ICT Audit

FINAL

Offices of the Police and Crime Commissioners for Gwent and South Wales and the Chief Constables Gwent Police and South Wales Police

Operational Review of Collaborative Change Control

2019/20

February 2020

Executive Summary

OVERALL ASSURANCE ASSESSMENT

No overall assurance assessment is provided as this was an operational, rather than an assurance review.

OVERALL CONCLUSION

Significant changes have been made to the collaborative change management arrangements between South Wales Police (SWP) ICT and Gwent Police/Shared Resource Service (GWP/SRS) subsequent to the access issues caused by the decommissioning of the GWP/SRS domain controller within the SWP domain although the underlying lack of resilience for the current GWP/SRS domain controller has not been addressed.

- **A resilient solution needs to be explored and implemented for the single GWP/SRS domain controller within the SWP domain.**
- **A long term solution that addresses the risks arising from the current separate domains and the risk arising from infrastructure failure needs to be explored and implemented.**
- **There is no current Memorandum of Understanding in place between the Forces for system collaboration.**
- **The interrelationships between the various Force domains have not been fully mapped.**

SCOPE

The review considered the systems and process employed by both South Wales Police and Shared Resources Services (SRS) in managing requests for change including an assessment of compliance levels against any established procedures and identification of any opportunities to strengthen the control environment in respect of Requests for Change both within and between the respective organisations. The review was undertaken as an advisory review rather than as an assurance review.

ACTION POINTS

Urgent	Important	Routine	Operational
2	2	0	3

Management Action Plan - Priority 1, 2 and 3 Recommendations

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
1	Compliance	Discussions with ICT staff from both South Wales Police (SWP) and Gwent Police/Shared Resource Service (GWP/SRS) during this review identified that there is currently no resilient solution in place and that in the event of the failure of the current GWP/SRS domain controller, the same situation would arise with the inability of GWP staff and officers to access those systems including Niche hosted on the South Wales Police domain. The provision of the 30 generic Niche accounts that can be activated at short notice provides a limited solution for accessing Niche and the increased technical knowledge gained from addressing the initial incident would enable a solution to be implemented much quicker in the event of a future failure but the underlying risk has not been addressed.	A solution be explored to provide resilience in the event of the future failure of the Gwent Police/Shared Resource Service domain controller within the South Wales Police domain.	1	*There was agreement for additional resilience and an initial proposal developed.* *GP Domain Controllers (DC) 3 and 4 implemented and configured in SWP.* *SWP have upgraded the DCs in GP.* *GP Netscalers (Citrix) configured.*	*Complete*	*Kathryn Beavan-Seymour, SRS* *&* *Andrew James, SWP*

PRIORITY GRADINGS

1	**URGENT**	Fundamental control issue on which action should be taken immediately.
2	**IMPORTANT**	Control issue on which action should be taken at the earliest opportunity.
3	**ROUTINE**	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
4	Compliance	The potential options to reduce or remove the risks arising from the current separate domains and the risks arising from infrastructure failure need to be evaluated.	The long term solution that minimises the risk of infrastructure failure be explored in the form of a business case that considers a single shared infrastructure and support provision, and which addresses the risks, the costs and the time involved in implementing the solution.	1	*The Policing Vision 2025, particularly with reference to the section "By 2025 local policing will be aligned, and where appropriate integrated, with other local public services to improve outcomes for citizens and protect the vulnerable."* *The operating model for an 'Integrated and Strengthened Service', as per the Policing Vision 2025, may be better defined when the strategic outline case options are identified.*	*Strategic Outline Case (SOC).* *31/03/20*	*U. Hussain & N. Stephens*
2	Compliance	A Memorandum of Understanding for system collaboration between Gwent Police, South Wales Police and Dyfed Powys Police was implemented but is now out of date and needs to be updated.	The Memorandum of Understanding for system collaboration be updated and re-signed by all parties.	2	*The existing document will be updated across the three Forces.*	*31/03/20*	*N Stephens, Chair JOINS*

PRIORITY GRADINGS

1	**URGENT**	Fundamental control issue on which action should be taken immediately.	2	**IMPORTANT**	Control issue on which action should be taken at the earliest opportunity.	3	**ROUTINE**	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
3	Compliance	No detailed service map has been prepared of the interrelationships between the various force domains and although there is awareness of the interrelationships between the various domains it isn't currently fully and consistently documented.	The interrelationships between the various force domains be fully identified and mapped.	2	*The inter relationships between services operating between the two forces will be undertaken through a review of data that traverses the firewalls between the two forces.* *The expectation is that this will provide clarity on current dependencies as well as providing options as to future capabilities.*	*30/06/20*	*ICT JOINS Technical Group*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.	2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.	3	ROUTINE	Control issue on which action should be taken.

Operational Effectiveness Matters

Ref	Risk Area	Item	Management Comments
1	Compliance	A Technical ICT Group be established for system collaboration along with appropriate contracts and service level agreements.	*JOINS has established a technical collaborative group to look at technical design, interoperability and technology consolidation.*
2	Compliance	Consideration be given to the co-ordinating of on call rotas/contacts between the Shared Resource Service and South Wales Police.	*Access to each other's on-call rotas will be established. This is on the basis that it will be an escalation route should the normal "FIM" process prove ineffective for a particular issue.* *Furthermore, the key issue is during a major incident where contact mechanisms are established as part of a major incident process.*
3	Compliance	South Wales Police and Gwent Police consider a shared Microsoft Premium Support contract.	*This will be considered and alignment implemented.*

ADVISORY NOTE

Operational Effectiveness Matters need to be considered as part of management review of procedures.

Detailed Findings

Introduction

1. This review was carried out in May to July 2019 as part of the planned internal audit work for 2019/20. Based on the work carried out an overall assessment of the overall adequacy of the arrangements to mitigate the key control risk areas is provided in the Executive Summary.

Background

2. The decommissioning of a Gwent Police/Shared Resource Service (GWP/SRS) domain controller within the South Wales Police (SWP) domain resulted in the inability of GWP staff and officers to access those systems including Niche that are hosted on the SWP domain. The GWP/SRS domain controller was decommissioned by SWP ICT at the request of GWP/SRS but the expected resilient solution did not operate as expected resulting in the access problems for GWP staff and officers that were not fully addressed for more than 24 hours until a solution was identified and implemented.

Materiality

3. The failure to have effective collaborative change management processes in place resulting in the inability of officers and staff to access critical systems such as Niche could have potentially catastrophic outcomes.

Key Findings & Action Points

4. The key control and operational practice findings that need to be addressed in order to strengthen the control environment are set out in the Management and Operational Effectiveness Action Plans. Recommendations for improvements should be assessed for their full impact before they are implemented.

Scope and Limitations of the Review

5. The review considered the systems and process employed by both South Wales Police and Shared Resources Services (SRS) in managing requests for change including an assessment of compliance levels against any established procedures and identification of any opportunities to strengthen the control environment in respect of Requests for Change both within and between the respective organisations. The review was undertaken as an advisory review rather than as an assurance review.

6. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan.

Disclaimer

7. The matters raised in this report are only those that came to the attention of the auditor during the course of the internal audit review and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

Acknowledgement

8. We would like to thank staff for their co-operation and assistance during the course of our work.

Release of Report

9. The table below sets out the history of this report.

Date draft report issued:	5th August 2019
Date revised draft report issued:	8th August 2019
Date management responses received:	12th February 2020
Date final report issued:	13th February 2020

10. The following matters were identified in reviewing the Key Risk Control Objective:

Compliance Risk: Failure to comply with approved policy and procedure leads to potential losses.

Background

10.1 An email was sent from a member of staff at the Shared Resource Service (SRS) to an Enterprise Specialist within the South Wales Police ICT Team on the 16th January 2018 requesting a change request to be raised within South Wales Police (SWP) to decommission Gwent Police's (GWP) remaining Microsoft Server 2008 R2 Domain Controller (DC) within the SWP ICT network. The e-mails advised that "Gwent's 2016 DC's have been in place since August 2017" and that "I am confident this will not give any downtime but just wanted to make you aware."

10.2 The Enterprise Specialist e-mailed the Service Delivery Analyst that administers the change management process requesting that a change request was raised to decommission the Domain Controller and that risk assessments be completed for the proposed change. The Service Delivery Analyst raised change request RFC 17063 which was subsequently referred to the Change Advisory Board (CAB) meeting held on the 2nd February 2018 for consideration. The change requestor at SRS was included as a recipient of all e-mails relating to the raising of the Request for Change (RFC) and the intention to review the RFC at the February 2018 CAB.

10.3 RFC 17063 was raised as a standard pre-approved change and assigned to the SWP ICT Active Directory Team for action. After initial assessment of the proposed change within SWP ICT, an email from an Enterprise Infrastructure Architect on the 17th January advised "as discussed, We'll wait until we have heard from GWP in that they need to de-promote the DC, remove it from the GWP domain, then once all that is done we can do the SWP DNS meta data clean-up for the Gwent DNS zone and finally remove the DC from the ESX." None of these tasks could be completed by SWP ICT other than the final removal of the Virtual Machine (VM) as all other tasks referred to needed to be completed within the GWP/SRS domain. All of the identified actions are standard practice when removing a DC and should have been completed as a matter of course by SRS.

10.4 The RFC was reviewed at the CAB meeting held in February 2018 and authorised although the change wasn't scheduled as SWP ICT were awaiting information from GWP SRS regarding the actions they needed to complete. An update was requested in August 2018 by the Change Team which was logged on the service desk express job ticket The change was subsequently actioned on the 20th February 2019 at 11.18 am by the Extended Technical Support Team as the job had been on the job queue for a significant period so was actioned as housekeeping with the DC being deleted rather than turned off. The SWP ICT team member that the change request had originally been allocated to had left SWP ICT in the interim period between the works order being raised and the works order being actioned, resulting in another team member having to pick up the outstanding job ticket.

10.5 Subsequent to the RFC being actioned and the DC de-commissioned, SRS began receiving calls to the SRS service desk advising that Gwent Police officers and staff could not access Niche. Niche is hosted within the SWP ICT network. To access Niche, GWP officers and staff authenticate through a domain controller within the GWP ICT network which has a trust relationship with the GWP domain Controller within the SWP ICT network which then authenticates the individual allowing access to Niche.

10.6 A fault was raised with SWP service desk by SRS via e-mail at 11.34 on 20th February 2019 subsequent to an incident being logged with SRS, ref 373788, advising that GWP staff were unable to access Niche. SWP incident ref 513225 was raised on service desk express (SDE) at 12.10. A team of SWP Enhanced Technical Support and ICT Enterprise Specialists and three SRS/GWP staff seconded to the Digital Services Division based at SWP HQ initially analysed the fault and attempted to implement a solution based upon SWP ICT recommendations that afternoon and evening until around 2.00 am on the morning of the 21st February. The initial incident was escalated into a problem by SWP ICT and involved ICT staff at all levels up to and including the Head of ICT. A separate remediation team was on site at SRS and telephone communication was maintained between the two teams throughout the afternoon and into the early hours of the following morning with no further contact from SRS after 2.00am.

10.7 The cause of the lack of connectivity, the decommissioning of the Server 2008 R2 Domain Controller and the failure of the resilient Server 2016 Domain Controller to take its place, was identified during the afternoon of the 20th February and an initial fix was implemented although this solution was unsuccessful, resulting in a number of ongoing fixes before stable connectivity was re-established.

10.8 SWP ICT were engaging with Microsoft during this process for support under the SWP/Microsoft Premier Support Agreement in place although the initial support provided by Microsoft was not provided at the expected levels under the contract and this has been raised directly with Microsoft by SWP ICT.

10.9 The GWP Server 2008 R2 DC was a virtual DC and attempts to re-store it caused a number of issues to the GWP domain. It is not best practice to re-introduce a DC from a backup and it was not initially recognised by SRS that their expected resilient DC was not resilient.

10.10 GWP initiated a Gold Group to manage the loss of connectivity that met six times between 8.40 am on 21st February and 3.35pm that day when the Gold Group was stood down as resilient connectivity had been restored. Attendance at the Gold Group meetings included GWP officers and staff, members of SRS and the Head of SWP ICT who joined meetings using Skype.

10.11 An interim measure that was put in place although it wasn't actually used was a contingency arrangement to re-assign GWP Niche accounts to provide emergency access in the event of a similar future loss of connectivity for GWP officers and staff to Niche. This contingency arrangement involved the creation of 30 generic accounts on the SWP active directory domain which will permit nominated Gwent users to login to SWP network services. The NICHE team within the Digital Services Division (DSD) would link these generic accounts to NICHE application login or outside of office hours a single point of contact (SPOC) within the Public Service Centre will perform this role when the use of these generic accounts is required. The re-assignment process has been fully documented and is available to provide limited access during a future similar event where GWP access to niche is not available through the GWP domain and has been formally adopted by SWP PSC.

Trust Relationship

10.12 Establishing trust between two very secure separate domains is never easy. Both the GWP and SWP domains are designed to be very secure.

10.13 The trust relationship across the GWP and SWP domains is between multiple DCs configured within the forest trust with two SWP root domain DCs and two GWP DCs. If a single DC fails then a resilient named DC within the forest trust configuration takes control of the trust. If a child domain fails within the SWP domain or within the GWP domain then the trust relationship between the two domains remains intact.

10.14 The analogy used to describe trust between networks is usually described in terms of forests and trees where the individual domains are referred to as trees of a forest. The current trust relationship is a forest trust between the SWP forest and the GWP forest enabling a 2-way transitive trust including child domains of that forest.

10.15 Trust can be established forest to forest where a number of trees (DCs) within each forest establish trust with each other. In this case if one tree fails, the trust relationship continues with the other trusted trees so connectivity would continue between the two domains. This is referred to as a trusted forest.

10.16 Forest or Domain trusts do not need to operate at the same forest functional level (FFL) or domain functional level (DFL) and this was the case with SWP and GWP domains. SWP were operating on FFL 2088R2 and DFL 20082, whereas GWP were on FFL 2008 non-R2. Currently GWP and SWP are operating different FFL/DFL and also different operating system server software with SWP running Microsoft Server 2008 and 2016 and GWP running 2016 only. Prior to the outage GWP were operating Windows Server 2008r2 and SRS would have had to do a meta data clean-up of the DC as it was not de-promoted as a domain controller or DNS server by SRS as part of SRS's de-commissioning process.

10.17 The secondary GWP/SRS DC within the SWP domain that was intended to provide resilience in the event of the failure (or removal) of the primary GWP/SRS DC did not operate as expected due to the trust relationship between the two domains. No testing of the resilient DC had been undertaken to confirm that it would operate as intended. Had the secondary DC been fully tested and found not to provide resilience as expected then an alternative solution to provide resilience could have been identified.

10.18 Discussions with ICT staff from both SWP and GP/SRS during this review identified that there is currently no resilient solution in place and that in the event of the failure of the current GWP/SRS DC, the same situation would arise with the inability of GWP staff and officers to access those systems including Niche hosted on the SWP domain. The provision of the 30 generic Niche accounts that can be activated at short notice provides a limited solution for accessing Niche and the increased technical knowledge gained from addressing the initial incident would enable a solution to be implemented much quicker in the event of a future failure but the underlying risk has not been addressed.

Recommendation: 1	**A solution be explored to provide resilience in the event of the future failure of the Gwent Police/Shared Resource Service domain controller within the South Wales Police domain.**
Priority: 1	

Change Management

10.19 GWP/SRS and SWP both have fully documented change control arrangements in place that are IT Infrastructure Library (ITIL) compatible but have been tailored to fit the different structures and roles within the two organisations. ITIL is the most widely accepted approach to IT service management and focuses on aligning IT services with business needs.

Gwent Police/SRS

10.20 SRS categorise changes as one of four categories, a normal change, a high priority change, an emergency change or a standard change. All requests for change (RFC) are logged within the Service Point service desk solution and are impact assessed by the members of the Change Advisory Board (CAB) to determine any potential impact on IT infrastructure, service levels, security, impact on other changes, available manpower and resources and necessary investment before the RFC is authorised. CAB members are also involved in planning and scheduling the change. A sample of changes are randomly selected each month by the Change Manager and evaluated through a Post Implementation Review (PIR) and the results fed back to the Senior Management Team and the Performance and Audit Board as part of a continuous improvement process.

South Wales Police

10.21 SWP categorises requests for change as either a normal change, a standard change or as an emergency change. Normal changes can be further categorised as minor changes defined as low risk/impact, significant changes defined as medium risk/impact or as major changes defined as high risk/impact. Normal changes with medium or high risk/impact are reviewed by the CAB and authorised by the Change Manager. All RFC are recorded on the service desk application. All RFCs are subjected to a technical pre-assessment process and may be rejected at this point if the application is incomplete or does not include sufficient reporting information. Normal RFC that pass the initial technical assessment undergo a peer review and higher technical assessment before being presented to the CAB for review and approval. Emergency RFC are subjected to an initial assessment and, if within normal working hours, are referred to an Emergency Cab (e-CAB) for assessment and approval. Emergency RFC received outside normal working hours are assessed and either addressed or deferred for referral to the e-CAB depending upon the circumstances. All changes are tested after being built prior to being released.

10.22 All RFC are managed centrally and are recorded on the SWP ICT planning calendar which automatically sends out meeting requests to the ICT Teams required for the RFC assessment process.

10.23 An ICT Strategic Board has been established to define and manage a gateway process for all projects and change work requiring ICT support, to review, for the purpose of approving or declining, all ICT Requests for Change (RFC's) which extend beyond business as usual moves and changes, to review, for the purpose of approving or declining, all requests for unfunded ICT growth, to prioritise ICT developments and change in order to maximise the delivery of Force objectives and to direct and oversee the work of the ICT Change Review Board. Terms of Reference that include the membership of the Board have been documented.

10.24 Monthly Business CAB meetings are attended by members of DSD, business areas and partner organisations like South Wales Fire and Rescue Service. SRS staff working with DSD attend the CAB meetings providing input from and feedback to SRS for those changes that affect the GWP/SRS Domain.

10.25 Fortnightly ICT CAB meetings are held which consider the technical issues around requested changes. Terms of Reference have been documented for the ICT CAB with membership including the SWP Service Manager, the SRS Service Manager, Technical Leads, the DSD Business as Usual Lead and the FRS Technical Authority with change requestors attending by invitation.

10.26 Weekly SWP/GWP ICT Operations Meetings are held on a Monday morning and are attended by SWP ICT, DSD and GWP/SRS. The meetings are driven by known Incidents, Problems, planned Changes from weekly Operations meetings and regular CAB Meetings. The role of the group is to review interdependent ICT (technical Stages) and Business related incidents, changes, implementation and plans both direct or indirect that could cause risk or will effect interrelated services between SWP and GWP, take a tactical view based on a 3 week rolling window of new incidents and problems since the previous meeting and of plans and changes, share best practice where possible, align processes where possible and provide a watching brief. Membership of the meetings includes the SWP ICT Delivery Manager, the SWP ICT Customer Services Manager, the DSD Business Manager, the SRS Service Manager, DSD Business Leads as required and the SWP ICT and GWP/SRS Technical Leads as required. The meetings report to and escalate to or from the ICT SMT, the SRS SMT the SWP/ SRS Weekly Operations Meetings and the DSD Technical Stage Board. Terms of Reference have been documented for the SWP and GWP Operations Meetings.

10.27 SWP have recently introduced the role of Programme Manager with responsibility for the change management process. The Programme Manager undertakes the role of the ITIL "Change Manager".

Changes since the incident

10.28 The SWP Change Advisory Board in place at the time that the original RFC was received to decommission the GWP/SRS DC in January 2018 was an internal SWP Board with no invites to or attendance by GWP/SRS or DSD staff. In June 2018 the role of the CAB was reviewed and GWP/SRS and DSD members were invited to attend. the role of the CAB was again reviewed in April 2019 with the introduction within SWP ICT of an ICT programme Manager role

10.29 DSD and SRS staff now attend the monthly CAB meetings and are able to provide input into RFCs that impact upon GWP.

10.30 Regular contact has been initiated between the SWP Service Delivery Manager (SDM) and his counterpart at SRS as well as avenues established for regular contact between the SDM, SRS and DSD.

10.31 An ICT Technical Stage Board was formed in June 2018 to review technical stage progress against business plans of approved DSD-ICT (SWP & SRS) Projects or Major Deliverables. The Stage Board meets bi-monthly and is chaired by the SWP Head of ICT or the GWP/SRS Collaboration Manager. Attendance at the Board includes Technical Architects and Project Managers from SWP and SRS and DSD Business Leads and Project Managers. The Stage Board reports to and escalates to and from ICT SMT, SRS SMT and the DSD Bronze Board. Terms of Reference have been documented for the ICT Stage Board.

The GWP/SWP relationship

10.32 The GWP/SWP ICT system collaboration was intended to be a collaborative arrangement but in practice is more of a service arrangement with SWP providing services to GWP rather than a truly collaborative arrangement. This has been continuously raised since the original delivery of the AD forest trusts for the hosting of Niche and other partners on the SWP domain as delivered through Joins ICT.

10.33 A Memorandum of Understanding for system collaboration between GWP, SWP and DPP was implemented but is now out of date and needs to be updated.

Recommendation: 2	**The Memorandum of Understanding for system collaboration be updated and resigned by all parties.**
Priority: 2	

10.34 There is no contract or service level agreement (SLA) in place although there have been continuous requests through the Joins ICT Board from SWP ICT to have a service review group.

Operational Effectiveness Matter: 1	**A Technical ICT Group be established for system collaboration along with appropriate contracts and service level agreements.**

10.35 No detailed service map has been prepared of the interrelationships between the various force domains although there is awareness of the interrelationships between the various domains but it isn't currently fully and consistently documented. There is a deliverable within the SWP Service Management Project that has the responsibility to deliver the new service management solution, Avanti, to review the feasibility of introducing and sustaining service mapping within SWP. This feasibility study will be based on Niche with a recommendation going to the ICT Strategic Board to expand this process across all levels of service and functions.

Recommendation: 3	**The interrelationships between the various force domains be fully identified and mapped.**
Priority: 2	

10.36 There are currently different on call/out of hours support arrangements in place for GWP and SWP. SRS operate an on call rota system for evenings and weekends that includes an on-call senior manager who would triage the issue and manage the resolution process. SWP operate an ad-hoc callout process when required with the callout initiated through the Force Incident Manager (FIM) within the SWP public service centre (PSC). An initial portal advises the FIM to determine which ICT technical point of contact to call. Once contacted by the FIM, the initial contact would triage the issue and determine who and what resources would be required. Contact is maintained throughout the process between the SWP ICT on call and the FIM until problem resolution. SWP do not have an on-call senior manager and it is the responsibility of the initial ICT technical point of contact to determine what resources are required at what level to address the issue. SRS and SWP ICT have no access to or sight of the on call point of contact of the other and there are no collaborative on call contract arrangements in place.

Operational Effectiveness Matter: 2	**Consideration be given to the co-ordinating of on call rotas/contacts between the Shared Resource Service and South Wales Police.**

10.37 The contact and escalation process between SRS and SWP for out of hours and weekend issues is potentially a convoluted process with SRS contacting the GWP FIM to notify them of an issue. The GWP FIM then contacts the SWP FIM who then contacts SWP ICT. There is no direct line of contact between the SRS on call manager and the SWP ICT on-call contact.

10.38 SWP have a Microsoft Premium Support contract (Unified) in place although the support provided by Microsoft during the DC incident fell short of what was required and expected. GWP don't have this level of support contract in place. Consideration should be given to a shared South Wales Police/Gwent Police Microsoft Premium Support Contract.

Operational Effectiveness Matter: 3	**South Wales Police and Gwent Police consider a shared Microsoft Premium Support contract.**

Possible future options

10.39 The National Enabling Programme (NEP) is reviewing the potential for a national identity management option through Azure Active Directory, initially for the rollout of Office 365 but followed by development for cloud integrated police software and applications. This may ultimately provide a solution for a national police identity management but given the delays in the NEP, this solution may take some time to be fully developed.

10.40 The option of SWP managing all GWP user accounts possibly through the use of a SWP domain account with a GWP prefix for GWP officers and staff is a possibility and this option would remove the requirements for the current GWP/SWP DCs and trust relationship for accessing applications within the SWP domain but this option would reverse the current situation. GWP staff and officers accessing applications hosted on the GWP domain would require a SWP DC within the GWP domain to authenticate users before access to GWP applications is granted, the mirror image of the current situation which requires GWP/SRS DCs within the SWP domain. This option may be of benefit if the more critical systems that staff and officers are required to access are hosted within the SWP domain rather than within the GWP/SRS domain.

10.41 The implementation of a copy of Niche and FIRMS within the GWP/SRS domain with real time replication between the SWP and GWP Niche and FIRMS would be another potential option to prevent the re-occurrence of the DC failover issues. This solution would present some significant challenges around replication and real time synchronisation across different firewalls and domain networks. Existing designs that originally required a year to implement would have to be revisited with a significant amount of resource time and effort to change.

10.42 The solution preferred by all ICT staff spoken with during this review would be a single combined network but this would require a single ICT service. An interim benefit of this solution would be both current network domains being managed centrally, enabling the removal of some of the current restrictors as both networks would be trusted, leading over time to the development of a single centralised ICT infrastructure including cloud services underpinning all GWP and SWP applications. This solution would provide seamless access for GWP staff and officers to all applications, improve resilience, provide significant financial savings for both Forces due to only having to implement and maintain a single network and a single DR solution, would simplify the current technical challenges, reduce the cost of investment in ICT hardware for both Forces and reduce the risks as highlighted by the current dual change management processes.

10.43 The potential options identified to reduce or remove the risks arising from the current separate domains and the risks arising from infrastructure failure need to be evaluated.

Recommendation: 4	**The long term solution that minimises the risk of infrastructure failure be explored in the form of a business case that considers a single shared infrastructure and support provision, and which addresses the risks, the costs and the time involved in implementing the solution.**
Priority: 1	
