

SHARED RESOURCE SERVICE

Summary of Internal Audit Activity

2019 – 20 Year to date

Introduction

The purpose of this report is to:

- Advise of the progress to date with the current year's Audit Plan (2019 – 20);
- Provide details of the audits finalised in the period; and
- Raise any matters relevant to the Finance & Governance Board role.

Audit Plan 2019 - 20

With regard to the 2019 – 20 internal audit plan then:

STAGE	NUMBER	%AGE
NOT ISSUED (NID)	2	15.38
ISSUED (ISS)	6	46.16
COMPLETED (COM)	5	38.46

CODE	NARRATIVE
P	Planned
I	Issued
C	Completed

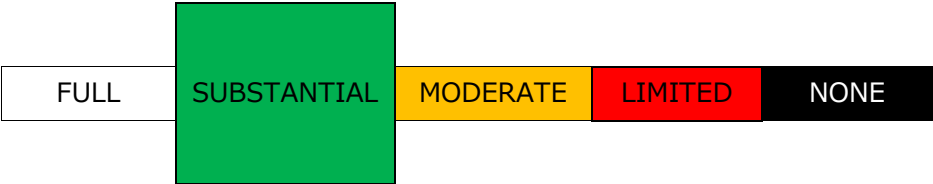
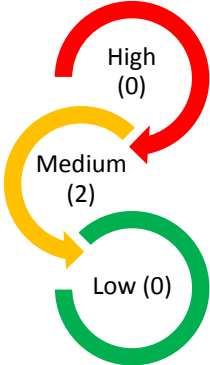
Ref	Stage	Type	Title	Quarter		
				P	I	C
SRS - 19003	COM	SYS	Enterprise Architecture Management	1	2	3
SRS - 19002	COM	SYS	Firewall	1	2	3
SRS - 19001	COM	SYS	IT Disposals	1	1	1
SRS - 19007	COM	FUP	Mobile Computing	4	3	3
SRS - 19008	COM	FUP	Supplier Management	3	3	3
SRS - 19010	ISS	SYS	CCTV / Control Centre	4	4	
SRS - 19006	ISS	FUP	Identity and Access Management	3	4	
SRS - 19011	ISS	SPL	Memorandum of Understanding ¹	3	3	
SRS - 19012	ISS	FUP	Performance Management	4	4	
SRS - 19004	ISS	SYS	Software Asset Management	2	3	
SRS - 19013	ISS	FUP	Virtualisation	4	4	
SRS - 19009	NID	SYS	Back Office ²	3		
SRS - 19005	NID	FUP	Cybersecurity ³	3		

¹ Delays in original report recommendation implementation dates prevents performance of the Business Continuity audit in the current year, so this was replaced with a special audit in respect of the Memorandum of Understanding which is awaiting officer action(s).

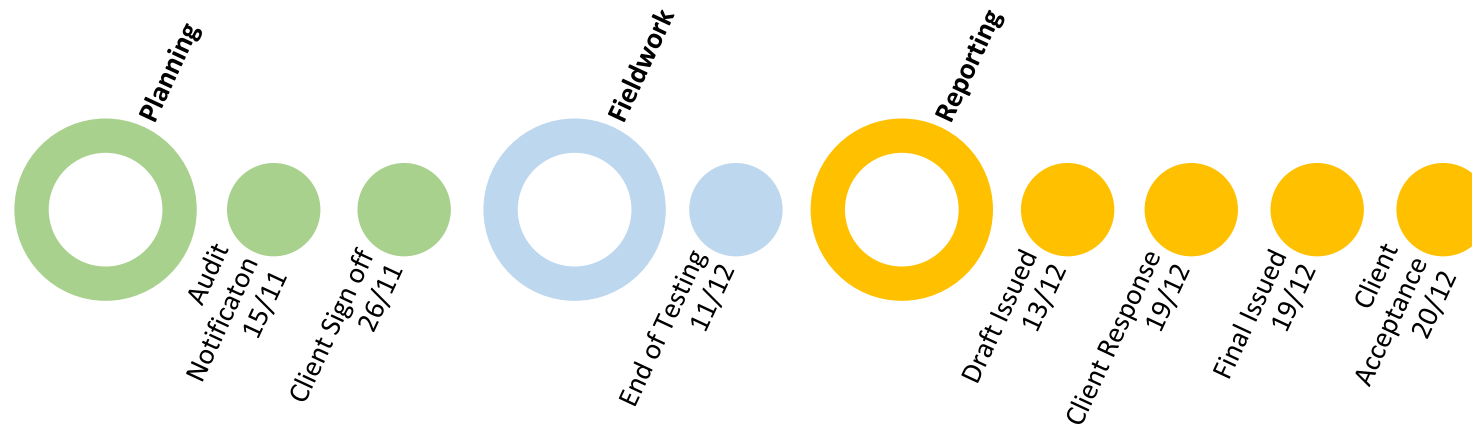
² Delays in the preceding plan audits has meant that this audit cannot be conducted in Qtr. 4 due to year end and will be undertaken in Qtr. 1 of 2020-21.

³ Rescheduled to 2020-21 due to the change in the dates of the IT Service Continuity Management audit (agreed August 2019 Finance and Governance Board) and the SIEM solution (ISLB) which impact significantly on the original actions.

Audits Completed in the Period

Audit Title: SRS – 19007 Mobile Computing	Audit Sponsor: Matt Lewis / Kathryn Beavan-Seymour	Final Report Issued: 19 December 2019
Assurance Opinion: 		Recommendations / Management Action(s) 

Audit Timeline: 36 days



ISS.2 - Mobile Strategy

Priority: Medium

Issue:

The mobile strategy that exists has only been issued internally and did not evidence approval by the SRS COO. Review showed that it does not reference removable media, data / device destruction, password management, and encryption.

The IT Disposal Policy that exists has a published status but does not reference software disposals.

Recommendation:

The Mobile Strategy needs to reference removable media, data/device destruction, password management, encryption and then be signed off by the SRS COO and issued.

The IT Disposal Policy needs to reference software disposals.

Management Response:

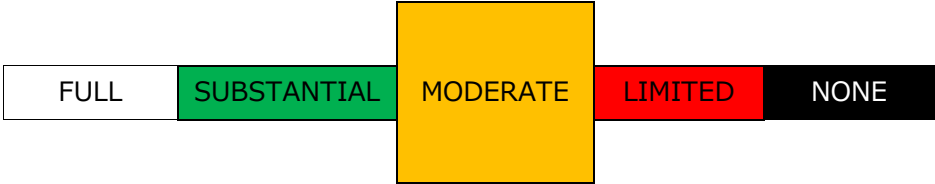
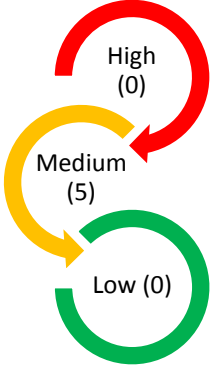
Agreed. A new process will be introduced to evidence the sign off/approval of all future policies/documentation. The Mobile Strategy and the IT Disposal Policy will be amended to address the aspects identified in the audit.

Mike Doverman

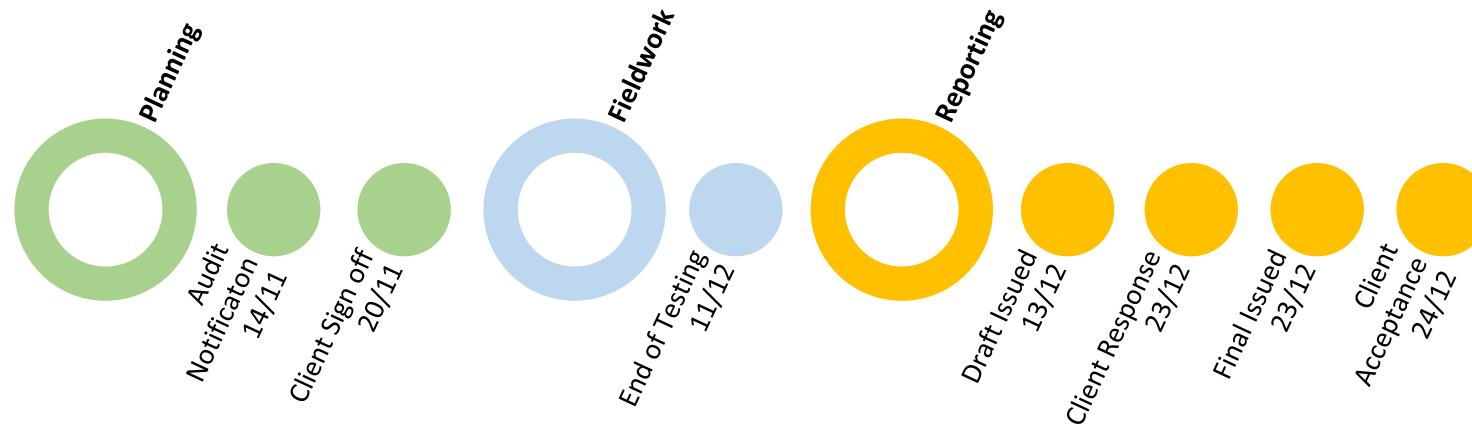
March 31, 2020

ISS.1 – Requirements Assessment		Priority: Medium
<p>Issue:</p> <p>The Information Security Team ISMS controls spreadsheet is blank, as such there is no evidence that the ISO requirement A.18.1.1 has been met.</p> <p>The lack of an MDM solution was added to the TCBC, BGCBC and MCC risk registers on Nov 18, 2019 (not May 2019) even though all Partners' have now adopted and have or are implementing an MDM solution.</p>	<p>Recommendation:</p> <p>A full (formal) assessment of all relevant statutory, regulatory and contractual requirements (and the current adherence situation) applicable to mobile computing should exist and be updated periodically. ISO27001 A.18.1.1.</p>	<p>Management Response:</p> <p>Agreed. A full (formal) assessment of all relevant statutory, regulatory and contractual requirements (and the current adherence situation) applicable to mobile computing will be produced.</p> <p>Mike Doverman</p> <p>February 29, 2020</p>

Audit Title: SRS – 19008	Audit Sponsor: Matt Lewis / Kathryn Beavan-Seymour	Final Report Issued: December 23, 2019
------------------------------------	--	--

Assurance Opinion: 	Recommendations / Management Action(s) 
--	--

Audit Timeline: 40 days



ISS.1 – Supplier Relationships

Priority: Medium

Issue:	Recommendation:	Management Response:
<p>The IS policy for supplier relationships (and associated supplier questionnaire) will be submitted to the Jan 2020 ISLB before being made LIVE. Review highlighted that it does not;</p> <ul style="list-style-type: none"> ▪ contain a distribution section, categorise suppliers (Strategic, Tactical, Operational, Commodity) ▪ link to other key documents that should exist (Supplier IS Agreement, Supplier IS Evaluation Process, Supplier Due Diligence Assessment Process, Cloud Computing Policy), ▪ contain an actual policy statement. <p>The questionnaire:</p> <ul style="list-style-type: none"> ▪ was issued to all suppliers not just those who have access to or could impact the information. ▪ doesn't contain wording to say that it represents a preliminary assessment of the security controls, from which a decision as to the level of physical audit required would be made, and that any deliberately false statements would be treated as a breach of contract/disqualify them from tendering services under the agreement and it doesn't 	<p>Prior to submitting the policy and questionnaire to the Jan 2020 ISLB, it should be amended to address the element identified in the issue.</p> <p>The questionnaire should:</p> <ul style="list-style-type: none"> ▪ in future only be issued to those suppliers who have or will have access to and be able to impact the information that exists; ▪ be amended to contain wording which highlights that it represents a preliminary assessment of the security controls, from which a decision as to the level of physical audit required would be made, and that any deliberately false statements would be treated as a breach of contract/disqualify them from tendering services under the agreement; ▪ also address relevant 3rd party security assessments. <p>Management needs to reassess and clarify its process for meeting the supply chain element of ISO27001 A.15.1.3.</p>	<p>Agreed. The policy and questionnaire will be submitted to the April 2020 ISLB after review/consideration of the information made available during the audit. Changes will be made where considered necessary e.g. introduce a supplier categorisation; a clear policy statement; address ISO27001:15.2 by including paragraphs on how Supplier Service Delivery will be monitored, reviewed and audited, and how changes to service by suppliers will be managed and the process for reassessing risks; clarifying current measures related to assessment of the supply chain.</p> <p>Given the nature of our procurement, we will continue to issue the questionnaire to all suppliers and not just those who have or will have access to and be able to impact the information that exists. It will be amended to contain wording which highlights that it represents a preliminary assessment of the security controls, from which a decision as to the level of physical audit required would be made, and that any deliberately false statements would be treated as a breach of contract/disqualify them from tendering services</p>

<p>mention or request any relevant 3rd party security assessments e.g. SAS 70, pentest.</p> <p>Regarding ISO27001 A.15.1.3, review of a sample of questionnaires showed that IS risks for ICT services could be captured/identified, but there is nothing reflecting IS risks for the supply chain and no supplier agreement was provided.</p>		<p>under the agreement.</p> <p>Mike Doverman</p> <p>March 31, 2020</p>
--	--	---

ISS.2 – Supplier Monitoring		Priority: Medium
<p>Issue:</p> <p>A review/audit of supplier service delivery is to be undertaken in December 2019, by the IS Team. Neither the Contract and Supplier Security Policy or any other procedure specifically addresses the monitoring, review, and audit of supplier service delivery.</p> <p>Nothing states that the approach will be based on the actual information at risk and linked to the supplier classification category e.g. starting with the Strategic ones.</p> <p>Management stated that there is no "mechanism" in place to identify changes in the provision of services by suppliers but para 5.1 of the policy (0050), states that on the contract anniversary, the business management team has to advise whether all the questionnaire answers are true or whether there are changes and the need for an updated questionnaire.</p>	<p>Recommendation:</p> <p>Prior to issuing policy 0050 as 'live' the opportunity should be taken to address within it the ISO27001:15.2.1, 15.2.2 requirements by:</p> <ul style="list-style-type: none"> ▪ specifying the arrangements/process for the monitoring, review and audit of supplier service delivery; ▪ clarifying the process for identifying and managing changes to the provision of services by suppliers, which will take account of the criticality of business information, systems and processes involved and re-assessment of risks; ▪ the policy specifying that the approach will be based on the actual information at risk and the supplier classification category; ▪ clarifying the conflicting view of Management (i.e. no "mechanism" in place to identify changes in the provision of services by suppliers) and para 5.1 of the policy (0050), which should identify changes but only on anniversary of the contract. 	<p>Management Response:</p> <p>Agreed. The policy will be amended to; specify the arrangements/process for the monitoring, review and audit of supplier service delivery; clarify the process for identifying and managing changes to the provision of services by suppliers; and specify that the approach will be based on the actual information at risk and the supplier classification category.</p> <p>Mike Doverman</p> <p>March 31, 2020</p>
ISS.3 – Contracts		Priority: Medium

<p>Issue:</p> <p>The current contracts register spreadsheet:</p> <ul style="list-style-type: none"> ▪ Is not sufficient as it does not contain all the fields expected; ▪ contains Proactis ID references that have no meaning/relevance; ▪ contains entries for suppliers for whom no contract exists e.g. (Caretower I.T Security Specialists, and Net-Ctrl Limited); 	<p>Recommendation:</p> <p>Management should consider:</p> <ul style="list-style-type: none"> ▪ revamping the current spreadsheet by adding in the necessary fields to meet the Cabinet Office requirements to produce a comprehensive and effective 'contracts register'; ▪ updating the contracts register through knowledge of existing (and necessary) contracts in place when a partner joins. 	<p>Management Response:</p> <p>Agreed. The contracts were not added to Proactis, and alternatives explored as we were informed that the use of Proactis would cease. A meeting has been requested with the Head of Procurement to clarify the Proactis situation. The outcome will result in the current spreadsheet being improved or an alternative solution implemented to provide a contract register.</p> <p>Annette Drew</p> <p>March 31, 2020</p>
<p>ISS.4 – Supplier Usage</p>		<p>Priority: Medium</p>
<p>Issue:</p> <p>Basis of sample: 7 suppliers from the revised 4 year spend data</p> <p>Testing against the set criteria (£5k to £25k - 3 quotes from suppliers on Sell2Wales or alternative agreed in writing by the Head of Procurement, £25k to £75k - tendered/advertised on Sell2Wales unless alternative agreed with the Head of Procurement, >£75k - Tendered by the Head of Procurement) noted the following:</p>	<p>Recommendation:</p> <p>Original recommendation is reiterated.</p> <p>When a partner joins the SRS, details of the contracts in place that need to be added to the contracts register, should be identified/confirmed to prevent false reliance and the failure to adhere to set requirements.</p>	<p>Management Response:</p> <p>Agreed. We will go through all contracts and ensure a contract is in place, in some instances we will be unable to go to another supplier as there is no alternative.</p> <p>Annette Drew</p> <p>March 31, 2020</p>

<ul style="list-style-type: none">▪ An instance, Alien Vault Inc, invoice 11 - 21103628, (£6,670), where only 1 quote existed on ServicePoint and no exemption or approval of the Head of Procurement had been obtained;▪ 1 instance where an order was placed with Net-Ctrl Limited for £38,220.00, with only one quote on ServicePoint and no contract in place;▪ 1 instance where an order was placed on 01 Oct 2019 with Caretower I.T Security Specialists for £31,278.98, although a contract did not exist;		
--	--	--

Key Points to Note

It is envisaged that the plan will be fully completed by the year end.

Audit Team

Name	Position	Telephone	Email
Peter Williams	Head of Audit	01495 742278	Peter.williams@torfaen.gov.uk
Michael Corcoran	Group Auditor	01495 742270	Mike.corcoran@torfaen.gov.uk
Arran Rosser	Senior Auditor	01495 742275	Arran.rosser@torfaen.gov.uk

Contact Information

Torfaen Internal Audit Service

Civic Centre, Pontypool NP4 6YB

Fax 01495 742439

mike.corcoran@torfaen.gov.uk

