The Scottish Government

Technical Assurance Review

NHS Greater Glasgow and Clyde

NHS Greater Glasgow & Clyde

Critical Incident – 1 October 2013

Report Status:	Final Report
Dates of Review:	16/10/2013, 17/10/2013 and 29/10/2013
Final Draft Report Issued to commissioning bodies:	30/10/2013
Final Report Issued to commissioning bodies:	01/11/2013

Contents

1. Background

NHS Greater Glasgow & Clyde (NHS GG&C) is a large and complex organisation employing over 40,000 staff with an IT estate comprising of 30,000 desktops and over 1,700 servers. Since its establishment in 2007 NHS GG&C has taken a corporate approach to ICT service provision. This has led to extensive rationalisation of infrastructure and application systems. The primary Active Directory (AD) domain XG GC accounts for 80% of desktops in Acute services.

2. Critical Incident

On Tuesday 1 October 2013 a software error on a computer server supporting a number of ICT systems in XGGC meant that a significant number of users (10,000+) were unable to access information that they needed to carry out key front-line functions. Although only a small proportion of the total appointments were cancelled as a result of information not being available via key ICT systems (and emergency procedures not affected), the impact was significant on a number of levels: to the patients who may have incurred distress as a result of postponed appointments; to the business operations disrupted and back-log created; and reputational damage. NHS GG&C were able to fully re-establish services in the early hours of Thursday 3 October.

The failure was quickly identified as being associated with the Active Directory software environment, but the nature of the problem was such that the corruption 'replicated' across the entire array of domain controllers that run the software. This complicated the recovery process and the NHS GG&C ICT team, working in conjunction with the prime supplier (Microsoft) and partner (Charteris), needed to invoke a complex recovery process that required a rebuild of existing hardware and further expert intervention by Microsoft subject matter experts.

3. Independent Review

The independent review was jointly commissioned by NHS GG&C and by Scottish Government eHealth Division. Its primary purpose is to give NHS GG&C assurance that its related technical environment follows recommended industry best practice and that the recovery measures that were invoked were sound. From the Scottish Government eHealth point of view the review will provide a series of "lessons learned" from the NHS GG&C experiences that can then be fed into a planned wider review of all NHS Scotland Health Boards' ICT resilience arrangements.

4. Review Team

The review team were selected by the Scottish Government Chief Information Officer (CIO) in discussion and agreement with NHS Greater Glasgow & Clyde and the eHealth Division of the Scottish Government.

The team have significant strategic, technical and operational IT experience gained in both public and private sectors over many years, particularly with Microsoft technologies. Their respective backgrounds and knowledge has allowed for an impartial and independent examination of the critical incident which took place on 1 October 2013.

5. Purpose and Conduct of the Review

The review team were tasked with considering the relevant NHS GG&C technical environment and the processes in place to handle incidents of the nature experienced on 1 October. In particular, the review team were asked to focus on:-

a. **NHS GG&C's implementation of Active Directory and its supporting technical environment.**

b. **The resilience of that technical environment to protect against service interruption.**

c. **The NHS GG&C ICT team's and suppliers' management of the incident, and the immediate aftermath and subsequent investigation.**

The review was conducted initially at NHS GG&C premises - Westward House – Paisley on the 16 and 17 October 2013 and subsequently at Scottish Government premises in Glasgow on 29 October 2013.

6. Microsoft Professional and Premier Support

Throughout this document there are references to both the Professional and Premier support that was provided by Microsoft during the critical incident. It is important that the differences between the two models is understood by the reader. The review team asked Microsoft to provide the following explanation.

Support

Microsoft offers a wide range of support services to match the breadth, depth and diversity of its customer base. Some support is available at no cost, while other services are paid for.
Two of the paid for support offers commonly subscribed to either by enterprises for their own IT (insourced or outsourced) or by service providers (who Microsoft often refer to as "partners") in support of their customers' IT.
These two support offerings are known as Professional Support and Premier Support. There are notable differences between them and each offer may have a number of options (such as Premier Mission Critical or Premier for Office 365) designed to allow customers to select the support mix that best matches their actual needs.
The major features are summarised below, and hence the differences, between these two support offerings.

Professional Support

Professional Support provides access to Microsoft experts, to help address problems encountered with the development, deployment and management of Microsoft software in commercial environments. Professional Support is available on a per incident basis, over the phone or via the web.
Microsoft Professional Support provides support in one single incident or "Pay-per-incident" (PPI). Incidents provide support that focus on troubleshooting a specific problem, error message, or functionality that is not working as intended for Microsoft products. An incident is defined as a single support issue and the reasonable effort to resolve it.
Professional PPI is available during normal business hours: 8:00 AM – 6:00 PM Monday to Friday, excluding Public Holidays. Response time will be between 2 and 8 hours, depending on severity.

Premier Support

Enterprises gain the most benefit from their IT infrastructure by pairing their business with Microsoft Premier Support. Dedicated support teams provide continuous hands-on assistance and immediate escalation for urgent issues, speeding resolution and helping keep mission-critical systems up and running. Premier Support helps evaluate an enterprise's IT health and provides training or tools teams need to "get healthy and stay healthy." Premier Support connects customers with the right subject matter engineers who can solve issues right away, and a technical account manager whose job it is to understand the customer's business challenges, ensuring customers receive unparalleled expertise, accelerated support, and strategic advice tailored to their unique IT environment.

With Microsoft Premier Support customers receive:

- Accelerated response times, speaking to the correct subject matter experts right when needed
- Access to a global network of experts with unmatched knowledge of Microsoft products
- Direct assistance with planning, rollouts, and rigorous health checks and remediation services
- Operations assessments to help streamline processes, including security measures and resource allocation
- Hands-on training and knowledge transfer to help increase IT staff expertise and improve alignment between business goals and IT investments

As businesses evolve, so do their systems, infrastructure, and the skills of their people (or their service provider's people). Microsoft Premier Support provides a wide range of services, including IT staff training, health and risk assessments, and best practices.

This approach helps customers identify and address potential issues and risks up-front to make sure that their IT systems are healthy and stay that way. But if things do go wrong, Microsoft Premier Support offers the best support to resolve problems as fast as possible.

7. Technical Assurance Review

NHS GG&C's implementation of Active Directory and its supporting technical environment.

The review team found that the design and implementation of the XGGC Microsoft Active Directory with associated services is a fit for purpose and resilient implementation. The design was created in 2008 and implemented with support from Microsoft Partner – Charteris. Subsequently, Microsoft completed an Active Directory Risk and Health Assessment Programme (AD RAP) in 2010 which concluded with a number of recommendations which have subsequently been implemented.

In May 2013, Charteris performed a similar assessment which identified some improvements which could be implemented to reduce the risk associated with operating the infrastructure and subsequently these recommendations have been implemented. The assessment concluded by stating:

"*Overall, the Active Directory infrastructure is well configured and in excellent health, and it conforms to Microsoft best practice*"

Of particular relevance to this critical incident the review team noted that the Charteris report stated:

"*The DNS configuration of the DNS servers and DNS hosted zones for XGGC are well configured and in good health*"

During discussions with Microsoft Premier Support personnel on 29 October 2013, they are also of the opinion that the DNS configuration on the XGGC Domain Controllers is consistent with a standard active directory deployment of this size.

Recommendation: None

Rationale: The review team consider the implementation of the XGGC Microsoft Active Directory with associated services is a fit for purpose and resilient implementation that has been validated by both Microsoft and Charteris.

The resilience of that technical environment to protect against service interruption

The existing technical environment relies heavily upon Microsoft Active Directory (AD) and integrated services for normal operation. In the event of a catastrophic failure of AD a substantial service impact across the entire technical environment is possible.

The review team note and wish to record that this reliance upon AD is commonplace globally. The AD product is the market leading directory services solution. AD has demonstrated considerable resilience and stability since its introduction to the marketplace over ten years ago. There are a number of features, built into the product and the XGGC design that should limit service impact in the event of the catastrophic failure of one or more servers.

During this critical incident there appears to have been an unprecedented failure within all XGGC AD domain controllers. Throughout the review it became clear that nobody who was interviewed or part of the review team has ever experienced a failure of this nature and complexity within AD. At the time of producing this final report the root cause for this failure is as yet undetermined.

Despite the extremely low likelihood of a failure of this nature, NHS GG&C's disaster recovery plan catered for this specific scenario where all AD services have been lost, users cannot authenticate and there is no alternative but to restore from backup. This ultimately was the procedure that was used to recover the NHS XGGC AD.

***Recommendation R1*:** Consider implementation of Specialist 3rd party AD backup software which aids and supports full recovery of the AD infrastructure.

Rationale: There are 3rd party Active Directory backup software products available which complement, and can be used in addition to, the existing backup software. These are designed to facilitate a faster recovery in the event of a catastrophic failure and may offer business value.

Recommendation R2: Microsoft Windows Server native backup should be used in addition to any third party backup solutions.

Rationale: In the event of a catastrophic failure Microsoft are better able to support recovery efforts if the Windows Server native backups are available.

***Recommendation R3*:** Consider implementing Active Directory auditing and configuration change software.

Rationale: Auditing of configuration changes to AD would allow conformation that no changes had been made by systems or AD integrated software prior to a failure

Recommendation R4: The restoration of backups from the XGGC domain should be tested to ensure full recovery can be achieved.

Rationale: To give confidence and increased familiarity with the restoration procedures and timings.

The NHS GG&C ICT team's and suppliers' management of the incident, and the immediate aftermath and subsequent investigation

Following the interviews it is the view of the review team that NHS GG&C handled the incident, and the immediate aftermath and subsequent investigation, professionally; particularly given the significant business impact and media attention.

Phase 1 – Incident Identification and Initial Response – Tues 01/1013 (08:00 -12:30)

On the morning of Tuesday 1 October, initial calls suggested that a priority 4 (P4) incident was evolving with symptoms of slow logons and intermittent access to systems were being reported by users.

By 10:00 the incident had escalated to priority 1 (P1) status and there was evidence of a significant problem with AD. At this point it is worthy of note that the NHS GG&C standard operating procedures instigated the establishment of the senior incident team. Additionally, Charteris were briefed on the problem, assigned an engineer to site and raised a problem ticket with Microsoft Professional Support.

Due to the increased volume of calls at this stage service desk immediately increased their resource level to alleviate workload pressure and reduce call abandonment rates. The review team believes that the actions taken here were commensurate with the additional demands being placed upon the service desk at this stage.

The review team specifically investigated if any recent changes to the AD environment had been made prior to the incident occurring. This identified that a domain controller within the environment was patched on 26 September 2013 in line with NHS GG&C's guidelines and acknowledged best practice. Normal operation was reported immediately after this patch was applied. Over the course of the following day and subsequently over the weekend normal business operation occurred. As such the review panel concludes that this patch was unlikely to be directly responsible for any subsequent failure.

Recommendation: None

Rationale: The review panel considers that this phase was handled in an assured and professional manner.

Phase 2 – Escalated Reponses and Management – Tues 12:30 – 00:00

By early afternoon the Charteris engineer had arrived on-site and immediately began liaising with Microsoft Professional Support to investigate the AD failure and identify recovery actions. Initial evidence suggested a failure within the DNS application partition with AD.

At this stage, NHS GG&C instigated two work streams. The first focused on recovery of the failed DNS application partition with AD and was led by Charteris and Microsoft. The second focused on the preparing a full AD recovery in the event that the DNS application partition recovery proved unsuccessful.

The exact details of the work undertaken by Microsoft Professional Support during the attempted DNS application partition recovery are unknown by the review panel as Microsoft Professional Support have been unable to take part in any interview sessions. However a number of written questions were submitted and subsequently answered providing some account of the actions and troubleshooting taken by Microsoft Professional Support during this period.

Microsoft Professional Support used remote hands software and connected to one of the failed domain controllers and began their initial investigation, which concurred with NHS GG&C and Charteris assessment that there was an issue with the DNS database stored within AD, The Networking Engineer from Microsoft Professional Support suspected that there was possible corruption at this point agreed with NHS GG&C that they would attempt to delete and recreate the partition.

The partition was recreated successfully but this did not resolve the name resolution issue.

The review team consider this two stream approach to be both sensible and pragmatic in preparing early for a full disaster recovery position.

In addition, the review team notes that NHS GG&C instigated appropriate workarounds offering effective base level services to critical clinical areas. The review panel considered this approach to be commendable.

This phase ended with the recommendation by Microsoft Professional Support that DNS application partition was unrecoverable and a full AD recovery was required.

Recommendation R5: Oversight of any third party vendor work being undertaken should be given greater attention and a decision log be maintained.

Rationale: At this stage the review team and NHS GG&C has been unable to establish the exact nature of the third party (Microsoft) work undertaken and decisions taken therein.

Recommendation R6: The immediate availability of spare or redundant hardware would be of assistance to NHS GG&C in the event of similar incident.

Rationale: In the event of hardware failure immediate availability will help reduce the time required to recover from any critical incident.

Phase 3 – Active Directory Recovered – Wed 00:00 – 09:30

Initial attempts to perform a full AD recovery proved unsuccessful due to the recovery mechanism applied requiring significant free disk space. Attempts were made to resolve this by deletion of temporary and unused files but ultimately led to server operating system becoming unstable. This made a full server rebuild necessary taking 6 hours to complete including the initial unsuccessful recovery attempts.

Following a subsequent period of AD clean-up initial assessment suggested that domain controller behaviour was consistent with the failed state as observed during phase 1. At this stage the newly built domain controller was disconnected from the network.

This phase ended with support personnel from NHS GG&C and Charteris handing over to counterparts.

Recommendation R7: The availability of other team resources during an incident such as this could prove to be beneficial to recovery of systems and services.

Rationale: During the rebuild process the review team consider that time could have been saved by the availability of additional expertise.

Phase 4 – AD Availability, Stability and Scalability – Wed 09:30 – 18:00

Following a period of disconnection from the network the recovered domain controller showed signs of AD services returning. In line with the NHS GG&C documentation all other XGGC domain controllers were isolated from the network. The decision was made to reconnect the recovered domain controller to the network at which point it started to process authentication and DNS requests normally. However, at this stage it was noted that Microsoft Distributed File Services (DFS) were unavailable. The impact of DFS being unavailable was to significantly increased user logon times and potentially limit access to applications.

At approximately 10:15 Microsoft internally escalated the support ticket from their Professional Support Services team to the Premier Support group, this involved raising a new support ticket in order to provide 'follow the sun' support. By 11:10 the Premier Support team were providing telephone assistance. Microsoft then offered to have a subject matter expert placed on site in Glasgow to assist NHS GG&C. Additionally, personnel from the Premier Support group and Microsoft Scotland attended site to support with logistics and escalations.

Without any additional changes, approximately 50% of the NHS GG&C user population are able to login, albeit slowly and access limited services. Subsequent changes to the network configuration allowed access to 100% of users.

Recommendation: None

Rationale: The review team consider the action taken to recover 50% of the estate was performed well and that the correct decision was taken to preserve service availability from the single domain controller until the arrival of the Microsoft subject matter expert on site, rather than attempt to recover additional services.

The review team note that within a matters of hours of notification, Microsoft Premier Support were fully engaged and had dedicated resources both on site and on the telephone providing assistance.

Phase 5 – Full Recovery – Wed 18:00 – Thur 03:00

Microsoft subject matter expert arrives on site at circa 18:00 and immediately begins reviewing the current position. NHS GG&C in consultation with the Microsoft subject matter expert, turn their attention to providing a second domain controller. The Microsoft subject matter expert focuses on the restoration of DFS with remote support from colleagues.

Due to the nature of the full AD recovery, key components of DFS were no longer available. The recovery involved in-depth remote telephone assistance from Microsoft technical specialists based outside of the UK.

The review team note that NHS GG&C staff and Charteris believe that without Microsoft Premier Support the DFS recovery may not have been possible.

The second domain controller is then made fully operational and DFS is recovered. Full recovery of a third and fourth domain controller including testing is completed by 03:00 on Thursday 3 October. At this point full AD and associated services were restored.

Recommendation R8: Consider the implementation of a Microsoft Premier Support agreement.

Rationale: In the absence of such support arrangements the review team believes that NHS GG&C would have been unlikely to recover from this critical incident within the time scales achieved. The review team also notes that Microsoft provided premier support including an on-site resource on a commercial goodwill basis.

Phase 6 – Post Recovery Actions – Thur 07:00 – Fri 17:00

NHS GG&C staff return and immediately confirm that AD and associated services are operating as expected. Remedial action plan and work begins establishing normal operation.

NHS GG&C then introduced an environment freeze to the XGGC AD and put extended on-call support arrangements including Charteris for a 9-day period.

NHS GG&C staff begin a review period of the critical incident and start asking questions of Microsoft (against the original support ticket) on both root cause and subsequent recovery actions undertaken. The review team notes that detailed responses are still awaited.

Service desk removes critical incident banner messages and begins processing calls normally. In the following hours normal operating levels are observed and work subsequently begins to close off all outstanding support tickets raised during the incident.

All parties (NHS GG&C, Charteris, and Microsoft Premier Support) attempted to determine possible root causes of this critical incident. The focus of NHS GG&C was the restoration of services as quickly as possible. In such circumstances, it is inevitable that evidential data will have been overwritten. It is the view of the review team that the priority that was placed on recovery was appropriate in the circumstances.

Technical snapshots of some of the servers involved in this incident (prior to the AD recovery) were passed to Microsoft Premier Support for investigation. Based on the evidence contained within these technical snapshots Microsoft Premier Support were unable to determine a particular root cause, however there was no evidence of any low level corruption within the AD databases on the snapshots provided to Microsoft.

It is worthy of note and based on feedback from Microsoft that some replication **was** occurring amongst the domain controllers during phases 1 and 2 of the incident. This was apparent because attempted changes made during the recovery of the DNS application partition were observed within the technical snapshots reviewed by Microsoft Premier Support.

Recommendation: None

Rationale: The review team considers that all post recovery actions were completed in a professional and timely manner.

8. Distribution of the Technical Assurance Review Report

The contents of this report are confidential to the commissioning bodies and their representative/s. It is for them to consider when and to whom they wish to make the report (or part thereof) available, and whether they would wish to be consulted before recipients of the report share its contents (or part thereof) with others.

The Review Team will not retain copies of the report nor discuss its content or conclusions with others.

Any request for copies of this Technical Assurance Report will be directed to the commissioning bodies.

Appendix A - Review Team and Interviewees

Review Team:

Review Team Leader:	Andy McClintock Chief Technology Officer Scottish Government
Review Team Member:	Neil Logan Chief Technology Officer Amor Group
Review Team Member:	Charles Bachelor Systems Transformation Manager Police Scotland
Review Team Member:	Kenneth Mclauchlan Active Directory Specialist Police Scotland

List of Interviewees:

Name	Organisation/Role
Robin Wright	NHS GG&C Senior Management
Alasdair Finlayson	NHS GG&C Senior Management
Stephen Harris	NHS GG&C Management
Calum Morrison	NHS GG&C Management
Linda Darroch	NHS GG&C Incident Management
Derek Johnson	NHS GG&C Incident Management
Gary Vogwell	NHS GG&C Team Lead
David Green	NHS GG&C Team Lead
Bob McCafferty	NHS GG&C Team Lead
Dave Watkins	NHS GG&C Technical Contributor
Steven Black	Charteris
Ian McGowan	Charteris
Colin Livingston	Microsoft
Anil Poulose	Microsoft
Ben Pearce	Microsoft
Tom Lanigan	Microsoft
Mark Ferrar	Microsoft
Rob Lane	Microsoft
Chris Norris	Microsoft
Ben Caird	Microsoft

Appendix B - Summary of Recommendations

Ref:	Recommendation	Importance	Status
R1	Consider implementation of Specialist 3rd party AD backup software which aids and supports full recovery of the AD infrastructure	Recommended	Under-consideration
R2	Microsoft Windows Server native backup solution should be used in addition to any third party backup solutions in use.	Essential	Implemented
R3	Consider implementing Active Directory auditing and configuration change software.	Recommended	Under-consideration
R4	The restoration of backups from the XGGC domain should be tested to ensure full recovery can be achieved.	Essential	In-progress
R5	Oversight of any third party vendor work being undertaken should be given greater attention and a decision log be maintained.	Recommended	Under-consideration
R6	The immediately availability of spare or redundant hardware would be of assistance to NHS GG&C in the event of similar incident.	Recommended	In-progress
R7	The availability of other team resources during an incident such as this could prove to be beneficial to recovery of systems and services.	Recommended	In-progress
R8	Consider the implementation of a Microsoft Premier Support agreement.	Recommended	Completed

Each recommendation has been given a importance level. The definition of each level is as follows:

ESSENTIAL - In order to minimise business risk and service availability actions should be taken to implement the recommendation without delay.

RECOMMENDED - To improve service availability and reduce the risk of a reoccurrence of service or system failures actions should be considered seriously by the business.

Each recommendation has been given a status level. The definition of each level is as follows:

IMPLEMENTED – The implementation recommendation has already been completed.

IN PROGRESS – The implementation of this recommendation is currently underway.

UNDER CONSIDERATION – The implementation of this recommendation is currently under consideration.