INTERNAL AUDIT REPORT

FROM:	Audit & Risk Manager	**SUBJECT:**	Guest Wireless Project
TO:	Head of Corporate & Community Services	**DATE:**	6 August 2013
C.C.	Chief Executive Deputy Chief Executive (AJ) Head of Finance ICT Services Manager ICT Infrastructure Engineer		

1. Introduction

1.1 In accordance with the Audit Plan for 2013/14, an examination of the above subject area has been undertaken and this report presents the findings and conclusions drawn from the audit for information and action where appropriate. This is the first time that this topic has been audited.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2. Background

2.1 The project is part of the wider 'Bring Your Own Device' project and the Guest Wireless project will allow people to connect their own devices to the internet, using the council's wireless network.

2.2 Once live, use will be restricted to two types of users who will have slightly different levels of security. Guest level access will be for corporate visitors and they will be required to request a day ticket for access.

2.3 Corporate guest access will be for senior staff members, and this will have a slightly different security setting but it will, essentially, offer the same basic rights regarding internet access for council owned devices.

2.4 There is also a separate Riverside House corporate wireless network (RVH Wireless), which allows general network access. However, this is not part of the guest wireless project and, as such, has not been covered under this review.

3. Scope And Objectives of the Audit

3.1 The audit was undertaken to review the general implementation and ICT security controls in place to support the project.

3.2 In terms of scope, the audit covered the following areas:

- Project scoping
- Risk assessment

- Physical security
- Logical security.

3.3 The audit programme identified the expected controls. The control objectives examined were:

- Customer demand and capacity requirements have been assessed for all WDC sites
- A risk assessment has been undertaken and has been utilised in developing the control environment
- Physical security controls protect wireless access points in public areas
- Appropriate logical security measures are in place.

4. Findings

4.1 Project Scoping

4.1.1 The ICT Infrastructure Engineer (IIE) provided a copy of the Wireless LAN Proposal from BT iNet which sets out the scope of work that they would provide. The document also includes details of the council's requirements.

4.1.2 However, whilst the requirements are shown, this does not detail how they were arrived at, i.e. what demand was in place, how demand for individual sites had been established etc.

4.1.3 The ICT Services Manager (ISM) confirmed that there was no formal business case, but advised that proposals had been put to the ICT Steering Group as part of a presentation looking into the council's 'Agile Working' project, related business drivers and relevant new technologies that could be implemented to support these.

4.1.4 Indicative costs were included in the presentation, although the ISM advised that the guest wireless costs had reduced as a result of a general network upgrade that was required to solve an existing business problem. The existing infrastructure has also determined which sites will initially be included in the project.

4.1.5 The IIE advised that the Cisco Prime system, which has been put in place to manage the guest wireless network, will produce alerts should any issues arise in terms of capacity, and will allow for monitoring to be performed.

4.1.6 However, he stated that the project had been specified to such a level that capacity was unlikely to become an issue (e.g. the controllers can support up to 250 devices, whereas the council currently has a license for 50, with only 29 currently being in place), and that formal monitoring was, therefore, unlikely to be required.

4.2 Risk Assessment

4.2.1 The IIE provided a copy of the risk log that had been drawn up for the project. Counter measures (controls) are identified on the log that show how each risk will be mitigated.

4.2.2 There is nothing on the log that identifies risks at specific locations, although the risk of Wireless Access Points being stolen from public areas is recorded.

4.3 Physical Security

4.3.1 The IIE also provided a list of the wireless access points that currently exist. He advised that, if any devices were stolen, they would not be able to 'talk' to the controller as they are only lightweight 'dumb' devices.

4.3.2 He also advised that all of the devices at the Town Hall are in individual rooms that are locked when not in use and that CCTV is in place. The other device in a public place is in the Housing 'Frontline' area which is generally staffed when Riverside House is open to the public.

4.3.3 He added that an element of physical security is present in that devices are locked onto the mounting brackets, so that someone could not just pick them up and walk away.

4.4 Logical Security

4.4.1 The IIE advised that all guest wireless access is routed through separate controllers, with rules being set to allow only certain traffic. This ensures that all of the traffic goes through the DMZ. This was confirmed via a review of the settings.

4.4.2 He added that the controller allows access to certain ports and allows back-ups. Specific rules also had to be set up to allow use of the Good Technologies, as this doesn't work via web ports.

4.4.3 The IIE also advised that the only people who had administrative access rights to the wireless controllers were members of the ICT Infrastructure Team.

4.4.4 This access is via a generic user ID, with only members of the team knowing the password. Helpdesk staff have a separate, generic, log-in which only allows limited access to provide access tickets. Again, a system review confirmed this to be the case.

4.4.5 The IIE highlighted that the firewall will control which ports can be accessed (i.e. it will only allow access to http and https sites). However, he advised that there is no proxy filter in place that will determine which internet sites can be accessed, although he highlighted that there was an option to put this filtering in place, but this was not possible within the funding available for the project. Whilst no specific recommendation is to be raised regarding this issue, it is considered worthy of note and future consideration of this issue may be warranted should funding become available.

4.4.6 The ISM is currently working on user guidance and sign-up documentation that will set out the terms and conditions of use and these are going to be completed before the service is rolled out. A draft working document was provided, which includes details of the different wireless networks, some frequently asked questions and a disclaimer for the guest wireless network.

4.4.7 The IIE advised that every SSID (Service Set Identifier) is secured using WPA2 AES encryption, to 802.11i standards, which is the highest standard available. This was confirmed upon review of the Cisco Prime system.

4.4.8 As noted above, the IIE highlighted that access to the Corporate Guest network is only provided to specific council owned devices (iPads). This is controlled via limiting access to the specific MAC addresses of the devices.

4.4.9 He also added that these devices would not be provided with access to the main RVH wireless network. Similarly, other council owned wireless devices (laptops) would not be given access to the Corporate Guest network.

4.4.10 The two guest wireless networks being used (guest and corporate guest) do not actually indicate that they are WDC SSIDs. The IIE highlighted that the Cisco Prime software would flag up any networks that were causing

interference and that lists of rogue APs (access points) are also available, with a sample list being viewed at the time of the audit review.

5. Summary & Conclusion

5.1 Following our review, we are able to give a SUBSTANTIAL degree of assurance that the systems and controls in place for the Guest Wireless Project are appropriate and are working effectively.

5.2 One issue was noted with regards to the lack of a proxy filter for the guest wireless networks, although no formal recommendation is thought to be warranted. However, this situation should be kept under review and be revisited should funding become available.

Richard Barr
Audit and Risk Manager