Final Report - Family Grocer IT And Risk Management Consulting Engagement

IT Adventure

Team 4
University of Toronto
School of Continuing Studies
SCS_3373_030 Enterprise IT Risk Management & Cybersecurity

Agenda

- **Operational Recommendations**
- **Strategic Recommendations**
- **Q&A**

Operational Actions

IT Regulations recommendations

- **PCI/DSS**
- **GDPR**
- **SOX**

Operational Actions

SAP Implementation

- **Asia**
  - **Implement user adoption strategy**
  - **Customize and Localize software to suit locale**
  - **Redefine project scope and timelines**
- **Latin America**
  - **Address legacy systems**
  - **Implement compliance with local regulations**
  - **Communication and training**

Operational Actions

What to do with CRM

- **SAP has the benefits as a CRM and incorporating the larger organization**
- **Gradual move of the CRM in batches**
- **Prepare an inclusive onboarding package for the marketing, sales and Customer experience department**
- **Implement a customizable SAP**
- **Continuous monitoring for the first year**

Operational Actions

IT internal control regarding cloud services : Adopting ISO/IEC 27017

- A robust encryption practice for data in transit and rest as payroll is on the cloud with PII
- Implement Identity and Access Management
- Best practices for security - like Password rotation, MFA, least privilege
- Regular data backups to different regions - of the cloud provider in instants of failure in a particular regions
- Developing a unique and independent DRP for cloud based services
- Periodically check updates to SLA - with providers and ascertain they always remain compliant with standards through their shared documents
- Always ensure it is always listed in asset inventory and risk evaluation as an entity - as it can be overlooked in risk assessment as no risk is totally transferred - PII for payroll makes it important

Operational Actions

Desktop Software

- **Get a value from the C-suite on a value they are willing to budget**
- **Bargain with the vendor and offer incentives appropriately**
- **License planning**
- **The vendor management plan using COBIT AP009 & COBIT AP010**
- **COBIT Processes AP009 - Managed Service Agreements**
- **COBIT Processes AP010 - Managed Vendors**

Strategic Actions

Drones

- **Engage with a vendor using vendor management process**
- **GPDR Compliance**

IOT

- **Security training**
- **Implement Network segmentation**
- **Use RBAC vendor selection**

Web Based Grocery Stores

- **Implement Strong authentication techniques**
- **Use encryption and protected payment software**

Strategic Actions

Social Media

- **Privacy considerations**
- **Comply with GDPR and CASL on acquiring and managing customer data on social media**

Analytics

- **Appropriately notifying users**
- **Collecting user consent**

Chain of pharmacies

- **Harmonizing IT systems (SAP) and processes between family grocer and acquisition.**

IT Outsourcing

- **Unknown variables affecting risk**
  - **Costs of IT outsourcing vs remaining in house**
  - **Internal cost of change management to migrate all IT to an outsourcing provider**
- **Factors outside of IT Adventure’s realm of expertise**
  - **Impact of change management on culture, HR on the ability for the company to meet objectives**

IT Outsourcing

Risk Management Considerations for outsourcing to a 3rd party

- **Family Grocer should have an end to end governance system in place. Will the 3rd party be able to participate in governance controls when managing IT including vendors?**
- **Profile of vendor**
  - **What accreditations (e.g. ISO27001, PCI/DSS) does the outsourcing firm have?**
  - **What governance frameworks are in place (e.g. COBIT 2019) within that organization themselves?**
  - **Ability to be audited fully by governmental regulators (e.g. SEC)**

IT Outsourcing

Cybersecurity Considerations when engaging a 3rd party outsourcing firm

- **Role of a FamilyGrocer CISO**
  - **Ability to fully implement cybersecurity controls and practices on the outsourcing firm staff as per AP013 (e.g. Zero Trust software, password management, XDR/SIEM tools).**
  - **Ability to shut down insecure tools/processes run by the outsourcing firm**
- **Cooperation and transparency in the case of an incident and subsequent investigations**

IT Outsourcing - Conclusion

- **IT adventure recommends extensive study into the risk profile of the proposed outsourcing firm before proceeding, as well as the risks associated with the change management process**
- **If outsourcing is seen as the only way to solve business challenges, one potential option is to investigate outsourcing some IT functions (e.g. lower risk) as a proof of concept**
- **CIO Role should not be outsourced**

Questions?