# WELLAND INTERNAL AUDIT CONSORTIUM
# Harborough District Council

Date: 10th March 2010 **CoCo IT Healthcheck – Onsite Security** REF: H/CICT/1/2010

## EXECUTIVE SUMMARY

## Context

The purpose of this report is to provide management with assurance that the Council meets the security requirements of the Government Code of Connection. The vulnerability assessment is a technical and systematic testing and scanning process of the security of servers, domain names, IP addresses, routers and firewalls. The testing identifies vulnerabilities that could be exploited by individuals from within the Council's networks (employees, Members, authorised contractors etc.). A separate report refers to the vulnerabilities from individuals who do not have authorised access to the Council's networks.

The testing was carried out by NTA Monitor Ltd to highlight and categorise any security issues identified and provide an explanation of the issues raised. NTA Monitor Ltd is an accredited company, commissioned by Welland Internal Audit Consortium to perform the appropriate testing required to comply with the Government Code of Connection. NTA produced a complex and technical report with significant detail which has been reviewed and analysed by the Acting Head of IT and the Consortium to develop an action plan to address the significant issues identified. This report is a summary of the main issues of concern.

## Overview

The security scan discovered a number of confirmed and unconfirmed security vulnerabilities, as summarised in the table below. Unconfirmed vulnerabilities are issues known to be associated with the software types and versions the Council is running but due to the risk of damage to systems through testing, their presence could not be completely confirmed.

| Severity | Confirmed vulnerabilities | Unconfirmed Vulnerabilities | Total Vulnerabilities |
|---|---|---|---|
| High Risk | 3 | 2 | 5 |
| Medium risk | 8 | 0 | 8 |
| Low risk | 11 | 0 | 11 |
| Informational | 0 | 0 | 0 |
| **Total** | **22** | **2** | **24** |

Overall, NTA's assessment of the onsite security level is **High Risk** and some security issues need to be addressed immediately.
The Head of Change accepts that some security issues were identified and steps have been taken to address the higher risk areas. However, some issues classified as High Risk by NTA, are considered less serious in the context of maintaining operational functionality for the Council, and action will be considered on an individual basis.

Although there are a number of separate security issues, the most significant found during this security scan are as follows:

**1. Regular password strength analysis**
A good password policy is fundamental to any security policy. However, password policies can be bypassed by users who meet the requirements but still choose insecure passwords (i.e.Password1). A procedure should be put in place along with a strong password policy. The procedure should include regular password analysis tests, with particular attention on accounts with elevated privileges (i.e. Domain admin).

**2. No restriction to sensitive area**
Some accounts of the Council's mysql database allows authentication through blank password. Furthermore one of the PHP applications i.e. phpMyAdmin allows unauthenticated access.

**3. Security patches have not been applied**
The Council's Windows servers had not had the latest security patches and service packs applied and hence are vulnerable to a number of issues including remotely executable flaws, remote buffer overflow and denial of service vulnerabilities.

As a number of risks have been identified and changes should be made, the assurance rating following this audit is

**MARGINAL**

*The recommendations are listed on the action plan.*

## Scope

The Code of Connection IT Health Check – Onsite Security included an examination of the following:

- Registry search and checks
- Onsite routing checks
- DNS search and checks
- Onsite router checks
- Firewall checks
- Onsite server checks
- Other visible system checks

## Acknowledgements

The help and co-operation of the Acting Head of IT and the IT Team was much appreciated by the Auditor.

NTA Monitor Ltd

## ACTION PLAN

| RECOMMENDATION | | Priority | Officer Responsible | Agreed Action and completion date |
|---|---|---|---|---|
| Internal policies should incorporate a strong password policy (if one does not already exist). Users should be encouraged to follow this policy and should be notified that regular password audits may occur. | | Medium | Head of Change | **30/09/10** |
| Password authentication mechanism should always be used to restrict unauthorised access to the sensitive area of the network such as database accounts and administration control panel. | | Medium | Head of Change | **30/09/10** |
| The latest service packs and hotfixes from Microsoft should be applied as soon as possible after they are released. | | High | Head of Change | **30/09/10** |
| The table of test findings presented in the detailed NTA report should be used as a checklist for investigation and recording action | | Medium | Head of Change | **30/09/10** |

**NOTES**:

| | | |
|---|---|---|
| Action Plan Grade Classification: | H-High, M-Medium, L-Low | Order of Priority of Implementation. Please note that it will normally be expected that all recommendations will be implemented within 6 months. |

The range of Assurance ratings is as follows:

| Audit Opinion: | Explanation: |
|---|---|
| GOOD | Minor risks have been identified. |
| | |

| | |
|---|---|
| SOUND | Some risks have been identified and some recommendations made. |
| MARGINAL | A number of risks have been identified and changes should be made. |
| UNSATISFACTORY* | Unacceptable risks have been identified and changes must be made. |
| UNSOUND* | Major risks exist and fundamental improvements are required. |

A rating of “Unsatisfactory” or “Unsound” requires immediate management attention and arrangements will be made for a further review to be carried out at a later (agreed) date.