CARDIFF COUNCIL
CYNGOR DINAS CAERDYDD

AUDIT COMMITTEE: 26 June 2018

UPDATE ON INTERNAL CONTROL ENVIRONMENT

REPORT OF CORPORATE DIRECTOR RESOURCES
AGENDA ITEM: 6.2

Reason for this Report

1.   This report has been produced in response to the Audit Committee's request for an update on governance and control within the Resources Directorate. This report also aims to provide assurance on the implementation of the recommendations made by Internal Audit.

Background

2.   Cardiff Council's Resources Directorate has responsibility for a wide and complex range of statutory duties, functions and services. The Directorate manages the following services through a net budget of £19.9 million and with an establishment of 870 officers.

- Commissioning and Procurement.
- Corporate Health and Safety.
- Digital services including ICT, Customer Services and the Capital Ambition Delivery Team.
- Finance including Accountancy, Internal Audit and Revenues.
- Human Resources.
- Information Governance
- Performance and Partnerships including corporate policy and Emergency Management.

3.   In addition, the Directorate has operational responsibility for the Cardiff and Vale of Glamorgan Local Government Pension Fund currently valued at £2 billion.

4.   In respect of all these services, the Directorate is concerned with managing risk at both the strategic and operational level and in respect of service delivery to citizens. The scale and scope of activities undertaken is illustrated by the following list of strategic priorities drawn from the Council's Corporate plan.

- Develop and appropriately skill the workforce to meet the changing needs and demands of the Council.
- Communicate and implement the Capital Ambition Delivery Programme.
- Promote the health and wellbeing of council employees.
- Support the implementation of local government reform and associated collaborative working, both within the directorate and wider council.
- Develop a robust planning framework that reflects the Council's priorities and enable effective decision making and achievement of outcomes.
- Further develop and embed corporate processes that are easy to use, more efficient and that foster innovation whilst clarifying accountability and responsibility.
- Ensure the Council meets its statutory obligations.
- Working with our partners and communities to tackle long standing issues in the community in cost effective and sustainable ways.
- Maximize economic, social, environmental and cultural well-being.

Issues

Risk management and monitoring arrangements.

5.   The Directorate has developed a clear structure and process for managing and monitoring strategic and operational risks related to its responsibilities and commitments as set out below

- **Directorate Delivery Plan** – This sets out key strategic and operational activities aligned to the Corporate Plan and to the Capital Ambition Delivery Programme. Consideration is given to resources required to deliver projects and initiatives together with statutory services along with associated risks.
- **Risk registers** – risks managed by the directorate are detailed on the registers and are monitored and reviewed quarterly at management meetings. Any risks that are identified as Red or Red/Amber are considered for escalation to the Corporate Risk Register. Risks associated with the delivery of council-wide activities have been identified and are monitored and reviewed alongside the directorate quarterly performance reporting arrangement.
- **Quarterly Performance Review** – performance is monitored and reviewed by the management team on a quarterly basis and updates are used to feed into a quarterly review of both directorate and Corporate Risk Registers. The management team considers progress made to deliver key commitments and activities and an evaluation is undertaken to determine the extent to which risks have been mitigated and whether any further action is required to manage down risks accordingly.
- **Risk Management Steering Group** – this is managed through the Resources Directorate which allows officers to have access to expert advice and developments at the earliest opportunity. A number of Risk Champions with skills in core disciplines, support directorate risk management on an ongoing basis.

Current Corporate Risks

6. The Resources Directorate currently collates the corporate position for twelve risks as the owner of associated policies and frameworks. The relative positions are summarised below, classified by the primary nature of each risk (strategic, financial, service delivery, legal and regulatory).

    - **Strategic**

7. The Directorate reports the corporate position against three risks to Council strategy.

    - **Delivering Capital Ambition Programme** – The risk of failing to deliver an effective programme of change to support the Administration's four year Capital Ambition Delivery Programme (CADP). The CADP replaced the Organisational Programme (ODP) as the corporate change programme in December 2017 following recommendations of an independent review in May 2017. The focus of the CADP is on a smaller number of transformational programmes, aligned to corporate priorities and budgets. Governance documentation such as the project brief and project acceptance criteria is in development.

    - **Workforce Planning** – The risk to the Council's capability and capacity of ineffective forecasting and planning for future workforce needs. There are active mechanisms in place to develop existing staff, such as the Cardiff Academy, and apprenticeships and traineeships are promoted to support a pipeline of talent. Cabinet will consider a new workforce strategy for 2018/21 in July 2018 and an IT solution for enhanced personnel data is scheduled to be sourced in 2018/19.

    - **City Security -** The risk of a Major security-related incident in the city as a result of international or domestic terrorism. The current focus is on making targeted incremental improvements through investment in the City infrastructure. There is active engagement in partnership working to prevent, protect and prepare for a major security-related incident, but this is against the backdrop of the UK threat level of 'severe'.

    - **Financial**

8. The Directorate reports the corporate positon against three risks to finance and internal control.

    - **Financial Resilience** – The risk of failing to deliver a balanced annual budget and a fully informed Medium Term Financial Plan, which would significantly weaken the financial resilience of the Council. The current Budget Gap of £91 million for the period 2019/20 to 2021/22 will be addressed through the budget planning process, which has been brought forward in recent budget setting cycles to allow more time for challenge and focus in achieving a deliverable budget.

- **Budget Monitoring (Control)** - Failure to achieve the budget set, inclusive of budgeted spend and savings across Directorates, with increased use of emergency finance measures and the drawdown of reserves. The Council's monitoring approach is robust and includes challenge sessions to provide assurance on the in-year financial monitoring position, through which we continue to report the actual and projected overspends are reported to SMT for review and mitigation. Cabinet portfolio holders are also kept informed of the monitoring position on a regular basis.

- **Fraud, Bribery and Corruption** - Fraud, financial impropriety or improper business practices may increase due to weak internal controls, which may result from stretched resources. Management assurances and the independent work of the Internal Audit function, indicate that the potential for impropriety is isolated to a minority of areas for which there are targeted actions in place to improve the internal control environment. The Council's refreshed Fraud, Bribery and Corruption Policy reinforces the significance given to robust stewardship, a culture of accountability and zero tolerance to impropriety.

- **Service Delivery**

9. The Directorate reports the corporate position against three risks to the delivery of services.

- **Performance Management** –The risk to embedding, consistently applying and continually developing performance management arrangements in line with the Council's evolving operating environment. The work done over the past few years has improved the Council's approach to performance management, and led to improved performance in many key areas. The primary challenge and focus going forward is to continue to improve service provision in the context of reducing finances and demographic growth.

- **Business Continuity** - The risk of a large-scale incident/loss affecting the delivery of services. As business as usual, we measure the criticality of our services and set recovery timeframes, which range from 0-1 hours to 5 working days for different priority activities. Directorates are required to prepare business continuity plans for time sensitive services, for which a programme of audits provide assurance and support. For dealing with internal incidents and external emergencies, we have a 24-hour incident management structure occupied by senior officers who are trained to take key roles and responsibilities.

- **ICT Platforms Unsuitable / Outdated** - The risk that ICT platforms (desktop, software, network, servers, and telephones) will not be able to support the technologies required by the corporate change programme, or will not provide a reliable service due to age and condition of equipment and systems. There is a renewal programme in place for ICT platforms, which is considered appropriate for the ambitions and resources of the

Council. New systems have minimum requirements for downtime, and ICT lifecycle monitoring and further support for directorates and schools are identified as areas to progress.

- **Legal and Regulatory**

10. The Directorate reports the corporate position against three legal and regulatory risks.

- **Health and Safety** – The risk of ineffective health and safety compliance through poor application and embedding of the 'Framework for Managing Health and Safety' in Cardiff Council. Over the last year, a number of appointments have been made to strengthen the corporate health and safety team, who have taken responsibility for the Council's RAMIS Statutory Maintenance system and targeting improvements in five key areas (asbestos management, fire safety, electrical safety, gas safety, and legionella control).

- **Information Governance** – The risk that information handled inappropriately could leave the Council exposed to intervention and financial penalties issued by the Information Commissioner (ICO), to include information held by Cardiff Schools. A number of measures have been put in place to prepare for the General Data Protection Regulation (GDPR), which came into force on 25 May 2018, supported by a programme of council-wide training. A GDPR Implementation Plan is in place, overseen by a GDPR Implementation Group with mechanisms for issues to be escalated to the Operational Manager for Information Governance and the Council's Senior Information Risk Owner (SIRO).

- **Cyber Security** - The ability to protect information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. The National Cyber Security Centre approach is used for an ongoing cyber-security assessment against 11 risk factors. Secure configuration, monitoring and corporate cloud security controls have been identified as areas for improvement. Measures to progress include the development of an asset register, ICT lifecycle and notification targets, privacy and cloud impact assessment reviews.

Senior Management Assurance Statement

11. The Directorate Management team is actively engaged in the review of the directorate's SMAS both at an individual level on behalf of their function and as part of the discussion that considers and collates the overall position. In carrying out this exercise the following picture sets out the thought process used.

12. As might be expected for this directorate the aspects around Risk and Budget Delivery were judged as Embedded while the vast majority of the other aspects have been identified as having a Strong application. Opportunities to improve the integration of risk registers with internal and external stakeholders, to formalise mechanisms for partnership assurances and to improve the future generation approach to decision making have been recognised. These areas for development are common for the Council as a whole and for which corporate actions are being progressed through the AGS action plan.

13. Regular discussions will continue at management meetings to further improve the position in time for the mid-year review.

Monitoring/Implementing recommendations made in Internal Audit reports

14. The audits undertaken for Resources during 2017/18 were:

Audit	Status	Assurance rating	Number of recommendations made	Number of recommendations agreed
Commissioning and procurement	Final report issued	Effective with opportunity for improvement	2	2
Effective Decision Making	Draft reports issued			

Governance	Final report issued	Effective with opportunity for improvement	2	2
Payroll	Final report issued	Effective	0	0
Cybersecurity governance	Final report issued	Insufficient with major improvement needed	4	4
ICT Business Continuity and Disaster Recovery	Final report issued	Insufficient with major improvement needed	3	3
Server virtualisation	Ongoing			
IT governance	Final report issued	Effective with opportunity for improvement	4	4
PCI DSS	Final report issued	Insufficient with major improvement needed	5	3
Insurance (CRSA and testing)	Final report issued	Effective	2	2

15. The latest position in respect of the above audits shown as "Insufficient with major improvement needed" is as follows:

Cyber security governance – all ICT related recommendations have been completed. The one recommendation not yet fully completed relates to Information Governance in respect of one information asset register that remains outstanding. The purpose and importance of Information Asset Registers has formed part of the 'Information Governance, GDPR and You training' seminars which have been delivered to all directorates.

On an ongoing basis the Information Asset Registers are used, and will continue to be used, as a point of reference as part of the work to support directorates move forward with complying with GDPR and the UK Data Protection Act 2018. This action is ongoing and will be included in as part of business as usual.

ICT BC and DR – one action has been completed. Work has been undertaken on the second in reviewing the business continuity fall back site locations, and the testing of the plans remains a work in progress.

PCI DSS – four of the actions have been completed, and one remains "in progress" (but with an action date of 31July 18). The open action relates to training of officers in PCI DSS requirements.

16. Audits were also undertaken on fundamental financial systems during the year:

Audit	Status	Assurance rating	Number of recommendations	Number implemented
Asset management	Fieldwork ongoing			
Council Tax 2016/17	Final report issued	Effective	1	1
Local Housing Allowances	Final report issued	Effective	0	0
Main accounting 2016/17	Final report issued	Effective	0	0
NNDR 2016/17	Final report issued	Effective	0	0
Treasury management	Final report issued	Effective with opportunity for improvement	3	3

17. The recommendations made for final reports issued are reported to every meeting of the Audit Committee on the Recommendation Tracker that is attached to the Internal Audit progress report. Managers are contacted before every Audit Committee meeting for an update on the implementation of recommendations, and the recommendations remain on the tracker until managers confirm that they have been fully implemented, at which point they are marked as closed.

18. Audit has been involved in the revision of the Contract Standing Orders & Procurement Rules and Financial Procedure Rules, which will come into force on 1 July 2018.

Audit Planning and liaison

19. The draft audit plan is presented to Audit Committee in January of each year to allow members to review the broad themes and time allocations. Once the draft plan has been agreed, the Relationship Manager will meet with the Director and management team to discuss the corporate themes and the number of audit days that will be allocated to each of those themes in the directorate. Also discussed at these meetings are any areas of concern that

the Director would like Internal Audit to review and the number of audit days that will be allocated to these assurance or consultation pieces.

20.	This is then presented back to Audit Committee in March for final agreement by members. During the year, there are regular, quarterly meetings with the Relationship Manager to discuss progress against the agreed plan and to discuss any emerging risks that might need to be reviewed during the year. Any audits that cannot be undertaken at that time (such as due to on-going system changes) will also be discussed at these meetings. If any changes are made to the agreed audit plan, these are reported to the next meeting of the Audit Committee for the members to agree.

21.	Auditors also meet with managers at the start of each audit for initial scoping of the audits and at the end of the audit prior to the draft report being issued to discuss the main findings. Managers will also contact Internal Audit for advice and guidance on any matters of internal control and auditors have been involved with system and process development.

Legal Implications

22.	The statutory functions of the Audit Committee include the duty to review, scrutinise and issue reports and recommendations on the appropriateness of the authority's risk management, internal control and corporate governance arrangements (pursuant to Part 6 Chapter 2 of the Local Government (Wales) Measure 2011). In discharging its functions, the Audit Committee must have regard to all relevant guidance, in particular the CIPFA guidance for Audit Committees.

Financial Implications

23.	There are no financial implications arising from this report.

Recommendations

24.	Audit Committee are requested to note the contents of the report.

CHRISTINE SALTER
CORPORATE DIRECTOR RESOURCES