KINETICS GROUP
making IT work for you

A Kambium Partner

I.T. Review

& Recommendations

For: Test Company

Prepared by:	**Kinetics Group**
Author:	Jim Smith
Date:	June 06 2018
Document Reference:	IT Review
Version	1.0

Executive Summary

Overview

Test Company have identified that, to be competitive, their staff need IT systems that are collaborative, reliable, and secure. In order to support this vision, Kinetics Group have reviewed the current technology systems and processes in place at Test Company, and put together a plan of recommendations to make the IT systems better suited to that way that Test Company staff work.

This document outlines the results of work done by Jim Smith from Kinetics Group and Joe Bloggs from Test Company in May 2018 to review the many questions in the IT best practice review.

The IT infrastructure in place at the Test Company is well managed, with good systems in place to reduce security risks and data loss. Cloud applications should continue to be investigated to ensure the applications in place continue to meet staff needs, whilst ensuring corporate governance and security.

We recommend that Test Company continue to focus on how technology can work for their staff to help achieve their goals. Areas of particular note include:

- Coaching of the staff on the IT systems provided should be improved.
- Information assets should be further secured by checking and implementing governance and security over departmental cloud services and websites.
- Implement better integration between systems and provide staff visibility to data.

This document outlines a proposed roadmap to implement the recommendations found, and also outlines some broader strategies. The document is broken into four sections:

1. This executive summary.
2. Outline of our understanding of the current state of Test Company.
3. A summary of the recommendations.
4. Details of the recommendations, broken into Must Do, Should Do and Could Do.

IT Strategy

People

- Coaching of the staff on the IT systems provided should be improved.
- Improve staff awareness of targeted financial and security attacks and provide tips to reduce the risk.

Process

- Information assets should be further secured by checking and implementing governance and security over departmental cloud services and websites.
- Investigate alerting on sensitive group membership changes.
- Improve processes around staff starting, changing roles and leaving to reduce risk of incorrect permissions.

Technology

- Implement better integration between systems and provide staff visibility to data.
- Investigate commodity cloud services at a corporate level to reduce complexity and take advantage of the latest collaboration platforms

Current State

Organisation

- Auckland (45), Hamilton (13), Tauranga (5), presence in Wellington (1)
- Approximately 64 staff, with 64 computers.
- Internal IT team, some IT outsourcing
- There are 3 IT staff.

Systems

- vTiger – on premise CRM
- Exchange 2016 – on premise email
- Dynamics GP - on premise financials
- SharePoint 2016 (Intranet) - on premise some lists and forms
- Skype for Business 2015 - on premise some inter office comms
- Cisco Call Manager Cloud based phone system from Spark
- Cloud applications used by some departments e.g. BaseCamp, Buffer, SurveyMoneky

Issues and Risks

- Security vulnerabilities is an ongoing concern - balancing the needs of the business against the ability to enforce good security practices.

Projects

- Antivirus change from Symantec to ESET suite in December.
- Looking at moving telephony to Skype for Business away from Cisco.
- CRM upgrade just completing
- Gradual hardware upgrade from Windows 7 to Windows 10. To be complete by end of 2018.

Recommendations Index

The following outlines an index of all recommendations. Note that all costs are approximate, and the approximate effort required to implement is included to give an indication of the work involved/complexity of the task:

Red	A large project, possibly ongoing and involving multiple parties
Orange	A medium size piece of work that will require some planning
Green	A small piece of work relatively easily achieved

Must do - Action immediately

Title	Effort
Cloud Usage	1 - 2 Months
Computer Encryption	1 - 2 Days
Unmanaged Cloud Services and Shadow IT	2 - 3 Days
Application Integration and Data Insights	4 - 8 Weeks
Criminal Record Checks	2 - 4 Hours
Public Website Security	4 - 7 Days
Financial Transaction Security	1 - 2 Days
User Account Processes and Audit	1 - 2 Days

Should do - Plan for Action

Title	Effort
Data Archiving	7 - 14 Days
Protecting Information Assets	1 - 2 Months
Security Group Membership Change Alerting	2 - 4 Hours
Password Policy	1 - 2 Days
Security Penetration Testing	1 Month
Remote Access Improvements	2 - 5 Days
Web Proxy Improvements	2 - 4 Days
Staff Training	1- 5 Days

Could do – Investigate

Title	Effort
Two-Factor Authentication	2 - 4 Days
Computer Hardware Rotation	2 - 4 Hours
Automated email Signature	7 - 14 Days

Must Do - Action Immediately

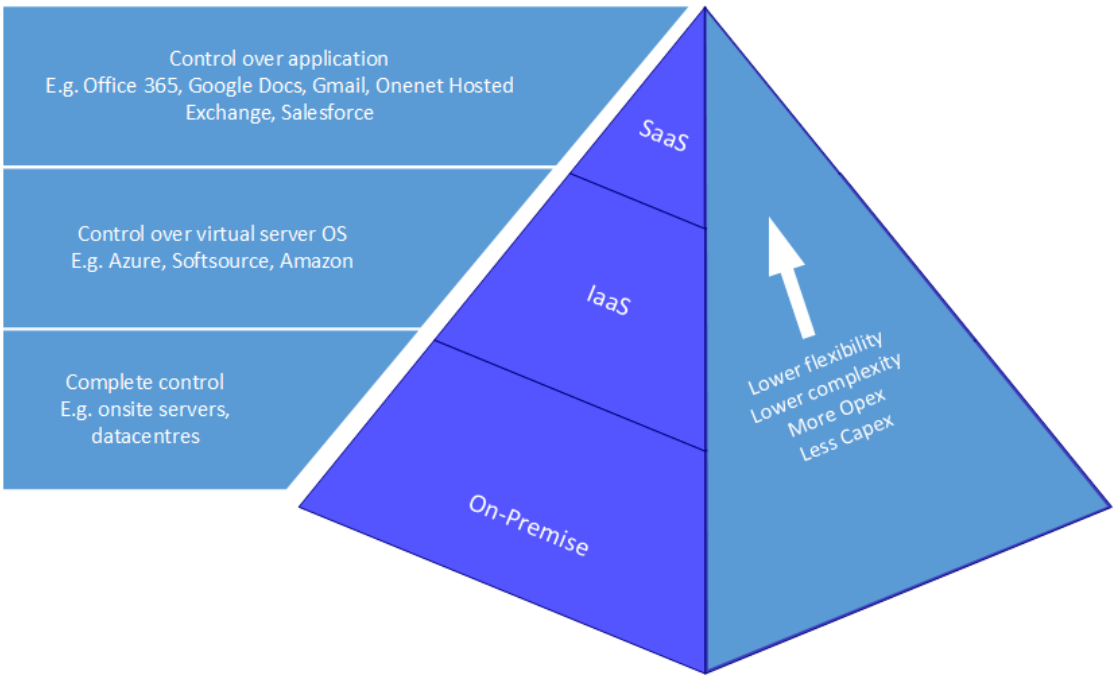
Information Assets

Cloud Usage

Business Problem

Can the use of cloud services provide Test Company added capability or capacity, or lower risks or costs? Currently the four cloud scenarios to consider are:

- **Software as a Service (SaaS)** – applications provided from the cloud such as Box.com or Office 365 for Email, SharePoint and Skype for business.
- **Infrastructure as a Service (IaaS)** – virtual servers provided from the cloud such as Azure/Amazon (in Australia) or Vocus (in NZ).
- **On premise or private cloud** – owned servers on premise or in a datacentre
- **Hybrid** – a mix of some or all of the above



Current Situation

Currently all systems at Test Company are hosted on premise, with no SaaS in use. SaaS systems such as Office 365 were investigated in the past but discounted due to cost.

Recommendation

As with everything, there are pros and cons to moving into the cloud. Although the cloud provides greater scalability, reduces infrastructure risk and provides applications that are unavailable on-premise it can reduce flexibility and performance.

We recommend that the Test Company continues to monitor and investigate SaaS solutions, such as Office 365, to see if the applications included can provide benefits to the organisation. The main benefits to the Test Company of these applications are the reduced ongoing maintenance costs, and the additional features that are only available in the cloud versions, such as SharePoint modern pages, Rights Management, Teams, Yammer, Planner and PowerBI.

Cost/Effort

Initial:	$TBC	**Ongoing:**	$0 - $500 per month
Effort:	1 Month(s) - 2 Month(s)		

Time frame

Jun 2018 - Jun 2019

Computer Encryption

Business Problem

Even a computer that has a password on it can have the data on it accessed by removing the hard drive and installing it in a second computer. There is a risk that if a laptop was stolen, sensitive data that is stored on the hard drive could be accessed. Enabling encryption, such as BitLocker, prevents access to the data on a computer without the password.

Current Situation

Test Company are not currently enforcing encryption on computers.

Recommendation

We recommend enforcing full disk encryption on all laptops that have a high risk of storing data locally initially. For Windows PCs this is Bitlocker, for Mac devices it is using the built-in encryption. The full disk encryption should be seamless to the staff unless there is a major hardware change to their devices. Note that TPM firmware updates should be applied before encrypting.

Cost/Effort

Effort: 1 Day(s) - 2 Day(s)

Time frame

Jun 2018 - Dec 2018

Unmanaged Cloud Services and Shadow IT

Business Problem

Do you know if any data is stored on unmanaged devices such as USB sticks or home computers? Or stored or staff personal cloud accounts such as DropBox, iCloud, Google Drive? This data can be removed without the organisation's knowledge and is more exposed to unauthorised access. If a staff member copies company data to their home PC, or Dropbox, and then leaves the company, we have no way of ensuring it is deleted or retrieved.

Current Situation

There are many cloud-based applications in use by departments within Test Company that are likely to be outside of the control or governance of the IT Test Company team. Applications such as Basecamp, Buffer are all in use by staff at Test Company and could have company data on them.

Recommendation

Often the reason staff use cloud apps or storage account is that it solves a problem for them - sharing and collaborating with internal or external staff in a way they can't currently do with existing systems.

We recommend reiterating with staff that there is a company cloud storage (DropBox) solution in place and they should use it where required.

We also recommend that the IT team ensure there is some sort of governance and security across the cloud applications in use - are user accounts/external sharing removed when they are no longer required? Is data removed from platforms when it is no longer required? Are the Test Company happy with the data privacy policies of the cloud apps in use?

Cost/Effort

Effort: 2 Day(s) - 3 Day(s)

Time frame

Jun 2018 - Dec 2018

Application Integration and Data Insights

Cyber Security

Criminal Record Checks

Governance and Management

User Account Processes and Audit

And so forth – many recommendations that stem from the structured interviews, all describing the business problem, current situation, recommendations, timing and costing

Should Do - Plan for Action

Information Assets

Data Archiving

Protecting Information Assets etc – many topics collated

And so forth – many recommendations that stem from the structured interviews, all describing the business problem, current situation, recommendations, timing and costing

Could Do - Investigate

Cyber Security

Two-Factor Authentication

And so forth – many recommendations that stem from the structured interviews, all describing the business problem, current situation, recommendations, timing and costing