Appendix 1a: Assurance and Themes

Assurance

High	**Satisfactory**	Partial	Minimal

Drug and Alcohol Commissioning Team Governance

Objective

To assess whether accountability for and the objectives of the Drug and Alcohol Commissioning team (DACT) were clearly defined and its performance effectively monitored.

Themes

The Drug and Alcohol Commissioning team (DACT) is the Council team responsible for the commissioning of drug and alcohol services across the borough and is funded by the Council. Its performance is influenced and monitored by the Council's Department for People and the Southend Community Safety Partnership Priority Leadership Group (CSP PLG).

Roles, Responsibilities and Accountabilities

The CSP PLG is the statutorily required Crime & Disorder Reduction Partnership for the borough. It meets regularly and has robust, terms of reference in place that clearly sets out:

- its role, remit and reporting requirements
- specific responsibilities in relation to the DACT, which are to:
  - set the strategic direction for its services, to approve strategic plans and policies and to performance manage progress in delivering them
  - give guidance as well as strategic and leadership support to the DACT Manager to enable the service's targets to be met.

Internally, the DACT reports to the Director of Adults and Housing within the Department of People, who ensures it is appropriately structured, resourced and managed.

Service planning

Whilst the aspects of what the service is required to deliver and the performance measures that are expected, appear in various Council and partnership documents, there is no one overarching plan that pulls them all together.

At a partnership level, the DACT's work is driven by:

- an annual Strategic Intelligence Assessment which identifies the local crime priorities e.g. increasing the number of people in drug treatment and tackling anti-social behaviour
- the Southend Drug and Alcohol Gambling Strategy for 2015-2018 and Alcohol and Problem Gambling Strategy Key Actions 2016-17, which it leads.

Appendix 1a: Assurance and Themes

Assurance

High	**Satisfactory**	Partial	Minimal

At a Council level, the DACT's role and work requirements are set out in Adults and Housing Service Plan for 2016/17. However, this only includes one performance indicator and four specific actions. Consideration should be given to developing a team plan that contains everything the service needs to deliver. This could then be monitored via the Council's normal performance management process (see below).

Performance monitoring and reporting

A DACT Managers Report is presented to each CSP PLG meeting and includes high-level narrative information as well as detailed appendices regarding:

- the performance of commissioned services and financial performance
- progress towards the procurement of drug and alcohol services in 2017.

There was evidence that issues with contractor performance were managed appropriately and in line with contract management principles set out in the Council's Contract Procedure Rules.

Delivery of the Council's Adults and Housing Service Plan is monitored monthly via Covalent (the performance management system).

Current management processes may not provide adequate mechanisms to identify and manage risks facing the DACT. This may result in avoidable risks materialising and mean that management do not have all information required to make effective decisions.

Number of actions agreed: 2

Airport Business Park Project Assurance

Objective

To assess whether effective project processes have been established for delivering the Airport Business Park Project to ensure it achieves the expected benefits, within the intended timeframes.

Themes

Governance

As at February 2017, when this audit was undertaken, it was possible to conclude that the arrangements:

- established to manage the Airport Business Park project were sound
- were documented within the Development Agreement between the Council and the project developer.

A Partnership Board provides strategic oversight of the project and meets quarterly. A Project Steering Board supports this. It has operational responsibility for the delivery of the development project, and meets monthly.

Appendix 1a: Assurance and Themes

Assurance

High	**Satisfactory**	Partial	Minimal

The Development Agreement includes terms of references for these Boards that cover all elements expected, which are integral to ensuring effective project governance. Meetings are minuted, actions are clearly defined with owners named and they are followed up at subsequent meetings to ensure they are delivered.

Every other week, the Council’s Project Manager provides key senior officers with an informal report that:

- summarises progress made against major project milestones
- highlights any issues requiring action.

However, it does not specifically cover key project control areas of time, cost, quality, scope, changes, risks, and benefits. The process would be strengthened by introducing more formal highlight reporting to the Boards, covering these areas, to ensure decisions taken are based on all the available information.

Benefits Management

The Airport Business Park Phase 1 Business Case, dated 11th January 2016, sets out the planned benefits of the project, at a high level. These are tangible deliverables, which in some instances are quantifiable e.g. number of new jobs to be created.

Further work is needed to produce detailed benefit profiles for the project, benefits management strategies or plans. This will help the Council to demonstrate the ultimate realisation of intended benefits and justify the project investment decisions.

The operational arrangements for managing delivery of expected project benefits also need to be defined to ensure there is clarity over:

- who is going to be accountable for doing what and where is this going to be reported?
- how benefits / dis-benefits are going to be identified, which are to be measured, how and over what timeframe?
- the milestones within the project when benefits reviews should be undertaken
- the arrangements for handing over and embedding activities, following the implementation of the each phase of the project.

Project Planning

The developer has provided a project plan for the current phase of the project, which:

- included fields to capture the required information, for example, task description, duration, start and finish dates
- outlines the critical path of activity.

Progress against key milestones is reviewed at Project Steering Board meetings. Updates are included within the Council Project Manager's fortnightly status reports.

Appendix 1a: Assurance and Themes

Assurance

High	**Satisfactory**	Partial	Minimal

Dependency Management

A draft dependency log (The Dependency Register) was in place, which will provide the means to monitor and manage dependencies throughout the project lifecycle. The draft 24th January 2017 version had 32 dependencies, which may affect eight project areas or milestones. However, it did not capture all the information expected, nor had it been fully completed.

The Council may incur avoidable delays, and resultant costs, if it does not fully understand and manage the dependencies across the project and therefore the impact of decisions and changes.

Number of actions agreed: 3

Cyber Security Governance

Objective

To assess whether the Council has designed as well as effectively operates a suitable cyber security governance framework for making and implementing decisions required to direct, monitor, evaluate and report on cyber security management within the business.

Themes

Cyber security strategy

A dedicated ‘Cyber Security Strategy Document’ should be produced, although cyber security principles are embedded within the extensive policy set and wider IT documentation. Security plans are in place. Delivering the cyber security action plan should result in the Council's accredited to the government-backed “Cyber Essentials” scheme (rather than the enhanced scheme). This will align Council activities to the National Cyber Security Strategy, make a clear statement of intent and help direct spending accordingly.

Cyber security governance

Since October 2016 restructure:

- the Director of Legal and Democratic Services became the Senior Information Risk Owner (SIRO)
- not all of the forums and committees involved in informing and updating the various stakeholders around cyber security, have met.

A clear plan is required setting out when they will be renewed and who will take part in them. Given these committees involved senior management across the Council, this presents a governance and communication risk.

Appendix 1a: Assurance and Themes

Assurance

High	**Satisfactory**	Partial	Minimal

Cyber security spending

It may help the Council to have a dedicated cyber security budget linked to a planned programme of initiatives that support the delivery of the cyber security strategy. Like many others, cyber security spend is not itemised within the general IT budget. Nevertheless, this spend is being tracked by management, and additional funds have been requested to enable the Cyber Essential programme to be delivered.

Good work has been done by the Information Governance team towards meeting the national standards. However, fewer resources have been invested in this area to date, so progress has been slower in terms of updating policies as well as training modules and the Information Governance toolkit.

Roles and Responsibilities

There was a clear reporting and escalation process for cyber security incidents, albeit under the previous senior management structure in the “Data Security Breach Management” document (last reviewed in 2013). Formalising the new accountabilities and responsibilities will help address these governance issues.

Furthermore, there was evidence that the data protection, information governance and breach management reporting appears comprehensive. This good practice is further enhanced through weekly IT management meetings and six-weekly data protection meetings.

The ICT team operates to a recognised industry-standard model (ITIL) where cyber security incidents are reported. The current incident management process contains the documentation that was expected. This could be improved by having an overarching policy as well as further enhancements to the process to monitor and track less critical incidents.

The Council’s Risk Management Policy details the risk management reporting structure. There is also a clear process for reporting data protection breaches or incidents. The Data Protection e-learning should cover cyber security when it is refreshed, and all employees should complete refresher training every two years.

Cyber security risks are being tracked at corporate and project levels. This provides some oversight but does not provide:

- enough detail to adequately manage the risk
- insight where single instances across multiple projects may present a larger issue
- a holistic view of the wider risks across the estate, as there is a gap between the corporate / service view and the project view.

The Customer Service Plan risk register had not been updated since September 2016 although a more formal risk management process was in place for reporting data protection issues. A risk assessment process is in place for new ICT systems but there were no plans to perform a Security Risk Assessment on existing / legacy systems.

Appendix 1a: Assurance and Themes

Assurance

High	**Satisfactory**	Partial	Minimal

There is a general understanding across the Council of the difference between an ‘information asset’ and a ‘system asset’. The development of a formalised and central Information Asset Register that are scored and associated with Business Impact Levels will:

- better help the Council to identify the location of its data (including its sensitive and protected data)
- enable ICT to apply proportionate controls to different levels of risk.

Clear guidance should also be created on how to store, transfer and delete different types of information at different levels of sensitivity e.g. public, internal or sensitive.

Number of actions agreed: 10

IT Data Security Policy Application

Objective

To assess whether the Council’s approach to IT Data Security is well managed, secure and helps deliver both effective IT and wider-Council services.

Themes

The Corporate Information Security Policy reflects recognised good practice guidance on IT data security and is available to staff on the Council Intranet. It refers to staff having to ensure that they conduct business in accordance with this Policy and all applicable supporting policies. This is supplemented by an appropriate level of staff training, presentations and posters that address Data Protection issues. However, the supporting policies are not identified and a number of those on the Internet were out of date. The Corporate Information Security Policy could be strengthened by naming them, ensuring that they are current and storing them in a single Intranet location for ease of reference by staff.

An Information Sharing Protocols Register is in place which shows the date of each protocol, the subject area and relevant Departmental lead. It covers the legal requirements for the effective control of data.

The Council is not following the Government Data Classification scheme yet and data is therefore not being classified. The need to do this was raised in the Information Commissioners Office (ICO) Data Protection Report in issued in February 2013. Therefore, proper consideration should be given to the costs and benefits of implementing such a scheme as well as the risks of not doing so, before a decision is made.

There is clear guidance in place covering serious incident and data security breach management dealing with section 29 (Police) requests and subject access requests which is in line with the Data Protection Act 1998.

Appendix 1a: Assurance and Themes

Assurance

High	**Satisfactory**	Partial	Minimal

A log of reported breaches is maintained with individual breach reports being sent to the Senior Information Reporting Officer (SIRO). It contains all the information expected when such reports are made and all were investigated with recommendations made to strengthen the arrangements where necessary. None required reporting to the ICO. Overall, the Council procedures for dealing with breaches are robust.

Access to the Council's network is protected with an effective password control while remote access uses a multifactor process using Active Directory account and a pinsafe Multi Factor Authentication security application. Laptops and USB sticks are encrypted and mobile phone data is contained within a protected environment. The Council is now looking to put a system in place that would provide the capability to review unsuccessful log-on attempts to determine unauthorised activity and also provide trend analysis. A more robust action planning and monitoring arrangement is required to ensure that issues arising from penetration testing are dealt with in a timely manner.

Overall, access to the IT suite is satisfactorily controlled, as is its environment e.g. air conditioning and fire suppression. However, protection of the new server room could be improved with the introduction of a visitor log and CCTV.

A backup process is in place. Nevertheless, the overarching backup strategy is being drafted, needs to be approved and then implemented to help ensure the backup regime is effective.

Disposal procedures are in place that ensures that data is cleansed and reports are provided to evidence this.

Number of actions agreed: 8

Financial systems work to support the production of the Council's financial statements

Objective

To confirm that the following key objectives and associated controls in each of the systems outlined below:

- are designed to prevent or detect material financial errors, and
- have been in place during 2016/17 and therefore, can be relied when producing the Council's Financial Statements.

Scope and Control Opinions

The key controls audited are detailed in the table below. The assurance assessment (*) reflects:

- the strength of the control design
- how well the control has operated in practice OR

Appendix 1a: Assurance and Themes

Assurance

High	**Satisfactory**	Partial	Minimal

- the assurance obtained from substantive testing, if the control could not be relied upon.

Key controls audited	**Assurance** (* refer above)
Accounts Receivable	
• Reconciliations between the Accounts Receivable and the General Ledger systems are complete, accurate and timely.	**High**
Accounts Receivable	
• All instructions from originating service areas for debtors to be raised are: • accurately and completely turned into an up to date, official Council invoice, on a timely basis • recorded on the Accounts Receivable system.	**Partial**
Business Rates	
• Reconciliations of property numbers and rateable values between the Business Rates system and the government's Valuation Office are complete, accurate and timely.	**High**
• Reconciliations between the Business Rates and the General Ledger systems are complete, accurate and timely.	**High**
Council Tax	
• Reconciliations of property numbers and rateable values between the Council Tax system and the government's Valuation Office are complete, accurate and timely.	**High**
• Reconciliations between the Council Tax and General Ledger systems are complete, accurate and timely.	**High**
• Data identifying single person discount fraud supplied by the Council's supplier Datatank is used to correct Council tax accounts on a timely basis.	**High**
General Ledger	
• Journals are accurate, authorised and supported by appropriate evidence to confirm their validity.	**Satisfactory**

Appendix 1a: Assurance and Themes

Assurance

High	Satisfactory	Partial	Minimal

Key controls audited	Assurance (* refer above)
• Reconciliations between the General Ledger and the bank account/s are complete, accurate and timely.	**Satisfactory**
Housing Benefit	
• Reconciliations between the Housing Benefit and General Ledger systems are complete, accurate and timely.	**High**
Payroll	
• Reconciliations between the Payroll and General Ledger systems are complete, accurate and timely.	**Satisfactory**

Accounts Receivable

A report comprising of invoice requests for debtors is run on the CIVICA system. Internal Audit was advised that 10% of cases detailed on the report are supposed to be checked by the Accounts Receivable Manager, as per the established control environment.

The details of the invoice request and the invoice are checked to ensure that the coding and value is correct. For each case checked, the report is annotated with his initials and the date to indicate that the check has been undertaken.

However, it was noted that the latest report was produced on the 19th September 2016, which comprised of invoices raised in August. The Accounts Receivable Manager advised that it is not always possible to perform the checks each month due to other work commitments. A view should be taken as to whether to tolerate this risk, amend the level or frequency of checking to be done or address the resourcing issues.

General Ledger

Journals

The Agresso system comprises a workflow, which ensures that journals can only be posted onto the system by users with the appropriate permissions. A report was provided by the ICT Team Leader, detailing the users on the Agresso system with access to post journals. Three users listed, Accounting Technician, Apprentice Financial Analyst and Finance Business Partner should not have had this level of access.

Appendix 1a: Assurance and Themes

Assurance

High [✓ **Satisfactory**] Partial Minimal

A report was produced detailing users who had posted journals since April 2016. It confirmed that no journals had been posted during this period by the three users who should not have this access.

Therefore, although no reliance could be placed on this control, the risk did not materialise during this financial year.

Reconciliation to bank accounts

Reconciliations between the Council's Cashbook and the General Ledger are:

- performed on a monthly basis by a member of the Accounting Team (usually the Accounting Technician)
- independently authorised by the Group Manager (Financial Planning and Control).

However, it was identified that these reconciliations only covered the period up until October 2016, meaning that the reconciliation processes were three months in arrears at the time of the audit. This was because the person whose role is to do this, was absent during this period.

Action is being taken to bring the reconciliations up to date. However, the delays in performing these reconciliations could result in discrepancies failing to be identified in a timely manner, potentially resulting in financial loss. The Director of Finance & Resources has confirmed that as at May 2017, the monthly reconciliations are fully complete to the end of February 2017 and the March 2017 reconciliation is in progress and nearly concluded.

Payroll

A reconciliation should be performed between the Council's Payroll system and the General Ledger on a monthly basis. However, as at January 2017, it was identified that:

- the payroll cash and control reconciliations had been completed for periods one to six (April 2016 to September 2016)
- the cashbook and bank reconciliations had been completed for periods one to seven (April 2016 to October 2016).

As above, this was because of staff absence. These outstanding reconciliations are also being completed. The Director of Finance & Resources has confirmed that as at May 2017, the monthly reconciliations are fully complete to the end of March 2017.

Number of actions agreed: 3