devonauditpartnership

Internal Audit

# Internal Audit Report

## Strata ICT Audit

## Strata Services Solutions - ICT Partnership organisation of Exeter, East Devon and Teignbridge

*January 2024*

**Official**

CUSTOMER SERVICE EXCELLENCE CSE

Support, Assurance & Innovation

## Devon Audit Partnership

Devon Audit Partnership (DAP) has been formed under a joint committee arrangement comprising of Plymouth, Torbay, Devon, Mid-Devon, South Hams & West Devon, Torridge and North Devon councils and we aim to be recognised as a high quality public sector service provider.

We work with our partners by providing professional internal audit and assurance services 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 (PSIAS) 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 (The Partners), East Devon District Council (EDDC), Exeter City Council (ECC) and Teignbridge District Council (TDC). At the time, the creation of Strata in 2014 represented an innovative approach.

The approach has proved successful as Strata has delivered in excess of one million pounds in cashable savings. Of significant importance moving forward is that it positioned the Partners well as many Councils around the country increasingly look to enter similar partnership arrangements.

In its Policy Briefing on Technology related trends for the public sector in 2019, SOCITM identified that 'Partnering and Sharing Locally' as a key trend for Councils who 'need to adopt and share in order to remain solvent'. It further identified that there is a requirement for deep integration of services across traditional boundaries.

Strata remains well positioned to add value to the Partners and fulfilling the role of an effective strategic enabler and an 'agent for change'.

***** SOCITM is the premier professional body for IT leadership and management and digitally enabled services delivered for public benefit

## 2 Audit Opinion

| | |
|---|---|
| **Reasonable Assurance** | There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited. |

# 3 Executive Summary

The past four years have been extremely challenging for Strata and the Partners alike, with the Covid Pandemic and ongoing financial constraints creating unfamiliar and difficult operational environments. Strata have also experienced a period of relative instability with a turnover of four IT Directors in a fourteen-month period and the loss of experienced managers and operational staff. These issues created a poor environment for effective change and service improvement and it is accurate to state that there was a period of relative stagnation.

The new (and permanent) IT Director commenced in their role in July 2023 and, being a permanent appointment, provides Strata with the opportunity for fresh impetus and the incorporation of effective ideas for service delivery improvement. They have introduced changes to the way that Workstream and Project prioritisation are governed and this should enable Strata to better focus on delivery.

DAP maintains its long-term position that Strata are a fundamental component for enabling change for the three Partner organisations. Recent years have seen the increasing of partnering arrangements and the rejuvenation of the Unitary Authority approach. The Partners still remain in a strong position to exploit their own enabler for change. With resources limited, Strata will provide best value for money if new projects and solution-based business change benefits all three Partner organisations.

Such are the financial pressures on Councils that there appear to be few opportunities to maintain services at a satisfactory level without fairly radical changes to end to end processes. The use of new technologies and taking advantage of existing opportunities such as those offered on the Microsoft 365 (M365) platform could all contribute. The Partners have very limited retained client capabilities and Strata should have a clear role in the identification of potential opportunities.

The IT Director has instigated material changes to both organisational structure and key functions. This should help improve operational value for money, make better use of available resources and further strengthen service delivery processes. The creation of a Technical Design Architect (TDA) strengthens future infrastructure estate design and ensures that potential new software applications are formally considered for alignment with strategies and technical direction.

The Cyber Threat Landscape continues to cause concern amongst the Information Commissioners Office (ICO) and security professionals. The recent National Cyber Security Centre's (NCSC) Annual Report highlights the ever-evolving cyber threat landscape and the need for compliance with its advice. DAP provided a brief overview of the changing risks within last years report and advocated that "*An assessment of the effectiveness of Information Security governance should be conducted to ensure that Leadership Teams at all Partner Councils are sufficiently informed of the cyber risk environment in which they operate.*" Strata need to continue to provide leadership and timely advice in this area.

DAP has utilised the NCSC Cyber Essentials framework to provide assurance that security baselines are in place and sufficiently mitigate common risks. Strata's strong IT security capabilities measuring well against this framework, which does remain a valid assessment tool. However, whilst we still consider this framework to be of value, the National Cyber Security Strategy (2021 to 2030) introduces the Cyber Assessment Framework (CAF). This dramatically improves on the "Ten Steps" which it effectively replaces and, provides a new framework upon which an organisations cyber resilience will be measured.

The emphasis in on taking a risk management approach to assessing each individual organisations needs so that mitigations are appropriate to its own requirements. The CAF will likely require much greater collaboration and standardisation between the Partners as risk and governance process differences will be highlighted as a weakness. Interestingly, the need to have greater policy standardisation has been identified within an Exeter City Council (ECC) audit report and this helps provide an example to be followed for areas of process related policies.

There remain opportunities to reduce software estates which would help free up capacity as well as reducing some information security risks, information management overheads and aid compliance (DPA 2018).

Despite the challenges of recent years, Strata remain well positioned to provide both Business as Usual (BAU) services and the enabling platform from which the Partners can look to perform the necessary Digital Transformation required to optimise financial and human resources. Much greater collaboration and alignment must be achieved if all parties are to gain best value for money, making service solutions more effective, efficient and economic to deliver.

# 4 Observations and Findings

## 4.1 Strategy & Governance

DAP's initial Strata IT report identified that *"potentially the biggest risk associated with the chosen strategic direction is that the three founding partners do not maintain a strong single vision for Strata."* Following their appointment, the new IT Director identified weaknesses in the governance structures which negatively impacted a range of areas, but also the ensuring of good customer satisfaction amongst Partner Senior Management.

This is something that may have been neglected in the past, there being a great deal of difference between the satisfaction of general users and that of the strategic decision makers. The IT Director has worked closely with the Partners to identify and introduce a new governance structure and Strata mandate. This will provide greater clarity of roles and responsibilities and help ensure that the Partners collectively identify and prioritise the work that Strata undertake.

The revised governance structure includes the Architecture Board, which will inform joint decision making on technology across the 3 partners. DAP have previously highlighted the lack of 'retained client' capabilities within the Partner authorities and the lack of an ICT Roadmap, with the latter recognised within Strata's Mandate and Key Responsibilities.

The objectives of the ICT Architecture Board capture the requirements for ensuring that previous weaknesses can be addressed as does the introduction of a Technical Design Architect role. This senior position will be responsible for the design of the future infrastructure estate and ensure any new software application is formally considered and complements the future direction.

Whilst Strata has successfully delivered significant cashable savings, the challenges faced by the Partner Council's require a collective and collaborative approach to drive shared digital transformation. This is fundamental to the Partners ability to successfully deliver its future services and they must better utilise Strata as a strategic enabler.

DAP is to look at governance during quarter four of the 2023/24 financial year.

## 4.2 Cyber Security

| *The Cyber Security Table of Disparity* | | |
|---|---|---|
| **Function** | **Partner Councils** | **Cyber Criminals** |
| ***Governance Arrangements*** | Complex, bureaucratic and slow to respond. | Clear, autocratic and responsive. |
| ***Business Objectives*** | Statutory, moral and complex. | Financial gain. |
| ***Financial Resources*** | Reducing and difficult to allocate to meet specific granular service objectives. | Growing, pooled and allocated as required to achieve financial gain. |
| ***Time Resources*** | Reducing and increasingly pressurised. | Allocated as required to meet with objectives. |
| ***Technological Resources*** | Cost limited and allocated to meet specific business needs. | Able to take advantage of rapid advances in computing power. |
| ***Knowledge Resources*** | Shrinking organisations with difficult recruitment & Retention environment. | Ever expanding with 'lesser' actors increasingly being provided with code to use and develop. |

## Background

The proliferation of the use of malware, and particularly ransomware, is an alarming consequence of the ever-increasing reliance upon information technology and use of logical data assets. The greater the opportunities, the greater the number of those wishing to exploit those opportunities. Almost all the logical data we hold has a financial value and Cyber Crime can be conducted from anywhere in the world.

The geo-political ramifications, especially of the Ukrainian conflict, adds additional jeopardy to this picture. The regular news accounts of Ransomware, which has afflicted a number of councils in the last five years, and the increasing threat of data being extracted as a form or extorsion to avoid disclosure, is all too common. These not only serve as a reminder of the impact that a cyber-attack can have on an organisation, but also the value of basic good practice.

Unsurprisingly the NCSC Annual Review 2023 identifies an increasing Russian threat within a specific case study, with 'Patriotic' actors able to work with less constraint than the state. But it is perhaps the highly successful Russian organised criminal gangs who also offer Ransomware as a Service (RaaS) that can potentially be considered of increasing concern.

NCSC write "*The ransomware model continues to evolve, with a well-developed business model, facilitating the proliferation of capabilities through RaaS. This is lowering the barriers to entry and smaller criminal groups are adopting ransomware and extortion tactics which are making a huge impact."* Again, it follows that the greater the number of actors, the greater the attacks, the greater the opportunity.

Within this 'Russian' case study the NCSC does confirm that it is poor cyber hygiene (not following NCSC advise), and not sophistication, being the main reason for falling victim to ransomware. This is confirmed by the Insurance sector that have recently identified that organisations following the Cyber Essentials framework made 80% less claims.

The recent Government Cyber Security Strategy (2022 to 2030) however introduces the Cyber Assessment Framework as the new standard Cyber approach for all UK government bodies and agencies. The Local Government Association has provided a Local Government variant which better meets the security posture expected of this sector.

Government and Industry consensus is that it is not a question of “if” but “when” organisations are compromised by a Cyber incident. The need to have resilience and recovery plans and, the ability to reinstate services following a successful cyber-attack, is now imperative.

**July 2023 Review Findings**

The level of control in the six areas reviewed remains at a good standard (Reasonable Assurance) with strengths being provided by technical, procedural and ‘human’ controls. Since our most recent review, there have been notable improvements have been made to strengthen the level of assurance of the overall control environment. Strata’s PSN Certification for the three councils was renewed/ achieved during February 2023.

It is very evident that Strata subscribes to the mantra of Security in Depth which adds redundancy and resiliency to limit the impact of a particular security control failing or, failure to detect a particular threat. The increasing use of a combination of local onsite service delivery and ‘Cloud’ (third party hosted) adds further complications. Robust change processes and attention to detail is required, particularly when formerly onsite solutions are migrated to the cloud, where the risks are often subtly different.

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 receiving 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.

High privilege accounts have always been a challenge to manage appropriately and securely. The Azure Active Directory (Azure AD) is used for hybrid and cloud platforms and offers additional functions and opportunities for organisations. Azure AD Multi-Factor Authentication (MFA) is utilised for all Strata high privilege accounts and use is appropriately restricted within the network and security teams. Further work is to be conducted to segregate and monitor global admin accounts which should only be rarely used.

A minimal number of ‘end of support’ servers exist and these must be appropriately managed to maintain security before update to SQL Server 2016 devices. The 2022 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.

DAP commonly advocate the rationalisation of the software estate for security, value for money and compliance reasons, as well as the administrative management and support overheads they create. This also applies to the use of servers, but with the increasing recognition of the material environmental impacts of ICT infrastructure and its carbon footprint.

The reduction of servers and the software they support should always be explored. 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.

Strata are experienced users of the Logpoint Security Information & Event Management solution (SIEM) for identifying threats from these technical logs from various systems

including MS Defender and will further explore the use of the Microsoft (MS) Sentinel SIEM if the licencing programme is upgraded to 'E5'.

Patch Management, Firewall and Malware arrangements utilise a combination of well-known solutions. The Head of Security and Compliance maintains an up-to-date awareness of current threats and mitigations, which allows for security and operational needs to be kept in balance. All four firewall appliances have been replaced as well as the network load balancer.

Overall IT business continuity has been improved by the introduction of joined-up Business Continuity Plan (BCP) Disaster Recovery Plan (DRP) testing across the Partners and Strata. However, there remains wok to be done to ensure that the detailed operational needs and incident responses of the Partner Council are better embedded into plans and understanding.

The ***details of observations and recommendations have not been published as part of this report.*** A total of nine recommendations were made by DAP, with two 'High', five 'Medium' and two 'Low' priority actions agreed with management.

The following table summarises our assurance opinions on each of the individual areas covered during the Cyber review. Detailed Opinion Statements can be found in Appendix A. Definitions of the assurance opinion ratings can be found in the Appendix B.

| | | |
|---|---|---|
| **1.** | **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. | **Reasonable Assurance** |
| **2.** | **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. | **Reasonable Assurance** |
| **3.** | **Access Control** - User accounts, particularly those with special access privileges (e.g. administrative accounts) are assigned only to authorised individuals, managed effectively and provide the minimum level of access to applications, computers and networks. | **Reasonable Assurance** |
| **4.** | **Malware protection** - Computers that are exposed to the internet are protected against malware infection through the use of malware protection software. | **Reasonable Assurance** |
| **5.** | **Patch Management** - Software running on computers and network devices are kept up-to-date and have the latest security patches installed. | **Reasonable Assurance** |
| **6.** | **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. | **Limited Assurance** |

## 4.3 Service Delivery

### 4.3.1 Alemba vFire ITSM & Asset Management

### Background

It is fair to say that the development of the Alemba vFire IT Service Management (ITSM) solution has been slow. The Covid Pandemic occurred soon after its implementation and operational focus was rightly on keeping services running and effective during a challenging period for all. There has also been a period of consolidation and leadership changes that also negatively impacted progress.

Alemba vFire incorporates ITIL best practice principles, including key functions such as Change, Incident and Problem Management and, Request Fulfilment. This marries well with the new IT Directors intent to further strengthen key ITIL processes. The use of workflows and ITIL based configuration within the solution provide opportunities to reduce BAU and take advantage of further automation.

Asset Management within Strata has previously been severely impacted by the lack of ITSM development. Having previously used a bespoke ‘in-house Configuration Management Database (CMDB) solution, that became impossible to maintain, a commercial offering was required. As an interim solution, spreadsheets were then utilised to provide the records of hardware and software assets. Understandably, these records contained inaccuracies and were difficult and time consuming to maintain.

Exeter City Council were sufficiently concerned to conduct their own audit which focussed of user devices and highlighted the weaknesses in record keeping and Joiner Mover Leaver (JML) processes as well as a lack of clarity about overall ownership of assets. Whilst the largely financial risk related issues identified by ECC have now been remedied, it must always be recognised that weak asset management provides poor operational value and introduces financial, reputational and security risks.

IT asset management (also known as ITAM) is the process of ensuring that all IT assets are accounted for, deployed, maintained, upgraded, and disposed of securely. In order to manage security risks to the organisation, a clear understanding of service dependencies is required. Assets should be clearly identified and recorded so that it is possible to identify those that are important to the delivery of the essential functions, and to know what needs to be protected.

Benefits that may be gained should relate to improvements in asset management and the CMDB. The use of a core repository to record hardware, software and end user devices potentially allows for more effective and efficient asset management and improved association of incidents and problems with Configuration Items (CI’s).

**Asset Management**

Strata have made significant and material progress to address previous weaknesses in administering IT assets. The fundamental requirement to create and maintain an accurate CMDB on the ITSM has been completed, although work to further improve data quality is ongoing and incorporated into BAU activities. By creating a CMDB upon a recognised internationally utilised ITSM, Strata can now gain the benefits the workflow and asset management tools available.

Housekeeping and other BAU activities are in place to continue to update and validate the accuracy and integrity of asset records. In using a dedicated and fully functioning CMDB, Strata can now take advantage of opportunities to use software tools and scripts to extract and triangulate logical data. Activities include linking payroll data with the Active Directory used to manage network devices and access.

Governance and ownership are also pending improvement, with responsibilities for hardware and software assets being formally assigned to positions within the re-structured Service Desk Team. The Service Desk Manager has also had formal conversations with the Team so that the importance of the asset management processes and the role that they individually perform.

An additional benefit of utilising structured quality data is that it creates opportunities to harvest intelligence to aid management decisions and allow for the publishing of real-time information using dashboards. Strata are currently using Microsoft PowerBI to create dashboards to create inward and outward facing information.

Whilst it is considered by DAP that the software tools, and associated operational tasks, that have been put in place, the performing of periodic spot checks to confirm user ownership and locality of devices may add an additional layer of validation. This would apply to both the CMDB record and the software tools and processes in place to manage hardware assets.

Using a range of intelligence sources to optimise hardware and software asset utilisation can always be improved to gain best value from all IT assets. Now that proper foundations have been put in place, Strata should continue to explore how this area can be continually improved.

In summary, the establishment of a robust CMDB has helped mitigate risks, improve value for money and improve security as follows:

| Function | Observed Improvements |
|---|---|
| Plan | Improves the ability to identify what ICT assets are required to meet the needs of the business and estimate future budgetary requirements. Potential for greater use of monitoring and metrics to provide intelligence around asset utilisation and the total cost of ownership. |
| Procure | Ensures that the assets are appropriately specified and best value is achieved when committing to a purchase. Also contributes to budgetary control and information security by reducing shadow IT and rogue IT procurements. |
| Deploy | Processes have been introduced to ensure all assets are built into the CMDB, labelled with unique reference, appropriately distributed and stored. |
| Manage | The ability to manage IT assets relies on accuracy and visibility and so the creation of an effective CMDB and processes to maintain quality dramatically improve the ability (and potential opportunities) to improve the other four asset management functions. |
| Retire | Provides greater visibility so that the suitability, warranty and age to manage retirement (understanding costs and arrange for safe disposal). |

### *4.3.2 Financial Management*

Strata have also made progress in terms of financial management, something that is remains a challenge to many local government IT service providers whose roots stem from their previous ‘in-house’ function. Of fundamental importance to Strata and the Partners is the ability to benefit from more granular budgeting monitoring and reporting, enabling better forecasting of budget underspend, which in turn will lead to better in year use of resource.

The more effective use of the CMDB, and associated use of validating software tools, allows for more detailed financial analysis. The allocation of cost centres against hardware and software Configuration Items (CI)*, is providing Strata with information to more accurately re-charge costs.

Software licenses can now be managed with the aid of PowerBI dashboards and benefit from having clearer visibility on key information required to administer them. This is not only important for improving compliance management, but crucially, allows for ensuring that licence costs can be minimised through optimising the licences allocated, better understanding minimal licence requirements and permitting more timely negotiation of new agreements. Reporting Dashboards have also been provided to facilitate the Partners in viewing up to date Contract Management information.

* Configuration Items are items within/ used within the network environment that must be uniquely distinguished to allow for their appropriate management.

### 4.3.3 Operational Functions

The lack of an evolved ITSM also limits the obtaining of value for money and delivery of service improvements. ITIL functions such as Event, Change and Incident Management processes all benefit from the existence of structured process mapping, workflow and data. Improvements again exist in the provision of up-to-date dashboard information.

Strata have employed a service design professional to assist with the development of their ITIL functions and processes. This is timely as this allows for better development of the ITSM processes and workflows which should add value to key processes and functions. Early results include the revision of Internal Service Level Agreements (SLAs) for Incident and Problem Management as well as Service Requests.

The effective fulfilment of non-standard work requests has previously been challenging and difficult administer. Work has been focussed over the past twelve months to address this so that these requests can be processed more efficiently and effectively. It is important to process non-standard work requests efficiently so that capacity can be maximised and reduce the need for formal projects to be created.

Agile principles have been applied and requested work displayed on a Kanban Board to provide the Partners with increased visibility. This allows them to see all scheduled work which, crucially, enables better prioritisation. This approach has resulted in a 20% reduction in the number of queued requests freeing capacity to focus on priority work.

### 4.3.3 User Management or Joiner/ Mover/ Leaver (JML) Process

JML processes are notoriously difficult to manage in a way that achieves high levels of process compliance that would better safeguard user and asset management standards. There remains a need to embed standard JML processes across the three Partner authorities. Utilising the CMDB to hold user information and assign CI's aids significant improvement to end-to-end JML processes.

Whilst work to ensure better consistency is underway, there may be a period of adjustment where practices are changed to facilitate alignment. As alluded to earlier in this report, the CAF will require better alignment of non-technical processes such as Supplier Management, Risk Management, and Business Continuity Planning. Any lesson learnt from any process alignment would be of value to any CAF related changes and any future partnership working.

A task to identify where a user has not logged onto the network for 30 days is undertaken so that the user account can be suspended, better safeguarding network security and, where appropriate, contact service areas for to understand the reason for network absence. This also provides a compensating control where Stata have not been appropriately updated by Partner HR services.

### 4.3.4 Minimising the Software Estate

There are material inefficiencies in maintaining too many business solutions for the Partners. DAP have always promoted to the importance for organisations to minimising the software estate and, with Strata providing services to the three Partners, there is both an increase in risk and opportunities.

One of Strata's new principles is that of 'system simplicity' and it is clearly defined that Strata will *"look to reduce and consolidate our software estate and collaborate and combine processes where appropriate"*. Whilst that some capacity would be required to undertake the work to reduce the estate, there are many financial, operational benefits to

be gained as well as mitigating information risks.

Most public sector organisations are struggling to maintain the necessary capacity to ensure that services are delivered and so the reduction of the number of systems administer contributes freeing up capacity that could be better utilised. The rationalising and alignment of the combined software estates to create financial savings and efficiencies has been one of the business change drivers for the Partners since the creation of Strata.

The reduction of the Partners software estate is not only fundamentally important to the reduction of costs and improved information management, but also information and network security.

There are four clear security weaknesses in having too large a software estate, namely:

- Knowledge - The expertise required to maintain a wide range of business solutions securely.
- Volume - The variety of middleware required to make them operate (often with known vulnerabilities).
- Capacity - Increased numbers of BAU and scan vulnerability remedial actions created consume resources.
- Patching – The higher the number of differing business systems, the easier it is to miss critical patching of the solution or supplementary software.

### 4.3.5 Information Security Governance

The true level of cyber threat is naturally only really understood by security professionals, Chief Information Officers (CIO) and appropriately knowledgeable IT Managers and IT professionals. It is, therefore, important that Strata continue to highlight the true nature and impact of a successful cyber-attack so that appropriate governance, communication and funding are consummate with the overall risk.

Individual services within the Partner Councils are overseen and governed by senior managers who are subject area experts and who understand how they can best operate with the resources they have. Since all IT Security expertise resides within Strata, there is a real and developing risk that information security understanding and decisions are not fully informed. Incorporating ‘security by design’ principles into the IT Roadmap and the Architecture helps ensure that new systems are fit for purpose in the current global threat landscape and also aid awareness and learning within key client-side roles.

Strata must continue to effectively convey a strong message so that the Partners recognise the level of risk posed by the need to modernise how we obtain, store and use information presents within the current cyber risk environment. Again, alignment of policy, practice and awareness training are significant contributors to effective risk management and mitigation.

## 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 and Opinion Statements to support the levels of assurance for each Risk/Area covered are provided in Appendix A. Definitions of the assurance opinion ratings can be found in the Appendix B.

| Risks / Areas Covered | | Level of Assurance |
|---|---|---|
| 1 | **Strategy & Governance** | Reasonable Assurance |

| | | |
|---|---|---|
| 2 | **Cyber Security** | Reasonable Assurance |
| 3 | **Service Delivery** | Reasonable Assurance |

The findings and recommendations in relation to each of these areas are discussed in the "Detailed Audit Observations and Action Plan" appendix. This appendix records the action plan agreed by management to enhance the internal control framework and mitigate identified risks where agreed.

## 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.

## Acknowledgements

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

**Craig Moodie**
**Senior Auditor**

**Appendix A**

## Opinion Statements

| 1. Area Covered: Strategy & Governance | Level of Assurance |
|---|---|
| **Opinion Statement:**<br>The Strategic approach remains both valid and in line with the concept of greater partnering and collaboration. Business Plans have remained of a high quality and assists in detailing and measuring the value of services delivered. The use of metrics to evaluate service delivery and satisfaction remain effective, though use of goal driven metrics to reflect key business objectives can always be better evolved to remain valid. Changes to approach and governance arrangements will help provide better prioritisation and potentially help improve satisfaction at senior management levels within the Partner organisations.<br>To date, the relatively low level of partnering and collaboration has limited the value of the delivery model and fails to take advantage of the opportunities available. The changes to both governance and the organisational structure made by the new IT Director should help to better inform work prioritisation and the IT Roadmap. This will assist in driving collaborative digital transformation, obtaining value for money and better serve Strata in its role as an enabler.<br>The need to maintain robust Cyber Security to help mitigate the ever-evolving cyber threat landscape remains paramount to safeguarding service delivery. Adherence to NCSC guidance and frameworks is proven in helping organisations maintain good cyber hygiene and mitigate risks. Strata should continue to lead in this area so that Partners remain informed and security is built into design and live operation. The NCSC Cyber Assessment Framework (CAF) will require better alignment of governance arrangements, including information security policies and recognition of the value of taking a risk management approach. | **Reasonable Assurance** |
| **2. Cyber Security** | Level of Assurance |
| **Opinion Statement:**<br>***Firewall -*** All four firewall appliances have been regularly updated to mitigate against disclosed vulnerabilities. Logging and monitoring accords closely with good practice, using a recognised solution (Logpoint) and further supplementing with Surecloud for vulnerability scanning and port status reporting on ‘undenied’ inbound port traffic. PSN CoCo Compliance was achieved in February 2023.<br>***Secure Configuration*** – Server infrastructure is well administered with best practice observed as appropriate. However, Windows Server versions are varied and this requires careful management as older versions become outdated, | **Reasonable Assurance** |

| | |
|---|---|
| unsupported and potentially insecure. There is also a need to keep compatibility with the many third party and in-house systems that tend to have a lag before supporting later versions. Again, another reason to rationalise and modernise.<br><br>The current operational requirement for approximately 480 servers represents a significant attack surface. Each server must be securely administered, costs money and has an environmental impact and the reduction in the number of systems used and the number of servers required would produce multiple benefits.<br><br>***Access Control –*** This commonly challenging area is managed with a great deal of awareness and, importantly, high privilege accounts are subject to logging and monitoring. The move to the M365 platform, and current threat landscape, has prompted a review which is being undertaken to inform both the administering of high privilege accounts and, new policy. A commitment to Microsoft E5 licence would provide material opportunities for security and compliance improvements.<br><br>***Malware Protection –*** Layers of controls ("defence in depth"), are provided by a variety of recognised software solutions providing good assurance. A proactive stance to email and web browser filtering is taken by the Security Team, helping to mitigate certain user behaviour risks. The deployment over a standard and more flexible desktop over the advantageous virtual desktop provides both administrative, security and incident response benefits.<br><br>***Patch Management –*** A range of Microsoft and VMWare solutions are used to administer this crucial area. These update a virtualised 'Golden Image' which provides the standardisation so important in maintaining secure devices and environments.<br><br>***Backup & Business Continuity –*** The key area of weakness relates to the increasingly hybrid arrangement with Microsoft 365 and the potential unavailability of services, most likely due to unforeseen internet connectivity issues. Business Continuity and Recovery plans are in place but these need to be revisited and finalised to better reflect current service area operational needs in the current threat environment. Good practice is followed in respect of frequent testing of the backup solution and the ability to restore systems and data, as is the existence of anti-ransomware for the Oakwood backup servers. | |
| **3. Area Covered: Service Delivery** | |
| **Opinion Statement:**<br><br>The new IT Director has identified the need for changes to a range of operational functions and processes. This will be further enhanced by the six month employment of a service design professional to assist in the embedding of new ITIL processes. Whilst ITIL processes have previously been followed, the IT Director is looking to instigate changes to better enable the delivery of the changing Partner requirements. This fits with the ITIL ethos of continual service improvement and that all processes must add value. | **Reasonable Assurance** |

| | |
|---|---|
| The application of ‘Agile’ principles, and the creation of dashboards to allow for greater visibility, have resulted in a 20% reduction in the non-standard service request backlog. This is a material benefit as it frees up capacity for undertaking higher priority work and acts as an example of the benefits of continual service improvement.<br><br>The previously underdeveloped Alemba vFire ITSM has seen notable improvements with the Configuration Management Database (CMDB) now containing sufficient information to allow for significantly better Asset and Financial Management. There are clearly financial and budgetary benefits in ensuring that all assets are fully utilised and that their distribution is known. This also allows for more accurate allocation of costs and the identification of assets reaching end of life use which supports better budgetary visibility and planning. There are also security benefits to be gained.<br><br>JML processes are improving wit compensating controls in place to provide for more timely an accurate administering of access to systems and data. However, further alignment of policy and process would provide better value for money, being more effective, efficient and economic to administer. | |

## Scope and Objectives

The objective of this report is to provide an overview summary of the effectiveness of Strata's ability to deliver IT services to the Partners and of the effectiveness of the internal controls and procedures in place.

## 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.

## Confidentiality under the National Protective Marking Scheme

This report is protectively marked in accordance with the National Protective Marking Scheme. It is accepted that issues raised may well need to be discussed with other offic within the Council, the report itself should only be copied/circulated/disclosed to anyone outside of the organisation in line with the organisation's disclosure policies. This repo prepared for the organisation's use. We can take no responsibility to any third party for any reliance they might place upon it.

| 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 l damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. |
| Official: Sensitive | A limited subset of OFFICIAL information could have more damaging consequences if it were lost, stolen or published in the media. This subset of informa should still be managed within the 'OFFICIAL' classification tier but may attract additional measures to reinforce the 'need to know'. In such cases where t a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: 'OFFICIAL–SENSITIVE'. All documents marke OFFICIAL: SENSITIVE must be handled appropriately and with extra care, to ensure the information is not accessed by unauthorised people. |

**Appendix C**

## Definitions of Audit Assurance Opinion Levels

| Assurance | Definition |
|---|---|
| Substantial Assurance | A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. |
| Reasonable Assurance | There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited. |
| Limited Assurance | Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited. |
| No Assurance | Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited. |

## Definition of Observation Priority

| | |
|---|---|
| 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 observations 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. |
| Opportunity | An observation to drive operational improvement which may enable efficiency savings to be realised, capacity to be created, support opportunity for commercialisation / income generation or improve customer experience. These observations do not feed into the assurance control environment. |

## Devon Audit Partnership

The Devon Audit Partnership has been formed under a joint committee arrangement comprising of Plymouth, Torbay, Devon, Mid Devon, South Hams & West Devon, Torridge, North Devon councils and Devon & Somerset Fire and Rescue Service. We aim to be recognised as a high-quality internal audit service in the public sector. We collaborate 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 conducting 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 tony.d.rose@devon.gov.uk