Internet, Email and Lync Misuse

City of York Council

Internal Audit Report 2013/14

Business Unit: Customer & Business Support Services,
Responsible Officer: Assistant Director, Governance and ICT
Service Manager: Head of ICT
Date Issued: 4th June2015
Status: Final
Reference: 10245/002.bf

	P3	P2	P1
Findings	**1**	**1**	**0**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

Almost all council staff and members are provided with access to the Internet and electronic communication methods such as email and Lync.

These systems are provided primarily for the purposes of business enablement, although some personal use is permitted, as long as it does not impact upon operational capability, as detailed in the council's Electronic Communications Policy.

It is important that robust systems are in place to manage the use of Internet and electronic communications, and that controls keep pace with technological developments. The Fraud Risk Assessment undertaken in February 2013 identified misuse as an area for further internal audit work to confirm whether appropriate controls are in place to manage the risks to the organisation.

In addition to the use of preventative technological measures and monitoring behaviour, this includes ensuring that all ICT users receive ongoing training to make them aware of their responsibilities.

Objectives and Scope of the Audit

The purpose of the audit was to provide assurance to management that the controls which it has put in place to manage key risks relating to the use of the Internet and electronic communications are effective.

The audit covered the following key risks:

- that systems are misused within working hours, leading to reduced employee efficiency and financial loss;
- that systems are used to access or distribute illegal or unacceptable material; leading to reputational damage or legal liability
- that the misuse of systems impedes network performance and leads to reduced efficiency; and
- that potential or suspected misuse is not thoroughly and promptly investigated.

Key Findings

The Council uses effective software to block unacceptable Web content from being viewed. There is a small number of users who have unlimited access because of their roles, and this is well managed. Appropriate logs of users' online activities are retained.

However, it is unclear which version of the Electronic Communication Policy is current, and policy reviews and revisions are not recorded. xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Overall Conclusions

It was found that the arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation but there is scope for improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided **Substantial Assurance**.

CITY OF YORK COUNCIL

Area Reviewed: Acceptable use policies

1 Issue/ Control Weakness	Risk
It is unclear which version of the Electronic Communication Policy is current, and policy reviews and revisions are not recorded.	Multiple sources and versions of policy information may create confusion for the user. Policy may not keep pace with technological developments.

Findings

A number of documents are available on the intranet relating to acceptable usage, including a 2006 Electronic Communications Policy (ECP) and a revised version from 2013. The 2013 ECP states that it is effective from August 2013 but this policy is still in draft and is awaiting approval from the Corporate Information Governance Group.

Neither version of the ECP includes a review or revision log so it is not possible to tell how often reviews or revisions have been carried out.

Users currently have to click 'ok' to confirm that they will abide by the terms of the ECP as part of the network log-on procedure but if there is any lack of clarity about which ECP is current then any acceptance is less meaningful.

The planned metacompliance system, which would involve users reading and acknowledging policies online and a record being kept of this acknowledgement, has not yet been put in place.

1.1 Agreed Action

The replacement ECP has now been signed off by CIGG and other groups and it does contain version control and version details.

Metacompliance or iComply is in place and has been deployed/used by 3 service areas including ICT staff to test the understanding of the new ECP ahead of its wider distribution.

The revised/replacement ECP will be distributed during the summer/early autumn this year (2014) and staff will have their understanding confirmed via iComply and the acceptance text will make reference to what version is being used.

Priority	3
Responsible Officer	Head of ICT
Timescale	30th October 2014

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

2	Issue/ Control Weakness	Risk
	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Findings

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

2.1 Agreed Action

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Priority	2
Responsible Officer	Head of ICT
Timescale	30th September 2015

Audit Opinions and Priorities for Actions

Audit Opinions	
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.	
Opinion	**Assessment of internal control**
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.