
6.3 Disaster recovery and continuity planning - How good are the plans for disaster recovery (DR) and business continuity planning (BCP)?	High	2.75	2.25
6.4 Data retention - How effective are controls to ensure that essential records are retained for an appropriate period and that regulatory requirements for data retention and destruction are met?	High	3.50	3.25

Appendix C:
Detailed questions and scores

Strategic decision-making | ICT Governance | ICT Management | Systems Quality | Systems support and change | ICT operations | **Information Security**

Question	Potential Impact Rating	Desired Control Strength	Current Control Strength
7.1 Security management - To what extent does the organisation place a high priority on the management of information security risks?	High	3.00	2.50
7.2 Security awareness and training - How effective are the steps taken to raise staff awareness of information security issues?	High	3.50	3.25
7.3 Identity and access management - How effective are processes for granting the right access to the right people?	High	3.50	3.00
7.4 Monitoring unusual and privileged access - To what extent are incidents or unusual events monitored and investigated?	Medium	3.25	2.75
7.5 Threat and vulnerability management - How well does the organisation identify threats and protect itself against them?	Very High	3.50	3.25
7.6 Data loss prevention - To what extent are endpoint devices (e.g. laptops) secured to prevent data loss?	High	2.75	2.50

Appendix D:
Background to the Benchmarking process

ICT Wheel – The page containing the qualitative review presents the detailed results of the benchmarking exercise performed against the 7 areas of good practice. The outcome from the benchmarking exercise identifies areas for focus over the forthcoming months and based on risk, colour coded according to the key accompanying the wheel. This assessment has been made based on the scores in the individual areas as well as a consideration of the importance of the areas in the context of the organisation.

Benchmark Data - Our benchmark database contains “audited” data, built up from equivalent reviews at other clients. It should be noted that the complete data set includes many clients who are large multinationals and as such will be governed by greater regulation around controls therefore we decided not to benchmark against this group on this occasion. As with all benchmarks, this analysis should be treated as indicative rather than comprehensive. It should also be noted that different companies may exhibit different risk profiles and may require different levels of control over their ICT activities. In addition, in any organisation, there needs to be a balance between cost and control. Consequently, there is not a single correct level of control for all organisations.

The scores and information used in this report were obtained through a facilitated workshop held with your senior ICT management and selected others . The attendees of the workshop were as follows; The Head of Technology **-** Systems and Customer Access, Service Operational Manager, Contracts Manager, Enterprise Application Manager, Project Manager and the Application Support Manager