

You are requested to attend a meeting of the Corporate Governance Committee to be held in The John Meikle Room, The Deane House, Belvedere Road, Taunton on 20 May 2013 at 18:15.

Agenda

- 1 Appointment of Chairman.
- 2 Appointment of Vice-Chairman.
- 3 Apologies.
- 4 Minutes of the meeting of the Corporate Governance Committee held on 11 March 2013 (attached).
- 5 Public Question Time.
- 6 Declaration of Interests
To receive declarations of personal or prejudicial interests, in accordance with the Code of Conduct.
- 7 Revenues and Benefits Investigation Team Report. Report of the Head of Revenues and Benefits (attached).

Reporting Officer: Heather Tiso

- 8 Update Report on Freedom of Information Act. Report of the Legal and Democratic Services Manager (attached).

Reporting Officer: Tonya Meers

- 9 Audit of Data Security Breaches. Report of the Legal and Democratic Services Manager (attached).

Reporting Officer: Tonya Meers

- 10 Corporate Governance Action Plan. Report of the Performance Lead (attached).

Reporting Officer: Dan Webb

- 11 SAP Controls - Update. Report of the Strategic Finance Officer (attached).

Reporting Officer: Maggie Hammond

- 12 Corporate Governance Committee Forward Plan (attached).
- 13 Corporate Governance Committee Forward Plan - details of forthcoming items to be considered by the Corporate Governance Committee and the opportunity for Members to suggest further items (attached)

Tonya Meers
Legal and Democratic Services Manager

16 September 2013

Members of the public are welcome to attend the meeting and listen to the discussions.

There is time set aside at the beginning of most meetings to allow the public to ask questions.

Speaking under “Public Question Time” is limited to 4 minutes per person in an overall period of 15 minutes. The Committee Administrator will keep a close watch on the time and the Chairman will be responsible for ensuring the time permitted does not overrun. The speaker will be allowed to address the Committee once only and will not be allowed to participate further in any debate.

Except at meetings of Full Council, where public participation will be restricted to Public Question Time only, if a member of the public wishes to address the Committee on any matter appearing on the agenda, the Chairman will normally permit this to occur when that item is reached and before the Councillors begin to debate the item.

This is more usual at meetings of the Council’s Planning Committee and details of the “rules” which apply at these meetings can be found in the leaflet “Having Your Say on Planning Applications”. A copy can be obtained free of charge from the Planning Reception Desk at The Deane House or by contacting the telephone number or e-mail address below.

If an item on the agenda is contentious, with a large number of people attending the meeting, a representative should be nominated to present the views of a group.

These arrangements do not apply to exempt (confidential) items on the agenda where any members of the press or public present will be asked to leave the Committee Room.

Full Council, Executive, Committees and Task and Finish Review agendas, reports and minutes are available on our website: www.tauntondeane.gov.uk



Lift access to the John Meikle Room and the other Committee Rooms on the first floor of The Deane House, is available from the main ground floor entrance. Toilet facilities, with wheelchair access, are also available off the landing directly outside the Committee Rooms.



An induction loop operates to enhance sound for anyone wearing a hearing aid or using a transmitter.

For further information about the meeting, please contact the Corporate Support Unit on 01823 356414 or email r.bryant@tauntondeane.gov.uk

If you would like an agenda, a report or the minutes of a meeting translated into another language or into Braille, large print, audio tape or CD, please telephone us on 01823 356356 or email: enquiries@tauntondeane.gov.uk

Corporate Governance Committee Members:-

- Councillor A Beaven
- Councillor S Coles
- Councillor B Denington
- Councillor E Gaines
- Councillor A Govier
- Councillor T Hall
- Councillor J Hunt
- Councillor L James
- Councillor R Lees
- Councillor D Reed
- Councillor V Stock-Williams
- Councillor P Tooze
- Councillor A Wedderkopp

Corporate Governance Committee – 11 March 2013

Present: Councillor D Reed (Chairman)
Councillor A Wedderkopp (Vice-Chairman)
Councillors Beaven, Coles, Denington, Govier, Hall, Horsley, Hunt,
Mrs Stock-Williams, Tooze, Mrs Warmington and Williams.

Officers: Shirlene Adam (Strategic Director), Mark Leeman (Strategy Lead),
Tonya Meers (Legal and Democratic Services Manager), Richard Sealy
(Corporate and Client Services Manager), Dan Webb (Client and
Performance Lead) Natasha Williams (Corporate Support Officer) and
Alastair Woodland (Audit Manager).

Also Present: Peter Lappin (Grant Thornton).

(The meeting commenced at 6.15 pm)

6. Apologies/Substitution

Apologies: Councillors Gaines, Miss James and R Lees.

Substitution: Councillor Horsley for Councillor Miss James.

7. Minutes

The minutes of the meeting held on 4 February 2013 were taken as read and were signed.

8. Grant Claims Report 2011/2012

Considered covering report previously circulated, which presented the External Auditors findings from their 2011/2012 review work.

Grant Thornton and the Audit Commission had certified four claims and returns for the financial year, relating to expenditure of £82 million.

The Certification of Claims and Returns report highlighted several areas where improvements could be made and the action plan reflected this.

It was reported that the number of claims that required certification had reduced. The Housing Revenue Account self-financing had meant that the base data return for the housing stock was no longer required and the Department for Communities and Local Government no longer required the audit certification of disabled facilities grants. Also, the Council had fewer claims amended in 2011/2012 than in 2012/2011.

The validation check report was discussed and it was recommended that future validation programme “bug” checks would be run before the claim was prepared.

Members discussed the difference in fees between 2010/2011 and 2011/2012. It was explained that the fee varied from year to year depending on the complexity of the cases sampled. Additional time had been spent on the qualification letter. With the validation “bug” report not being run before the preparation of the claim meant that the results had to be followed up.

Peter Lappin (Grant Thornton) thanked the officers of Taunton Deane Borough Council for their work.

Resolved that the Certification of Claims and Returns report be noted.

9. Update on Health and Safety

Richard Sealy (Corporate and Client Services Manager) updated Members on the progress of a range of Health and Safety matters across the organisation, which included:-

- The situation with regard to the vacant Health and Safety Advisor position;
- The arrangements for the Health and Safety Committee;
- The progress being made on re-establishing Joint Health and Safety Inspections;
- Discussions with UNISON on the introduction of the ‘Fair and Just Culture’;
- The current position with regard to the consolidation and compliance audit;
- The South West Audit Partnership (SWAP) Audit on Health and Safety;
- Accident and Incident Data for the period 1 April 2012 to 31 January 2013; and
- General Health and Safety Issues.

Health and Safety refresher training for Leads/Managers was scheduled for March and April 2013.

Members discussed the importance of Health and Safety and the findings of the audit review. Partial assurance was given in relation to the areas reviewed.

It was intended for relevant service managers to provide an update at future Corporate Governance Committee meetings if a partial assurance had been achieved.

Mr Sealy advised that there were no significant risks or incidents to report.

Members thanked Mr Sealy for providing cover over the past few months and the good progress achieved since the retirement of the Health and Safety Advisor.

Resolved that the progress made on the delivery of the strategy and the initiatives to improve the Council’s operating culture be noted.

10. TDBC Response to the Equality Act

As part of the 2012/2013 Audit Plan, a review had been undertaken to assess the adequacy of the controls and procedures in place for Equality and Diversity - Equalities Analysis Integration across the Authority. Although good progress had been made against three Corporate Equality Objectives, the SWAP had identified significant inconsistencies and high inherent risks against the four key issues identified.

In response to the findings, a Corporate Equality Action Plan (CEAP) had been prepared which would be implemented during 2013/2014. CMT would further consider the CEAP on 4 March 2013.

Progress against the CEAP would be monitored and reported upon twice a year with findings circulated to Members.

Members of the Corporate Governance Committee discussed the need for an interim update every quarter as well as the availability of equalities training for Members.

Resolved that the:-

- Performance against requirements and targets be noted; and
- The proposed response in the form of the Corporate Equalities Action Plan (Appendix 3) be supported.

11. Risk Management

Considered report previously circulated, updating Members on the current position of Risk Management. This was the process by which risks were identified, evaluated and controlled and was one of the key elements of the Corporate Governance Framework.

The Corporate Management Team (CMT) had recently undertaken a review of the Corporate Risk Register. A Summary Risk Profile and list of 17 risks had been included in the report.

A Risk Management Action Plan was also included in the report which outlined the key areas of focus to further improve and embed Risk Management during 2013.

Dan Webb (Client and Performance Lead) updated Members of the perceived risks. It was advised that the new West Somerset Joint Partnership project would be included in future risk profiles. Members discussed the importance of this project being included.

Members discussed the following risks:-

- Growth;
- Regeneration of Taunton Town Centre and retail scheme;
- Health and Safety; and

- Gypsies and Travellers.

Resolved that:-

- (a) Progress with the Corporate Risk Management be noted;
- (b) The Corporate Risk Register review be discussed at a future meeting;
- (c) The Risk management Action Plan be approved; and
- (d) The new Taunton Deane Borough Council and West Somerset Joint Partnership project be included on the Corporate Risk Register.

12. Internal Audit Plan Progress 2012-2013

Considered report previously circulated, which summarised the work of the Council's Internal Audit Service and provided:-

- Details of any new significant weaknesses identified during internal audit work completed since the last report to the Committee in September; and
- A schedule of audits completed during the period, detailing their respective assurance opinion rating, the number of recommendations and the respective priority ranking of these.

Members noted that where a partial assurance had been awarded, Internal Audit would follow up on the agreed management responses to provide assurance that risk exposure had been reduced.

Members were advised that the review of the Acolaid System was now at the report stage. Also one further change had been made to the Internal Audit Plan with the System Development Life Cycle deferred to Quarter 1 of the 2013/2014 plan.

The reported showed that there were a total of 39 reviews covering the 2013/2014 plan. 31 were at a report status and 8 were in progress.

All audit field work should be materially completed by the end of March 2013 to ensure 100% delivery of the Internal Audit Plan.

Resolved that the progress made in the delivery of the 2012/2013 Internal Audit Plan be noted.

13. Internal Audit Plan 2013/2014

Submitted for consideration the Internal Audit Plan 2013/2014.

The Internal Audit Plan was a flexible plan that could be amended during the year to deal with shifts in priorities.

Members were advised that if the SWAP continued to move forward to become a Company Limited by Guarantee, it would result in changes to roles and responsibilities within the Partnership. In addition, the Public Sector

Internal Audit Standards (PSIAS) would become mandatory, effective from 1 April 2013. These changes would have an impact on the Internal Audit Charter which was last reviewed by the Corporate Governance Committee on 12 March 2012. Therefore it was proposed that the review of the Charter be deferred until April 2013.

Resolved that the:-

- Internal Audit Plan for 2013/2014 be approved; and
- The Internal Audit Charter review be deferred until after April 2013.

14. Forward Plan

Submitted for information the proposed Forward Plan of the Corporate Governance Committee.

Members discussed the need for quarterly updates with regard all reviews that received a partial assurance. Shirlene Adam advised that the reviews would be incorporated into future Forward Plans.

Resolved that the Corporate Governance Committee Forward plan be noted.

(The meeting ended at 7.52pm).

Taunton Deane Borough Council

Corporate Governance Committee – 20 May 2013

Revenues and Benefits Investigation Team Report

Report of the Head of Revenues and Benefits

(This matter is the responsibility of Executive Councillor Mrs. Stock-Williams)

1. Executive Summary

<p>This report provides information to Members with an update on the activities and performance of the Fraud Investigations Team during 2012/13 as well as developments for the next financial year.</p>
--

2. Background

- 2.1 Fraud is a crime that undermines confidence in the benefit system. The work of Revenues and Benefits Investigation Team helps to redress this and contributes towards the Council improving its value for money in delivering effective services.
- 2.2 The Investigation Team conducts investigations into alleged fraudulent claims of Housing Benefit (HB) Council Tax Benefit (CTB) and Council Tax Support (CTS), as well as investigating potentially fraudulent applications under the “right to buy” scheme” and home improvement grants. The Team seeks to prevent fraud through raising awareness both internally and externally, prosecuting offenders and recovering losses.
- 2.3 The Investigations Team is made up of a Team Leader (who also undertakes supervision in recovery of overpaid Housing Benefit and Clerical Support staff) and 2 Investigators. Investigation staff are PINS qualified Accredited Counter Fraud Specialists and the Team Leader holds a management qualification for Professionalism in Security. Given the sensitive nature of their duties, Investigation Officers work to a specific Code of Conduct. They carry out their activities in accordance with the Social Security Administration Act 1992 and follow guidance from the Police and Criminal Evidence Act 1984 and Criminal Procedures and Investigations Act 1996 to bring a case to criminal prosecution.
- 2.4 The funding for counter-fraud activities is paid through the general administration grant the Council receives from the Department for Works and Pensions (DWP). The Investigation Team’s performance is monitored on a quarterly basis by line managers as well as being reported to the Executive Portfolio holder for Corporate Resources and the Council’s 151 Officer.

- 2.5 We currently have over 9,600 customers receiving HB or CTS in council owned, privately rented and privately owned properties and we pay benefit of over £37 million a year. Taunton Deane Borough Council has a duty to protect the public funds it administers. Our Anti-Fraud and Error Policy sets out in detail how we provide officers, Members and residents of Taunton Deane with assurance that as far as possible, we are taking all reasonable steps to protect the public funds we administer. Failure to investigate will see money leaving the Council by way of fraud and error and failure to tackle this could lead to qualified subsidy claims and loss of revenue to the Council.
- 2.6 It is important we focus resources on fraud reduction, to identify, investigate and rectify administrative weakness and assure Members of the integrity and quality of investigations. Countering fraud is the responsibility of everyone working or having responsibility in the Revenues and Benefits Service. It is an integral part of that administration for everyone to be aware of the risks.

3. The Revenues and Benefits Investigation Team

- 3.1 The team aims to reduce fraud and the risk of fraud by using effective processes to prevent, detect and investigate abuse of Housing Benefit, Council Tax Benefit and other income related benefits. The activities undertaken can be summarised as:
- Taking action against those who commit fraud and seeking to prosecute and sanction offenders where appropriate, in accordance with the Council's Anti-Fraud and Prosecution Policies;
 - Minimising the risks of landlord fraud and where it has been proven they have been involved in fraudulent activity, give consideration on whether we can continue to make direct Housing Benefit payments to them in the future under "Fit & Proper Person" rules;
 - Remaining compliant with the guidance set out in the Verification Framework and continued operation of the "do not re-direct" (DNR) scheme as well as security of prime documents.
 - Participation in data matching schemes such as the Housing Benefit Matching Service and National Fraud Initiative (NFI) as well as membership of the National Anti-Fraud Network (NAFN);
 - Promotion of an anti-fraud culture and provision of fraud awareness training to all staff involved in Revenues and Benefits administration;
 - Working closely with the Department for Work and Pensions (DWP) and other agencies to combat claim related fraud;
 - Publicising all successful prosecutions and use of the Council's website to publicise some of our most notable cases;
 - Recommendations of changes to working practices and procedures if weaknesses are identified;
 - Using all legislative powers available and sharing intelligence with other agencies where Data Protection Act permits;
 - Using the Operational Intelligence Unit (OIU) to assist us in obtaining employment and pension details;
 - Maintenance and support of the Benefit Fraud Hotline

4. Review of Performance

- 4.1 In 2012/13 the team received 320 referrals. Of these, once preliminary checks had been carried out, there was sufficient justification to conduct investigation into 205 cases.
- 4.2 The Council subscribe to two Data Matching schemes. A monthly match is conducted with the DWP (HBMS) using their own and HMRC records and a bi-annual exercise is undertaken through the Audit Commissions "National Fraud Initiative" (NFI).
- 4.3 We reviewed our Risk Management procedures (this review takes place annually) and amended them to meet current needs and expectations. All cases except those referred by HBMS are risk assessed.
- 4.4 The Team Leader thoroughly reviewed all closed cases as well as conducting on-going management checks and providing appropriate authorisation.
- 4.5 We remained committed to joint working with our CFIS colleagues at the DWP and continued to work to the DWP/LA Counter Fraud Joint Working Partnership Agreement.
- 4.6 We attended regular liaison meetings between South West Local Authorities and our CFIS colleagues.
- 4.7 The Investigation Team liaises with our local DWP CFIS team when deciding the most appropriate sanction. All sanctions are advised to our local CFIS team who update the DWP system (FRAIMS).
- 4.8 The following summarises our performance:

Reported fraud by year

Year	Referrals	Cases accepted for investigation
2010/11	227	100
2011/12	317	189
2012/13	320	205

Outcome of investigations

Year	Cases investigated	Cases sanctioned	Value of overpayments
2010/11	100	18	£78,842.33
2011/12	189	25	£60,012.72
2012/13	205	23	£116,872.94

Sanction activity

Year	Administrative Penalty	Formal Caution	Prosecution
2010/11	3	10	5
2011/12	4	7	14
2012/13	0	8	15

- 4.9 Of the 15 cases approved for prosecution in 2012-2013, 14 were successfully prosecuted and sentencing included fines, community service orders, conditional discharge and suspended custodial sentences. Wherever possible, press articles are released. This is integral to enhancing the reputation of Taunton Deane Borough Council to hopefully discouraging those individuals who may consider committing fraud. It also reinforces the perception of the honest majority of Taunton Deane residents, that we are committed to protecting the public purse.
- 4.10 Based on the recommendation of our local Department for Work & Pensions Office we use a Solicitor employed by Sedgemoor District Council who specialises in Benefit Fraud cases. This has proved to be a very successful partnership as the solicitor is extremely effective and provides a highly professional and cost effective service. This is demonstrated through increases in successful prosecutions since this arrangement began.
- 4.11 We actively pursue all overpaid Housing Benefit making use of all available recovery methods. Fraudulent overpayments that are recovered from ongoing Housing Benefit entitlement are collected at the enhanced Fraud Rate of £18 a week. Full recovery of overpaid benefit through invoicing is carried out within 12 months whenever possible.
- 4.12 The Investigation Team work closely with local partners, most significantly the DWP Investigation Team. This year has seen an increase in referrals from the Housing Benefit Matching Service (HBMS). National Fraud Initiative (NFI) 2012/13 data matches were received with referrals being dealt with by the Investigation Team.
- 4.13 The principal sources of allegations are from anonymous referrals and from the Housing Benefit Matching Service (HBMS). The nature of the fraud allegation is varied, but the majority of investigations are where there is a suspicion a customer has failed to declare they are living with a partner. These cases are known as "Living Together as Husband and Wife - LTAHAW).
- 4.14 We still target performance against old Best Value Performance Indicators. In 2012/13 we carried out 37 investigations for every 1,000 claims – this was against a target of 29 investigations. For the same period, we obtained 3 sanctions for every 1,000 claims.
- 4.15 These measures do not necessarily correlate with the success of our efforts to prevent and detect fraud. The service aims to provide a secure gateway to the benefits system for those who are entitled to it and actively discourage those who have fraudulent motives from entering the system. High results could be viewed as desirable for the above measures as it could be indicative of an active and effective investigative regime. However, it could equally point to ineffective verification leading to fraud and error entering the system. It could also point to the authority failing to adequately convey a "zero tolerance to fraud" message to customers. We therefore take a holistic view whereby we carry out effective investigations to detect fraud while balancing this with preventative measures.

5. The Future

- 5.1 The changes within the UK Government's Welfare Reform Bill include the introduction of Universal Credit from 2013. Universal Credit will replace income related benefits (including Housing Benefit) over the period 2013 to 2017 and will be administered by the DWP.
- 5.2 As part of this reform a Single Fraud Investigation Service (SFIS) will be created. SFIS is a key part of the Government's strategy in tackling fraud and error within the tax credits and benefits system by £1.4bn nationally by March 2015. SFIS will consist of Local Authority, DWP and HMRC and will be responsible for conducting single investigations covering the totality of benefit fraud. This will include Housing Benefit, but not the Local Council Tax Support Scheme.
- 5.3 The SFIS pilots and pathfinders will be implemented from April 2013 until March 2015 when LA investigators will become SFIS in name and then transfer over by 2017. It is still unclear as to when policies/terms and conditions will change
- 5.4 Representatives from LA's and DWP met in August 2012 and agreed 4 pilot studies to look at the SFIS process. Each of the four pilots (Corby, Glasgow, Hillingdon and Wrexham) will test specific aspects of the Service. Until such time that the pilots have been completed and evaluated, it is agreed that Council Investigation staff will remain located and employed locally, continuing to take the lead in investigating Housing Benefit and the new Council Tax Scheme. It is anticipated that there will be no impact on service delivery until April 2014 at the earliest.
- 5.5 The Audit Commission's report in 2012 "Protecting the Public Purse" (Appendix 2) identified high risk fraud that in Taunton Deane would be concentrated on:
 - Business Rates
 - Council Tax Support Scheme
 - Housing Tenancy Fraud
 - Right to Buy
- 5.6 Taunton Deane Borough Council faces significant changes in the services we provide, including:
 - The ability to retain half of the local business rates we collect from April 2013
 - An increase in the discount available under Right to Buy Legislation from April 2012
 - The function of administering Local Council Tax Support from April 2013
 - Creation of a Single Fraud Investigation Service (SFIS) from April 2014
- 5.7 The Revenues and Benefits Investigation Team acknowledge there are significant changes and the challenge this will present. However, this is also an opportunity for consideration to be given on a corporate approach to Fraud Investigation.

- 5.8 Over the next two years there is an opportunity for the Investigation Team to review the resources needed to commit to the Single Fraud Investigation Service (SFIS) over 2013/14 and 2014/15 and to realign activity to high risk corporate fraud areas to realise additional income or reduce expenditure for the Council. The Team consists of qualified and dedicated individuals who maintain a high professional standard and are committed to being flexible and have a desire to meet any new challenges head on.
- 5.9 Any corporate investigation service would aim to investigate allegations of corporate or benefit fraud and proactively seek out fraudsters, using an intelligence led approach to the prosecution of offenders through the Court System. To address the changes, it will be necessary for the Investigation Team to concentrate upon two distinct areas:
- Developing the role from what is essentially a benefit fraud investigation remit into a wider corporate anti-fraud role.
 - Strengthening the Council's Fraud and Corruption Risk Management and its Corporate Governance, through promoting greater awareness of the fraud risk.
- 5.10 The main fraud risks to the Council will be identified and work targeted to areas which are most likely to generate the highest level of income or reduction in expenditure. In addition, the team will help further improve existing arrangements for the prevention and detection of fraud and corruption, with close liaison with SWAP.
- 5.11 By adopting a "phasing in process", the Council will be in a position to establish the viability of a formal Corporate Fraud Team as potential income levels (grant and fraud recovery income) will be clarified. This will enable a formal business case to be drawn up to support the creation of a Corporate Fraud Team that could have a key role in combating fraud and corruption across Taunton Deane Borough Council and would also generate income and/or reduce expenditure through reducing fraud losses. Administration grant funding from the Government will remain throughout this "phasing in" period, and so there is no financial risk to the Council.
- 5.12 Due to a change in funding arrangements from 2013-14 it will be essential that the Council continues to ensure fraud in respect of Council Tax Support is investigated and full use of available deterrents employed. This is because future funding will be based on a pre-determined grant rather than the previous arrangements when expenditure was covered by Department for Work and Pensions at the end of the financial year. Protecting funds will mean that monies claimed fraudulently can be re-directed to those most in need. We will also carry out our annual review of Council Tax discounts to identify potential single person discount fraud.
- 5.13 Local Authority powers to investigate and prosecute fraudulent claims for Council Tax Benefit are not available for use in localised Council Tax Support schemes. While false claims for Council Tax Support will remain a possible offence under the Fraud Act 2006, replacement powers and offences have been set out in the Detection of Fraud and Enforcement Regulations 2013 (SI 2013/501) to ensure Councils can secure evidence of wrongdoing and prosecute.
- 5.14 We will need to authorise individuals to undertake investigations and require information from individuals/organisations. The powers to require information are broadly similar to those available for Housing Benefit and Council Tax Benefit.

However these new powers are restricted to the “prevention, detection and securing evidence of the commission of an offence”.

- 5.15 Offences have been created, that cover
- (a) Intentional delay or obstruction of an authorised officer,
 - (b) Making a false statement to obtain a reduction and
 - (c) Knowingly failing to give a prompt notification of a change in circumstances affecting a reduction.
- 5.16 We will be able to offer to impose a penalty on an individual, rather than undertake a prosecution. If the person agrees, then they will need to both repay the outstanding council tax and pay a penalty. The level of the penalty will be calculated based on 50% of the “excess reduction” that the person received. This “excess reduction” would be from the date that the incorrect reduction was awarded, to the date that we become aware (or reasonably should have become aware) that it had been awarded. The minimum penalty is £100 with the maximum being £1,000.
- 5.17 There are similar powers for us to impose fixed financial penalties (£70), to those currently available in relation to council tax discounts:
- (a) Where a person is negligent in making an incorrect statement or
 - (b) Where a person, without reasonable excuse, fails to notify a change in circumstances,

In both cases, these are for situations where the person is not believed to have committed a criminal offence.

- 5.18 We will need to amend our Anti-Fraud and Error Policy to ensure we set out how we will deliver penalties as an alternative to prosecution. We will also need to decide on administrative processes to ensure consistency of approach in the imposition of non-criminal penalties as well as issuing notices to individuals and including the penalty on the Council Tax bill.

6. Finance Comments

- 6.1 Annual expenditure on Housing and Council Tax Benefit in 2012/2013 was in excess of £37m. The Council has a duty to protect the public purse and the Anti-Fraud and Error Policy assists in minimising potential loss to the Council.
- 6.2 The government provides Administrative Subsidy to the Council for the Benefits service, some of which is intended to be used to offset the cost of anti-fraud measures.
- 6.3 In Somerset, the cost of Council Tax collection and fraud investigation is borne by District Councils. The County Council receives a larger share of the Council Tax and would therefore receive the greatest part of the additional income that arises from identifying single person discount fraud. However, the County does not contribute financially to the cost of identifying any fraud.
- 6.4 Any income raised from Single Person Discount Fraud penalties would be kept by Taunton Deane Borough Council. The cost of prosecutions under the Fraud Act is borne by Taunton Deane Borough Council and as such, prosecutions should only be taken where it is financially viable to do so.

7. Legal comments

- 7.1 The legislation concerning matters within the Revenues & Benefits Service’s Anti-Fraud and Error Policy is mainly contained in:

- Social Security Administration Act 1992
- The Fraud Act 2006
- Regulation of Investigatory Powers Act.
- Local Government Finance Act 1992
- Police and Criminal Evidence (PACE) Act and the Criminal Procedure and Investigations Act.

8. Links to Corporate Aims

8.1 HB, CTB, CTS, Council Tax and Business Rates administration is most closely linked with the corporate aim of 'Tackling Deprivation and Sustainable Community Development'.

9. Environmental implications

9.1 Not applicable

10. Community Safety implications

10.1 Not applicable

11. Equalities Impact

11.1 Legislation is fully complied with during an investigation and therefore no-one is disadvantaged within our prescribed processes. An Equality Impact Assessment was completed for our Anti-Fraud and Error Policy and is shown in Appendix 1.

12. Risk Management

12.1 There is a risk that fraud and error will occur. However this is managed through the controls and policies that Taunton Deane Borough Council has in place. Fraud referrals are risk assessed and intelligence graded in relation to level of risk involved before being accepted for investigation/rejection

13. Partnership Implications

13.1 None arising from this report.

14. Recommendations

14.1 The Corporate Governance Committee is requested to note and support the activities contained in this report.

Contact: Helen Vile
Team Leader
Revenues and Benefits Service
01823 356437
h.vile@tauntondeane.gov.uk

Heather Tiso
Head of Revenues and Benefits
Revenues and Benefits Service
01823 356541
h.tiso@tauntondeane.gov.uk

Impact Assessment form

What are you completing this impact assessment for? E.g. policy, service area	Revenues & Benefits Service Investigation Team Anti Fraud & Error Policy		
Section One – Aims and objectives of the policy /service			
<p>Taunton Deane Borough Council is committed to ensuring that claimants receive the benefits and discounts to which they are entitled and will ensure that benefits and discounts are taken up by those people who need access to the service. However, the Council recognises that some people will try to obtain benefits and discounts to which they are not entitled. The Council will not tolerate abuse of the system and will take proactive and reactive steps to prevent and detect fraud and recover overpayments.</p> <p>This Policy details our approach to reduce the opportunity for fraud and error to occur and sets out our commitment to use all legal sanctions available, including prosecution</p>			
Section two – Groups that the policy or service is targeted at			
<p>We have a statutory duty to provide benefit or discounts regardless of the gender, sexual orientation, religion or belief or ethnicity of the customer. People of all ages will be our customers. However statutory provisions will apply in the calculation of Housing Benefit or Council Tax Benefit dependent on age. Additional Housing Benefit or Council Tax Benefit is payable where there is a specific impairment/disability benefit in payment. Discounts for Council Tax will be applied where there is a specific impairment/disability to be considered.</p>			
Section three – Groups that the policy or service is delivered by			
Taunton Deane Borough Council's Revenues & Benefits Service.			
Section four – Evidence and Data used for assessment			
<p>Annually we carry out a satisfaction survey of Revenues & Benefit customers. Data provided shows no evidence of dissatisfaction as a direct or indirect result of how we deliver our service in meeting our duties under the Equality Act 2010.</p>			
Section Five - Conclusions drawn about the impact of service/policy/function on different groups highlighting negative impact or unequal outcomes			
<p>The Anti-Fraud & Error Policy aims to prevent, detect and deter Housing Benefit, Council Tax Benefit and Council Tax Discount Fraud in Taunton Deane Borough. It provides:</p> <ul style="list-style-type: none"> • Assurance to residents of Taunton Deane Borough Council that those who attempt to defraud will be sanctioned; • Consistency of approach in dealing with cases of proven fraud • Guidance for Officers • Ensures good stewardship and that we are proactive in addressing fraud <p>As the policy will be applied consistently regardless of the gender, sexual orientation, religion or belief or ethnicity of the customer, there should be no negative or unequal outcome on different groups.</p>			
Section six – Examples of best practise			
<p>Our policy has been developed taking into consideration advice given by the DWP HB/CTB Good Practice Guide, "Carrying out Counter Fraud Activities"</p> <p>http://www.dwp.gov.uk/local-authority-staff/housing-benefit/performance-and-good-practice/hbctb-good-practice-guide/part-one-good-practice/carrying-out-counter-fraud/</p>			
Signed: Manager completed by		Signed: Group Manager/Director	

Taunton Deane Borough Council

Corporate Governance Committee – 20 May 2013

Update Report on Freedom of Information Act

Report of the Legal and Democratic Services Manager

(This matter is the responsibility of the Leader of the Council)

1. Executive summary

<p>This report provides an update on how the requests for Freedom of Information Act have increased and how they are dealt with by the Council.</p>

2. Background

- 2.1 The Freedom of Information Act 2000 came into effect on the 1st January 2005 and applies to around 80,000 public bodies.
- 2.2 The Act gives anyone the right to request any recorded information held by the Council and the general rule is that if we have the information we will provide it.
- 2.3 However, the Act does provide for some exemptions to this which are generally if the information is legally privileged, reasons of security, personal, confidential, commercial interest, vexatious, or if it is available through other avenues.
- 2.4 Anyone requesting information under the Act must apply in writing and the Council must respond in writing. The Council has 20 working days in which to respond to the request and all requests are logged, and responded to, by the FoI Administrator although the requests are sent to the relevant service unit(s) for a response.
- 2.5 Generally the Council cannot charge for the information we supply unless it is estimated that to provide the information would exceed £450. This amount is set down in regulations.
- 2.6 The number of requests over the last five years has increased considerably year on year. 2009 – 269 requests, 2010 – 326 requests, 2011 – 432 requests and 2012 – 520 requests. This year we have received 214 requests since January at the time of writing the report.
- 2.7 The reason for this increase is probably due to the various organisations such as Taxpayers Alliance, Whatdoyouknow.com and various newspapers who are making more requests for information together with the government's drive to ensure public bodies are transparent and provide as much information as possible.
- 2.8 In terms of costs to the Authority in responding to these requests, we do not currently have time recording system in place for all areas of the Council so staff have not kept a record of time that they have spent on this particular area. In addition due to the

varied nature of the requests they are dealt with by a variety of different officers throughout the organisation.

- 2.9 For those requests that are of a recurring nature then these can be dealt with fairly quickly and standard responses are given. However some responses can be quite detailed and therefore officers have to assess how easy it is to provide the information or whether it involves spending a number of days looking at different systems.
- 2.10 The Council's ethos is to provide the information or as much of it as we can but clearly there are times when this is not always possible.
- 2.11 From this new financial year, performance monitoring of FOI requests will form part of the corporate scorecard as it is now something that needs to be monitored at a corporate level rather than a service level and will help the authority in determining whether resources will need to be allocated differently in order to deal with the growing number of requests.
- 2.12 Members will be aware that from April 2012 responsibility for FOI was passed to the Monitoring Officer and monitoring of the numbers of requests and response times has been kept. Details for 2012/13 are set out below:-

	Q1	Q2	Q3	Q4
Acknowledged within 5 days of receipt	98%	94%	91%	99%
Closed within 20 days	76%	74%	77%	79%
Closed within the Quarter	72%	77%	81%	89%
Queries rolling forward to next Quarter	24%	4%	19%	11%
Closed outside the 20 days with extension	0%	22%	13%	7%

3. Finance comments

- 3.1 There no financial comments in this report.

4. Legal comments

- 4.1 Should the Council fail to provide the information within the 20 working days then a requester can apply to the Information Commissioner. In addition if a requester is not happy with the response they can request a review. If they are still not happy with the Council's response following that review then they can appeal to the Information Commissioner.
- 4.2 The Information Commissioner can put an authority on a 'watch list' if it regularly does not provide information in a timely manner.

5. Links to Corporate Aims

- 5.1 There are no links to the corporate aims in this report.

6. Environmental and community safety implications

- 6.1 There are no implications for the environment or community safety.

7. Equalities impact

7.1 An impact assessment is not required in respect of this report. .

8. Risk management

8.1 The risk of not complying with the Act means that they can be monitored by the Information Commissioner.

9. Recommendations

9.1 The Committee is asked to note the report.

Contact

Contact officer: Tonya Meers
Telephone: 01823 358691
E-mail: t.meers@tauntondeane.gov.uk

Taunton Deane Borough Council

Corporate Governance Committee – 20 May 2013

Audit of Data Security Breaches

Report of the Legal and Democratic Services Manager

(This matter is the responsibility of the Leader of the Council)

1. Executive Summary

<p>This report provides a progress update following the audit carried out by South West Audit Partnership on the 15th February 2013. In addition members are asked to approve the Data Security Breach Management policy for implementation.</p>

2. Background

- 2.1 As part of the 2012-13 audit plan a review was undertaken to assess the adequacy of the controls and procedures in place for Data Security Breaches across the Council.
- 2.2 The conclusion of the report gave the Council a partial assurance in relation to the areas that were reviewed and made a number of recommendations. A copy of the audit report is attached at Appendix A.
- 2.3 There were a total of eleven recommendations. Two of those recommendations are a priority 4, four are classed as a priority 3 and 5 are a priority 2.
- 2.4 The implementation date for the majority of the recommendations is the 30th June although two of the recommendations have already been completed.
- 2.5 The majority of the recommendations will all flow from recommendation 1.1(a) which is to develop an Information Security Incident Management Process.
- 2.6 Annexed at Appendix B is a copy of that Management Process which members are asked to approve.

3. Finance comments

- 3.1 There are no financial implications in this report. Although it should be noted that any breach of Data Protection can have a severe financial impact on the Council's finances.

4. Legal comments

- 4.1 There are no legal implications in this report although it is good practice to have a policy in place to manage any such incidents should they occur.

5. Links to Corporate Aims

5.1 There are no links to the corporate aims in this report.

6. Environmental and Community Safety Implications

6.1 There are no implications for the environment or community safety.

7. Equalities impact

7.1 An impact assessment is not required in respect of this report. .

8. Risk management

8.1 The risk of not implementing this policy leaves the Council exposed should there be a breach of data protection.

9. Recommendations

9.1 The Committee is asked to approve the Information Security Incident Management Process and note the report.

Contact

Contact officer: Tonya Meers
Telephone: 01823 358691
E-mail: t.meers@tauntondeane.gov.uk

Taunton Deane Borough Council

► Data Security Breaches

Issued to: Tonya Meers
*Legal & Democratic Services
Manager*

Keith Wiggins
ICT Client Lead

Shirlene Adam
Section 151 Officer

Peter Lappin
Audit Manager

Gerry Cox
Head of Audit Partnership

Working in partnership with



Date of Report: 15 February 2013

Issued by: Neil Roper
Audit Manager

Hayley Pattenden
Lead Auditor

Data Security Breaches

Management Summary

As part of the 2012-13 audit plan a review has been undertaken to assess the adequacy of the controls and procedures in place for Data Security Breaches across the Authority.

The Governance, Fraud and Corruption Audit process focuses primarily on key risks relating to cross cutting areas that are controlled and/or impact at a Corporate rather than Service specific level. It also provides an annual assurance review of areas of the Council that are inherently higher risk. This work will enable SWAP to provide management with assurance that key controls are in place.

SWAP will use the findings of these reviews to support the assurance that is required as part of the Council's Annual Governance Statement; it will also provide assurance to the External Auditor on areas that they have requested specific assurance, such as data quality.

Local authorities face a number of regulations with regards to information security. Perhaps the most significant of these is the Data Protection Act, enforced and overseen by the Information Commissioner's Office (ICO). Since April 2010, the ICO has the power to impose on data controllers, such as local authorities, a civil penalty of up to £500,000 for serious breaches of personal information. Substantial fines, a number exceeding £100,000, have already been imposed on councils for breaches involving personal information and the ICO has proved to be unsympathetic to the difficult financial situation that councils face. Indeed Christopher Graham, the Information Commissioner, commented: *"There is too much of this sort of thing going on across local government. People who handle highly sensitive personal information need to understand the real weight of responsibility that comes with keeping it secure."*

Councils need to ensure that they have effective controls in place to counter data security breaches. These controls should provide a framework for a comprehensive, professional and integrated approach to addressing this issue. An effective framework should include the following three key elements:

- Enforcing an Information Security Strategy that encompasses data classification. *This should ensure that the Council's information assets are surrounded by the appropriate level of security in accordance with this classification.*
- Identifying the possible risks posed by data security breaches and adopting the appropriate measures to counter them.
- Creating and maintaining a strong culture of information security awareness amongst staff.

When the Data Security Breaches audits have concluded at all the reviewed organisations in the partnership we will issue a report to the participants giving an overall view of the arrangements in place.

Summary of Significant Corporate Risks

The following table records the inherent risk (the risk of exposure with no controls in place) and the manager's initial assessment of the risk (the risk exposure on the assumption that the current controls

are operating effectively) captured at the outset of the audit. The final column of the table is the Auditors summary assessment of the risk exposure at Corporate level after the control environment has been tested. All assessments are made against the risk appetite agreed by the SWAP Management Board.

Areas identified as significant corporate risks, i.e. those being assessed as 'high' or 'very high' risk areas in line with the definitions attached should be addressed as a matter of urgency.

Risks	Inherent Risk Assessment	Managers Initial Assessment	Auditors Assessment
Users do not recognise a data security breach when it occurs.	High	Medium	High
Third party discloses council held information that has been shared with them.	High	Low	Low
The organisation fails to report appropriately an information security breach.	High	Medium	High

Summary of Significant Findings

The following were identified as key findings for the service and therefore categorised, in accordance with the definitions attached, as a level '4' or '5' priority in the action plan.

- Central record of information security incidents
- Information Sharing Agreements

Further details of audits' findings can be viewed in the full audit report, which follows this Management Summary.

Conclusion and Audit Opinion

▲★☆☆ Partial

I am able to offer partial assurance in relation to the areas reviewed and the controls found to be in place. Some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

The Council does not have a documented security incident or response plan for data security breaches. Staff are not required to attend mandatory or refresher training on information security and the Council's policy and guidance in these areas. The corporate induction for new staff provides limited information on information security. Staff that had been trained did not know where to access the Council's information security policies and guidance. Additionally, staff were not aware who they should contact and how in the event of a data security breach or what action should be taken.

A significant finding was that the Council do not maintain a central log or record of all information security incidents. It follows that we were unable to locate evidence that any data security breaches had occurred and subsequently been properly investigated and reported to the ICO as necessary. This was highlighted when our work at another local authority identified a theft of client data from a third party that is likely to have included TDBC client data. We believe that this was reported to TDBC but no found no record of this or any action to establish the extent or impact of the incident at TDBC. Additionally, it was unclear whether this had been reported to the ICO.

The Council do have some arrangements in place with third parties that they may share information with. The Model Service Delivery Contract between TDBC and Southwest One makes it clear that Southwest One are data processors in the contract and covers issues such as staff and sub-contractor training.

However there is no specific Information Sharing Agreement between TDBC and South West One that supplements the data protection clause in the contract to address the best practice described in the ICO guidance on information sharing agreements. Whilst Information Sharing Agreements are not a statutory requirement, they should help specify and justify data sharing and the ICO will take this into account should they receive a complaint about the data sharing practices at an authority.

However there are areas of positive practice with regards to data security. The Council have authorised to connect to the GSi / GCF under the GCSx Code of Connection (CoCo). Email Protective Marking (EPM) is now in use across the authority and appropriate staff have GCSx mail accounts. The Council also have an Information Security User Guide in place and a member of the Client Team attends a quarterly Information Security Officers (ISO) Meeting along with South West One and members of SCC Client Team to discuss information security issues.

Detailed Audit Report

Objectives & Risks

The key objective of the service and risks that could impact on the achievement of this objective were discussed and are identified below.

Objective: To ensure that the organisation has in place the appropriate and up to date working practices and procedures to identify, record and respond to information security breaches.

Risks:

- Users do not recognise a data security breach when it occurs.
- Third party discloses council held information that has been shared with them.
- The organisation fails to report appropriately an information security breach.

Method & Scope

This audit has been undertaken using an agreed risk based audit. This means that:

- the objectives and risks are discussed and agreed with management at the outset of the audit;
- the controls established to manage risks are discussed with key staff and relevant documentation reviewed;
- these controls are evaluated to assess whether they are proportionate to the risks and evidence sought to confirm controls are operating effectively;
- at the end of the audit, findings are discussed at a close-out meeting with the main contact and suggestions for improvement are agreed.

The audit was identified in a risk review meeting with the s151 officers of the SWAP client group as one of the common themes across the authorities in the partnership. The scope of the work is to address the following points:

- How are breaches and potential breaches managed?
- Is there a lessons learned process?
- Information security / classification.
- What is public and what's not - how should information be disseminated?
- Member awareness and training.
- Review ICO Reports and IA findings from previous years.

The main emphasis of the work is therefore around information governance, incident reporting and response management arrangements at each authority.

Findings

The following paragraphs detail all findings that warrant the attention of management.

The findings are all grouped under the objective and risk that they relate.

1. Risk: Users do not recognise a data security breach when it occurs.

1.1 The GovConnect Code of Connection requires the connected body to have an information security incident management process. I can confirm that the authority are compliant with the GovConnect Code of Connection however I was unable to confirm that the security incident management process has been documented or if sets out the arrangements to identify, respond to, recover from and follow-up information security incidents.

Without a documented process published to all staff there is a risk that a lack of awareness could lead to information security incidents going unreported and subsequently investigated.

1.1a I recommend that the Monitoring Officer ensures that the authority has a documented Information Security Incident Management Process in place. This should include how information security incidents are identified, responded to, recovered from and followed up and the responsibilities for these.

1.2 We sent a questionnaire to 54 staff working in a range of services that handle personal and sensitive information to capture information about their awareness of security policies, incident reporting, protective marking of information and their views on the effectiveness of training. As at 5 October 2012 only 6 responses had been received, a response rate of 11%.

Whilst it is not possible to draw definitive conclusions from such a small sample the responses we received suggest that:

- Not all staff have received information security training. Nor are staff routinely required to sign an acknowledgement that they have been trained. The respondents who had not been trained did not know how to access the Council's information security policies and guidance, or who and how to contact information security staff and the action to take in respect of security breach.
- Whilst all respondents would apply protective markings to information they handle and pass on to others however few correctly identified the "Restricted" and "Protect" protective markings that are applied to information shared by local and central government agencies. It follows that protectively marked may not be handled appropriately, or information may not appropriately marked.

1.2a I recommend that the Monitoring Officer reviews the information security training provided to ensure that all staff who handle sensitive information are trained, are required to acknowledge receipt of the training and are included in a programme of periodic refresher training.

1.2b I recommend that the Monitoring Officer and ICT Client Lead develop guidance and explanation on the application and use of protective markings to email, documents and

records. This guidance should be included in training materials and made available on the intranet.

- 1.3 The authority have an Information Security User Guide that sets out rules for keeping information secure, security classification, and legislative and policy links. The Guide is available to all staff via the TDBC staff intranet.

The contact details for the Data Protection Officer stated in the guide are out of date. There is a risk that information security incidents or issues could be reported to the wrong person or not be reported.

The advice in the Guide is succinct. For example information classified "Restricted" must be encrypted on portable devices but the guide does not indicate how this should be achieved or how information marked "Protect" should be handled on portable devices.

The Guide gives a version number and date but no version history or indication of who approved the document and when it was approved. There is a risk that the document will not be periodically reviewed and updated if necessary.

- 1.3a I recommend that the ICT Client Lead reviews and amends the Information Security User Guide. This should include updating the name and contact details of the Data Protection Officer for the authority. This should also include a record of the version history of the Guide and a date for the next periodic review.**

- 1.4 There is no regular forum for communication between TDBC and Southwest One (SWOne) on information security issues. SWOne facilitate a quarterly Information Security Officers (ISO) Meeting for all their customers. The TDBC ICT Client Lead attends together with the ICT Client Lead and the Information Governance Officer from Somerset County Council (SCC). The meeting does discuss ICT-related information security issues but this is not a permanent item on the agenda. Data security breaches and any lessons learned from them are not discussed.

Although the ISO meeting is useful in terms of ICT technologically-related issues, it would be useful to have a forum whereby TDBC could meet with both SWOne and SCC to share experiences of data security issues or lessons learned from data security breaches that have occurred within individual organisations. Without this, there is a risk that lessons learned from data security breaches will not be shared and the likelihood of a similar breach occurring again could be heightened.

- 1.4a I recommend that the Security Services Team Manager ensures that ICT Data security is made a permanent item on the agenda of the quarterly Information Security Officers Meeting. This should include sharing any lessons learned from data security breaches at Southwest One's customers.**

- 1.5 Staff attend a Corporate induction day when they join the authority. A 20-minute presentation on data protection issues, the DPA and FOI legislation forms part of this induction. The induction does not appear to include:

- security classification of documents and information although basic guidance is given on how to process and store information
- equipment disposal

- how to identify and report information security incidents.

There is a risk that staff will be unable to identify data security breaches or know how to report a breach if information is not provided during induction training.

1.5a I recommend that the Monitoring Officer ensures that a greater focus is given to data security awareness during induction training. This should include guidance on how to identify and report information security incidents.

1.6 There is no programme of periodic refresher training on information security policies or procedures. Without refresher training or a periodic review of staff awareness there is a risk that staff will not be aware of information security policies or procedures that have been updated. This could lead to an information security incidents remaining undetected and unreported.

However I am able to report that the Clear Desk Policy is effective. A walk-around was performed at the offices after staff had gone home. All office areas checked were found to have clear desks i.e. no confidential or personal data was left in clear view on desks.

1.6a I recommend that the Monitoring Officer liaises with HR to establish a refresher training programme for staff or periodic updates with regards to information security policies and procedures.

2. Risk: Third party discloses council held information that has been shared with them.

2.1 We were initially advised that the Council does not share information with third parties and therefore does not have a practice of creating and monitoring information sharing agreements. Subsequently we were provided with the Information Sharing Agreement between SCC and TDBC for the joint Customer Contact service provided by SWOne. This was signed in 2009 by the Senior Responsible Officer for the SWOne contract for SCC and for TDBC by the then Data Protection Officer.

SWOne provide ICT, Facilities and HR services to the Council and delivering these services involves hosting and processing personal data. There is no information sharing agreement between TDBC and SWOne in respect of the services provided by the SWOne to the Council. Whilst such an agreement is not required by law, the ICO considers them to be good practice. The explanation presented to us is that the Model Service Delivery Contract (MSDC) sets out the responsibilities of the parties with respect to data protection (s 17) and the use of authority data (s 18) and that the organisational and technical controls are described in the Information Security Controls (ISec) document that describes the security services provided by SWOne.

We can confirm that the MSDC sets out the data protection requirements in the terms used by the DPA and includes requirements that SWOne to adhere to the authority's Data Protection and Information Security policies and to train staff and sub-contractors who have access to personal data. However the MSDC does not specify the level of detail outlined in the ICO guidance for an information sharing agreement. For example common rules for retention and deletion of data, a single point of contact and procedure for subject access requests and an explanation or justification of the sharing of data between the two parties.

Without information sharing agreements there is a risk that the Council will be unable to

demonstrate that has considered and recorded the relevant compliance issues. In addition the parties in a service that needs to share information may lack clarity as to the information that should be shared and the information governance arrangements that should apply. Information sharing agreements do not provide legal indemnity however the ICO will take them into account in the event of a disclosure or complaint about information sharing.

2.1a I recommend that the Monitoring Officer reviews existing partnerships, contracts and shared service initiatives to ensure that all those that involve information sharing are identified and the type of data shared and the basis on which it is shared are properly recorded. Furthermore an Information Sharing Agreement template should be prepared for use when personal data is shared.

2.1b I recommend that the Monitoring Officer works with SWOne to create a formal Information Sharing Agreement that extends the information in the Model Service Delivery Contract and ISeC to that outlined in the ICO guidance on data sharing agreements.

3. **Risk:** The organisation fails to report appropriately an information security breach.

3.1 I could find no evidence that TDBC have a documented response procedure for data security procedures.

Without this, there is a risk that staff would be unaware of procedures to follow should a data security breach occur. This could increase the likelihood that a data security breach goes unreported to the Monitoring Officer and, should the incident involve significant personal information, the ICO.

3.1a I recommend that the Monitoring Officer and the ICT Client Lead develop a response plan for information security incidents and publish and promote this to all staff at TDBC. This should describe how and to whom security incidents should be reported and provide those officers responsible for investigating and responding to incidents with process and recording guidance.

3.2 There is no central record of information security incidents maintained by TDBC or by SWOne on behalf of TDBC. Security incidents that involve ICT equipment, such as damage to or loss of devices, are reported to the Service Desk. However the Service Desk do not maintain a central log of such incidents or details of any data loss that may have occurred as a result.

Work at another local authority uncovered a security breach that had occurred which is likely to have involved the loss of TDBC data. A third party contracted this local authority had been broken into and SSDC/TDBC client data had been stolen. This included names, addresses, bailiff reference numbers and Council tenant reference numbers.

The above breach occurred in September 2012 and that data was never recovered. This is still a live breach at the local authority concerned and we were unable to ascertain whether this had been reported to the ICO.

There is a risk that TDBC could be unaware of incidents that occur or the data lost or disclosed in an incident. This could mean that data security breaches involving personal data go unreported to the ICO (Information Commissioner's Office) and the ICO may be more likely to take enforcement action as the lack of a record could be seen as a deficiency in the Council's DPA compliance arrangements.

3.2a I recommend that the Monitoring Officer works with Southwest One to create a central record of information security incidents. The log should record details of the incident, any data lost and any subsequent investigations into the breach.

The log should also record whether the breach has required reporting to external bodies such as the Information Commissioner's Office (ICO) or SW WARP.

The Agreed Action Plan provides a formal record of points arising from this audit and, where appropriate, the action management has agreed to take and the timescale in which the action will be completed. All findings have been given a priority rating between 1 and 5, where 1 is low and 5 is high.

It is these findings that have formed the opinion of the service's control environment that has been reported in the Management Summary.

Data Security Breaches

Confidential

Draft Action Plan

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
<p>Objective: To ensure that the organisation has in place the appropriate and up to date working practices and procedures to identify, record and respond to information security breaches.</p>					
<p>1. Users do not recognise a data security breach when it occurs.</p>					
<p>1.1a Information Security Incident Management Process</p>	<p>I recommend that the Monitoring Officer ensures that the authority has a documented Information Security Incident Management Process in place. This should include how information security incidents are identified, responded to, recovered from and followed up and the responsibilities for these.</p> <p style="text-align: right;"><small>SWAP Ref: 20050</small></p>	<p>3</p>	<p>Agreed. TM will review current documentation & produce a new, easy to use incident Management Process. This will be rolled-out to staff via a Leads meeting, staff team meetings & specific training, as required.</p>	<p>Monitoring Officer</p>	<p>30 June 2013</p>
<p>1.2a Not all staff have received information security training</p>	<p>I recommend that the Monitoring Officer reviews the information security training provided to ensure that all staff who handle sensitive information are trained, are required to acknowledge receipt of the training and are included in a programme of periodic refresher training.</p>	<p>2</p>	<p>Agreed. See actions under 1.1a. The roll-out to Leads & staff will be completed by 30 Jun 2013.</p>	<p>Monitoring Officer</p>	<p>30 Jun 2013</p>

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
	<i>SWAP Ref: 20004</i>				
1.2b Staff do not understand the protective marking scheme	<p>I recommend that the Monitoring Officer and ICT Client Lead develop guidance and explanation on the application and use of protective markings to email, documents and records. This guidance should be included in training materials and made available on the intranet.</p> <p style="text-align: right;"><i>SWAP Ref: 20005</i></p>	3	Agreed.	Monitoring Officer and ICT Client Lead	30 June 2013
1.3a Update to the Information Security User Guide	<p>I recommend that the ICT Client Lead reviews and amends the Information Security User Guide. This should include updating the name and contact details of the Data Protection Officer for the authority. This should also include a record of the version history of the Guide and a date for the next periodic review.</p> <p style="text-align: right;"><i>SWAP Ref: 20046</i></p>	2	Agreed & already completed	ICT Client Lead	Complete
1.4a Information security incidents and practice at Information Security Officers	<p>I recommend that the Security Services Team Manager ensures that ICT Data security is made a permanent item on the agenda</p>	2	Agreed & already completed	Security Services Team Manager	Complete





Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
(ISO) meeting	<p>of the quarterly Information Security Officers Meeting. This should include sharing any lessons learned from data security breaches at SouthwestOne's customers.</p> <p style="text-align: right;"><i>SWAP Ref: 20047</i></p>				
1.5a Induction training information security awareness and incident reporting	<p>I recommend that the Monitoring Officer ensures that a greater focus is given to data security awareness during induction training. This should include guidance on how to identify and report information security incidents.</p> <p style="text-align: right;"><i>SWAP Ref: 20044</i></p>	2	<p>Agreed. Monitoring Officer to pick up as part of the action plan referred to in 1.1a above</p>	Monitoring Officer	30 June 2013
1.6a Refresher training programme or periodic updates for information security practice and incident management	<p>I recommend that the Monitoring Officer liaises with HR to establish a refresher training programme for staff or periodic updates with regards to information security policies and procedures.</p> <p style="text-align: right;"><i>SWAP Ref: 20045</i></p>	2	<p>Agreed. This will be implemented via periodic refresher training at Leads meetings & the provision of specific training as required.</p>	Monitoring Officer	On-going
2. Third party discloses council held information that has been shared with them.					
2.1a Contracts and partnerships	I recommend that the	3	Agreed	Monitoring	30 June 2013

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
that involve information sharing have not been identified and recorded	Monitoring Officer reviews existing partnerships, contracts and shared service initiatives to ensure that all those that involve information sharing are identified and the type of data shared and the basis on which it is shared are properly recorded. Furthermore an Information Sharing Agreement template should be prepared for use when personal data is shared. <i>SWAP Ref: 20048</i>			Officer	
2.1b Personal information stored and processed by Southwest One on behalf of TDBC is not governed by a specific information sharing agreement	I recommend that the Monitoring Officer works with SWOne to create a formal Information Sharing Agreement that extends the information in the Model Service Delivery Contract and ISeC to that outlined in the ICO guidance on data sharing agreements. <i>SWAP Ref: 21077</i>	4	Recommendation understood. However is our view The SWO contract already covers data protection & processing responsibilities in sufficient detail.	Monitoring Officer	N/A
3. The organisation fails to report appropriately an information security breach.					
3.1a Documented response plan for breaches	I recommend that the Monitoring Officer and the ICT Client Lead develop a response	3	Agreed. As in 1.1a TM will review current documentation & produce a	Monitoring Officer and ICT Client Lead	30 June 2013

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
	<p>plan for information security incidents and publish and promote this to all staff at TDBC. This should describe how and to whom security incidents should be reported and provide those officers responsible for investigating and responding to incidents with process and recording guidance.</p> <p style="text-align: right;"><i>SWAP Ref: 20043</i></p>		<p>new, easy to use incident Management Process. This will be rolled-out to staff via a Leads meeting, staff team meetings & specific training, as required.</p>		
<p>3.2a Central record of information security incidents</p>	<p>I recommend that the Monitoring Officer works with Southwest One to create a central record of information security incidents. The log should record details of the incident, any data lost and any subsequent investigations into the breach.</p> <p>The log should also record whether the breach has required reporting to external bodies such as the Information Commissioner's Office (ICO) or SWWARP.</p> <p style="text-align: right;"><i>SWAP Ref: 20049</i></p>	<p>4</p>	<p>Agreed. TM will set up and maintain a central electronic database of security incidents.</p>	<p>Monitoring Officer</p>	<p>30 April 2013</p>

Audit Framework Definitions

Control Assurance Definitions

Substantial		I am able to offer substantial assurance as the areas reviewed were found to be adequately controlled. Internal controls are in place and operating effectively and risks against the achievement of objectives are well managed.
Reasonable		I am able to offer reasonable assurance as most of the areas reviewed were found to be adequately controlled. Generally risks are well managed but some systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Partial		I am able to offer Partial assurance in relation to the areas reviewed and the controls found to be in place. Some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
None		I am not able to offer any assurance. The areas reviewed were found to be inadequately controlled. Risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

Categorisation Of Recommendations

When making recommendations to Management it is important that they know how important the recommendation is to their service. There should be a clear distinction between how we evaluate the risks identified for the service but scored at a corporate level and the priority assigned to the recommendation. No timeframes have been applied to each Priority as implementation will depend on several factors, however, the definitions imply the importance.

Priority 5: Findings that are fundamental to the integrity of the unit's business processes and require the immediate attention of management.

Priority 4: Important findings that need to be resolved by management.

Priority 3: The accuracy of records is at risk and requires attention.

Priority 2: Minor control issues have been identified which nevertheless need to be addressed.

Priority 1: Administrative errors identified that should be corrected. Simple, no-cost measures would serve to enhance an existing control.

Definitions of Corporate Risk

Risk	Reporting Implications
Low	Issues of a minor nature or best practice where some improvement can be made.
Medium	Issues which should be addressed by management in their areas of responsibility.
High	Issues that we consider need to be brought to the attention of senior management.
Very High	Issues that we consider need to be brought to the attention of both senior management and the Audit Committee.

Appendix B

TAUNTON DEANE BOROUGH COUNCIL

INFORMATION SECURITY

INCIDENT MANAGEMENT PROCESS

Taunton Deane Borough Council
Council Offices
Belvedere Road
Taunton
TA1 1HE

www.tauntondeane.gov.uk

WHAT TO DO IF THERE IS A BREACH OF THE DATA PROTECTION ACT 1998

A POLICY ON INFORMATION SECURITY - INCIDENT MANAGEMENT PROCESS

The Council has a responsibility under the Data Protection Act 1998 (DPA) to ensure appropriate and proportionate security of the personal data it holds. Although the Council takes this duty very seriously there may be an occasion where there is a data security breach. In these circumstances staff should follow the procedure set out below:

1. Immediately notify the Council's Data Protection Officer (DPO) (The Council's Monitoring Officer) or in her absence another member of the Legal Department, you will need to advise the DPO of the nature of the breach i.e. has the data been lost, shared, stolen or unlawfully processed, the amount of data involved, how many people will be affected and the content of the information. You will also need to notify the DPO of any steps you have taken to contain or recover the breach. A Data Protection Breach Response Evaluation Form is annexed to this policy at Appendix A for this purpose.

2. The DPO will then offer advice on any immediate actions that can be taken and commence an investigation. The DPO will also set out a detailed action plan of what should happen next.

The investigation and action plan will deal with the following:

a) Containment and recovery

- Who needs to be made aware of the breach
- Who is needed to assist with the investigation and any containment exercise
- How can the breach be dealt with: can it be contained by simply finding the lost piece of equipment e.g lost laptop, or access codes changed

- Is there anything that can be done to recover any losses and limit any damage
- Do the police need to be informed

b) Assessing the risks

- What type of data is involved
- How sensitive is the data – some data is sensitive because of its personal nature e.g. medical information whilst other data is sensitive because of what might happen if it was misused e.g. bank account details
- If data has been lost or stolen, are any protections in place such as encryption
- What has happened to the data – if stolen is it possible that its use could be harmful to individuals
- Regardless of what happened to the data what could the data tell a third party about the individual
- How many individuals' personal data are affected by the breach
- Who are the individuals affected
- What harm could come to those individuals
- Are there any wider consequences to the loss
- If the data includes bank details consider contacting the banks as they may be able to assist in preventing fraudulent use

c) Notification of breaches

- Notify the individual(s) affected. If the breach has been contained and the DPO's investigation concluded they should be advised of this. Otherwise they should be informed that an investigation has been commenced and what immediate steps have been taken to contain the situation
- Consider notification to the Information Commissioners Office (see notes below)

- Are there any other bodies that need to be notified

Deciding whether to notify the ICO:

It should be noted that there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, but the Information Commissioner believes serious breaches should be brought to the attention of his Office

There is no definition of a serious breach but the following should assist in deciding whether or not a report should be made:

Potential harm to individuals

Where there is significant actual or potential harm as a result of the breach, whether because of the volume of data, its sensitivity or a combination of the two, there should be a presumption to report.

Where there is little risk that individuals would suffer significant harm there is no need to report.

Volume of the data involved

There is a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Every case must be considered on its own merits but a reasonable rule of thumb is any collection containing information about 1000 or more individuals should be reported.

However it may be appropriate to report much lower volumes in some circumstances where the risk is particularly high perhaps because of the circumstances of the loss or the extent of information about each individual. If the Council is unsure whether to report or not, then the presumption should be to report.

Sensitivity of the data

There should be a presumption to report to the ICO where smaller amounts of personal data are involved where the release could cause a significant risk of individuals suffering substantial harm. This is most likely to be the case where that data is sensitive personal data as defined in section 2 of the DPA. As few as 10 records could be the trigger if the information is particularly sensitive.

Making the report

Where the DPO decides that a report should be made to the ICO it should be done as follows:

By email at: mail@ico.gsi.gov.uk

or by letter to: *Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.*

The notification should include:

- The type of information and number of records
- The circumstances of the loss / release / corruption
- Action taken to minimise / mitigate effect on individuals involved including whether they have been informed
- Details of how the breach is being investigated
- Whether any other regulatory body has been informed and their response
- Remedial action taken to prevent future occurrence
- Any other information you feel may assist us in making an assessment

What will the Information Commissioner's Office do when a breach is reported?

The nature and seriousness of the breach and the adequacy of any remedial action will be assessed and a course of action determined. They may:

- Record the breach and take no further action
- Investigate the circumstances of the breach and any remedial action which could lead to:

- 1) no further action
- 2) a requirement on the data controller to undertake a course of action to prevent further breaches
- 3) formal enforcement action turning such a requirement into a legal obligation

It should be noted that the Information Commissioner does not have the power to impose a fine or other penalty as punishment for a breach. Their powers only extend to imposing obligations as to future conduct.

d) Evaluation and response

- Evaluate the risks and where they lie
- How can the risks be minimised
- Has the breach identified any weaknesses in security measures, how can this be rectified
- Are staff aware of their duties, is further training needed

The investigation and any remedial action should be fully documented and kept centrally by the DPO.

APPENDIX A - Data Protection Breach Response Evaluation Form

Questions	Answers
What is the data?	
How many people are affected?	
Where is the data now and how many people have seen it?	
What is being done to recover the data?	
How did the data loss occur?	
What policies are in place?	
What training/ awareness raising measures have been taken in the light of this episode?	
When did this episode begin?	
Has this happened before?	

Taunton Deane Borough Council

Corporate Governance Committee – 20 May 2013

Corporate Governance Action Plan

Report of Performance Lead

(This matter is the responsibility of Executive Councillor Stock-Williams)

1. Executive Summary

This report shows progress against the Corporate Governance Action Plan as at the end of April 2013.

2. Background

- 2.1 Each year, the Council receives a number of reports and assessments which result in recommendations for improvement. These normally contain individual action plans which can prove challenging to manage and monitor. Therefore an aggregated plan provides the Council with details, in one place, of the scale of improvements required and progress against them.
- 2.2 The Corporate Governance Action Plan currently includes 18 actions, which have emerged from external audits (ie Audit Commission) – specifically, recommendations from the Annual Governance Reports from the last two years - 2010/11 (report Sept 2011), 2011/12 (report Sept 2012).
- 2.3 Actions progress monitoring is undertaken quarterly by the Performance Lead and a summary features in the Corporate Performance Scorecard. The Corporate Governance Officers Group is provided with an overview of the plan.

3. Progress (as at end April 2013)

3.1 The Corporate Governance Action Plan currently lists **18 actions**. Progress monitoring against implementation by the target dates has revealed the following:

Priority	Total	Closed ☺	On Target ☺	Some Concern ☹	Off Target ☹
High	8	5	2	1	
Medium	8	4	2	2	
Low	2	1	1		
Total	18	10 (56%)	5 (28%)	3 (17%)	0

Therefore, a total of **83% (15/18) audit actions are now closed or 'on target'** - a slightly improved position compared to 81% in the previous report in December 2012.

3.2 There are three actions given an 'Amber' status (ie 'some concern'). One of these is rated as 'High priority', and the other two actions rated as 'Medium priority'. These are:

- Ref. 4) Update the Workforce Strategy (ensuring there are clear links to financial planning) and complete & agree a new workforce plan (High priority)
- Ref. 2) To fully review the Financial regulations (Medium priority)
- Ref. 14) Develop benchmarking to support decisions in allocating resources (Medium priority)

Further detail is found in the table in Appendix A

4. Finance Comments

Recommended improvement actions in relation to Managing Finances are included in the Corporate Governance Action Plan.

5. Legal Comments

Recommended improvement actions in relation to legal / Corporate Governance issues are included in the Corporate Governance Action Plan.

6. Links to Corporate Aims

The Corporate Governance Action Plan supports all aspects of the Council's corporate aims and operations.

7. Environmental and Community Safety Implications

Any recommended improvement actions in relation to Climate Change will be included in the Corporate Governance Action Plan.

8. Equalities Impact

Any recommended improvement actions in relation to Equalities & Diversity will be included in the Corporate Governance Action Plan where relevant.

9. Risk Management

The Corporate Risk Register includes the risk:
There is a risk of failure to comply with key internal controls & corporate governance arrangements (ie compliance with audit recommendations).

The Corporate Governance Action Plan is a key control measure, however there are a number of risks associated with not completing the recommended actions within the Corporate Governance Action Plan (eg External Audit opinion, reputation, financial).

10. Partnership Implications

Recommended improvement actions in relation to partnership working, are included in the Corporate Governance Action Plan.

11. Recommendations

It is recommended that Members scrutinise progress of the Corporate Governance Action Plan.

Contact:

Dan Webb

Performance Lead

01823 356441

Ext: 2504

d.webb@tauntondeane.gov.uk

Corporate Governance Action Plan 10 May 2013

APPENDIX A

Number	Section	Audit Name	Recommended Action	Priority	Created Date	Original Target Implementation Date	Responsible Officer	Contributors	Source	Success Criteria	Progress	Revised Target Implementation Date	As At (Date)	Status
1	Business Continuity	Complete Business Continuity (BC) and IT disaster recovery planning (including SW1 services)	1. Ensure adequate BC plans in place at corporate and service level, including key partners. 2. Annual testing of BC plans	H	20/03/2012	31/03/2012	Richard Sealy	Fiona Kirkham & SW1 IT / John Lewis	External Audit- 2009/10 VFM conclusion report Sept 2010	Plans updated. Testing regime in place. Building security plan in place	Plans in place and tested. 1. Service plans updated as part of annual service planning. Corporate plan updated March 2013 in line with most recent SWAP report. 2. Corporate BC exercise held October 2012. Exercise plan in preparation.	On-going	09/05/2013	Green
2	Corporate Policy	To fully review the Financial regulations	To complete review of the financial regulations	M	20/03/2012	30/04/2012	Shirlene Adam		External Audit- Annual Governance Statement 2008/09	Simple Financial Procedure Rules in place to support the Financial Regulations. They are used and valued by Budget Holders throughout the organisation	A new financial regs document produced. Financial Regs have been received and are still fit for purpose. Financial Procedures have been drafted by the Strategic Finance Officer and presented to the S151 Officer for review and sign off. This will be completed and adopted summer 2013.	Sep-13	09/05/2013	Amber
3	Democratic Services	In preparing its draft financial statements, the Authority should ensure that it has received a completed annual declaration from all members of any related party interests and those of close family	TBC	H	18/01/2013	13/05/2013	Tonya Meers	Paul Fitzgerald Southwest One Financial Services Manager	External Audit - Annual Governance Report 2011/12		Completed.		09/05/2013	Closed
4	Human Resources	Update the Workforce Strategy (ensuring there are clear links to financial planning) and complete & agree a new workforce plan	August 2011 - review statistical data in draft workforce strategy. By November 2011 - Revised workforce strategy to compliment four year budget strategy.	H	22/03/2012	31/03/2012	Richard Sealy	Martin Griffin	External Audit- 2009/10 VFM conclusion report Sept 2010	Workforce Plan completed in 2013 as part of Corporate Business Plan. match new priorities. Clear linkages to Corporate Training Plan.	Draft Workforce Development Plan submitted alongside new 3 year Corporate Business Plan (Feb 2013). Further development of Plan now dependant on: outcome of Members' service prioritisation work, other major projects (eg review of SW1 services, West Somerset joint-working). Unison have been briefed and feedback requested. Amber due to uncertainty (ref dependencies above), and HR resources/capacity issues.	Oct-13	09/05/2013	Amber
5	ICT Contract Performance	Update the IT Strategies and ensure there are clear links from these to financial planning.	Establish an IT work group	H	20/03/2012	30/04/2012	Shirlene Adam	Keith Wiggins & SW1 IT	External Audit- 2009/10 VFM conclusion report Sept 2010	Clarity on the Councils IT Strategy and Action Plan to Achieve this.	TDBC Strategic ICT forum (attendees from CMT and SW1) met in July and October 2012, the latter meeting receiving from SW1 ICT the first draft of an ICT Strategy for 2012 - 2014 linked to the Council's Business Plan. SW1 have now produced the IT Strategy and this has been accepted by CMT. The Retained ICT Lead (post recently brought back in-house) will now further refine the strategy and this will be reported to the Council in the autumn.		09/05/2013	Closed
6	Main Accounting	All transactions on the SAP financial system should contain sufficient narrative to identify the purpose of the transaction, the timing and the source	1) Consider whether TDBC requires descriptions from AP, AR and other feeder transactions to populate GL Description fields in SAP. Prepare/agree RFS if required. 2) Users to be reminded that sufficient narrative should be included on GL transactions such as journals 3) Business process for journals and virements will be reviewed to: i) provide clear guidance on descriptions protocol; ii) build control checks and quality assurance into the process	M	18/01/2013	31/12/2010	Shirlene Adam		External Audit - Annual Governance Report 2009/10		Still some improvement necessary in descriptions used on financial transactions. Don't think the problem is completely resolved, but it is much improved. There is regular challenge by the s151 Officer.		27/02/2013	Closed
7	Main Accounting	Reconcile the information in payroll and the ledger for members' expenses	TBC	M	18/01/2013	31/05/2013	Maggie Hammond	Paul Fitzgerald Southwest One Financial Services Manager	External Audit - Annual Governance Report 2011/12	No audit concerns raised for 2012/13 Accounts.	Complete: The process was updated in order to respond to auditor queries during the audit of 2011/12 accounts. The standard working practice for 2012/13 Accounts will follow this updated method.		28/02/2013	Closed
8	Main Accounting	Reconcile housing stock figures so that there is consistent disclosure in the accounts and business plan	TBC	M	18/01/2013	31/05/2013	Maggie Hammond / Stephen Boland	Paul Fitzgerald Southwest One Financial Services Manager	External Audit - Annual Governance Report 2011/12	Housing Service and Southwest One Property Service will ensure separate databases are reconciled and stock count is agreed. It is recognised that figures quoted in the Business Plan may include an element of projection/assumption that could differ from actual data at future dates.	Reconciliation process has worked well and is virtually complete. Evidence to support the completed review will be collated for the audit pack.		09/05/2013	Green
9	Main Accounting	Review the method of calculating the impairment of debtors taking into account the aged of the debt and recovery rates.	TBC	H	18/01/2013	31/05/2013	Maggie Hammond	Paul Fitzgerald Southwest One Financial Services Manager	External Audit - Annual Governance Report 2011/12	No audit concerns raised for 2012/13 Accounts.	Complete: The debt impairment method was reviewed for the 2012/13 financial year end activity.		28/02/2013	Closed
10	Main Accounting	Ensure that income from investment properties is disclosed in the accounts for 2012/13	TBC	M	18/01/2013	31/05/2013	Maggie Hammond / Mark Green	Paul Fitzgerald Southwest One Financial Services Manager	External Audit - Annual Governance Report 2011/12	Disclosure requirements for 2012/13 are compliant with the Code of Practice Guidance, and no audit concerns are realised for 2012/13 Accounts.	The Retained Property Manager is currently working with SWOne Property to review assets classed as Investment Properties. This work needs to be completed and then the accounting information updated to ensure costs and income are reallocated to the new code.		09/05/2013	Green

11	Main Accounting	Review the actual costs to support the basis of recharges from the HRA to the General Fund.	TBC	M	18/01/2013	31/05/2013	Maggie Hammond	Paul Fitzgerald Southwest One Financial Services Manager	External Audit - Annual Governance Report 2011/12	Recharge basis uses up to date information to provide assurance over accuracy of recharged amounts	Complete: The HRA Accountant has worked with the service to ensure the accuracy of coding for shared costs, so that year end figures are readily available for reporting purposes. This has also been used for preparation of the 2013/14 Budget.		28/02/2013	Closed
12	Main Accounting	Review the method to reconcile the year end NNDR position and ensure that this is in line with the Authority's contribution to the national pool.	TBC	M	18/01/2013	31/05/2013	Maggie Hammond	Paul Fitzgerald Southwest One Financial Services Manager	External Audit - Annual Governance Report 2011/12	No audit concerns raised for 2012/13 Accounts.	Complete: part of the year end activity in April/May 2013.		28/02/2013	Closed
13	Main Accounting	Update the HRA financial model for actual changes in housing stock - such as sales, demolitions and voids	TBC	H	18/01/2013	31/05/2013	Maggie Hammond	Paul Fitzgerald Southwest One Financial Services Manager	External Audit - Annual Governance Report 2011/12	No audit concerns raised for 2012/13 Accounts.	Complete: The HRA financial model has been refreshed as part of the preparation of the revised Business Plan approved in December 2012. The model, by definition, will include an element of projections and assumptions as it is used as a forecasting tool covering a 30-year period.		09/05/2013	Closed
14	Main Accounting	Develop benchmarking to support decisions in allocating resources	TBC	M	18/01/2013	31/05/2013	Simon Lewis	Dan Webb	External Audit - Annual Governance Report 2011/12	~ Provide a robust & meaningful VFM analysis to support CMT & Members with strategic decision-making ~ High-level and more detailed VFM analysis to be undertaken - this will help inform new 'Streamlined, modern services' project during 2013	1. Cost & performance benchmarking data being included in refreshed 2013 Service Profiles to inform Members and Directors service prioritisation work (Spring-Summer 2013). 2. County-wide Housing Service cost and performance data has been submitted and is currently being analysed by a project team - findings to be reviewed and discussed by relevant Housing Managers from Somerset Districts spring-summer 2013.	Aug-13	09/05/2013	Amber
15	Main Accounting	Determine spending priorities and reduce expenditure to ensure that future budgets are balanced by closing the gap between expenditure and projected income	None	H	20/03/2012	31/03/2012	Shirlene Adam	Simon Lewis / Dan Webb	External Audit- Annual Governance Report 2010/11 (Sept 11)		A new 3 year Business Plan was approved by Full Council (22 Jan 2013). Further work on service prioritisation was undertaken with Members - with support from LGA (24 April 2013). A project plan ('Achieving Financial Sustainability') is in place and the aim is to have completed this and have a sustainable financial plan agreed by Autumn 2013.	Oct-13	09/05/2013	Green
16	Main Accounting	Strengthen the arrangements to ensure the accuracy of the whole of government accounts submission.	Arrangements for the preparation of the WGA will be reviewed and strengthened to ensure accuracy.	L	20/03/2012	31/07/2012	Maggie Hammond	Paul Fitzgerald Southwest One Financial Services Manager	External Audit- Annual Audit Letter (Oct 11)	No audit concerns raised for 2011/12 Accounts.	Complete: Draft Accounts presented to S151 Officer in line with agreed timetable. The WGA accuracy was improved for 2011/12. No material errors were reported by the auditor, and the auditor issued an 'unqualified opinion' for the 2011/12 WGA.		28/02/2013	Closed
17	Partnership Arrangements	Maintain a register of partnerships and prepare a protocol for establishing new partnerships	1. Compile comprehensive partnership register. 2. Confirm involvement and they meet authority's aims and objectives. 3. Introduce protocol for establishing membership prior to commitment. 4. Establish framework and categorisation of partnerships. 5. Widen scope of Members Task & Finish Group re membership on outside bodies	L	20/03/2012	30/09/2011	Tonya Meers		External Audit- 2009/10 VFM conclusion report Sept 2010		Partnerships adequately controlled and managed. Protocol completed and will be reviewed by CMT June/July 2013.	Aug-13	09/05/2013	Green
18	Section 106 Agreements	Improve control and monitoring of Section 106 Agreements	1. Implement regular monitoring and reporting to Executive, PH & Senior Management 2. Implement process of management of the payment or other obligation 3. Project team to be established 4. Quarterly reports to Theme Managers' group	H	20/03/2012	30/09/2011	Tim Burton	Debbie Arscott	External Audit- Housing Inspection		S106 agreements in Acolaid - regular monitoring, reporting and prompt raising of invoices. Prompt escalation where non-payment The especially created Master database containing all live and completed Agreement information from August 2011 continues to be updated. Monthly S106 meeting are continuing. Escalation of non-payments is on-going. We are complying with audit requirements		27/02/2013	Closed

Taunton Deane Borough Council

Corporate Governance Committee – 20 May 2013

SAP Controls - Update

Report of the Strategic Finance Officer

(This matter is the responsibility of Executive Councillor Mrs Vivienne Stock-Williams)

1. Executive Summary

TDBC introduced a new financial system which has been used since 1 April 2009.

There are controls built into the SAP system and these are a crucial part of the internal control regime.

Work continues in this area to reduce/eliminate risk to the council.

2. Background

2.1 On 1st April 2009 Taunton Deane Borough Council introduced a new financial system call SAP (Systems, Applications and Products). This new system covered both payment of invoices and the raising of sundry debtors.

2.2 2012/13 was the fourth year of the council using SAP and officers have continued to work on the controls within SAP to reduce risk to the council.

3. SAP Controls

3.1 There are controls built into the system and these inherent controls are a crucial part of the internal control regime.

3.2 The appendices attached to this report give details of the risks identified within the separate modules of SAP, the current controls in place and any ongoing work on controls

3.3 There are 4 appendices being Payroll/OM Structure Appendix A, Creditors Appendix B, Debtors Appendix C, Master Data Appendix D.

- 3.4 Following the loading of an upgrade a control issue has come to light. Before the upgrade a person requesting goods and services via a purchase order could not approve their own order. Following the upgrade this is now possible, where the approver is absent and the requester is listed on SAP as the substitute for the approver. This is not widely known.

SAP continues to work on this to resolve the issue. In the interim a list is produced weekly of any instances where the requisitioner and the approver are the same person. Since October 2012 there has been just one incident and closer investigation showed that the order was correct.

4. Finance Comments

- 4.1 This is a finance report and there are no further comments to make.

5. Legal Comments

- 5.1 It is essential that adequate controls are in place to ensure the council pays its invoices on time in order to avoid incurring any additional cost through non-payment and potential court actions. This report identifies what controls are in place.

6. Links to Corporate Aims

- 6.1 The SAP system supports the whole organisation and therefore supports all of the corporate aims indirectly.

7. Environmental Implications

- 7.1 There are no environmental implications of this report

8. Community Safety Implications

- 8.1 There are no community safety implications of this report.

9. Equalities Impact

- 9.1 This is an information only report and has no equalities issues to assess.

10. Risk Management

- 10.1 The controls that are in place within SAP are there to reduce risk of both a financial and reputational nature.

11. Partnership Implications

- 11.1 SAP is supported by Southwest One.

12. Recommendations

- 12.1 This is an information only report and there are no recommendations attached to this report.

Contact: Maggie Hammond
01823 358698
m.hammond@tauntondeane.gov.uk

Risk	SAP Controls in Place	Ongoing work
Positions created/deleted/amended without authorisation	The Retained HR Manager or Strategic Finance Officer approve any changes to The OM structure within SAP	
The OM structure within SAP does not match the organisations structure	SW1 HR has been running an exercise with SW1 Finance and Theme Managers to cleanse the OM structure from posts which are not required and are not budgeted for.	The structure will be regularly reviewed and the completion of the SAP establishment report will be a further opportunity for this to be undertaken.
A fictitious employee is paid.	<p>Quarterly reports are provided by SW1 to Theme Managers to confirm staff on payroll.</p> <p>The Authorised Signatory list has been overhauled during 2011/12 and half yearly reviews built into the process of ensuring that this is kept up to date. This is signed off by the Retained HR Manager and Strategic Finance Officer.</p> <p>If new employee documentation comes through with the incorrect signatures then there is an agreed escalation procedure in place before they are added to the Payroll</p>	
<p>Periodic reconciliation of the payroll system to personnel records does not take place.</p> <p>Individual departments do not review</p>	A report is produced on a quarterly basis which is issued to Theme Managers asking them to review the list of staff and report back any errors.	

the accuracy of their payroll bills.	Any errors identified are investigated and corrected where necessary.	
False Allowance claims are paid.	Expenses claims are made through SAP and following the OM structure for authorisation. No paper claims apart from Non ESS staff are accepted by payroll.	
Payroll costs are not coded accurately	Monthly budget monitoring includes details of salary costs for budget holder review. Any errors are discussed with the accountant and are rectified within the Payroll System.	
There is missing equalities data on SAP	SWOne HR has during 2012/13 carried out an exercise with staff to ensure that the equalities details are completed by staff.	

CREDITORS (invoice payment)

Appendix B

Risk	SAP Controls in Place	Ongoing work
Transaction or event has not occurred or does not relate to the authority	SAP will confirm that a scanned document is either an invoice or credit note. Those items that fail this control are rejected by the system. This ensures that TDBC does not pay on invalid invoices	
Fraudulent/Duplicate payments made	<p>Duplicate payment identification is made throughout the whole process with potential duplicate payments being identified manually or through a computer program.</p> <p>Process Director flags potential duplicate payments as well as a program call Etesius.</p> <p>Etesius is run prior to all payment runs to identify potential duplicate invoices. These are manually investigated and where proved to be a duplicate are removed from the payment run. This is a manual process and during 2012/13 there were 3 duplicate payments made to a value of £1,561.17. All of these have been recovered in full.</p>	During 2013/14 the Strategic Finance Officer will be reviewing the high incidences of potential duplicate payments within SAP, looking at the reasons for the potential duplicates and how these can be stopped at source.
Training is insufficient	<p>Quick reference guides are available for all payment processes within SAP that breakdown the process and have screen shots for staff to follow.</p> <p>There are also SAP champions throughout</p>	

	<p>the organisation to help staff that have any issues using SAP.</p> <p>The sharepoint site for SAP also has a document that gives staff details of the escalation process should they have any problems with SAP.</p>	
Outputs from the creditors system are reconciled regularly to the information in the General Ledger	Bank reconciliations are carried out that ensure the output from the creditors system (that appear on the bank statement) are within the SAP General Ledger.	
All invoices received are not loaded onto the system	During the various stages of scanning invoices to upload into SAP SWOne are able to quickly identify and correct any issue through daily reconciliations.	
<p>Direct input bypasses all controls and incorrect payments are made.</p> <p>(Direct input is used in exceptional circumstances only)</p>	<p>The use of Electronic Payment Requests is Monitored by SWOne. Any payments that appear to have been paid incorrectly by this method are investigated and the person who raised the payment is contacted.</p> <p>Direct Input is only used in exceptional circumstances with agreement from TDBC</p>	SWOne will continue to monitor these payments.
Duplicate vendors created	<p>Vendor cleansing continued in 2012/13</p> <p>During 2012/13 the process of vendor creation was moved from 2 separate departments into one. Controls are in place to ensure that duplicate vendor records are not created.</p>	

<p>All invoices are not correctly authorised before being paid.</p> <p>Payment is incorrect</p> <p>Invoices are not paid to terms agreed</p>	<p>All invoices are processed through SAP.</p> <p>All cost centres within SAP have position numbers against them that can authorise spend within a given band. SAP uses this delegation table to pick authoriser for spend.</p> <p>SAP will only allow invoices requiring a purchase order to be paid through the 3 way match process (automatic payment on receipt of an invoice without manual intervention) if the invoice quotes a valid purchase order number and the good receipt input by staff matches the invoice. The approval comes from the purchase order which is approved by an Officer from the delegation table.</p> <p>When an invoice is received that does not require a purchase order (i.e. a utilities bill) then SAP will require a member of staff to “code” the invoice. By doing this the member of staff is confirming that the invoice is correct and which budget line the expenditure is to be shown against. There is then an approval stage where the authorisers for that code from the delegation table can release the invoice for payment. The invoice will not be paid until both stages are fully completed.</p> <p>As long as staff following the process that has been communicated to them in a timely manner invoices will be paid within the suppliers agreed terms. Staff receive prompts direct to their inbox to remind them that they</p>	
--	---	--

	<p>have invoices awaiting their approval or coding and SWOne produce regular reports to the retained Finance Officer to highlight staff who have high volumes of invoices in the system awaiting payment</p>	
--	--	--

Risk	SAP Controls in Place	Ongoing work
All invoice request forms are not authorised, before information is put onto the debtors system	Not all members of staff have access to raise sundry debtor accounts. For those staff that do not have access there is a form to complete to request a debtor account is raised. If the form is not completed or data is missing the request is passed back to the service.	
Debts are not recovered.	<p>When an account is not fully paid then the recovery processes begins. SAP produces an initial reminder if the account has been marked ok for recovery and the account exceeds its payment terms. If the customer still does not pay the account then the customer will either receive a final reminder produced by SAP or will be contacted by the AR team.</p> <p>SAP has an aged debt report suit which allows managers to check their debts at a high level, service level or customer level. This highlights to managers debts that are not being repaid and any areas of concern</p>	<p>Aged debts will be monitored as part of the budget monitoring process.</p> <p>The Financial Planning Team Continues to monitor the level of debt in their monthly meetings.</p> <p>SWOne is working on improvements to the debt recovery process in terms of both the timetable employed in TDBC and also processes for identifying problem debts through a tool called SAP scripting</p>
Procedures are not adhered to	<p>Quick reference guides are on the SAP sharepoint site. Any changes to the procedures are communicated via the Business Support Units.</p> <p>Any issues around procedures are discussed at the Business Review Group (BRG) and best practice is shared between officers.</p>	

	There is an AR user group in place which has TDBC representation	
All credit notes are subject to appropriate level of authorisation.	An authorised signatory list has been compiled on a Theme basis which gives details of who can approve these changes. There is segregation of duties within SAP that ensures that a person who raises a credit note cannot release it.	
A block on recovery is not removed.		SAP scripting is being developed that will identify those accounts with a “dunning block” so SWOne can investigate and remove the block wherever necessary.
Not all invoices are printed and issued	A list of invoices that should be printed is produced. A manual check is performed daily and any missing invoices re-printed.	
All write offs are subject to appropriate level of authorisation	The AR team are aware of the write-off procedure. A debt will not be written off without the agreement of the s151 officer, head of paid services or executive (depending on debtor value)	

MASTER DATA

Appendix D

Risk	SAP Controls in Place	Ongoing work
Users may have unauthorised access to update master data records.	Only those staff with the approved role can amend master data records. A segregation of duties matrix ensures that this role is not assigned to staff with conflicting roles.	
Incorrect data/changes are processed	<p>The creation of and amendment of Supplier and customer details follow a strict process. Forms for the creation of new data are required along with supporting documentation which is checked.</p> <p>Updating supplier and customer details are thoroughly checked as this is a major fraud area. The master data team have stopped some potential frauds by following a robust process</p> <p>SWOne carry out significant internal checking of all master data changes to customers and vendors, this is also independently verified by SWOne's own business controls team and by SWAP</p>	
New cost centres are created without approval. Funds can be misappropriated or discrepancies hidden.	All new cost centres and GL accounts are approved by the Strategic Finance Officer before creation after a case for creation has been reviewed.	

TAUNTON DEANE BOROUGH COUNCIL
CORPORATE GOVERNANCE COMMITTEE
FORWARD LIST OF AGENDA ITEMS 2013

MEETING	DRAFT AGENDA ITEMS	LEAD OFFICER
4/2/13 Special Meeting	Internal Audit – The Future Governance of SWAP (Decision)	Shirlene Adam
11/03/13	Audit of Grant Claims Health & Safety Update Report Equalities Audit – Progress Update Risk Management Update Internal Audit Plan 2012/13 - Progress Report Internal Audit Plan 2013/14	Peter Lappin (Grant Thornton) Richard Sealy / Martin Griffin Mark Leeman / Simon Lewis Dan Webb Alastair Woodland (SWAP) Alastair Woodland (SWAP)
20/05/13 1hr 40 m	Revenues & Benefits – Update on Fraud Prevention / Detection (40 mins) Data Security Audit Findings (20 mins) FOI & Complaints Process (15 mins) Corp Governance Action Plan Update (20 mins) SAP Controls Update (5 mins)	Heather Tiso Tonya Meers Tonya Meers Dan Webb Maggie Hammond
24/06/13 1 hr 35m	Health & Safety Update Report (15 mins) Draft Annual Governance Statement 2012/13 (30 mins) External Audit – Fees Report 13/14 (5 mins) External Audit Plan 2012/13 (5 mins) Annual Report of SWAP (15 mins) Internal Audit – Review of Charter (5 mins) Internal Audit – Review of Effectiveness (5 mins) Risk Management Update (20 mins)	Richard Sealy / Martin Griffin Maggie Hammond Peter Lappin (Grant Thornton) Peter Lappin (Grant Thornton) Alastair Woodland (SWAP) Alastair Woodland (SWAP) Shirlene Adam Dan Webb

23/09/13	<p>Health & Safety Update Report</p> <p>Audit Commission – Annual Governance Report 2012/13</p> <p>Approval of Statement of Accounts 2012/13</p> <p>Internal Audit Plan – Progress Report</p> <p>Risk Management Update</p>	<p>To be confirmed</p> <p>Peter Lappin (Grant Thornton)</p> <p>Paul Fitzgerald</p> <p>Alastair Woodland (SWAP)</p> <p>Dan Webb</p>
9/12/13	<p>Health & Safety Update Report</p> <p>Grant Thornton – Annual Audit Letter 2012/13</p> <p>Grant Thornton – Fees 2012/13</p> <p>Internal Audit Plan – Progress Report</p> <p>Corporate Governance Action Plan Update</p>	<p>To be confirmed</p> <p>Peter Lappin (Grant Thornton)</p> <p>Peter Lappin (Grant Thornton)</p> <p>Alastair Woodland (SWAP)</p> <p>Dan Webb</p>

24/06/2013, Report:Update on Objection to Accounts re Taxi Fee's
Reporting Officers:Scott Weetch