devonauditpartnership
Internal Audit

Internal Audit Report

Strata ICT Audit

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

July 2022

Official

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). The creation of Strata in 2014 represented an innovative approach that has positioned the Partners well as many Councils around the country increasingly look to enter similar partnership arrangements.

Strata has been in operation for seven years on 1st November 2021 and has established itself as a successful provider of IT services within the South West region. Despite encountering both expected and unexpected challenges during this period, a common infrastructure platform and desktop technology are now well established, benefitting the Partners and Strata alike. This has been achieved whilst exceeding expectations, including substantial and tangible financial savings. The current Strata Business Plan (2021 and Beyond) reinforces the desire to continually improve and fulfil the critical role of enabling technology driven transformational change.

Reduce Cost, Reduce Risk and Deliver a Capability and Capacity for Change.

Computer technologies continue to evolve at pace leading to big advances in the enabling of remote working for staff and in improving customer engagement. These areas alone have provided opportunities for the Partners to improve service delivery, engagement and create operational efficiencies. These are fundamental components in delivering services at a time when Council's around the Country reach financial tipping points and as they struggle to deliver services with the resources available.

As stated in our July 2020 report, Strata have positioned themselves well to add value to the Partners and fulfilling the role of an effective strategic enabler and an 'agent for change'. The Covid 19 pandemic has also reinforced the importance of Strata as a vital 'Business as Usual' (BAU) enabler.

Based on the risks Strata are currently exposed to, this report focusses on key strategic risks with a more granular review being commenced in March 2022.

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

Entering its eighth year of operation, Strata is potentially facing its most challenging period since the early years and creation of a unified delivery platform upon which it provides ICT services to the Partners. The chosen delivery model remains a robust and relevant to business change needs within extremely challenging financial constraints. Indeed, as highlighted within last year's report, the partnering approach has become increasingly popular.

The ongoing Covid 19 pandemic introduced unforeseeable challenges for Strata and the Partners alike. This has impacted the ability to evolve and deliver business change, with the provision of BAU service rightly being prioritised. This, however, has understandably created varying degrees of frustration within Strata and for the Partners.

The departure of the Infrastructure & Support Team Manager in late 2021 and now the IT Director not only represents a significant loss of expertise and wisdom, but also potentially has a destabilising effect on Strata as a whole. The loss of the IT Director potentially undermines stability and creates uncertainty across the entire Strata business. Any reduction in staff morale represents a significant risk to organisational progress and the potential value adding benefits of Strata will decrease or be lost.

The annual review of Cyber Security using the technical basis of the Governments Cyber Essentials scheme confirmed that Strata continue to provide a strong network security baseline on which the Partners can deliver their respective services. The absence of critical and high risk issues identified by the PSN Health Check and positive comments from the inspection all provide notable assurance. However, the level of threat posed by Cyber criminals in particular is concerning and this must be recognised by Strata and the Partners.

The Cyber risk environment has changed considerably since Strata's inception, and it is imperative that all organisations suitably reflect this in mitigating strategies and operational processes. The importance of this cannot be overstated due to the high level of reliance of the Partners upon technology to provide essential services and deliver essential business change.

The Log4Shell incident that impacted Strata during December 2021 provided assurance that Strata have the necessary processes and capabilities to respond in a timely and effective manner to potentially damaging security incidents. It also served as a relatively pain free reminder that there are endless computerised vulnerabilities that are exploited by a wide range of would-be attackers.

A Freedom of Information request by a UK privacy group found that 114 councils experienced at least one cyber-attack between 2013 and 2017. However, it is the three high profile local government ransomware attacks occurring in the past three years that provide the starkest picture of the impact of a major cyber security compromise.

The ransomware attacks on Copeland, Redcar & Cleveland (Redcar) and Hackney Borough Councils serve as a warning that Local Authorities must not stand still but continue to strengthen and evolve their security operations and strategies. Without doing so the Partners risk sleep walking into a major security incident that would

cause significant disruption to services beyond the bounds of the individual Partner Council's and impact the members of the local community. In financial terms, the cost of recovering after such a major cyber-attack could create in unaffordable budgetary impacts.

We are yet to fully understand the extent of the Gloucestershire attack that occurred just prior to Christmas 2021. However, the attack used 'sleeper malware' that made its way into the local authority's system embedded in an email that had been sent to a council officer.

The question needs to be asked of the Partners "how would you deliver services without your network being available?". Business Continuity Planning (BCP) exercises commonly reveal that organisations and individual service areas incorrectly see cyber BCP as an IT Department/ Service responsibility.

Within its Policy Themes for 2021, SOCITM* identifies the value of partnering, collaboration and sharing proven best practice with both the Service design and Transformation and, Modernising ICT service delivery themes. The message highlights that by combining financial and knowledge resources in an effective and well governed manner, authorities can optimise service delivery and modernisation opportunities.

In establishing Strata in 2014, the Partners established a delivery platform that provides significant opportunities to take advantage of the strengths it offers. Despite seven years having elapsed since Strata was established, no combined ICT Roadmap exists, which undermines the ability to obtain best value for money from Strata.

As a minimum, a combined ICT Roadmap that includes core enterprise requirements such as data storage, communication and, key operational drivers to achieve value for money, must be in place. The recently created Digital Strategy provides an opportunity for the Partners to identify opportunities for greater technological alignment. However, if the Partners cannot agree upon a combined and collaborative IT Road Map, then serious consideration must be given to how the current strategic and operational weaknesses this creates can be best managed.

Teignbridge District Council (TDC) have largely completed the first stage of a project to implement Microsoft Office 365 (M365), commissioning a specialist company to assist with service design and configuration. This resulted in disproportionally focussed and consumed resource however this should assist the other Partners as M365 will need to be delivered to a greater or lesser extent to both of them.

The M365 platform does provide many opportunities to modernise operational processes to bring about much needed transformational business change. However, the overall platform, and the range of potential service options and configurations it offers, is vast and complex. It is therefore key that the M365 project must not deliver a collection of technologies, but a platform that's service design and configuration that is secure and drives efficiency and improved service delivery. Crucially, it would benefit Strata and all of the Partners if a collaborative approach to identifying business goals, functional requirements and opportunities is achieved, with this delivered sooner rather than later.

There are significant security and information governance risks associated with poor M365 configuration and practices, hence it is critically important that both financial and resource investments are made to ensure risks are understood and mitigated.

* *.Socitm is the professional network for digital leaders in the transformation of local public services. It is the membership association for these professionals – those who work in local and central government – as well as the broader public and third sectors, and suppliers to those sectors.*

4 Observations and Findings

The Cyber Security Table of Disparity

	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.

The Changing Cyber Risk Environment

Strata and the Partners must learn from the growing catalogue of high profile cyber-attacks, paying particular attention to the ever increasing use of ransomware. This goes beyond acknowledging their occurrence and being aware of the details surrounding these significant incidents. They confirm increased levels of frequency, complexity and, for those perpetrating them, profitability.

Strata benefit from having individuals who have been part of regional information security and management bodies and communities that create a high level of awareness of current incidents, trends and risks. However, DAP consider that, in line with many organisations, the level of understanding within the Partners is unlikely to reflect the current level of risk.

Globally, cyber-crime is already more profitable than the drugs trade and its low risk high reward nature will continue to encourage an ever increasing proliferation. Ransomware in particular is an increasingly profitable criminal activity and is fuelled by private sector companies generally calculating that it's more cost effective to pay out. It is therefore imperative to understand the resources available for cyber criminals to continually advance their capabilities.

The position is now so serious that a global coalition of technology companies have

called for “aggressive and urgent action”. Microsoft, Amazon the FBI and the National Crime Agency (UK) have joined the Ransomware Task Force in giving 50 recommendations to governments around the world.

All organisations increasingly rely upon its computerised systems to provide modern digital services, administer key services, communicate with the public and create the efficiencies required within current financial constraints. This increase in technological reliance has been incremental and so, as such, the understanding of the risks and rewards associated with greater technological reliance has been largely overlooked.

There also needs to be a reflection on the progressive split access to some systems, where some are in the ‘cloud’, which is systems and data held in third party data centres and needing a stable internet, and others operating from the local (Strata) environment. Both have their strengths and weaknesses, however without a well planned design, in the event of an internet or computer network failure this could result in challenges to access the complete suite of systems needed to deliver the key services.

The true level of cyber threat is naturally only really understood by security professionals and a limited number of IT Managers and infrastructure engineers. 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.

The responsibility for keeping an organisation Cyber secure resides with all within an organisation. In order to ensure that this is achieved, corporate leadership must provide a strong top down message based on a level of understanding that allows for risks to be properly considered and informed decisions to be made with regard to mitigating actions.

Information Security Governance

The ability to deliver modern local authority services in a cost effective and efficient way is almost totally reliant upon its IT infrastructure and business solutions. Despite this, many local authorities have not fully recognised this reliance within their Information Governance and IT Security governance structures, often with a wide variety of approaches taken.

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. 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.

Strata operate processes to appropriately control the introduction of new solutions, whether as part of the Data Protection Impact Assessments (DPIA) or as part of the project management and business change processes. However, these ensure security on a granular level. The current and evolving level of strategic and operational threat heightens the risk of sleepwalking into a significant cyber incident. 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.

Organisational Risks

The level of both costs and service disruption associated with a major cyber incident would make an already resource critical position worse. The severity and range of the impacts are such that it should be recorded within each Partner Council's Strategic Risk Register and the risk appetite formally recorded. The high-level granular risks include those associated with:

- The fulfilment of their statutory and moral obligations.
- The ability to deliver statutory and non-statutory services.
- Making payments to service providers, suppliers, those in receipt of Housing Benefit.
- Procuring/ paying for operationally critical goods such as fuel and vehicle maintenance supplies.
- Denial or Loss of Information Assets.
- Receiving and processing income.
- The compiling of the Council's accounts and Housing Benefit (HB) subsidy claims.
- Reputational damage.
- Short and Medium term financial impacts.

There is no doubt that suffering a major cyber-attack would damage the Partner Councils reputation, but the reputational damage to Strata would inevitably also have a significant impact. The Partners rely on Strata for security expertise, even though it is they that have the overriding legal and moral responsibilities to the local citizens that they serve.

It is in Strata's interest to maintain its reputation for being a secure IT service provider. Failure to do so could significantly impact its future viability as an IT service provider. It is, therefore, important that Strata provide effective guardianship to inform and protect the Partners from the growing Cyber threat and that, in turn, the Partners understand and respect the need for Strata to fulfil this critical role.

Lessons Learnt

The key message from the October 2021 Hackney cyber-attack is that a local authority whose IT security was of a high standard can be operationally crippled by a successful cyber compromise. It could be argued that Hackney had a much more prioritised and well-funded approach to safeguarding their network and information systems prior to the attack than the Partners/ Strata currently have.

Hackney had top-down buy-in from Senior management, underpinned by the existence of a director level Information Governance Group and a Chief Information Officer (CIO) led ICT Security Group. Of note, is that Hackney had conducted a ransomware exercise during 2016, at very least demonstrating an understanding of the risk.

Another key message is that the exploit utilised a sequence of relatively low risk vulnerabilities and a limited number of operational errors. The level of expertise and skill demonstrated by those conducting the attack was highly impressive. The

window of opportunity for conducting reconnaissance, seeding and detonating the attack was extremely limited. How do the Strata ensure that this level of risk is mitigated?

However, all of the good governance and operational practices were undermined due to the failure of an individual technician to comply with expected good practice and having access privileges that could be considered to be excessive for the role being undertaken.

In the light of the Hackney incident, both Strata and the Partners must consider the following:

- How extensive are your current security assurances and how will you identify knock on / combination risks?
- How do you know that your policies are fully implemented all the time?
- How extensive could an attack be and how will you recover (suggest using a range of scenarios)?
- How well do you understand the data you hold and associated potential risks?
- How are you using data retention management to reduce risk?
- What is your organisations risk appetite and insurance position against (a range of) these risks?
- Are all staff sufficiently cyber aware and understand and recognise cyber risks and potential cyber-attacks?

Minimising the Software Estate

There are material inefficiencies in maintaining too many business solutions for the Partners. Within Strata much needed capacity can be consumed that could be better utilised, including undertaking security or project related tasks.

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. However, 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.

Cyber Security Cyber Essentials Review

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 Appendices.

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 using 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.	Reasonable Assurance

The level of control in the six areas reviewed continues to provide Reasonable Assurance (***previously defined as 'Good Standard'***). DAP continue to use and advocate the National Cyber Security Centres' (NCSC) Cyber Essentials scheme and it is pleasing to note that Strata intend to obtain the Cyber Essential Plus accreditation. The involves an independent assessment by an NCSC approved company to confirm compliance with the schemes control framework. It is envisaged that best value could be provided by timetabling DAP's work in this area to preclude any Cyber Essentials Plus assessment.

Strata's latest Public Sector Network (PSN) Certification was achieved on 1st July 2021 providing a further level of assurance from what constitutes a mandatory and independent security assessment. Furthermore, no high or critical (risk) issues were identified, other than the 'end of life' Server 2008 issues, with the PSN

assessor commenting that good compared to other organisations.

The extended use of LogPoint by Strata to log and record Firewall changes and send alerts is considered by DAP to be good practice. The use of LogPoint for other intelligence also provides further assurance. The LogPoint system was upgraded during 2021 which provides 'SOAR' (security orchestration, automation and response) capability is planned to be trialled once capacity allows. This should better identify cyber threats to the network, in particular unusual events.

The management of high-privilege network accounts provide some compensating controls to help mitigate some of the risks associated with this area. To further manage the associated risks, Strata have significantly reduced the number of the highest privilege accounts providing least privilege accounts in their place targeted to each purpose.

A minimal number of 'end of support' servers still exist, with appropriate mitigations being put in place to ensure continued PSN certification. The network server environment benefits from ongoing investment with SQL Server 2016 and 2019 being introduced. The continuing upgrade of network infrastructure is an essential BAU component in ensuring that the Partners respective networks operate on an up-to-date platform that is both secure and optimises the opportunity to potentially take advantage of new technologies.

The monitoring of network logs is conducted to allow for more effective monitoring to supplement the alerts and warnings already embedded within existing software and workflow configuration. Strata also possesses the capability to use log data available to conduct effective analysis to identify potentially unusual activity or anomalies.

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.

The need to ensure that software solutions operate using the most recent 'patches' and updates available can't be over emphasised. The lack of Critical and High risk issues identified as part of the latest PSN Health Check help provide good assurance that the essential patch management processes are effective. This is largely due to performing monthly network scans which has significant benefits in safeguarding the network.

Whilst not part of the Cyber Essentials scheme, incident response is a critical component in ensuring that when incidents occur, they are dealt with in the most appropriate and timely manner. Two incidents have occurred during the timeframe of this report, with one relating to the deployment of a new mobile solution and the other a global software vulnerability event. In both instances the response, remediation and organisational learning were of a high standard.

Strategy

There are no ‘silver bullets’ when it comes to selecting a local authority's IT Service delivery model, but the current trend is to retain a higher degree of control through in-house or local authority partnering arrangements. This helps demonstrate that the Partners positioned themselves strongly in creating Strata when they did and should be ahead of the game in fulfilling current best practice. However, despite Strata now being well established with strong technical foundations, the Partners are yet to fully optimise its value.

Having three ‘masters’ was always the greatest challenge, and risk, to the success of the chosen delivery model. The existence of three separate organisations, with their own respective leadership, strengths, weaknesses and cultures, creates significant strategic differences. However, the services they deliver and the extreme financial pressures they are exposed to binds them through common future challenges. Closer alignment is an inevitability, either via organisational change or financial necessity.

DAP highlighted in June 2016 that there were clear strengths that the chosen strategic direction that continues to benefit the three founder partners. These included:

- Assisting in protecting the local economy through local employment:
- Mitigating financial risks associated with entering an unsustainable outsourcing contract and returning tangible savings:
- Retains the ability to make considered and timely decisions about future service delivery and retain multiple delivery options:
- Ensures partners have control and better transparency of ICT costs:
- Ensures that partners have direct input on information governance and security arrangements:
- Offers some opportunity for leverage in the marketplace.

The approach taken by the Partners has successfully fulfilled all the advantages listed in our 2016 report. However, having created a robust and modernised core network services the value of collaborative change now becomes of paramount importance. DAP have increasingly highlighted the change in Strata’s value to the Partners, with emphasis on its value as the key enabler for collaborative transformational change.

It is fair to say that whilst an extremely solid baseline from which to offer BAU and business change services has been established, Strata is not being utilised fully as an enabler for cross partnership change (using best practice). The approach to achieving transformation business change remains too disparate to fully exploit the opportunities that have been created.

The current Strata Business Plan SWOT analysis is well constructed and identifies weaknesses and threats that negatively impact the ability to optimise transformational digitalised change. DAP would like to highlight the following four identified issues:

- Limited IT visioning or needs analysis coming from the three authorities, Strata expected to be reactive, without any clear authority lead IT Strategy

- Lack of roadmap knowledge on installed products and solutions
- Lack of a clear IT Strategy for each of the three authorities meaning that Strata do not understand the direction of travel of the authorities.
- One of the partner authorities choosing to take a different direction in terms of IT than the other two authorities leading to Strata needing to deliver a two-tier IT platform / service.

Strata continues to demonstrate value to the Partners in the way of tangible financial savings that comfortably exceed those forecasted within the original Business Case produced in 2014. The delivery of £3.65m of savings over the last six years of operation for a relatively small IT service is to be commended, especially since the service delivery costs are typical using industry benchmarking.

The Business Plan (2021 & Beyond) is once again of a high standard with a notable level of measurable detail, including that provided for how services will continually improve perform the role of an effective enabler for transformational change. Strata's monthly performance monitoring and reporting continues to be of a high standard, providing the Partners with meaningful data and metrics. This is crucial in helping to remove unhelpful and misplaced subjectivity which negatively impacts customer perception and staff morale alike.

The current IT Director left Strata at the beginning of April 2022, which follows the departure of the Infrastructure & Support Team Manager in late 2021. This comes at a time of diminishing morale and frustration within the management team and wider Strata organisation as demonstrated in annual staff surveys. Failure to identify this as a significant risk to Strata and the Partners would potentially result in creating operational deficiencies in capacity and knowledge. This, in turn, would have a disruptive effect on BAU service provision, business change and projects alike.

Strategically, Strata has benefitted from the leadership and expertise that the management team has provided over the past seven years. It is essential that the Board recognise this and ensure that all appropriate steps are taken to support Strata's management team and help safeguard future morale and the culture of the organisation, which has underpinned the success of Strata.

Service Design and Transformation

The absence of a truly joined up strategic IT Roadmap demonstrates a lack of collective appetite or, full realisation of how to optimise value for money from Strata. Whilst DAP consider there are good practices in respect of administering business change and project work, there are few examples of truly collaborative transformation projects that would provide material organisational changes to safeguard future service delivery. This also limits the opportunity to link associated functional requirements, so limiting the opportunity to identify processes and solutions that can be re-used in other end to end service delivery designs.

A 'Digital Strategy' has now been developed by the three authorities to define a roadmap as to where the authorities wish to move in relation to how best the authorities support their citizens with Digital technologies and channels over the coming years. The challenge is now to map the existing IT environment against this

Digital Strategy to identify what projects Strata need to undertake to provide the IT environment upon which the authorities can deliver their Digital vision. Strata had engaged a 3rd party (Agilisys) to undertake a review of the organisation's Digital readiness, the results of this exercise were presented back to the authorities during the first quarter of 2022/23.

Investment in good service design helps deliver value over the full service lifecycle as the business solution and associated processes create efficiency and save revenue costs. Whenever possible, Strata's finite resources should be focused on the delivery of projects that deliver the most value for money, and preferably, to all three partner authorities.

TDC have identified M365 as a means of transforming core functions within the Authority and are well on the way to completing their first phase. This, along with other TDC projects, has resulted in the consumption of considerable and disproportionate Strata resources. Whilst it may be considered that TDC are acting as a pathfinder, it is difficult to see how a configuration blueprint that truly fulfils the specific business needs of all the Partners can be achieved in this way without continued review and input from all through the project lifecycle.

The number of ways that M365 can be used for communicating and sharing information or documentation is considerable, which from an information governance perspective is concerning. The Devon Information Security Partnership (DISP) has identified M365 configuration as potentially introducing significant risks.

DISP includes information governance and security practitioners from local government, health and emergency services in the region and the membership have raised a wide variety of challenges and concerns. These are significant enough for the subject to be replacing the GDPR as a key agenda item, not least because of the clear risks to organisational data protection compliance.

Being the most popular 'office suite' in the world, the selection of M365 as a solution is both common and understandable. However, it must be understood that in not looking at end to end processes and undertaking a competitive procurement process creates a range of risks and project weaknesses. The review of a range of methods and means of providing end to end solutions is crucially lost, which can limit the opportunity to understand the variety of ways core business functions can be provided. This can limit the potential for radical and cost effective change as well the resultant service configuration or, for configuration to be myopic in nature.

Assuming TDC's M365 project is perceived as being successful, Strata resources will be consumed through a greater number of incidents and problems during the implementation, release, and early life phases. This will impact implementation, support and training resources. This is clearly inefficient and highly disruptive for both Strata and The Partners and a likely contributor to dissatisfaction on all sides.

As a 'fallback' it is imperative to capture all lessons learnt in respective of M365 so that any potential future implementations within ECC and EDDC benefit from the knowledge and experience gained during the TDC deployment. However, it would be far more effective to ensure that all Partners had a defined and collaborative design that ensured that respective organisational requirements were appropriately balanced and delivered.

The delivery of solutions utilising Software as a Service (SAAS) and hosted environments requires an understanding of different and additional risks that require different thinking and mitigating controls. There is a clear distinction between project risks and the risks associated with a specific IT solution and the operational end to end process. The later assessment is fundamental to ensuring that the organisations data assets are appropriately safeguarded in live operation.

Transition/ Change Management must also recognise risks effectively, particularly as IT platforms continue to evolve at pace to meet with changing business requirements. The need to assess risks effectively within each discipline, and merge them where appropriate, must not be lost. It would, therefore, be of value to all of the Partners to manage and mitigate these risks through collaborative effort and mirrored end to end processes. The current project framework allows for this, but regular review of its effectiveness in managing risk would be beneficial.

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

4 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 Appendices.

Risks / Areas Covered		Level of Assurance
1	***Strategy & Governance***	Reasonable Assurance
2	***Service Delivery***	Reasonable Assurance
3	***Cyber Essentials***	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.

Tony Rose
Head of Partnership

Appendix A

Detailed Audit Observations and Action Plan

1. Area Covered: Strategy & Governance			Level of Assurance
Opinion Statement: The Strategic approach remains both valid and in line with the concept of greater partnering and collaboration. The latest Business Plan is of a high quality and assists in detailing and measuring the value of services delivered. However, the level of partnering and collaboration limits the value of the delivery model and fails to take advantage of the opportunities available. The ever increasing cyber threat changes the risk environment in which Strata and The Partners operate and essential transformational change is delivered. There is an urgent need for all organisations to re-evaluate their respective information governance structures, with particular regard to IT security.			**Reasonable Assurance**
No.	Observation and implications		
1.1	The loss of the IT Director and the Infrastructure & Support Team Manager potentially undermines the stability that Strata has enjoyed over the past five years. This also comes at a time of much frustration and diminishing moral. The loss of other members of the management team or, other key staff, represents both an operational and potentially strategic risk.		
	Recommendation	Priority	Management Response (Including action plan and responsible officer)
1.1.1	The Strata Board should oversee current IT Directors exit interview.	High	A transition plan has been drawn up and presented to the board enabling identified key activities to be handed over to either members of the management team or to the incoming Interim Director of IT and Digital Transformation. The outgoing IT Director will complete an exit questionnaire and will be requesting an exit interview as part of the process. Actioned: March 2022
1.1.2	The reasons for the Head of Infrastructure & Support's departure must be captured as part of the IT Directors exit process.	Medium	An exit form was completed by the Infrastructure and Support team manager and submitted to the IT Director and HR for analysis.

			Actioned: October 2021
1.1.3	Upon the appointment of the new IT Director, the new incumbent should capture and formally report back to the Board Strata's Management Team's observations and concerns for the future of Strata.	Medium	It is expected that the incoming Director of IT and Digital Transformation will undertake a review of Strata within the first 100 days, capturing initial observations and concerns, with Strategic and operational recommendations. This analysis would then be presented back to the Strata Board. Actioned: March 2022
No.			
1.2	The risk environment is continually changing due to the increasing Cyber threat. The level of cyber risk is such should that organisations should be suitably recognised this within their respective risk management processes. It is of utmost importance that senior management within the Partner Council's properly understand the risks and that investment and budget are appropriately maintained.		
	Recommendation	Priority	Management Response (Including action plan and responsible officer)
1.2.1	In the light of the current Cyber threat, Strata must re-evaluate the suitability of information governance structures within the respective Partners and if the level of support, advice, and influence that Strata currently provide is sufficient. Strata should ensure that their role in providing the Partners with specific information security expertise is appropriately recognised.	High	The Partners and Strata have agreed to use the NCSC Incident in a Box series of scenarios to better understand the various needs and interactions of information governance. One iteration of this exercise has been undertaken with the three partners and Strata all participating, including the BCP leads from each authority.
1.2.2	Strata and the Partners should ensure that the Cyber threat is appropriately recorded within their respective corporate risk registers.	High	Cyber threat is recorded within the Strata Risk register which is maintained by the Strata Head of Security and Compliance. Risk is reviewed as a standing item at each Strata Board meeting. The Council also hold Cyber as a corporate risk in their own registers.

2. Area Covered: Service Delivery (Service Design)	Level of Assurance
Opinion Statement: Whilst it is understandable that a single Partner Council will choose a specific transformational path that fits with their own respective business needs, this also potentially erodes the Strata's value as an enabler for change. Furthermore, this potentially creates a range of risks to itself, Strata and the two other Partners since resources are being disproportionally consumed. This not only applies to the project phase, but potentially for the lifetime of the M365 solution if the two remaining Partners choose an alternative solution or differing elements of the M365 application suite. The TDC M365 project must not deliver a collection of technologies, but a platform that's service design and configuration that is secure and drives efficiency and improved service delivery. Crucially, it would benefit Strata and all the Partners if a collaborative approach to identifying business goals, functional requirements and opportunities is achieved. Strata are a member of the Devon Information Partnership (DISP) who recognise the potential risks that poor configuration represents. It would be highly beneficial for the shared knowledge within DISP to help inform the TDC project. Strata and the Partners have made progress in converging software solutions, but the security aspect of having to maintain large numbers of software solutions must be increasingly factored into decision making. The use of Multi Factor Authentication (MFA) solutions is becoming more common and represents an effective means of mitigating the considerable risks associated with ongoing poor password practices by network users.	**Reasonable Assurance**

No.	Observation and implications		
2.1	Strata are a member of DISP who are to include M365 as a standing agenda item in the short and medium term. Due to the number and range of organisations attending, this shared understanding and learning is an invaluable source of information regarding configuration and associated risks.		
	Recommendation	Priority	Management Response (Including Action Plan and responsible officer)
2.1.1	All intelligence obtained from attendance at DISP should be provided to the project team. Where necessary, information should be used to inform/ revise the Data Protection Impact Assessment (DPIA).	Medium	DISP is a valuable resource however this has been supplemented by technology and security specialists to increase the delivery and governance capability to better inform the project. Target Date: Ongoing

No.	Observations and implications
2.2	The number and variety of business solutions administered by Strata not only creates operational pressures and inefficiencies but heightens the security risks.

	Recommendation	Priority	Management Response (Including Action Plan and responsible officer)
2.2.1	Strata should continue to advocate convergence and rationalisation of the Partners software estates, further highlighting the security risk posed by maintaining high numbers of differing software solutions that all require varying knowledge and patching requirements.	Medium	Given the upcoming Digital drive which includes further adoption of hosted solutions, this would appear to be the appropriate vehicle to support these considerations and objectives. Target Date: Ongoing
No.	Observations and implications		
2.3	Most organisations struggle to ensure that their network users comply with password policies and comply with organisational policy and best practice initiatives.		
	Recommendations	Priority	Management Response (Including Action Plan and responsible officer)
2.3.1	Consider the introduction of additional security measures to supplement network and application passwords and use of MFA such as the use of biometric solutions such as Windows Hello.	Medium	Biometrics could be considered but also come with real concerns on the use of personal data. There is also the need to ensure that each biometric solutions False Rejection Rate and in particular False Acceptance Rate are suitable for the access needs. Windows Hello for Business relies on specific hardware. Target Date: Ongoing

3. Area Covered: Cyber Essentials Review			Level of Assurance
Opinion Statement: The annual review continues to provide 'Reasonable Assurance'* that the controls provided by Strata to mitigate against the most common cyber threats are effective. The intention to attain the Cyber Essentials Plus accreditation is also considered to a further positive. The requirement for a formal assessment by a duly accredited IT security assessor will not only provide further assurance, but also ensure that Strata is seen as a secure provider of IT services by potential would be partners. Good cyber security also requires robust and effective incident response processes to administer the impacts and remediations required following a security compromise. The two incidents that have occurred in recent months, evidence that Strata have the capability to respond and remediate effectively and appropriately. Furthermore, a high level of review and organisational learning was demonstrated.			**Reasonable Assurance**
No.	Observation and implications		
3.1	In conducting the annual cyber security review the following observations, recommendations and opportunities have been identified.		
	Recommendation	Priority	Management response and action plan including responsible officer
3.1.1	There have been no Business Continuity tests conducted in the past twelve months with continual focus on Covid and Covid recovery. It is recommended that the planned Business Continuity and Disaster Recovery testing should resume at the earliest opportunity.	High	Cyber tests have now been prioritised above Business Continuity., However, it is becoming increasingly evident that Cyber can be considered an additional threat type, but that follows the BC approaches. An initial NCSC Exercise in a Box was undertaken in March 2022 with a commitment to take actions forward and complete further Exercise in a Box sessions. Target Date: Ongoing
3.1.2	The Server Build Standard 11 Checklist does not make specific reference to changing default passwords. However, it is noted that the form does require sign off by the Security Team. It is recommended that a prompt in the Server Build Standard 11 Checklist is introduced to ensure that engineers consider and action any changes to default passwords and that this is checked as part of the sign off process.	Low	Server passwords are managed by LAPS for domain joined and otherwise for non-joined and the passwords are entered in the password system. It is noted that there is not a direct reference to changing the passwords and this can be added even though practice and vulnerability scanning does not show this to be an issue. Target date: Sep 2022 (checklist update)

3.1.3	From April 1st, 2021, Strata have been informed of leavers via a feed from the Partners payroll systems (iTrent). However, there is not a common leaver processing place across all three clients. It is recommended that a standard/common process for identifying and processing leavers of each client organisation is introduced.	Low	Due to other commitments, especially those caused by Covid and the associated activities this low priority exercise to develop a common process has not been undertaken. There is an expectation that there will be a wider focus on processes within Strata over the next 12 months of which this will be one of.
3.1.3	There are two non-standard email routes. One relates to a company needing to route via M365 directly and the another supports the requirement for some members to have emails forwarded from Devon County Council (DCC) to their TDC account. It then becomes necessary for that individual to create DMARC exceptions. It is recommended that Request Management Response regarding confirmation/explanation that the level of email filtering for non-standard routed email is subject to adequate filtering (in line with/equivalent to standard routed email filtering).	Low	The company which needs M365 direct routing has limited and specific email requirements that we feel are mitigated. The DCC email account is reviewed and once that Councillor moves to M365 this option will need to be withdrawn as the filtering approach appears to be different at DCC resulting in additional threats being received but not managed as effectively as they are seen to come from a trusted source 'DCC' We have also implemented Trend Cloud One security that does a secondary scan of all email entering and existing M365.
3.1.4	At present Strata do not have a documented response plan(s) /Playbook for use in the response to a significant malware/ransomware incident. An incident response plan "playbook" should be developed for use when a significant incident (malware or other incident effecting IT Services) occurs.	Low	These are likely to be developed as part of the Incident in a Box exercises. The upgrade of Logpoint now includes SOAR capability, which provides automated threat response will also develop playbooks. Target Date: 31/03/2023

Appendix B

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 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.
Opportunity	A recommendation 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 recommendations do not feed into the assurance control environment.

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.
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 information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: 'OFFICIAL–SENSITIVE'. All documents marked OFFICIAL: SENSITIVE must be handled appropriately and with extra care, to ensure the information is not accessed by unauthorised people.