devon audit partnership

# Internal Audit Report

## Strata ICT Audit 2017/18
## Strata Services Solutions

*September 2018*

**OFFICIAL**

CUSTOMER SERVICE EXCELLENCE CSE

Auditing for achievement

## Devon Audit Partnership

The Devon Audit Partnership has been formed under a joint committee arrangement comprising of Plymouth, Torbay and Devon councils. We aim to be recognised as a high quality internal audit service in the public sector. We work with our partners by providing a professional internal audit service that will assist them in meeting their challenges, managing their risks and achieving their goals. In carrying out our work we are required to comply with the Public Sector Internal Audit Standards along with other best practice and professional standards.

The Partnership is committed to providing high quality, professional customer services to all; if you have any comments or suggestions on our service, processes or standards, the Head of Partnership would be pleased to receive them at robert.hutchins@devonaudit.gov.uk.

## Confidentiality and Disclosure Clause

This report is protectively marked in accordance with the National Protective Marking Scheme. Its contents are confidential and, whilst it is accepted that issues raised may well need to be discussed with other officers within the organisation, the report itself should only be copied/circulated/disclosed to anyone outside of the organisation in line with the organisation's disclosure policies.

This report is prepared for the organisation's use. We can take no responsibility to any third party for any reliance they might place upon it.

# 1 Introduction

Strata Service Solutions has three founding partners; East Devon District Council, Exeter City Council and Teignbridge District Council (The Partners). The three founding partners took an innovative approach in setting up Strata, with shared service arrangements often being the model of choice for two-tier district authorities.

In creating Strata the partners have created a dedicated ICT company that provides opportunities in terms of costs, enhancing workforce capacity and, potentially, some additional leverage in the marketplace. The strategic path enables each individual Council to better maintain its own aims, objectives and service delivery priorities. This does not limit the opportunities for creating financial and operational benefits of using identical computerised solutions and, potentially, end to end business processes where considered appropriate by the Partners.

Core processes and functions are both maturing and considered to be of a 'good standard'. With the first two phases of Strata's strategy effectively delivered, there are increasing opportunities to measure the demand for services from the individual Partners. This allows for Strata to further refine its operational processes, better identify capacity requirements and evolve its strategic focus.

As highlighted in last year's report, once a strategic path has been chosen then it is crucial that the benefit realisation is optimised. Strata's principle objectives are to:

- *Reduce Risk;*
- *Reduce Cost;*
- *Increase Capability to Change.*

Strata now offer the Partners greater opportunities in delivering affordable services in the short and medium term. This report will predominantly focus on the operational baseline upon which Strata deliver ICT services to the Partners and the security afforded to their computerised information assets. It will also summarise the ongoing progress made in respect of Strata's ability to fulfil the third principle object and assist the Partners in delivering transformational change to the Partners.

# 2 Overall Audit Opinion

| | |
|---|---|
| **Good Standard.** | The systems and controls generally mitigate the risk identified but a few weaknesses have been identified and / or mitigating controls may not be fully applied. There are no significant matters arising from the audit and the recommendations made serve to strengthen what are mainly reliable procedures. |

# 3 Executive Summary

Strata has been in operation since 1st November 2014 for three and a half years has established itself as a successful provider of ICT services to its founder Partners. Whilst there have been challenging times, not least the establishing of the global desktop, there is clear recognition of progress against the original business plan.

A former weakness of Strata, and indeed most public sector IT service providers, was in the way 'customer satisfaction' was managed, or more precisely, customer perception. Customer satisfaction relies upon perception and Strata must continue to manage client and user perception through effective communication strategies if their value is to be fully realised.

The work undertaken by the IT Director and his Management Team to improve the quality of performance reporting and customer satisfaction over the past twelve months has paid dividends. The overall level of customer satisfaction and the overall appreciation of the services Strata provides is significantly greater than at any time since the company was created. This benefits both Strata and the Partners as it creates an environment of trust and allows more measured conversations to be had regarding both current and future services.

On an operational level Strata demonstrate that they discharge fundamental IT operational activities to a good standard. From a user perspective, the problems experienced in rolling out the Global Desktop across the whole estate have been resolved, although some server performance issues remain.

The 'Global Desktop' demonstrated its value during the snow events of March 2018, allowing staff to work remotely and effectively whilst away from their respective office locations. The global desktop provides a good example of what are the risks and benefits of adopting 'bleeding edge' technologies. However, above all, it demonstrated a will to make things work for the benefit of the Partners and gain resolutions to issues that were mainly beyond their direct control.

The overall level of Cyber Security is of a good standard, with the majority of controls according to those generally accepted as being good practice for an organisation of its size and resources. The virtual environment operated by Strata offers some benefits in the event that the network is breached by malware. There are, however, issues to be addressed in respect on the use and management of some high privilege network accounts.

Since the last years audit, good progress has been made to establish governance structures and working practices to manage and support the respective change programmes of the Partners. The existence of a Joint IT Steering Group (JITSG) that can identify potential projects that would benefit the Partners as a whole is good practice. This should also help provide the JSC, JEC and Strata Board with a clearer and more holistic view of potentially mutual benefits.

Efforts continue to evolve processes and procedures to enable Strata to more successfully deliver projects to meet with the Partners requirements and manage the resources it needs to achieve this. The adoption of a new project management process, based on protocols developed by the Association of Project Managers, is being implemented with key staff having received training on the methodology.

### 3.1.1 Key Operational Functions

Overall operational functions and processes continue to be assessed as of a good

standard and appropriate to what should be expected from a relatively small public ICT service. Strata, and the Partners, benefit from the broadly standardised technical baseline that has been established. These are both materially evident in the level of service provided by Strata and, crucially, in the demonstrable savings delivered.

The majority of operational risks are being appropriately mitigated, although the concept of continual service improvement that Strata has demonstrated to date should not be lost now that a sound operational baseline has been achieved. Where appropriate, the provision of timely and well-reasoned arguments to the Partners for investment in new infrastructure remains essential for safeguarding availability and security.

Looking forward, operational knowledge must be maintained, whilst programme and project management processes must contribute to the identification of skill requirements for new or developing service solutions. Where possible, staff should continue to be mentored and upskilled to enhance capacity and, maintain high service availability and incident remediation.

### 3.1.2 Service Design (& Delivery)

The primary objective of this part of this review was to assess the effectiveness of processes to transform the strategic requirements of Strata into effective business solutions. It is pleasing to report that progress has been made to lay the foundations for improved service delivery in this area. However, it is clear that there is both opportunity and an appetite within Strata to improve programme delivery and what are essentially intelligent client functions.

The delivery of transformational projects is now a fundamental requirement for Strata. Overall governance structures have improved and the creation of the Joint IT Steering Group (JITSG) provides a degree of transparency and control over the Partners three individual project streams. This also provides a holistic view of the three programmes in order to better identify opportunities for all of the Partners.

A knowledge hub has been created, not only to capture internal knowledge and learning, but to create a repository of market awareness. The hub can be used to detail technological opportunities identified by staff, but also to record information provided by suppliers regarding their products and capabilities. Financial and human resource information can also be stored to help with future costings and provide an understanding of what skills and capabilities may be required.

The prioritisation and timetabling of individual projects becomes more challenging when the requirement for transformational change is driven by the need for cross organisational cost saving. In Strata's case, they have to serve the needs of the three Partner Councils. An internal review conducted by the Strata Management Team revealed that some projects had stagnated, generally as a result of the volume of projects being managed.

Strata have invested time and effort into the production of a 'Priority' matrix in order to more scientifically identify and highlight what projects were of most importance to the individual Partners. This is considered by Internal Audit to provide a baseline process for gaining an effective over view of which projects potentially add most value to the individual Partners.

The provision of greater visibility of what projects remained on the project portfolio has also allowed decisions to be made to reduce their number to more manageable numbers. Moving forward, the ability to manage the project portfolio effectively is a

challenge that Strata need to meet in order to maximise the potential for timely delivery of new service solutions.

As a minimum, Strata and the Partners need to gain timely visibility into what financial, staff and knowledge resource is required to deliver individual projects. It is hoped that the new project methodology will add significant value to financial, capacity and knowledge management. However, for the methodology to be successfully implemented a not insignificant degree of operational and cultural change will be required within Strata and the Partners.

Internal Audits initial opinion on the new project management process is that it appears to offer potential to add value to Strata's project management and, potentially, other functions. Two additional positions, of Project Manager and Supplier Manager, have also been created to provide additional roles and skills to supplement those that exist within Strata.

### 3.1.3 Cyber Security

The level of control in the six areas reviewed was considered to be of a good standard with strengths being provided by technical, procedural and, 'human' controls.

The loss or compromise of individual network devices can present an organisation with a range of challenges, but the virtualised VMWare environment adopted by Strata provides certain benefits. With all data being held centrally, the Partners data is more readily protected against a potential malware infection spreading across the computerised estate. A further advantage exists due to all user devices receive a new image each time a session is commenced and so any compromised device is effectively re-built, negating the need to physically re-image individual machines.

The area of most concern related to the use of high privilege network accounts. The number of these accounts used to manage Strata's network is excessive and bears no resemblance to what is advocated as best practice by Microsoft. The reduction of Domain Admin accounts within the Active Directory will take time to fully address as alternative lower privilege accounts need to be configured.

Some older server infrastructure still exists and these have to be appropriately managed to maintain security. The continued modernisation of the windows server infrastructure introduces more security by default and the ability to manage security using security through default and fine tuning using the Security Compliance Manager. The ongoing upgrading of server infrastructure is a major contributor to network security and Strata must continue to advocate the ongoing update of network hardware to benefit from technological advances.

Additional steps have been taken to improve the quality of information provided by logs. Monitoring is conducted to permit logs to be more effectively analysed and supplement alerts and warnings already embedded within existing software and workflow configuration. Patch Management, Firewall and Malware arrangements utilise a combination of well-known solutions. The Compliance & Security Manager maintains an up to date awareness of current threats and mitigations, which allows for security and operational needs to be kept in balance.

### 3.1.4 Follow Up (of previous issues and recommendations)

A total of eight recommendations were considered to have been fulfilled, whilst a further eight were considered ongoing and worthy of further review as part of the

2018/19 audit review process. Strategic recommendations are ongoing and the time allocated within the IT Audit Plan will be used to measure overall strategic progress.

The detailed findings and recommendations regarding these issues and less important matters are described in the Appendix A. Recommendations have been categorised to aid prioritisation. Definitions of the priority categories and the assurance opinion ratings are also given in the Appendix C.

## 5 Assurance Opinion on Specific Sections

The following table summarises our assurance opinions on each of the areas covered during the audit. These combine to provide the overall assurance opinion at Section 2. Definitions of the assurance opinion ratings can be found in the Appendix C.

| Areas Covered | | Level of Assurance |
|---|---|---|
| 1 | **Key Operational Functions** - Key operational functions and processes provide stable services that help deliver business outcomes. | Good Standard |
| 2 | **Service Design** - Processes to transform the strategic requirements of Strata into effective business solutions are effective. | Good Standard |
| 3 | **Cyber Security*** - Cyber (Security) can be considered to be a body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access. | Good Standard |

* Work undertaken was based on the Government's Cyber Essentials Scheme. It is often stated that compliance with the Cyber Essentials framework assists in guarding organisations against 80% of malware attacks. However, additional controls have been included within this programme in order to add the potential for further assurance to be obtained.

The findings and recommendations in relation to each of these areas are discussed in the "Detailed Audit Observations and Action Plan" ***Appendix A***. This appendix records the action plan agreed by management.

## 6 Scope and Objectives

As part of the formal audit planning process five key areas were identified for review within what was year one of a three year audit cycle, namely:

- Key Operational Functions;
- Service Design;
- Cyber Security

The work undertaken was to perform a high level review of these key areas in order to assess if there were any significant weaknesses, or risks, that Strata, and the Executive Board, should be aware of. Recommendations to mitigate any risks and to identify, or highlight, areas of improvement are also made. The programmes of work utilised to perform the reviews are based upon industry best practice.

The scope and objectives for the four individual audit areas reviewed as part of the plan of work for are provided in ***Appendix B***.

## 7 Inherent Limitations

The opinions and recommendations contained within this report are based on our examination of restricted samples of transactions / records and our discussions with officers responsible for the processes reviewed.

## 8 Acknowledgements

We would like to express our thanks and appreciation to all those who provided support and assistance during the course of this audit.

**Robert Hutchins**
**Head of Partnership**

**Appendix A**

## Detailed Audit Observations and Action Plan

| **1. Area Covered: Key Operational Functions -** Key operational functions and processes provide stable services that help deliver business outcomes. | **Level of Assurance** |
|---|---|
| **Opinion Statement:**<br>The level of control across core ICT functions is considered to be of a 'good standard". Having established a technical baseline for core ICT services, Strata are now in a position to evolve and refine their technical solutions and operational processes in order to deliver service improvements where possible. In terms of the core functions, this will often be in the form of greater resilience or security rather than providing more visible service improvements.<br>The maintenance and development of the core operational functions is reliant on having a good understanding of developments within the ICT industry. The further development of Strata's 'intelligent functions' has a direct impact on the ability to maintain it's Business As Usual (BAU) tasks effectively and not just the transformational programmes of the Partners. | **Good Standard** |

| No. | Observation and implications |
|---|---|
| 1.1 | In order to ensure that changes to legislation or best practice are understood and embedded into policy and procedure there needs to be processes in place to recognise relevant changes and perform period policy reviews. This is recognised by the Compliance & Security Manager who is to create a timetable for the Strata policy suite. |

| | Recommendation | Priority | Management response and action plan including responsible officer |
|---|---|---|---|
| 1.1.1 | Ensure that Strata's policy suite remains valid and up to date by timetabling review dates. | Low | Will be reviewed in May<br>Responsible Officer: Head of Security & Compliance<br>Target Date: 31/05/2019 |
| No. | Observation and implications | | |
| 1.2 | There is no formal Network Strategy in place to capture and define the future network requirements of Strata, the Partners, or potential future business opportunities. However, a Business Case for network improvements has been written/ is pending. | | |

| | Recommendation | Priority | Management response and action plan including responsible officer |
|---|---|---|---|
| 1.2.1 | As the new project management processes embed and 'intelligent functions' evolve, consideration should be given to:<br>• Identifying and detailing the Strategic objectives for Strata and the Partners;<br>• Producing a Strategy or strategic statement to detail and list strategic priorities;<br>• Identifying and documenting Architectural Principles to provide a clear and standardised development direction; | Opportunity | The new project management process is being successfully embedded. The process is already adding value to Strata and the Partners whose prioritised needs can now be understood and delivered more effectively. This, and the developing governance structures, will also help limit the number of platforms and technologies to those within Strata's Service catalogue and preferred technical direction.<br>Working in Partnership with the Partners, Strata is looking to follow the principles of the Local Digital Declaration , this initiative which is prescribed by central government for the delivery of applications within the public sector prescribes a code of conduct which it is looking for authorities to adopt. This initiative will also greater collaboration across the authorities through knowledge sharing and sharing of best practice. Further examples of standards followed by Strata are the OWASP application security standards.<br>The new processes also help ensure that business continuity and data security requirements are understood early in any project, again assisting in maintaining standards.<br>Responsible Officer: Strata Senior Management Team (SMT)<br>Target Date: Ongoing |
| No. | Observation and implications | | |
| 1.3 | Business Continuity & Service Level Management – IT Business Continuity Plans for 'Critical IT Systems has been produced, but the IT business continuity requirements of the Partners still need refining and documentation. Completion of a full IT BCP to reflect the operational needs of the Partners would also provide a valuable strategic overview that would inform proposals for a new data centre. | | |

| | Recommendation | Priority | Management response and action plan including responsible officer |
|---|---|---|---|
| 1.3.1 | Continue to work with the Partners to improve BCP arrangements, including the maintenance of prioritised schedules for the recovery of key business systems and solutions. | Medium | The Business Continuity position has now changed significantly over the past year, with a standard recovery priority list provided These define Recovery Time (RTO) and Point Objectives (RPO). Strata have also now further developed the capability of the Oakwood Disaster Recovery (DR). Strata are also undergoing an 11 stage process as part of the GDIP programme to demonstrate that investment is being made into making sure the technology is stable, flexible, but also has the capability and capacity to meet with the ever changing requirements of the three authorities. . Work conducted to improve BCP is also informing discussions and considerations for the potential development of a more suitable secondary Datacentre.<br>Responsible Officer: Strata SMT<br>Target Date: Ongoing |
| No. | Observation and implications | | |
| 1.4 | Network and Information Security (High Privilege Accounts) - Default 'super user' or 'system' accounts only exist to perform known functions that assist in the maintenance, integrity and resilience of the application or database and their use is monitored. | | |
| | Recommendation | Priority | Management response and action plan including responsible officer |
| 1.4.1 | Consideration should be given to producing a policy to govern the use of all high privilege accounts. Further consideration should be given to managing any such policy through the Change Advisory Board (CAB). | Low | A guidance document for the use of high privilege application accounts will be produced as part of the DPO data protection awareness programme.<br>Responsible Officer: Head of Security & Compliance<br>Target 31/12/2018 |

| No. | Observation and implications | | |
|---|---|---|---|
| 1.5 | Backup Arrangements - There is currently no schedule of tests to verify whether the backups made will actually be sufficient to rebuild a system and, therefore, no full system recoveries have been carried out. If backups have never been used to perform a full system recovery (including tests of the system by the business) they do not provide any assurance of resilience in the event of a system failure.<br>Noted: There are ad hoc recoveries performed for files and servers. Veem can bring back multiple servers. | | |
| | Recommendation | Priority | Management response and action plan including responsible officer |
| 1.5.1 | Strata should plan towards conducting full BCP failovers once arrangements for BCP and data centre provision have been finalised. | Medium | In line with the original Strata Business Plan, business continuity testing will be conducted to reinstate multiple business solutions following a major incident. As planned, Strata are commencing this during Summer 2019, building confidence in new SRM and Veeam configurations that support the failover.<br>Responsible Officer: Head of Security and Compliance<br>Target Date: 31/08/2019 |
| No. | Observation and implications | | |
| 1.5 | Backup Arrangements – Backup arrangements have been configured by IT staff based on technical requirements. However, without approval, or agreement, from the individual business area, there is no way of knowing that the customer is satisfied with the level of service provided. As a minimum, the ability to restore on a timely basis should be included as part of business continuity planning, which would also identify prioritisation of key business systems. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) have been discussed with BCP Leads from the three clients, which provides Strata with a clear measure of what their ‘customers’ expect. | | |

| | Recommendation | Priority | Management response and action plan including responsible officer |
|---|---|---|---|
| 1.5.2 | Strata should formally recognise the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) identified within the BCP as defining the level of service required by the individual business areas for BAU purposes. Strata should also confirm that the current technical and procedural elements accord to these BCP specifications. | Low | Actioned<br>Strata have now agreed RTO & RPOs with the Partners for key systems and applications. Strata are working to deliver the infrastructure to support the required RTO's and RPO's. In addition, the Business Continuity Lead (TDC) has sent out communications to all senior managers at TDC outlining their roles and responsibilities in respect of data retention, backup and recovery. |

| **2. Area Covered:** Service Design - Processes to transform the strategic requirements of Strata into effective business solutions are effective. | **Level of Assurance** |
|---|---|
| **Opinion Statement:**<br>Strata have demonstrated both an appetite and ability to make tangible improvements in this difficult area. The progress made in the past six months already demonstrates that Strata are putting the correct processes in place to improve the design and delivery of new service solutions for the Partners. The ability to recognise that there was room to make improvements in service delivery and to act upon it in a timely and swift manner not only provides assurance that service design and delivery will improve further, but also lends assurance to the Partners about Strata as a valued service provider.<br>The ICT industry continues to evolve rapidly which necessitates an awareness of what opportunities exist to provide benefit to the Partners. The initiatives to improve project and supplier management can all contribute to gaining market visibility and the timely identification of new solutions whether for visible service improvement or to provide greater warranty and security for the Partners. Strata should continue to develop their 'intelligent' functions so that the Strata Board has good visibility of opportunities, warranty and security and compliance requirements.<br>Few recommendations have been made to support service improvements at this stage as work has already commenced to review this area. As part of this work, more specific observations will be made along with more granular recommendations. | **Good Standard** |

| No. | Observation and implications |
|---|---|

| | | | |
|---|---|---|---|
| 2.1 | Strata are looking to undertake a timely and effective change to the project management processes and associated interdependencies. Time has, therefore, been allocated to look at the new project management process and those in place to assist with the delivery of new service solutions. | | |
| | Recommendation | Priority | Management response and action plan including responsible officer |
| 2.1.1 | DAP and Strata's IT Director to agree upon suitable Terms of Reference (TOR) to provide assurance that the approaches taken are appropriate to the needs of the Partners. | High | Actioned |
| 2.1.2 | DAP and Strata's IT Director to agree upon suitable Terms of Reference (TOR) for the audit time to add further value by identifying additional opportunities where appropriate. | High | Actioned |
| 2.1.3 | DAP to provide formal feedback during the third quarter of 2018/19, detailing observations, recommendations and opportunities by way of a formal situation report or report as deemed appropriate. | High | Agreed<br>Responsible Officer: DAP Senior Auditor (IT)<br>Target Date: 30/10/2018 |

| **3.1 Area Covered: Boundary firewalls and internet gateways** - Information, applications and computers within the organisation's internal networks are protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices. | **Level of Assurance** |
|---|---|
| **Opinion Statement:**<br>Boundary firewalls and internet gateways are considered to be configured and managed to a 'good standard'. The Fortinet Firewall was used to protect all three of the Partners prior to Strata, and the limited number of staff who administer it benefit from many years' experience with Fortinet products. The use of Logpoint to log and record Firewall changes and send alerts was considered to be of good practice. The use of Logpoint for other intelligence also provides further assurance. | **Good Standard** |

| No. | Observation and implications | | |
|---|---|---|---|
| 3.1.1 | Penetration testing is performed by an appropriately on a periodic basis so that vulnerabilities and weaknesses can be proactively identified. However, the annual IT Health Check testing (ITHC), and quarterly testing by the Compliance and Security Team has been conducted using the same company in recent years. Whilst there are some advantages in this, best practice would require the use of a variety of companies so that testing was approached using varied methodologies and personnel. | | |
| | Recommendation | Priority | Management response and action plan including responsible officer |
| 3.1.1.1 | Consideration should be given to periodically using different (accredited) security assurance companies to provide penetration testing and IT Health Checks (ITHC). | Medium | Actioned<br>This was already planned and is included within the new Strata Business Plan to have half yearly ITHCs, using alternative suppliers. Surecloud, used for the PSN compliance process, are to be retained as they are well recognised and this fits in with the onsite vulnerability testing platform that we use from them. Alternative companies will also be used for independent penetration tests of key systems. |

| **3.2. Area Covered: Secure Configuration** - Computers and network devices are configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role. | **Level of Assurance** |
|---|---|
| **Opinion Statement:**<br>Controls in this area are generally of a good standard. Network devices are built from a standard image and 'due to the environment employed, re-built for each session. This is undertaken in the DMZ, access to which is limited by firewall rules. However, for the main network Servers, normal Microsoft services are left enabled to avoid unexpected disruption.<br>All default passwords that exist to administer initial server build are changes and tested, before safeguarding the new 'complex' passwords. In the medium term, modernising the server infrastructure to predominantly use Windows Server 2012 and beyond would significantly strengthen network security by default. Whilst all current servers are hardened in line with best practice, the production of a policy template to define and potentially record the hardening process would strengthen current procedures. | **Good Standard** |

| No. | Observation and implications | | |
|---|---|---|---|
| 3.2.1. | There is no formal policy/ procedural guidance to define what steps server engineers take to 'harden' the security of servers/ network devices as part of the installation process. There have been various procedures put in place however these are not currently enforced.<br>Noted: All hardening done in the DMZ – using 2012 within DMZ. About 30>50% on Windows Server 2012 (Hardened by default). | | |
| | Recommendation | Priority | Management response and action plan including responsible officer |
| 3.2.1.1 | Consideration should be given to producing a Server Hardening policy/ template to define and record new server build standards. | Medium | Actioned<br>Strata have already identified this and went through the process of testing Group Policy Objects, however at the time there was considerable concern that this may cause failures. With the introduction of Server 2016 and the withdrawal of 2008 Servers the default hardening from Microsoft is now much improved and subject to a final review will become the default. |

| No. | Observation and implications | | |
|---|---|---|---|
| 3.2.1. | Approximately half of the server infrastructure is older than Windows Server 2012. Whilst these servers can still be managed to ensure that they are fundamentally secure, there are security and administration advantages in utilising newer server infrastructure. | | |
| | Recommendation | Priority | Management response and action plan including responsible officer |
| 3.2.1.1 | Strata Management Team should continue to advocate the value of using up to data server infrastructure, incorporating any associated principles within any future IT Strategy or Roadmap. | Low | Actioned<br>Strata SMT will continue to advocate the value of suitably specified server infrastructure. Windows Server 2008 will remove just under 200 Servers from the estate by January 2020, most being rebuilt as 2012 and 2016 Windows Servers.<br>Where necessary, and if appropriate, Strata will consider the use of cloud based applications. |

| **3.3. Area Covered: Access Control** - User accounts, particularly those with special access privileges (e.g. administrative accounts) are assigned only to authorised individuals, managed effectively and provides the minimum level of access to applications, computers and networks. | **Level of Assurance** |
|---|---|
| **Opinion Statement:**<br>The area of most significant weakness related to the use of high privilege Active Directory (AD) accounts that deviates considerably from common and long established best practice within the ICT industry. This represents a potentially significant vulnerability to the Councils network in the event that the network perimeter was compromised.<br>The number of Domain Admin accounts is exaggerated by the existence of four separate domains. However, the number of Domain Admin users is excessive and inappropriate to operational requirements and increases the risk of severe compromise of the network and the information assets held upon it. A process to administer and authorise additional higher AD privileges is in place which is considered to be good practice.<br>The three Partners still operate individual user management processes that, whilst interacting with the Strata Service Desk, provide information through differing processes. This is both inefficient and requires Service Desk operatives to have knowledge of the three differing processes. Efforts to bring about a single process that utilises automated workflow to create operational efficiencies should be appropriately resourced to add further value to the HR/ Payroll convergence. | **Improvements Required** |

| No. | Observation and implications | | |
|---|---|---|---|
| 3.3.1 | The number of Domain Admin accounts far exceeds what is considered to be acceptable good practice. | | |
| | Recommendation | Priority | Management response and action plan including responsible officer |
| 3.3.1.1 | A work stream to reduce the number of Domain Admin accounts should be initiated and a timeline should be agreed to perform the following remedial actions:<br>• A policy or standard should be produced to define to whom high privilege accounts are allocated applying the principle of least privilege in all cases. The standard should meet with best practice including the need for domain admins to | High | Work continues to reduce the number of true Domain Admin accounts within the Partners network domains.<br>All use of domain admin accounts are being logged and monitored and account creation requires the approval of the Head of Security & Compliance. Initiatives to better inform their use and to change behaviours are also ongoing.<br>Responsible Officer: Head of Security & Compliance |

| | | | |
|---|---|---|---|
| | have separate network user accounts and prohibiting the provision of an email account to domain admin accounts;<br>• A review of domain admin account holders should be undertaken and inappropriately allocated accounts deleted and replaced with new AD accounts that provide appropriate access;<br>• All changes should be managed through the Change Advisory Board (CAB) so that all risks to service availability are formally assessed and any potential risks are appropriately mitigated. | | Target Date: Ongoing |
| No. | Observation and implications | | |
| 3.2.1 | The three Councils have historically used their own respective starter/ leaver user access management processes to get the notification to Service Desk. The lack of a single standardised process creates operational inefficiencies for the Service Desk. Furthermore, the overarching Information Security Policy (ISP) produced by Strata to ensure that policy standards converge does not currently include User Access Management (Starters, Changes, Leavers), or password standards. This issue was originally raised within last year's report (Appendix A Item 4.4).<br>Strata are striving to have a single process and this issue is also recognised by the three Council business leads, but progress has been slow, partially due to the use of two different HR systems. The convergence to the iTrent HR/ Payroll system allows for these issues to be more easily rectified. | | |
| | Recommendation | Priority | Management response and action plan including responsible officer |
| 3.2.1.1 | All the opportunities presented by the introduction of the iTrent HR/ Payroll system should be captured to inform the introduction of a single user access management processes for all three Partner organisations. | Medium | Due to personnel changes within TDC, the project stalled. However the project is now being championed and good progress being made. It is hoped that a decision to 'go live' will be taken in the Autumn.<br>Responsible Officer: Strata SMT<br>Target Date: Ongoing |

| | | | |
|---|---|---|---|
| 3.2.1.2 | Policies for user access management and password quality should be written into the Acceptable Use and IT Supplier sub policies. | Medium | Agreed<br>Responsible Officer: Head of Security & Compliance<br>Target Date: Ongoing |
| 3.2.1.3 | Consideration should be given to capturing the functional requirements for creating efficient workflows to highlight any deficiencies within the current Service Desk solution. | Opportunity | The process to select a new Service Desk is now well advanced having seen four alternative systems. The creation of effective and efficient workflows is considered to be of high importance.<br>Responsible Officer: Strata SMT<br>Target Date: Ongoing |

| **3.4. Area Covered: Malware protection** - Computers that are exposed to the internet are protected against malware infection through the use of malware protection software. | **Level of Assurance** |
|---|---|
| **Opinion Statement:**<br>Malware protection is provided through layers of controls provided by a variety of protection software solutions. Appropriate protection was found to be provided to safeguard servers and end user devices utilising real-time protection and a range of security products. Some legacy computers are not as well protected as the majority of network devices, but this is to be addressed in the coming months.<br>The VMWare environment operated by Strata provides additional malware protection benefits, not least because data is held centrally and not on individual devices. The Virtual Desktop Infrastructure (VDI) virtual machine becomes blank and effectively rebuilt each time the local device is re-booted. Therefore, any potential infection does not get through to an individual or local machine. However, obtain reports to help administer tis area contain excessive ‘noise’ and currently require refining using Logpoint. Logpoint is also used to send real-time alerts to four members of staff in the event of an infection. | **Good Standard** |

| No. | Observation and implications |
|---|---|
| 3.4.1 | None made. |

| **3.5. Patch Management** - Software running on computers and network devices are kept up-to-date and have the latest security patches installed. | **Level of Assurance** |
|---|---|
| **Opinion Statement:**<br>Software and hardware patches were found to be appropriately managed using a combination of Microsoft and VMWare products to administer patches and updates. Windows patches are largely automated managed using the Microsoft System Centre Configuration Manager (SCCM) and the Windows Server Update Service (WSUS). Business applications and other third party software patches and updates are managed using VMWare App Volumes and App Stack. These provide the ability to update software utilised within the virtualised environment and add to the baseline 'Golden Image'.<br>Business critical servers are managed by way of manual deployment to better manage the potential risk of service outages. There is some caution taken with applying patches, but only when balancing potential negative impacts with security risks. Appropriate 'checks and balances' exist in the form of security layers and overall awareness.<br>The amount of legacy software is limited to a very few desktops. Any risks highlighted as part of the IT Health Check procedure are managed and remediated. | **Good Standard** |

| No. | Observation and implications |
|---|---|
| 3.5.1 | None Made |

| **3.6. Area Covered: Backup & Business Continuity** - Backup procedures exist to safeguard the system and system data and provide for an appropriate 'point in time' restoration that accords to business needs.. | **Level of Assurance** |
|---|---|
| **Opinion Statement:**<br>Comprehensive backup processes exist to provide a good standard of assurance. The performing of monthly test restores is good practice as is the existence of anti-ransomware protection for the Oakwood backup servers. This affords the backup servers more protection in the event that the network gets compromised by determined attackers.<br>Improvements to current IT Business Continuity Planning (BCP) would further strengthen this area and ensure that there is a direct relationship between backup and restore schedules and the timescales agreed as part of the BCP process (See Appendix A Section 1.5 above). | **Good Standard** |

| No. | Observation and implications |
|---|---|
| 3.6.1 | All recommendations made as part of the Key ICT Functions review (See Section 1.5 for recommendations). |

**Appendix B**

## Terms of Reference for Individual Audits

### Key Operational Functions & Processes

To perform a high level review of core operational processes using best practice principles that include; the ISO 27001/2, ITIL v3, the Information Commissioners Office (ICO) and industry best practice.

The review will identify any areas of significant weakness and highlight potential areas for future improvement. The review will also inform potential areas of work to be included within the ICT Audit Plan for 2016/17 and 2017/18.

Audit Scope will include:

- ICT Policies & Procedures;
- Core Infrastructure;
- User Management;
- Backup Procedures & Business Continuity;
- Compliance, including Public Services Network (PSN), DPA, Software Licensing.

### Service Design (and Delivery)

During the first two years of the current IT Audit Plan, DAP have concentrated on four key areas of IT service delivery as described within the ITIL v3 framework, namely:

- IT Strategy;
- Service Transition -Change Management;
- Service Operation (Process);
- Service Operation (Function).

**Service design** - The key area that has not been reviewed to date is that of ***Service Design*** and a review will be conducted to assess the effectiveness of delivery in this area. The primary objective of this review is to assess the effectiveness of processes to transform the strategic requirements of Strata into effective business solutions.

### Cyber Security

To undertake a high level review of network arrangements with an emphasis on arrangements in place to protect the corporate networks provided by Strata Service Solutions. The audit will, therefore, refer to the HM Government's "Cyber Essentials Scheme" which forms a baseline for the basic controls that organisations implement to mitigate the risk from common internet based threats.

The audit will focus on and provide opinion based recommendations regarding its effectiveness of the following areas and associated processes:

- Boundary firewalls and internet gateways;
- Secure Configuration;
- Access Control;
- Malware Protection;

- Patch management;
- Backup & Availability.

**Follow-Up on Previous Recommendations**

As part of the audit process progress against existing recommendations will be assessed. Consideration will be given to the overall progress made and the high level review will look to identify evidence of continued service improvement. Any outstanding issues will be managed appropriately, with any significant weaknesses being included as part of the 2017/18 report.

**Appendix C**

## Definitions of Audit Assurance Opinion Levels

| Assurance | Definition |
|---|---|
| High Standard. | The system and controls in place adequately mitigate exposure to the risks identified. The system is being adhered to and substantial reliance can be placed upon the procedures in place. We have made only minor recommendations aimed at further enhancing already sound procedures. |
| Good Standard. | The systems and controls generally mitigate the risk identified but a few weaknesses have been identified and / or mitigating controls may not be fully applied. There are no significant matters arising from the audit and the recommendations made serve to strengthen what are mainly reliable procedures. |
| Improvements required. | In our opinion there are a number of instances where controls and procedures do not adequately mitigate the risks identified. Existing procedures need to be improved in order to ensure that they are fully reliable. Recommendations have been made to ensure that organisational objectives are not put at risk. |
| Fundamental Weaknesses Identified. | The risks identified are not being controlled and there is an increased likelihood that risks could occur. The matters arising from the audit are sufficiently significant to place doubt on the reliability of the procedures reviewed, to an extent that the objectives and / or resources of the Council may be at risk, and the ability to deliver the service may be adversely affected. Implementation of the recommendations made is a priority. |

## Definition of Recommendation Priority

| Priority | Definitions |
|---|---|
| High | A significant finding. A key control is absent or is being compromised; if not acted upon this could result in high exposure to risk. Failure to address could result in internal or external responsibilities and obligations not being met. |
| Medium | Control arrangements not operating as required resulting in a moderate exposure to risk. This could result in minor disruption of service, undetected errors or inefficiencies in service provision. Important recommendations made to improve internal control arrangements and manage identified risks. |
| Low | Low risk issues, minor system compliance concerns or process inefficiencies where benefit would be gained from improving arrangements. Management should review, make changes if considered necessary or formally agree to accept the risks. These issues may be dealt with outside of the formal report during the course of the audit. |

## Confidentiality under the National Protective Marking Scheme

| Marking | Definitions |
|---|---|
| Official | The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. |
| Secret | Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime. |
| Top Secret | The most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations. |