ARGYLL & BUTE COUNCIL

Internal Audit Section

INTERNAL AUDIT REPORT

CUSTOMER DEPARTMENT	**CUSTOMER SERVICES**
AUDIT DESCRIPTION	**RISK BASED AUDIT**
AUDIT TITLE	**INFORMATION COMMUNICATIONS TECHNOLOGY**
AUDIT DATE	**MAY 2015**

2014/2015

1. AUDIT SCOPE AND OBJECTIVES

A review of Information Communication Technology (ICT) within the Customer Services Department has been planned as part of the 2014-15 Internal Audit programme.

The ICT Strategy 2013 – 16 looks at the major challenges to be addressed during that period within national strategies, Scottish Wide Area Network (SWAN) and Next Generation Broadband Project as well as information management and security, mobile working, collaborative and shared services, cloud computing and further innovation. This Strategy complements the Council's corporate objective to become a "forward looking and ambitious" organisation.

Argyll and Bute Council will continue to take advantage of ICT, plan and procure better and share future developments and operations where the benefits to the Council clearly deliver better services the people of Argyll and Bute.

Obligations in participating in the Public Service Network (PSN), dictate that organisations undertake annual security health checks and maintain appropriate security policies including Acceptable use and lockdown policies. The Code of Connection requirements for accessing the PSN are stringent.

The ICT service was successful in obtaining PSN accreditation on 26 September 2013. The service submitted a renewal for PSN accreditation on 24 December 2014 but was declined. The submission was deficient in the format of the remediation plan and the Baseline Personnel Security Standard (BPSS) requirement for all users to have Disclosure Scotland or PVG scheme membership. These deficiencies have now been addressed/ mediated and a renewed compliance certificate issued.

2. AUDIT SCOPE AND OBJECTIVES

The scope and objectives of the audit are limited to:

- Assessment of compliance with the Public Service Network Code of Connection (PSN CoCo).

3. RISKS CONSIDERED

Strategic Risk Register (SRR): ICT infrastructure and asset base does not meet current and future requirements. Infrastructure and asset base is not being used or managed efficiently or effectively.

Operational Risk Register (ORR): Failure to ensure availability of IT applications when business needs them or to meet demand from services for assistance with implementing new technological advances

Audit Risk: Non-compliance with Public Services Network Code of Connection (PSN CoCo).

4. AUDIT OPINION

The level of assurance given for this report is Substantial.

Level of Assurance	Reason for the level of Assurance given
High	Internal Control, Governance and the Management of Risk are at a high standard with only marginal elements of residual risk, which are either being accepted or dealt with.
Substantial	Internal Control, Governance and the Management of Risk have displayed a mixture off little residual risk, but other elements of residual risk that are slightly above an acceptable level and need to be addressed within a reasonable timescale.
Limited	Internal Control, Governance and the Management of Risk are displaying a general trend of unacceptable residual risk and weaknesses must be addressed within a reasonable timescale, with management allocating appropriate resource to the issues.
Very Limited	Internal Control, Governance and the Management of Risk are displaying key weaknesses and extensive residual risk above an acceptable level which must be addressed urgently, with management allocating appropriate resource to the issues.

This framework for internal audit ratings has been developed and agreed with Council management for prioritising internal audit findings according to their relative significance depending on their impact to the process. The individual internal audit findings contained in this report have been discussed and rated with management.

5. FINDINGS

Argyll and Bute Council successfully achieved re-accreditation to allow access to the Public Service Network on 23 January 2015. To achieve this, a validated information assurance assessment was carried out against a series of stated conditions to gauge compliance; evidence and explanations are provided in support of each response:

Network Diagrams & Scope

A technical diagram providing a pictorial, high level overview of Argyll and Bute Council's external network connections accompanied with supporting explanation was provided to evidence compliance.

Information Risk Management

The Executive Director of Customer Services is the nominated Senior Information Risk Owner. A risk management policy based on a technical risk assessment is in place and agreement reached that this will be regularly reviewed by the Council's Information Security Forum.

Physical Security

It was evidenced that access to each of the Council's data centres hosting PSN equipment is strictly controlled using dedicated swipe cards allocated to users according to their needs of access.

Personnel Security

It was evidenced that all Council staff have recently undergone BPSS checks to enable access to Council network and systems.

User Education

It was evidenced that the Acceptable Use Policy has been recently updated and includes ICT user guidance and references to further more specific guidance for staff. This policy must be signed by all members of staff in agreement of its requirements prior to being allowed access to Council networks and systems.

Incident Response

It was evidenced that the Council has considered the PSN incident Management process and has updated existing procedures accordingly. Incidents are managed and escalated as required with immediate investigation carried out.

Configuration

It was evidenced that only designated ICT staff have administrator access to ICT hardware and software configurations. A change management process is in place requiring testing and approval before rolling out patches and updates to Council ICT equipment. Requests for additional and removable media access must be approved by management prior to enablement.

Compliance Checking

Surecloud Check Consultant identified 6 areas receiving a Common Vulnerability Scoring System (CVSS) score of more than significant-medium risk. It was evidenced that mitigating actions are in place which reduce scoring to low or low-medium residual risk assessment for these 6 areas.

Patch Management

IT was evidenced that a patch management policy has been implemented to ensure that all critical patches are applied within one month of release and non-critical within 3 months unless operational problems have been identified.

Access Control

It was evidenced that all members of staff are allocated a unique user name to access the Council's network and applications connected to the active directory following completion and submission of a signed and authorised acceptable use policy. Individual applications not connected to the active directory will require additional user names allocated by the administrator for that system. Leaver reports are received from the Council's HR team and used to suspend these users for 6 weeks prior to full deletion. Access levels to systems are authorised by management according to business requirements as are mobile and remote working facilities.

Boundary Controls/ Gateways

IT was evidence that the Council has deployed a protective marking system that is based on the Government Classification Scheme. Strict network controls are in place including firewall configurations, infrastructure changes managed using Prince2 methodology, content analysis including anti-virus and checks for malicious content on email and attachments and filters to allow attachments file types from a white list of allowed files.

Removable Media

It was evidenced that the standard build of Council PCs prevents the use of removable media, however, where business needs require access the removable media policy allows for senior management to authorise access on an exceptional basis.

Malware Protection

It was evidenced that servers are set to check for malicious content on web and email traffic and block when identified. Additional anti-virus software is active on all file server and desktop devices to identify malicious software including that from removable media and remove according to anti-virus policy

Mobile/ Home Working

It was evidenced that mobile/remote/home working solutions are exercised in accordance with the Council's remote/mobile working policy. User guidance is provided within the policy and allows for users to access Council systems to the same level as they would be permitted within Council premises. Full disk encryption and CISCO VPN client are installed on all council owned laptop computers as part of the standard build for remote working equipment, access to Council network and systems still requires user's 2 factor authentication (usernames and passwords) consistent with office based use. VPN certificates are deployed to laptops to verify that it is a council supplied device. Users are not allowed to access Council networks and systems from their own devices.

Wireless Networks

It was evidenced that the Council's wireless networks are segregated from guest access with the policy identifying and mitigating the risks of using wireless networks/devices.

Network Obfuscation

It was evidenced that annual security testing is undertaken to ensure that internal network information remains confidential and not available externally.

Protective Monitoring

All Council equipment that attaches to the corporate networks have static IP addresses and unique network names. Network and server teams monitor logs of user activity, exceptions and information security events on a daily basis to identify issues and unusual events, these are analysed, investigated, resolved and escalated to management where appropriate.

eMail

It was evidenced that the Council is using appropriate labelling that is in line with the Government Protective Marking Scheme.

5. Conclusion

This audit has provided a substantial level of assurance. There were no recommendations for improvement identified at this time.

Contact Details

Name	Mhairi Weldon
Address	Whitegates, Lochgilphead, Argyll, PA31 8RT
Telephone	01546 604294
Email	mhairi.weldon@argyll-bute.gov.uk

www.argyll-bute.gov.uk

Argyll & Bute – Realising our potential together