VERSION 2.0

DECEMBER 20, 2016

SHARED RESOURCE SERVICE

AUDIT STRATEGY 2017 – 2020 AND RISK ASSESSMENT

PRODUCED BY: MIKE CORCORAN

TORFAEN COUNTY BOROUGH COUNCIL

INTERNAL AUDIT SERVICE

TABLE OF CONTENTS

1. INTRODUCTION AND APPROACH

1.1. Introduction

1.1.1. Internal Audit objectively examines, evaluates and reports on the adequacy of the control environment as a contribution to the proper, economic, efficient and effective use of resources. This opinion forms part of the framework of assurances that the Shared Resource Service (SRS) receives and should be used to help inform the Annual Governance Statement. The purpose of this document is to set out the proposed SRS three year internal audit plan for the period 2017 – 2020 and the associated risk assessment.

1.2. Approach

1.2.1. In summary the approach to develop the risk assessment and annual internal audit plan is set out below. See Appendix 3 for a more detailed description.

Step 1 - Understand the SRS's Key Strategic Priorities and Risks

The following were obtained from which information was used:

- SRS Partner Strategy 2016-2020;
- SRS Business Plan 2016-17;
- SRS Risk Register;
- Partner Risk Registers where relevant to SRS service provision.

Step 2 Define the Audit Universe

Determine all auditable units within the SRS i.e. "any key functional area of the SRS, as agreed with the Key Contacts, and closely aligned with the Service provision structure".

Step 3 Assess the Risk and Control Environment

Assess the risk of each auditable unit, based on inherent and control risk factors and materiality considerations, including their potential impact on achievement of the SRS's priorities.

Step 4 Determine the Frequency of Audit Review

Determine the frequency of audit review for each auditable unit, taking into account the assessment of the risk and control environment for each unit, including the activities that comprise each of them.

Step 5 Determine the Audit Plan

Determine the timing / scope of audit work based on SRS priorities, available audit resources, discussions with Key Contacts and knowledge of developments over the period of the SRS / Partner Plans.

Step 6 Other Considerations

Consider additional audit requirements to those identified from the risk assessment process, including:

- provision of annual assurance to the SRS partners;
- the planned activities of external audit and inspection agencies;
- preparation of the Annual Governance Statements of the Partners; and
- potential unplanned audit reviews and investigations.

1.3. Basis for the Plan and the Internal Audit Conclusion.

1.3.1. This plan allows the Head of Internal Audit to meet the responsibilities placed on him by the Public Sector Internal Audit Standards – Planning Standards, namely:

2010 Planning "The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organisation's goals."

The Head of Audit is responsible for developing a risk-based plan and will take into account the SRS's risk management framework, use the risk appetite levels set by management for the different activities or parts of the organisation. Where a framework does not exist, he will use his own judgment of risks after consideration of input from senior management and the board. He will review and adjust the plan, as necessary, in response to changes in the SRS's business, risks, operations, programs, systems, and controls.

2010.A1 "The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process."

2010.A2 "The chief audit executive must identify and consider the expectations of senior management, the board and other stakeholders for internal audit opinions and other conclusions."

2010.C1 "The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value and improve the organisation's operations. Accepted engagements must be included in the plan."

1.3.2. The annual audit opinion will be based on and limited to the internal audits completed over the year and the control objectives agreed for each individual audit.

In developing the risk assessment we have taken into account the requirement to produce an annual internal audit opinion by determining the level of audit coverage over the audit universe and key risks.

1.4. Other Sources of Assurance.

1.4.1. We have taken into account other sources of assurance available (see below) e.g. external regulatory, assessment bodies and considered the extent to which reliance can be placed upon them.

- Wales Audit Office (WAO)
  - Corporate Assessment Report Issued: September 2016 Document reference: 463A2016.
  - Review of the Shared Resource Service Issued: May 2015 Document reference: 288A2015
  - Technology Review Feedback Issued: September 2011 Document reference: 366A2011.
- British Standards Institute (BSI)
  - ISO27001 Accreditation Report.
- .
  - IT Health Check
- Society of IT Managers (SOCITM)
  - Benchmarking Report [GPA, MCC, TCBC] Issued: September 2015.

1.5. Key Contacts

1.5.1. Meetings were held with the following key personnel during the planning process:

Name / Email / Phone	Position /	Partner
Matt Lewis 07837 170928	Chief Operating Officer	SRS
Richard Edmunds 01495 742545	Head of Strategic & Democratic Services	Torfaen
Nigel Stephens 07967 831529	Assistant Chief Officer Resources	Gwent Police
Mark Howcroft 07967 481999	Assistant Head of Finance	Monmouth
Dave McAuliffe 01495 355055	Chief Finance Officer	Blaenau Gwent
Meirion Rushworth		Newport City Council

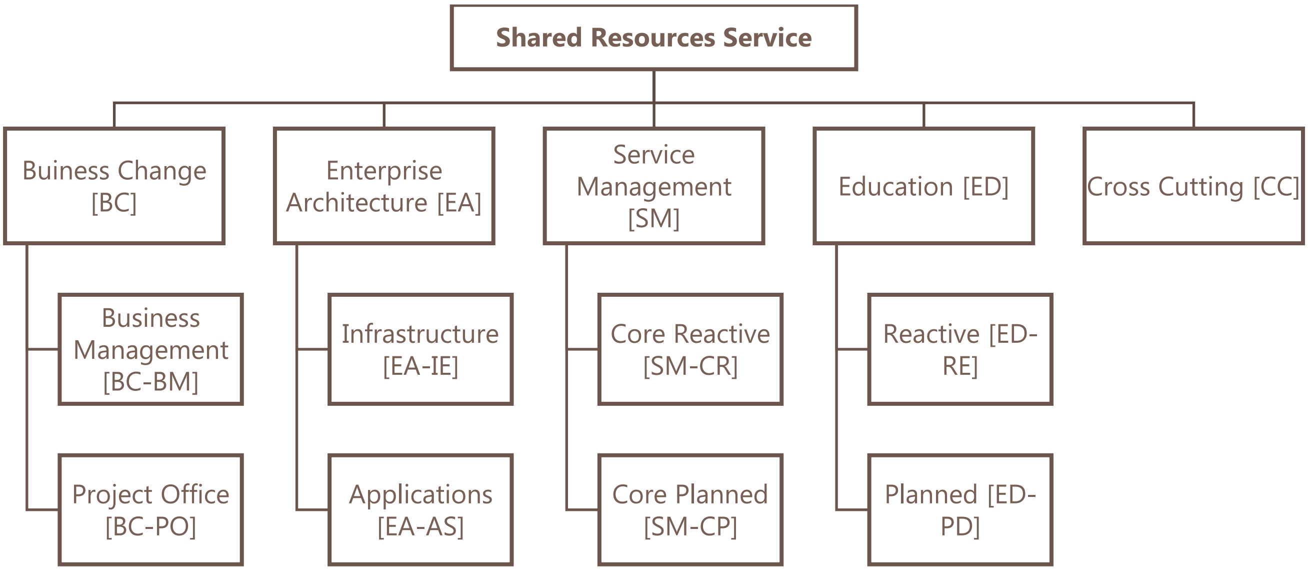
1.5.2. A copy of this document was issued to the appointed external auditors of the SRS partners for consideration and comment.

1.5.3. Newport City Council will be joining the SRS as a partner from 01 April 2017. Their key contact (as noted above) will be contacted in relation to audit coverage.

"The internal audit arrangements, which are set out and agreed with the SRS Board will need to be reviewed to incorporate the changing size of the organisation. NCC will need to align their existing arrangements for ICT audit into this process."

2. AUDIT UNIVERSE

2.1.1. The SRS audit universe is shown below:



3. RISK ASSESSMENT

3.1.1. We determined the frequency of audit review for each auditable unit, taking into account our assessment of the risk and control environment for each unit, including the activities that comprise each of these, in accordance with the methodology set out in Appendix 3.

Ref	Auditable Unit / Risk Overview	Risk Category	Risk Indicator	Review Frequency
CC	**Cross-cutting**			
CC	Information Security Management (Service Design)	**Critical**	**1**	Annual
	Failure to ▪ ensure the confidentiality, integrity and availability of information, data and IT services if appropriate technical and organisational measures have not been designed. ▪ ensure that all security mechanisms are subject to regular testing. ▪ review security measures and procedures at an appropriate frequency with the result that they are no longer in line with the risk perceptions of the business and they are not regularly maintained and tested. ▪ ensure key process elements exist e.g. Availability/ITSCM/Security Testing Schedule; Event Filtering and Correlation Rules; Information Security Policy; Information Security Report; Security Advisories; Security Alerts; Security Management Information System (SMIS); Test Report; Underpinning Information Security Policy. Security incidents are not effectively managed and the impact of a security breach is not minimised.			
CC	IT GOVERNANCE	**Significant**	**2**	2 Years
	Ineffective performance management framework at all levels. IT is not viewed as a strategic enabler. Lack of: ▪ a clear vision, strategic plan, understanding as to how the SRS supports / enables the achievement of objectives, investment return on the IT spend. ▪ communication and accountability resulting in the SRS failing to provide the required types and levels of service based on the IT investment. Leadership is not sufficient to enable and sustain alignment of the SRS and partner objectives. Limited resources are not focused on doing the right things at the right time. Role / responsibilities of the SRS to achieve objectives are not properly identified / defined.			
CC	FINANCIAL MANAGEMENT FOR IT SERVICES (Service Strategy)	**Significant**	**2**	2 Years
	Capacity Management does not feed through changes in IT capacity requirements and are not reflected in the costs. Failure to ▪ assign IT Service costs fairly and proportionally to users of the service. ▪ budget effectively resulting in poor control over IT expenditure and increased risk of overspending and unreliable budget predictions where actual costs are not compared with predicted costs. ▪ provide accurate and cost effective stewardship of the IT assets and resources used in providing IT Services. Lack of ▪ IT accounting resulting in the inability to gauge the efficiency of the IT service provision;			

Ref	Auditable Unit / Risk Overview	Risk Category	Risk Indicator	Review Frequency
	determine areas in which costs could be saved; provide financial transparency and aid management decision making. ▪ Key Performance Indicators (KPIs) [do predicted budgets match actual expenditure? does management feel more confident in their ability to predict costs in IT planning?] resulting in the inability to assess whether financial management for IT services has been successfully deployed. Service Level Management does not provide the key information regarding required service levels and therefore an inaccurate basis for calculations. The costs expended in providing the IT Services negotiated and agreed in the service level agreement (SLA) are not planned, controlled and recovered.			
CC	RISK CALCULATION & MANAGEMENT (Service Design)	**Moderate**	**3**	3 Years
	Failure to: ▪ identify Risk Owners and determine, implement and maintain the required risk mitigation measures. ▪ monitor the progress of implemented counter measures and taking corrective action where necessary. Lack of a: ▪ Business Impact and Risk Analysis and resulting 'Risk Register' (prioritised list of risks) resulting in the non-identification of risks to be managed and addressed by risk mitigation measures. ▪ defined Risk Management framework, no specification of how risk is quantified, what the risk appetite is, and who is in charge of Risk Management. ▪ process and asset valuation resulting in an ineffective Risk Analysis as the value of the process / asset to the business is not known. ▪ Risk Management Policy resulting in the business approach to managing risk not being described / communicated. Risks to the assets of the business are not identified, assessed and controlled.			
CC	STRATEGY MANAGEMET FOR IT SERVICES (Service Strategy)	**Significant**	**2**	2 Years
	Failure to: ▪ gather the business planning information from clients & external service providers resulting in the ability to devise an effective Service Strategy. ▪ perform a Strategic Service Assessment (SSA) resulting in a lack of knowledge in respect of the service provider (weaknesses, strengths, opportunities) within its current market resulting in the wrong set of services being offered. Lack of: ▪ a Strategic Action Plan setting out the steps required to implement the defined Service Strategy resulting in tasks / responsibilities not being adequately defined / assigned and a failed implementation / execution of the initiatives in the strategy. ▪ an IT Steering Group resulting in no set direction and Service Strategy; no review of the business and IT strategies resulting in a misalignment. ▪ Key Performance Indicators (KPI's) resulting in the inability to assess the success of the Service Strategy. Service Strategy is not derived from a SSA, resulting in the failure to define: the overall goals to be pursued; the services to be offered to customers; and translate customer needs into a distinctive and cost effective set of capabilities / resources to satisfy those needs.			
BC	**Business Change**			

Ref	Auditable Unit / Risk Overview	Risk Category	Risk Indicator	Review Frequency
BC	SERVICE PORTFOLIO MANAGEMENT (Service Strategy)	**Moderate**	3	3 Years
	Failure to: ▪ assess the Service Portfolio at regular intervals and ensure that the service provider is offering economically viable services aligned to the Service Management Strategy with the result that the Service Portfolio is out of date. ▪ define the desired outcomes of a new / changed service, analyse the impact on existing services in the Service Portfolio, and determine the assets required to offer the service. ▪ manage the service portfolio and ensure that the right mix of services exist to meet required business outcomes at an appropriate level of investment. ▪ monitor the achievement of expected returns. ▪ preserve essential records and assets when the service has reached end of life.			
BC	DEMAND MANAGEMENT (Service Strategy)	**Moderate**	3	3 Years
	Failure to: ▪ identify a 'Demand Manager'. ▪ understand, anticipate and influence customer demand for services. ▪ work with Capacity Management resulting in the service provider not having sufficient capacity to meet the required demand. Lack of Patterns of Business Activity (PBA's) [workload profiles describing the demand for particular services] resulting in the failure to anticipate and influence service demand.			
BC-BM	CCTV	**Moderate**	3	3 Years
	23 Jun 2014 - SUBSTANTIAL ▪ Data Loss. ▪ Provision of the Service(s) without a SLA. ▪ Service is not sufficiently resourced. ▪ The CCTV arrangements do not deliver an effective service and/or meet external requirements (DPA Code of Practice). ▪ The Control Room is not operating effectively and in accordance with set procedures.			
BC-BM	SOFTWARE ASSET MANAGEMENT	**Moderate**	3	3 Years
	Failure to: ▪ effectively manage, control and protect software assets and the information about related assets needed in order to manage the software assets through all stages of their lifecycle. ▪ reduce IT expenditure, human resource overhead and the compliance risks inherent in owning and managing software assets. Lack of proven processes and procedures for managing and optimising the businesses IT assets.			
BC-BM	SERVICE CATALOGUE MANAGEMENT (Service Design)	**Moderate**	3	3 Years
	Failure to provide a single source of consistent information on all agreed services and ensure that it is widely available to those approved to access it. Lack of a Service Catalog or the existence of one that does not contain accurate information (current details, status, interfaces & dependencies) on all operational services and those being prepared to be run operationally.			
BC-BM	SUPPLIER MANAGEMENT (Service Design)	**Moderate**	3	3 Years

Ref	Auditable Unit / Risk Overview	Risk Category	Risk Indicator	Review Frequency
	Failure to: ▪ ensure key process elements exist e.g. Supplier and Contract Management Information System; Supplier and Contract Review Meeting Minutes; Supplier Evaluation; Supplier Service Level Report; Supplier Strategy; Underpinning Contracts. ▪ ensure that all contracts with suppliers support the needs of the business, and that all suppliers meet their contractual commitments. ▪ ensure/verify that the contractually agreed performance is actually delivered, and define improvement measures where required. ▪ evaluate prospective suppliers in accordance with the Supplier Strategy with the result that the most suitable supplier is not selected. Lack of: ▪ a binding contract with a supplier. ▪ a contract renewal process with the result that some contracts may not be relevant and not terminated when no longer needed. ▪ a Supplier and Contract Management Information System (SCMIS). ▪ guidance and standards for the procurement of services / products.			
BC-BM	FACILITIES MANAGEMENT (Service Operation)	**Moderate**	**3**	3 Years
	Failure to manage the physical environment in which the IT infrastructure is located.			
BC-PO	PROJECT MANAGEMENT / TRANSITION PLANNING & SUPPORT (Service Transition)	**Significant**	**2**	2 Years
	Failure to consider all aspects of a new or changed service, make plans for the transition of a service to the LIVE environment and coordinate the required resources. Service requirements (in the form of Service Design Package) don't arrive into service operation.			
BC-PO	PROJECT & PORTFOLIO MANAGEMENT	**Significant**	**2**	2 Years
	Failure to: ▪ ensure that the 'right' projects are done in the 'right' way with optimal resource allocation. ▪ facilitate the outcome(s) customers want and deliver 'value'. ▪ make the right investment decisions resulting in less benefits than expected or unnecessary and wasted expenditure being incurred. Lack of a clear business case for a new / changed service.			
BC-PO	BUSINESS ELATIONSHIP MANAGEMENT (Service Strategy)	**Moderate**	**3**	3 Years
	Failure to achieve a mutual understanding of the business and IT, take advantage of new opportunities, properly evaluate investments, align provider services to business need if there is no Business Relationship Manager or they are not involved in the ITiL processes they should be e.g. Service Portfolio Management, Demand Management, and Financial Management. There is no documented customer portfolio, customer agreement portfolio or they are not up to date or linked to the service portfolio / service catalogue.			
EA	**Enterprise Architecture**			

Ref	Auditable Unit / Risk Overview	Risk Category	Risk Indicator	Review Frequency
EA	COMPLIANCE MANAGEMENT (Service Design)	**Moderate**	**3**	3 Years
	Failure to: ▪ allocate the responsibility for ensuring standards and guidelines are followed to a compliance manager or equivalent. ▪ conduct compliance reviews and document the results of process / system compliance assessments and any deviations from compliance requirements. IT services, processes and systems fail to comply with enterprise policies and legal requirements. Lack of: ▪ a Compliance Register resulting in a lack of knowledge of compliance requirements and the measures applied to ensure their enforcement. ▪ enterprise policies and regulations required in order for the compliance management process to operate.			
EA	DESIGN COORDINATION (Service Design)	**Moderate**	**3**	3 Years
	A service design policy does not exist or fails to provide guidance on: how to ensure a consistent approach is applied to all design activities; specifying which projects / changes are required to undergo formal Service Design and who needs to be involved. Failure to coordinate all the service design activities, processes and resources resulting in inconsistent and ineffective IT services, service management information systems, architectures, technology, processes, information and metrics. Service Design Packages are not built upon the Service Level Requirements; do not specify the requirements from the client viewpoint; do not defines how they will be fulfilled from a technical and organisational point of view.			
EA	QUALITY MANAGEMENT	**Moderate**	**3**	3 Years
	Failure to ensure that all work carried out is of a suitable quality to reliably meet business objectives / service levels. Lack of a complete set of quality standards, procedures and responsibilities.			
EA	IT SERVICE CONTINUTIY MANAGEMENT ITSCM (Service Design)	**Significant**	**2**	2 Years
	Failure to: ▪ ensure key process elements exist e.g. Availability/ITSCM/Security Testing Schedule; Business Continuity Strategy; Disaster Recovery Invocation Guideline; Index of Disaster Relevant Information; IT Service Continuity Report; IT Service Continuity Plan; IT Service Continuity Strategy; Recovery Plan; Test Report. ▪ ensure that all preventative measures and recovery mechanisms for disaster events are regularly tested. ▪ ensure that: IT staff with responsibilities for fighting disasters are aware of their duties; all relevant information is readily available when a disaster occurs. ▪ manage risks that could seriously impact IT services. Inability to reduce the risk from disaster events to an acceptable level and plan the recovery of IT services, thus not always being able to provide the minimum agreed Service Levels. Lack of ITSCM review resulting in the possibility that disaster prevention measures are not in line with risk perceptions from the business side, and continuity measures and procedures may be ineffective if not regularly maintained and tested.			
EA	CAPACITY MANAGEMENT (Service Design)	**Moderate**	**3**	3 Years

Ref	Auditable Unit / Risk Overview	Risk Category	Risk Indicator	Review Frequency
	Failure to: ▪ consider all resources required to deliver the IT service, and plans for short, medium and long term business requirements. ▪ ensure that the capacity of IT services and the IT infrastructure is able to deliver the agreed service levels in a cost effective and timely manner. ▪ manage, control and predict the performance and capacity of operational services with the result that they do not meet agreed targets. ▪ manage, control and predict the performance, utilisation and capacity of IT resources and individual components. ▪ provide other Service Management processes and IT Management with information related to service and resource capacity, utilisation and performance. ▪ translate business needs / plans into capacity and performance requirements for services and IT infrastructure, and ensure that future capacity and performance needs can be fulfilled. Lack of key Capacity Management process elements e.g. Capacity Management Information System, Capacity Plan, Capacity Report, Event Filtering and Correlation Rules.			
EA	AVAILABILITY MANAGEMENT (Service Design)	**Moderate**	**3**	3 Years
	Availability, resilience and recovery mechanisms are not subject to regular testing with the result that they may not work or be effective when called upon. Failure to: ▪ define, analyse, plan, measure and improve all aspects of the availability of IT services. ▪ design the procedures and technical features required to fulfil the agreed availability targets. ▪ ensure key process elements exist e.g. Availability Design Guidelines; Service Desk Availability Guidelines; Availability Management Information System; Availability Plan; Availability/ITSCM/Security Testing Schedule; Event Filtering & Correlation Rules; Maintenance Plan/SOP; Recovery Plan; Technical/Administration Manual; Test Report. ▪ ensure that all IT infrastructure, processes, tools, roles etc. are appropriate for the agreed availability targets. ▪ provide information related to service and component availability (e.g. comparison of achieved vs agreed availability, identified areas where availability improvement is required) to other Service Management processes and IT Management.			
EA	TECHICAL MANAGEMENT (Service Operation)	**Moderate**	**3**	3 Years
	Lack of technical expertise and support for the management of the IT infrastructure.			
EA-IE	ARCHITECTURE MANAGEMENT (Service Design)	**Moderate**	**3**	3 Years
	Application Frameworks do not promote the re-use of components and the standardisation of technologies on which applications are based. Failure to define: ▪ / document the Enterprise Architecture (the essential components of the business and interrelationships) covering the Business, Information, Application and Technology domains. ▪ a blueprint for the future development of the technological landscape.			
EA-IE	STORAGE (Data) MANAGEMENT	**Moderate**	**3**	3 Years
	Data loss and legislative breaches. Lack of an inventory of storage (and related) resources or deployment map. Storage system is not efficient, secure or cost effective resulting in present / future business needs not being met. Wasted expenditure.			
EA-AS	RELEASE & DEPLOYMENT MANAGEMENT (Service Transition)	**Moderate**	**3**	3 Years

Ref	Auditable Unit / Risk Overview	Risk Category	Risk Indicator	Review Frequency
	Failure to ▪ build, test and deliver services to the customers specified service design. ▪ deploy releases into operation and establish effective use of a service and deliver value to the customer. ▪ ensure the integrity of a release package and its constituent components throughout the transition activities resulting in them not being accurately recorded in the configuration management system. ▪ effectively transfer knowledge resulting in customers / users not being able to optimise their use of the service to support their business activities. ▪ transfer skills and knowledge to operations and support staff with the result that they cannot effectively and efficiently deliver, support and maintain a service according to required warranties and service levels.			
EA-AS	APPLICATION DEVELOPMENT (Service Transition)	Moderate	3	3 Years
	Applications and systems fail to provide the required functionality for IT services. End-users do not have adequate documentation describing how to use the application / system. Lack of adequate documentation to run and maintain a type of application or infrastructure component.			
EA-AS	APPLICATION MANAGEMENT (Service Operation)	**Significant**	**2**	2 Years
	Failure to: ▪ develop the skills required to operate the applications and effective employee training plans if there is no skills inventory identifying the skills required to deliver IT services, or the individuals possessing those skills. ▪ manage applications through their lifecycle i.e. Application requirements are not gathered or are not based on business need; the requirements are not translated into specifications / components required; the built application is not what was specified; with the result that: they are deployed even though they have not been sufficiently designed, tested; the service required by the business is not delivered; operational and management costs increase.			
EA-AS	SERVICE VALIDATION & TESTING (Service Transition)	**Moderate**	**3**	3 Years
	Failure to ▪ ensure that deployed Releases and the resulting services meet customer expectations, and that IT operations are able to support the new service. ▪ specify how a Release will be tested and quality assured (testing concept and specific test cases to be used during Service Validation are not defined). ▪ ensure that only components which meet stringent quality criteria are allowed to enter the intensive testing phase, or are deployed into the live productive environment. ▪ ensure that all conditions for a new service to be activated are met, and obtain a binding consent from the customer that the new service fulfils the agreed Service Level Requirements.			
SM	**Service Management**			
SM	PERFORMANCE MANAGEMENT	**Significant**	**2**	2 Years
	Failure to ensure that the technical resources in the infrastructure provide the best possible value for money and that they are behaving in the manner assumed / described in the technical documentation.			
SM	IT OPERATIONS MANAGEMENT (Service Operation)	**Moderate**	**3**	3 Years
	Ineffective day-to-day maintenance and management of the IT infrastructure resulting in the failure to deliver the agreed level of IT services to the business / customers.			
SM	KNOWLEDGE MANAGEMENT (Service Transition)	**Moderate**	**3**	3 Years

Ref	Auditable Unit / Risk Overview	Risk Category	Risk Indicator	Review Frequency
	Failure to: - ensure that all information used within Service Management, is stored in a Service Knowledge Management System and that it is consistent and readily available. - gather, analyse, store and share knowledge and information within the business resulting in the inability to improve efficiency as 'knowledge' has to be rediscovered.			
SM	SERVICE LEVEL MANAGEMENT (Service Design)	**Moderate**	**2**	3 Years
	Failure to: - capture, document and initially evaluate the desired outcomes (customer requirements) for new services / major service modifications with the result that alternatives are not sought at an early stage for those requirements not technically or economically feasible. - ensure that contracts are only signed off after completion of Service Transition; that Service Acceptance Criteria are fulfilled; OLAs are signed off by their Service Owners and the SLA signed off by the customer. - ensure that Operational Level Agreements and Underpinning Contracts are appropriate. - negotiate SLAs with customers and design services in accordance with the agreed SLAs. Lack of a Service Level Report which monitors / reports on achieved service levels and compares them with agreed service level targets.			
SM-CR	SERVICE DESK	**Moderate**	**3**	3 Years
	Inability to resolve incidents without escalation resulting in poor customer satisfaction, increased 'fix time' costs and operating inefficiency. Failure of the service desk to understand business needs and customer requirements. Service Desk staff are not sufficiently trained leading to the slow turnaround of customer / user requests, the incorrect categorisation and prioritisation of service requests. Function does not have agreed service levels / metrics and these are not regularly reviewed / collected.			
SM-CR	INCIDENT MANAGEMENT (Service Operation)	**Moderate**	**3**	3 Years
	Disruption to other staff Failure to: - reduce the impact on the business (e.g. a full disk will prevent printing, saving work and copying files) - restore the service to the customer in a prompt timeframe. Forgotten, incorrectly handled, or badly managed incidents. Incidents are not logged, recorded, managed / escalated, and resolved. Inefficient use of support staff making them less effective Lack of coordinated management information resulting in the inability to provide service quality information to customers. Reassessment of incidents from first principles rather than referring to existing solutions in a knowledge database.			
SM-CR	PROBLEM MANAGEMENT (Service Operation)	**Moderate**	**3**	3 Years

Ref	Auditable Unit / Risk Overview	Risk Category	Risk Indicator	Review Frequency
	Absence of detailed data on incidents Failure to: ▪ link incident records with problem/error records. ▪ set aside time to build and update the call log or incident sheets which will restrict the delivery of benefits. Inability to determine accurately the impact on the business/organisation of incidents and problems; with critical incidents / problems not given the correct priority. Lack of management or leadership commitment, so that support staff cannot allocate sufficient time to structural problem solving activities. Poor incident control process Service Desk is dealing with multiple reports of incidents and the technician is not fully aware of the extent of the problem.			
SM-CR	EVENT MANAGEMENT (Service Operation)	**Moderate**	3	3 Years
	Failure to: ▪ collected event data if monitoring and control systems based on monitoring tools (active or passive) are not established resulting in failed or delayed detections e.g. incidents, . Increased expense and resource use if real time monitoring is used to monitor activity that could be monitored by exception using Event management. Ineffective service operation if the status of the infrastructure is not known and 'events' are not detected. Lack of: ▪ operational information if actual performance and behaviour is not compared against design standards and SLA's. ▪ understanding of what types of event need to be detected.			
SM-CR	EMPLOYEE PROVISIONING MANAGEMENT	**Moderate**	4	3 Years
	The provision to employees of the required technology tools (computers, phones, tablets, printers, software, application access etc.) and involves the scope areas (Onboarding, Moves & Changes, Self Service, Offboarding). Failure to: ▪ automate provisioning tasks and allow the reassignment of IT staff for higher value work. ▪ eliminate rework for your IT staff, incident calls related to the scope processes and execute requests flawlessly. New employees of the partners are unable to start working fully from the first day. Partner is unable to be as productive, effective, competitive and agile as possible.			
SM-CR	REQUEST FULFILMENT (Service Operation)	**Moderate**	3	3 Years
	Failure to: ▪ handle requests differently to incidents. ▪ source and deliver the components of requested standard services. Lack of defined metrics resulting in the inability to judge the effectiveness and efficiency of the process. The process does not vary according to the type of request; is not geared to the use of self-help practices for the generation of service requests. Users: ▪ / customers unaware of the availability of services and the procedure for obtaining them. ▪ do not have adequate channels to request & receive standard services and cannot therefore improve their productivity or the quality of business services and products.			
SM-CR	SERVICE ASSET & CONFIGURATION MANAGEMENT	**Moderate**	3	3 Years

Ref	Auditable Unit / Risk Overview	Risk Category	Risk Indicator	Review Frequency
	(Service Transition)		🟩	
	Failure to: ▪ account for, manage and protect the integrity of service assets and configuration items through the service lifecycle where unauthorised components are used and unauthorised changes made. ▪ identify, control, record, report, audit and verify service assets and configuration items. ▪ optimise the performance of service assets and provide a visible and accurate representation of a service, release or an environment resulting in poorly planned changes / releases, poor incident / problem resolution, non-delivery of service levels, non-conformances to standards, legal and regulatory obligations, untraceable changes, inability to identify service costs. ▪ provide accurate and correct configuration management to assist decision making and higher numbers of quality and compliance issues. Lack of an accurate and complete configuration management system.			
SM-CR	ACCESS / IDENTITY MANAGEMENT (Service Operation)	**Moderate**	**3**	3 Years
	Failure to: ▪ ensure that the right to use a service is only granted to authorised users and that they only have access to the service(s) needed to carry out their job/role effectively. ▪ protect Confidentiality, Integrity and Availability of data and intellectual property e.g. not removing access when users change roles / jobs, not regularly auditing permissions to ensure they are correct. Inability to provide required data for forensic / other investigations. Lack of regulatory compliance, Unskilled users may cause errors in critical services.			
SM-CP	CHANGE MANAGEMENT (Service Transition)	**Moderate**	**3**	3 Years
	Failure to: ▪ handle changes efficiently and promptly if the methods and procedures used are not standardised resulting in unauthorised changes; unplanned outages; low change success rate; high number of emergency changes; and delayed project implementations. ▪ respond to the changing business requirements of customers; maximise value or reduce incidents. The Configuration Management System is not accurate and effective if changes to service assets and configuration items are not recorded.			
SM-CP	CHANGE EVALUATION (Service Transition)	**Moderate**	**3**	3 Years
	Failure to assess major changes (introduction of a new service, substantial change to an existing service) before the change is allowed to proceed. Formal Change evaluation results are not captured in a Change Evaluation Report.			
ES	**Education Services**			

Key to Risk Indicator and Frequency of Internal Audit Work

Risk Category	Risk Indicator	Review Frequency	Number in Assessment
Critical	1	Annually	1
Significant	2	Every 2 Years	9
Moderate	3	Every 3 Years	32
Minor	4	Every 4 Years	1
Negligible or N/A	-	Not included in Plan or reliant on external review	

4. 3 YEAR INTERNAL AUDIT PLAN

4.1.1. The following table sets out the internal audit work planned for 2017-18 (in detail) and 2018-19, 2019-2020 (in summary). The plan is cross-referenced to the SRS Key Priorities and Risk Register, as set out in Appendix 1.

Ref	Auditable Unit / Risk Indicator	Plan Days	Priority / Risk Ref	Focus / Scope
17/18				
BC-BM-7801	CCTV / Control Room	5	PS5, PS6, BP3, 10	Follow up of the 16/17 Audit
BC-BM-7802	Back Office	5	PS2,	Follow up of the 16/17 Audit
CC-7801	Cybersecurity	20	PS1, PS5, PS6, 35, CRR 2	MCC Commissioning Paper GPA Commissioning Paper
CC-7802	ISO27001	15	PS1, PS5, PS6, 35, CRR 2	External Accreditation Requirement
CC-7803	Information Technology Governance	8	PS3, PS4, PS5, PS6, PS7, PS8, BP1, BP4, 6, 8, 9, 10, 21, 25, 30, 31, R_1, R_2	Follow up of the 16/17 Audit
EA-7801	IT Service Continuity Management ITSCM	20	PS1, PS5, PS6, BP3, 35, CRR 2	MCC Commissioning Paper TCBC Audit Cycle
EA-AS-7801	Application Development / Management	5	PS1, PS4, PS6, PS9, BP1, BP3, BP4, 35, 16, 23, R_1	Follow up of the 16/17 Audit
EA-IE-7801	Email	5	PS1, PS5, PS6, PS9, BP2,	Follow up of the 16/17 Audit
EA-IE-7802	Architecture Management (Service Design) Inc. Cloud – One Wales	30	PS1, PS3, PS5, PS6, PS9, BP1, BP2, BP4, 10, 16, 23, R_2	Examine the adequacy and effectiveness of partner efforts to integrate systems architecture and administration and realise efficiencies from systems on a single platform. MCC Commissioning Paper TCBC Commissioning Paper GPA Commissioning Paper
SM-7801	Performance Management	15	PS1, PS3, BP1, BP3, BP4, 1, 22, 8, 9, 10, 16, 23, 25	Audit of the degree to which: ▪ the SRS performance targets and critical success factors are sufficient and met; ▪ customer SLAs operate and design services accordance with the agreed SLAs;

Ref	Auditable Unit / Risk Indicator	Plan Days	Priority / Risk Ref	Focus / Scope
				▪ Operational Level Agreements and Underpinning Contracts are appropriate; ▪ service levels are reported and delivered to the agreed service level targets; ▪ the desired outcomes (customer requirements) for new services / major service modifications are captured, documented and initially evaluated. TCBC Commissioning Paper
	Total	**128**		
18/19				
BC-BM-8901	Supplier Management (Service Design)	15	PS1, PS3, PS6, PS7, BP1, 8, 10	Audit to evaluate ▪ whether binding contracts with suppliers exist where required and they support the needs of the business, and suppliers meet their contractual commitments; ▪ the effectiveness of the Supplier Contract Management Information System (SCMIS); ▪ the guidance and standards for the procurement of services / products is adequate; ▪ whether prospective suppliers accordance with the Supplier Strategy and result in the most suitable supplier being selected; ▪ whether contractually agreed performance is delivered, and improvement measures are defined where required; ▪ the effectiveness of the contract renewal process to ensure all contracts are relevant and terminated when no longer needed; ▪ whether key process elements exist e.g. Supplier and Contract Management Information System; Supplier and Contract Review Meeting Minutes; Supplier Evaluation; Supplier Service Level Report; Supplier Strategy; Underpinning Contracts;
CC-8901	Cybersecurity	5	PS1, PS5, PS6, 35, CRR 2	Follow up of the 17/18 Audit
CC-8902	Mobile / Smart / Bring Your Own Device (BYOD) Devices	25	PS1, PS3, PS4, PS6, BP2, BP3, BP4, CRR 2,	MCC Commissioning Paper GPA Commissioning Paper
CC-8903	ISO27001	15	PS1, PS5, PS6, 35, CRR 2	External Accreditation Requirement
EA-8901	IT Service Continuity Management ITSCM	5	PS1, PS5, PS6, BP3, 35, CRR 2, 10	Follow up of the 17/18 Audit

Ref	Auditable Unit / Risk Indicator	Plan Days	Priority / Risk Ref	Focus / Scope
EA-IE-8901	Architecture Management (Service Design)	5	PS1, PS3, PS5, PS6, PS9, BP1, BP2, BP4, 10, 16, 23, R_2	Follow up of the 17/18 Audit
EA-IE-8902	Virtualisation	15	PS3, PS5, PS7, PS9, BP1, BP3, 8, 9, R_2	Audit of the control environment following the move to Hyper V.
SM-8901	IT Operations Management (Service Operation)	15	PS1, PS3, PS4, PS5, PS6, PS8, BP2, BP3, 35, 8, 10, 25, 31	An audit to assess the adequacy of IT Operations Management by undertaking a 'Service Operation Readiness Assessment'.
SM-8903	Performance Management	5	PS1, PS3, BP1, BP3, BP4, 1, 22, 8, 9, 10, 16, 23, 25	Follow up of the 17/18 Audit
SM-CR-8901	Access / Identity Management (Service Operation)	15	BP3, 30	Audit to evaluate whether: ▪ the right to use a service is only granted to authorised users and it is only that needed to carry out their job/role effectively; ▪ the Confidentiality, Integrity and Availability of data and intellectual property is protected; ▪ users have inappropriate access and have / could cause errors in critical services; regulatory compliance is ensured and the data required for forensic / other investigations is effectively provided;
	Total	**120**		
19/20				
BC-BM-9201	Supplier Management (Service Design)	5	PS1, PS3, PS6, PS7, BP1, 8, 10	Follow up of the 18/19 Audit
CC-9201	Mobile / Smart / Bring Your Own Device (BYOD) Devices	5	PS1, PS3, PS4, PS6, BP2, BP3, BP4, CRR 2,	Follow up of the 18/19 Audit
CC-9202	ISO27001	15	PS1, PS5, PS6, 35, CRR 2	External Accreditation Requirement
EA-9201	Compliance Management	15	CRR 2, 30	Audit to evaluate the degree to which: ▪ IT services, processes and systems comply with enterprise policies and legal requirements; ▪ knowledge of the compliance requirements and the measures applied to ensure their enforcement exist in a Compliance Register;

Ref	Auditable Unit / Risk Indicator	Plan Days	Priority / Risk Ref	Focus / Scope
				▪ compliance reviews are carried out and deviations managed; ▪ enterprise policies and regulations exist to allow the compliance management process to operate; ▪ the responsibility for ensuring standards and guidelines are followed is allocated and met.
SM-9201	IT Operations Management (Service Operation)	5	PS1, PS3, PS4, PS5, PS6, PS8, BP2, BP3, 35, 8, 10, 25, 31	Follow up of the 18/19 Audit
SM-CR-9201	Access / Identity Management (Service Operation)	5	BP3, 30,	Follow up of the 18/19 Audit
	Total	**50**		

5. APPENDIX 1: KEY STRATEGIC PRIORITIES AND RISKS.

5.1.1. The SRS's key strategic priorities and risks are reflected in the:

- **SRS Partner Strategy 2016-2020**

Ref	Strategic Priority
PS1	To be an organisation that delivers great digital services / solutions to its partners using open standards through a cloud model and a standard service catalogue of commodotised services and integrated provision.
PS2	To move staff from reactive services into proactive, disruptive ones.
PS3	To increase the value for money (as defined from the customer point of view) delivered.
PS4	To focus the partner investment in technology to achieve corporate priorities.
PS5	Deliver effective ICT services from a single combined unit.
PS6	Improve services to provide a solid foundation upon which partner organisation's can operate.
PS7	Ensure the investment in ICT is focused on delivery of the corporate priorities of the partner organisations'.
PS8	Develop a capable, professional workforce that can meet the challenges within ICT over the coming years.
PS9	Provide a collaborative platform for public sector organisation's to share common ground.

- **SRS Business Plan 2016-17**

Ref	Aim / Priority
BP1	To develop a 3 to 5 year roadmap that the SRS and its strategic partners can use to develop options which exploit the latest technologies / methodologies and support public sector innovation.
BP2	To operate as a flexible, agile and integrated platform.
BP3	To deliver highly available systems and delight our customers. ▪ Improve the core service. ▪ Implement a supportive organisational structure. ▪ Improve customer service and reduce the amount of time customers wait for a resolution.
BP4	To deliver business value through the implementation of new ideas and maximise the investment made in existing technologies. ▪ Implement an agile project management structure ▪ Implement a supportive organisational structure

	- Build the 3-5 year roadmap - Deliver the commissioned project items

- **Risk Registers**

Ref	Risk Description
Torfaen	
35	Failure to provide services through any complete failure of critical IT systems for longer than 48 hours.
Blaenau Gwent	
CRR 2	The ICT provision supporting Council services is not resilient and fails to provide assurance requirements in terms of operational functionality and data security. Medium to long terms loss of IT systems.
Gwent Police Authority	
4824	GPA / SWPA issues with uploading force records to the PND (GPA 9 months behind) so forces carrying out searches do not have accurate and up to date information. An FTP solution sends and collects files to/from South Wales for the STORM system automatically but access is limited and it cannot be loaded. Extractions are incomplete / inaccurate e.g. number of arrests since Niche went live.
Monmouth	
Shared Resource Service	
1, 22,	Failure of the service level agreement process due to a lack of partner organisation input.
2	Failure of the change management process in managing the addition of a new partner.
3, 4,	Failure to fully anticipate the full cost(s) e.g. infrastructure, employee skilling, of taking on an additional partner.
6	Lack of required capacity to deal with the addition of a new partner.
8	Failure to effectively manage the resources of the SRS.
9	Failure to implement a structure aligned to a Core/Projects split; to deliver a robust and reliable service to the partner organisation's which is costed appropriately.
10	Failure to effectively manage partner requirements of the SRS.
16, 23,	Failure to deliver high value collaboration opportunities (with a roadmap) due to the partners not specifying collaboration needs.
17, 18	The opportunity cost of having to return a resource to the configuration required by its landlord.

19, 20,	Failure to benchmark and improve due to funds not being available.
21	Failure to prioritise work demands.
25	Failure to deliver the strategy due to the need to meet savings targets.
30	Failure to meet the reporting requirements of partners due to the configuration of the system / tools available.
31	Failure to demonstrate the effectiveness of operation and the delivery of stated business benefits due the measures in existence being deficient.
R_1	The commissioning statements do not specify the required business strategy.
R_2	The SRS cannot deliver against the strategy requirements.

6. APPENDIX 2: RISK ASSESSMENT CATEGORIES

6.1.1. We assessed the risk of each auditable unit, based on inherent and control risk factors and materiality considerations, including their potential impact on achievement of the SRS / Partner's priorities.

6.1.2. We categorised the risk of each auditable unit and the activities that comprise them as follows:

Risk Category	**Potential Impact**
Critical	▪ impact on the SRS's operational performance; or ▪ monetary or financial statement impact; or ▪ consequences or material fines from breach in laws and regulations; or ▪ impact on the reputation of the SRS, which could threaten its future viability.
Significant	▪ impact on the SRS's operational performance; or ▪ monetary or financial statement impact; or ▪ consequences or significant fines from breach in laws and regulations; or ▪ impact on the reputation of the SRS/Partners.
Moderate	▪ impact on the SRS's operational performance; or ▪ monetary or financial statement impact; or ▪ consequences or fines from breach in laws and regulations; or ▪ impact on the reputation of the SRS/Partners.
Minor	▪ impact on the SRS's operational performance; or ▪ monetary or financial statement impact; or ▪ consequences or fines from breach in laws and regulations; or ▪ impact on the reputation of the SRS/Partners.
Negligible	▪ impact on the SRS's operational performance; or ▪ monetary or financial statement impact; or ▪ consequences or fines from breach in laws and regulations; or ▪ impact on the reputation of the SRS/Partners.

7. APPENDIX 3: DETAILED METHODOLOGY

Step 1 - Understand the SRS's Key Strategic Priorities and Risks

In developing our understanding of the SRS's strategic objectives and risks, we have:

- reviewed the SRS's strategic plan and the SRS / Partner Risk Registers
- drawn on our wider knowledge of the SRS
- met with the Key Contacts.

Step 2 - Define the Audit Universe

The internal audit plan reflects the SRS's operational and management structures. We have identified an audit universe for the SRS, which is made up of a number of auditable units. Auditable units can include service functions, processes and systems. Any processes or systems that apply SRS-wide are identified as single auditable units.

Step 3 - Assess the Risk and Control Environment

The internal audit plan focuses on the most risky areas of the SRS's business. We assessed the risk of each auditable unit, based on inherent and control risk factors and materiality considerations, including their potential impact on achievement of the SRS's priorities.

The risk assessment is determined by:

- mapping the SRS's identified Strategic Plan objectives to the auditable units
- mapping the SRS's identified risks to the auditable units
- our knowledge of the SRS's operating environment, and
- discussions with the SRS/Partner's senior management
- our knowledge of the SRS's internal control environment
- information obtained, where relevant, from other assurance providers
- the outcomes of previous internal audit reviews and improvement actions implemented.

Step 4 – Determine the Frequency of Audit Review

We determined the frequency of audit review for each auditable unit, taking into account our assessment of the risk and control environment for each unit, including the activities that comprise each of these. Our risk assessment considered both inherent and controls risks, in addition to the SRS's current key priorities and risks.

We have concluded, from our risk assessment and taking account of available audit resources, that we can provide audit coverage of every identified auditable unit (see Section 3) at an appropriate frequency within a 4-year timeframe. However, this is based on current circumstances and assumptions, and both the frequency and the longer-term timeframe may be revised as we revisit our risk assessment on an annual basis.

Step 5 - Determine the Audit Plan

We determined the timing and scope of audit work based on corporate priorities, available audit resources, discussions with Key Contacts and our knowledge of developments over the period of the SRS's business plan.

Step 6 - Other Considerations

We considered additional audit requirements to those identified from the risk assessment process.

These include:

- provision of annual assurance to external parties
- planned activities of external audit and inspection agencies;
- preparation of the SRS's Annual Governance Statement; and
- potential unplanned audit reviews and investigations.

The estimated resource requirements for these have been identified separately in the audit plan, as far as possible.