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 audit plan then:

STAGE	NUMBER	%AGE
NOT ISSUED **(NID)**	9	66.66
ISSUED **(ISS)**	2	16.67
COMPLETED **(COM)**	2	16.67
DEFERRED **(RFP)**	1	

CODE	NARRATIVE
P	Planned
I	Issued
C	Completed

Ref	Stage	Type	Title	Quarter		
				P	I	C
SRS - 19001	COM	SYS	IT Disposals	1	1	1
SRS - 19002	COM	SYS	Firewall	1	2	3
SRS - 19003	DFT	SYS	Enterprise Architecture Management (Service Design)[2]	1	2	
SRS - 19004	ISS	SYS	Software Licensing / Management[3]	2	3	
SRS - 19005	NID	FUP	Cybersecurity	3		
SRS - 19006	NID	FUP	Identity and Access Management	3		
SRS - 19007	NID	FUP	Mobile Computing	4		
SRS - 19008	ISS	FUP	Supplier Management[4]	3	3	
SRS - 19009	NID	SYS	Back Office	3		
SRS - 19010	NID	SYS	CCTV / Control Centre	4		
~~SRS - 19011~~	~~RFP~~	~~FUP~~	~~IT Business / Service Continuity~~ [1]	~~4~~		
SRS - 19012	NID	FUP	Performance Management - SRS	4		
SRS - 19013	NID	FUP	Virtualisation	4		

[1] Delays in original report recommendation implementation dates prevents performance of the audit in the current year.
[2] Draft Report issued Nov 14, 2019 for discussion.
[3] Audit Scope meeting to be held Dec 04, 2019.
[4] Meeting to discuss implementation of systems audit action plan Nov 20, 2019.

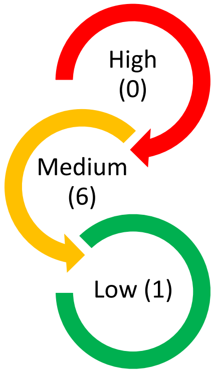
Audits Completed in the Period

Audit Title: SRS - 19002 Firewall	**Audit Sponsor:** Matt Lewis / Kathryn Beavan-Seymour	**Final Report Issued:** 25 October 2019

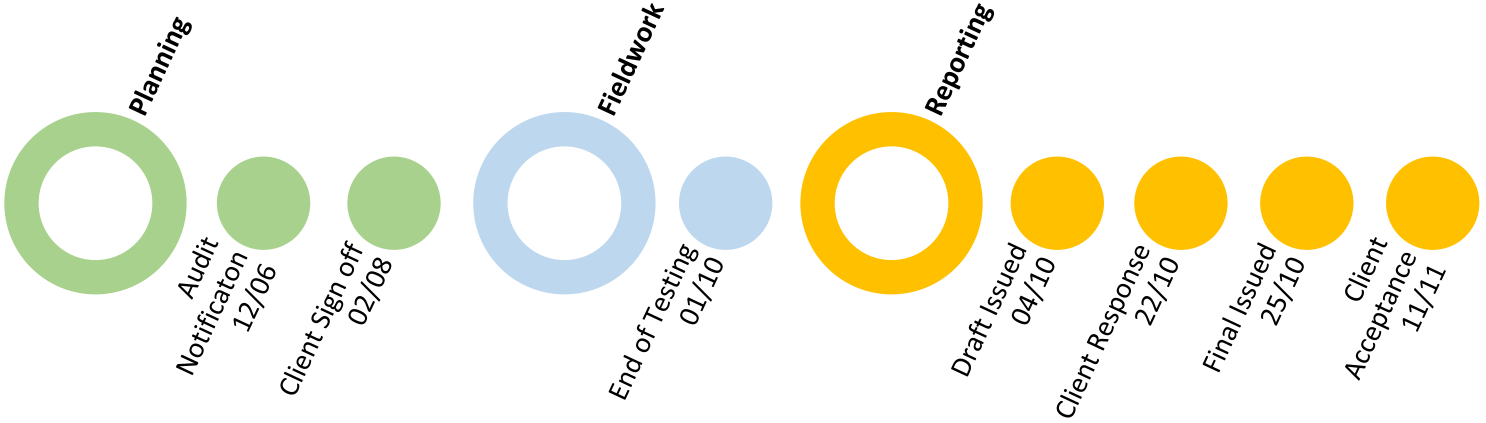
Assurance Opinion:

FULL [✓ SUBSTANTIAL] MODERATE LIMITED NONE

Recommendations / Management Action(s)



Audit Timeline: 152 days



ISS.1 – Change Details		Priority: Low
Issue: Basis of sample: 16 Firewall Rule Changes covering all partners In 3 instances the detail recorded was not enough to be able to determine the reason for the change (Ref 5549 (BGCBC), Ref 5679 (TCBC), Ref 4780 (MCC)).	***Risk:*** Lack of Management information which increases the chance of a change being made without a clear objective and justification. ***Recommendation:*** The narrative for each firewall change should include the reason for the change to ensure that it is warranted.	***Management Response:*** Agreed. Including the reason for change is in current procedure and staff will be reminded of this. **Kathryn Beavan-Seymour** **Deputy Chief Operating Officer** **October 31, 2019**

ISS.2 – Risk Assessment		Priority: Low
Issue: Basis of sample: 6 'New' Firewall Rules Operational procedures detailing how firewall rules should be configured i.e. new rule Impact Assessment, what constitutes a new rule or a rule change, where the rule is applied in the rule base, naming conventions, what additional information requires recording - Change ref etc. do not exist, the officer responsible for each partners firewall has their own methods. The current process requires "new rules" to be risk assessed through an Impact Assessment carried out by the Change Advisory Board. For 1 of the 6 new rule sample, approval from the CAB was not recorded (Ref 5219 - BGCBC)	***Risk:*** Inconsistency in operation. New rules are applied without the required approval. ***Recommendation:*** Firewall Configuration procedures should exist to ensure that all partners follow a consistent process. The risk assessment process should ensure that all new rules and changes to existing ones are assessed by persons with the necessary knowledge. The results of the CAB should be recorded in the change control system.	***Management Response:*** Agreed. A procedure will be introduced addressing the issues identified and staff will be reminded of the need to evidence CAB approval. **Jon Price** **Service Manager** **November 30, 2019**

ISS.3 - Ruleset Review		Priority: Low
Issue: No annual ruleset review is carried out, officers indicated that the tasks are done as part of routine housekeeping, but instances were noted where rules should've been reviewed/disabled and they hadn't.	***Risk:*** Firewall is not operating as intended or becomes too complicated to control. ***Recommendation:*** Management needs to have an effective mechanism (housekeeping or annual review) which ensures that rules no longer required are disabled/removed and all active firewall rules enforce the principle of least privilege.	***Management Response:*** Agreed. An annual review of the firewall rulesets will be introduced in line with the maintenance window and this will be added to the procedure being produced. **Jon Price** **Service Manager** **August 31, 2020**
ISS.4 - Decommissioning		Priority: Low
Issue: The removal of rules relating to decommissioned systems should be done as part of housekeeping because they would no longer be receiving any hits, but this could not be confirmed. There is no set naming convention for firewall rules.	***Risk:*** Rules are in place for systems that no longer exist. ***Recommendation:*** A mechanism to identify and remove all related rules for a decommissioned system in a timely manner needs to operate. A standard naming convention for firewall rules should be used that includes the system to which it relates, initials of officer, date of change e.g. spoint_aa_240919.	***Management Response:*** Agreed. Decommissioned systems will be addressed as part of the annual review and a standard naming convention will be used. This will be reflected in the procedure produced. **Jon Price** **Service Manager** **November 30, 2020**

ISS.6 - Rulebase

Priority: Low

Issue:

Basis of sample: The rule base for each partner

The rules with a "Source" or "Destination" of "ANY" and "ACCEPT" were reviewed. The following represent instances where the use of "ANY" could not be determined or the rule should have been disabled:

Partner	Rule	
NCC	143	several Sources that could not be explained and required further investigation
BGCBC DMZ-DB-MYSQL-01toNorthASA Corp_NorthtoSouthASA	1 1	rule purpose unknown, further investigation required rule deleted as a result of audit query - was originally used for testing but not disabled
TCBC	52 203	Already under review by the Security Team Purpose of the rule unknown, requires further investigation
MCC	38 123	For both; Purpose of the rule unknown, requires further investigation

Risk:

Potential conflict in rules may go undetected.

Firewall rules may not be performing as expected or required.

Recommendation:

Those rules identified as requiring additional investigation should be reviewed to ensure their suitability.

Management Response:

Agreed. The rules identified will be investigated and assessed as part of each annual rule base review in future. This will also be set out in the procedure produced.

Jon Price, Service Manager

November 30, 2020

ISS.7 – Change Requests		Priority: Low
Issue: Basis of sample: 7 Firewall Change Requests (3 GPA, 4 NCC) Discussions with staff suggested that all partners except BGCBC record the change request reference against the rule in the comment's column. Review of the partners rule bases did not support this for Gwent Police and Newport. Review of the comments field in both rule bases showed that although change request references were occasionally recorded, they were in the minority. None of the 3 sample Gwent Police firewall Change Requests had the change request reference recorded, and 3 of the 4 sample Newport firewall Change Requests had the reference recorded.	***Risk:*** Lack of management trail. ***Recommendation:*** Each rule should have the corresponding Change Request Reference recorded to allow correlation with the supporting information.	***Management Response:*** Agreed. All future rules will reflect the change request reference. This will be set out in the procedure produced. **Jon Price** **Service Manager** **November 30, 2020**

ISS.5 – Log File Verification		Priority: Medium
Issue: There is no definitive/agreed retention period for the Checkpoint log files (i.e. 1 month, 3 months, 1 year etc.), they are only used when an issue is identified and not subject to a routine check of their integrity and availability. Regarding BGCBC, as the only log files are those held in the buffer, which is constantly overwritten, they would not be available when required.	***Risk:*** Risk of log files not being available when required. ***Recommendation:*** There should be an appropriate retention policy in place to ensure that log files are available if needed (following an appropriate period). Log files should be routinely reviewed to ensure that their availability and integrity are maintained.	***Management Response:*** Agreed. Approval to scope a SIEM product has recently been obtained and this will inform product selection, for which there is no firm timeframe. **Kathryn Beavan-Seymour** **Deputy Chief Operating Officer** **October 31, 2020**

Key Points to Note

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

Audit Team

Peter Williams
Head of Audit
Tel 01495 742278
Peter.williams@torfaen.gov.uk

Michael Corcoran
Group Auditor
Tel 01495 742270
Mike.corcoran@torfaen.gov.uk

Arran Rosser
Senior Auditor
Tel 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

TORFAEN COUNTY BOROUGH
BWRDEISTREF SIROL TORFAEN