CITY OF VANCOUVER

Internal Audit Summary Report

September 14, 2015

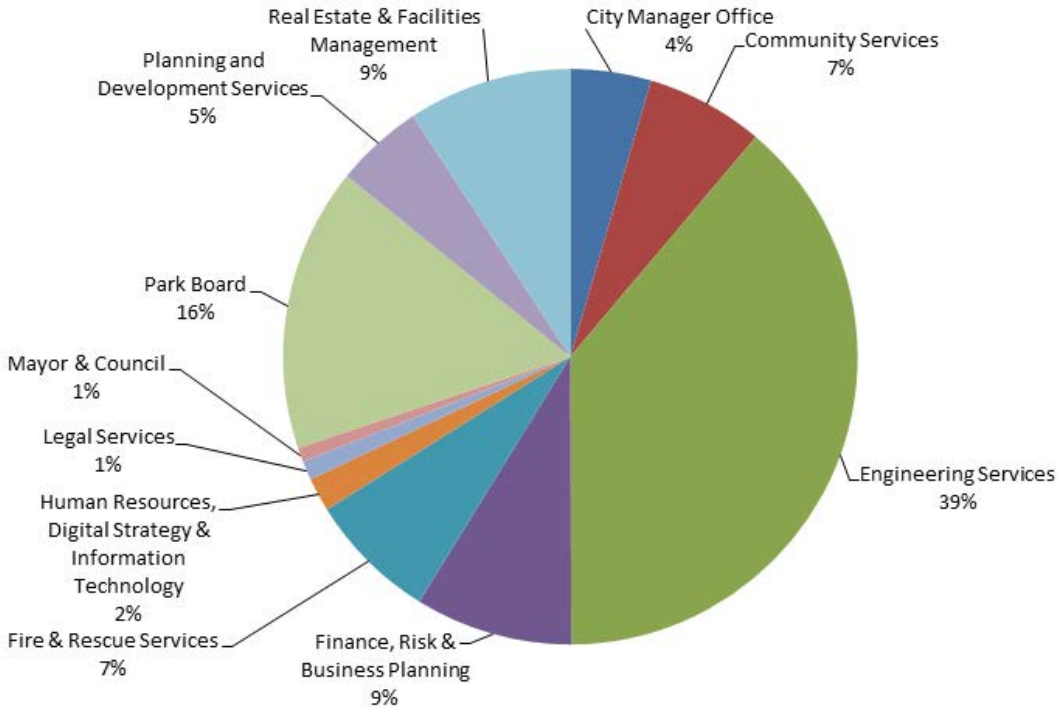
Mobile device audit

Background

The features that make mobile devices useful; such as portability, access connectivity, data storage and processing power, also make them a security concern when these devices contain City data. Major features of mobile devices that represent a risk include their small size so they can be easily lost, stolen, or misplaced; weak user authentication mechanisms that can be easily compromised or simply disabled by the user; and their ease of connectivity.

The Telecommunications branch of the Information Technology Department is responsible for telecommunication services and the provision of smartphones and standard cellphones. The City had three wireless providers: Rogers, Telus and Bell and has moved to Bell as the sole provider to achieve efficiency gains and reduce administrative efforts. The tool Cimpl is used for reporting on usage.

Over 2100 mobile devices are used by City employees; the breakdown of cell phones and smartphones by departments is as follows:



It is estimated that the new Bell plan will cost approximately $840,000 annually which represents a projected saving of 25% over the 2014 actual costs.

Scope

Our audit objectives were to provide assurance to management that mobile devices are managed effectively, deployed economically and data and devices are secure.

The audit was initiated for the purpose of determining:

- that data is secure;
- that assets are protected;
- that devices are used efficiently;
- that policies and procedures are sufficient and applied consistently; and
- that processes are effective and efficient over management monitoring of device usage.

Cell phones, smartphones, and to some extent tablets and laptops were examined. Other mobile devices such as USB sticks were excluded from this audit.

Conclusion

Mobile device business processes need improvements in oversight and monitoring, and internal controls relating to the protection of data should be tightened. Management has committed to strengthen data security, formalize policies and procedures and improve usage monitoring.

The more significant findings and recommendations are:

1) Update and finalize mobile device policies and procedures

As there have been a number of changes relating to mobile technology at the City, related policies and guidelines need to be updated and finalized. Management has agreed to:

- Establish encryption for Windows-based tablets and laptops;
- Finalize and approve the Mobile Technology Acceptable Use Guideline;
- Finalize and approve the Mobile Technology Policy;
- Update Policy AG-021-01 – City Hall Complex Security Access; and
- Remove the outdated "City Cell, Smartphone, and Accessories Standard" from CityWire and update related pages on CityWire.

2) Strengthen monitoring controls for extra charges

Currently threshold reports are sent to users and managers if certain limits are exceeded. However, an answer from the business unit is not required and no follow up is performed.

Implementing a formal follow up process by asking for responses and approval would ensure costs are appropriate. Management has agreed to:

- Establish a formal follow up process on threshold reports;
- Follow up on unused devices and deactivate devices as needed;
- Monitor roaming charges with the new Bell plan for appropriateness; and
- Follow up with users that have multiple devices.