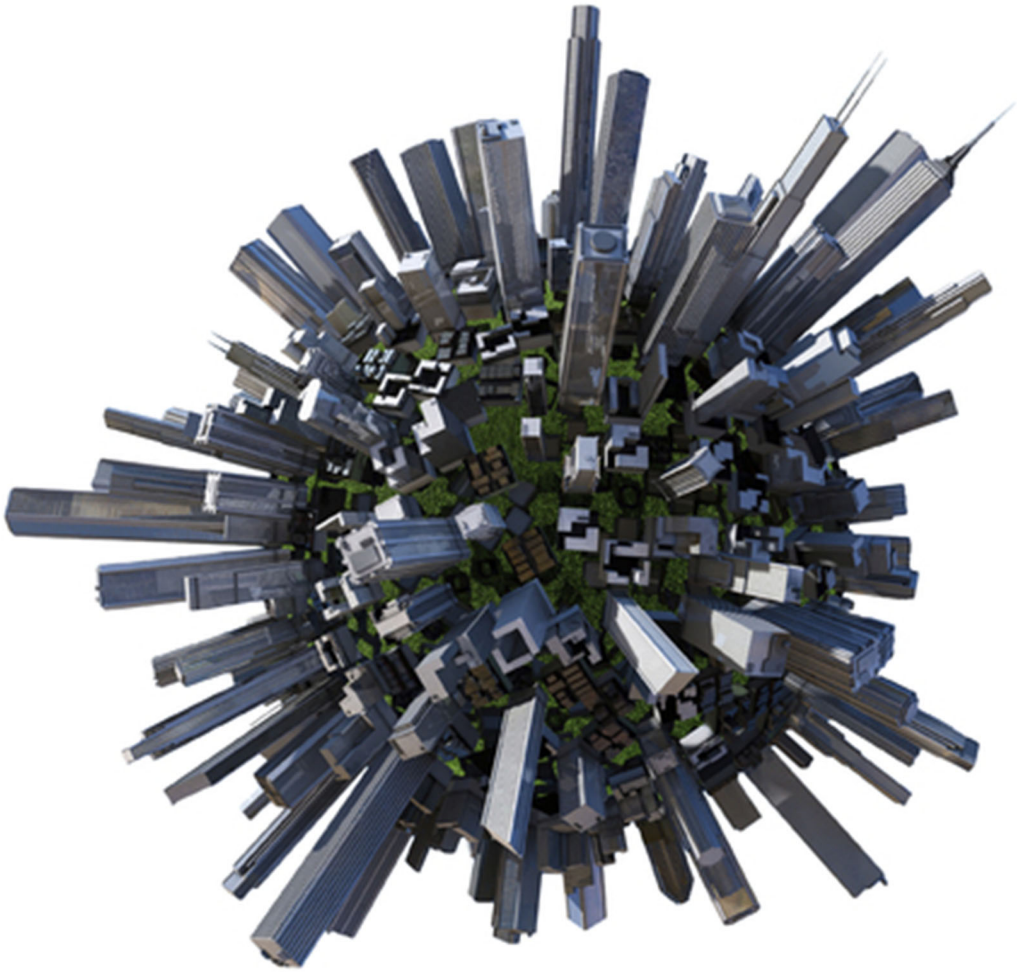
Deloitte.



The Corporation of the City of London

SaaS Application Review

Audit Performed: March 2021 – July 2021
Report Issued: October 21, 2021

Table of contents

Executive summary

Background

The City of London (the "City") aspires to enhance its security posture relating to the use of Software-as-a-Service (SaaS) applications within the organization. To this regard, the City recognizes the opportunity to improve controls and governance over SaaS applications usage by the City's employees and requested that the internal audit focus on leading practices for consideration. Internal Audit has provided guidance and leading practices with respect to tools, policies and procedures for consideration by management as the City continues to improve its SaaS application governance strategy. The leading practices within this report can be used to enhance visibility, governance and oversight over SaaS applications to decrease risk appetite from use of unapproved and unmanaged SaaS applications.

Objectives and scope

As part of the 2020-2021 Internal Audit plan, Internal Audit conducted a review of the controls and governance over Software-as-a-Service (SaaS) applications currently used by the City of London (the "City") employees. The purpose of this review was to assess the adequacy of relevant policies and procedures, and provide guidance in consideration of industry leading practices of tools, policies and procedures. The intent of the audit was to decrease the potential use of unapproved and unmanaged SaaS applications by enhancing visibility, accountability and oversight.

The detailed Internal Audit scope can be found in *Appendix 1: Internal Audit detailed scope* of this report.

Areas for continued enhancement

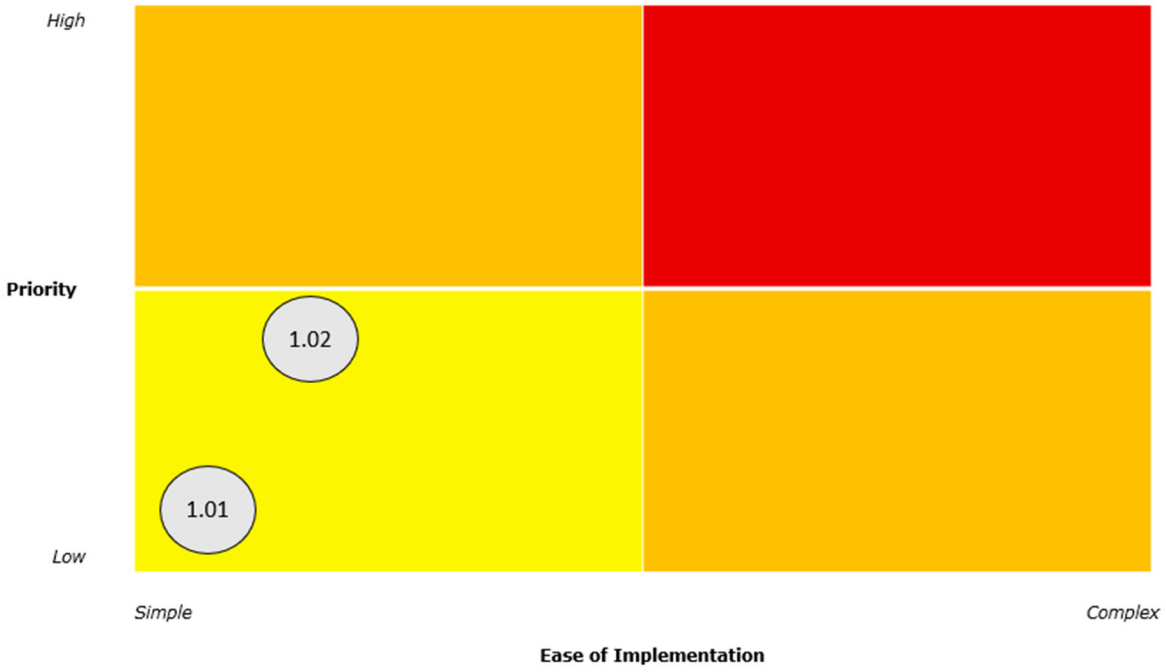
Based on our review of the City's SaaS application program, we identified one low and one medium priority observations that The City of London should consider going forward. Please refer to *Appendix 2: Internal Audit rating scale* for definitions of the four-point scale.

High priority	Medium priority	Low priority	Leading practice
0	1	1	0

Priority	Domain	Observation Id	Observation Summary
Medium Priority	People	SA 1.01	**IT Security Training:** Existing training does not include explicit content on SaaS applications. Accountability on continued use of non- sanctioned SaaS application is not clear.
Low Priority	Process	SA 1.02	**Policy and Procedure for SaaS application lifecycle**: Generic policy exists and is not reviewed and approved periodically.

Priority heat map

Based on our assessment of the City's SaaS application process the following image maps areas of continued enhancement based on priority and anticipated ease of implementation of our leading practice recommendations.



Conclusion

Based on our assessment of City's SaaS application process, we have identified **one low and one medium** priority observations, that should be addressed to improve internal controls and process efficiency. The identified considerations and observations noted in this report should be addressed in a timely manner to enhance current controls and mitigate relevant risks.

Areas for continued enhancement

In completing the procedures noted in *Appendix 4: Audit procedures performed*, Internal Audit identified the following areas for continued enhancement:

	Medium Priority	**SA 1.01 – IT Security Training**
Observation		While the document Handbook - Corporate Technology Section 7 mentions that no software should be installed on a COL computer without permission, it isn't specific to SaaS application access. Additionally, the current employee training does not yet include the usage of SaaS applications (Sanctioned and Non-Sanctioned). Accountability and repercussions of continued use of unsanctioned applications is not clear in the current policy.
Implication		Without updated training that explicitly includes considerations of SaaS application usage, employees could unintentionally expose the City to added risk, threatening the security of City's data and the integrity of corporate network.
Recommendation		We recommend expanding the existing training to include includes threats of unsanctioned SaaS applications. The Acceptable Use policy should also be updated to include information on the importance of compliance with such policies and discourage employees from non-compliance. The attendance for training should be monitored, and any deviations from the policy should be recorded and followed upon to reinforce the understanding of and compliance with the policy.
Management Comments		Management will take the following actions: 1. Update existing training to include specific information regarding SaaS applications, associated threats and potential impact to the delivery of Public Service 2. Update the Use of Technology Administrative Procedure to include SaaS specific information that is directly connected to procedure compliance
Responsible Party and timing		Mat Daley, Director, Information Technology services, Enterprise supports 3/31/2022

Low Priority	SA 1.02 – Policy and Procedure for SaaS application lifecycle:
Observation	While a policy (Use of Technology Administrative Procedure) exists, it is generic and does not explicitly cover the procurement, monitoring and reporting of SaaS applications. Additionally, policies were not reviewed and approved periodically. The policy was last reviewed in 2019.
Implication	The lack of well-maintained, formal policies and procedures can result in lack of compliance and inconsistent practices across organization.
Recommendation	We recommend documenting policies and procedures that are specific to SaaS application lifecycle Management. Policies such as following are recommended: • SaaS Vendor Onboarding and Offboarding (including periodic review) • SaaS Application Security • SaaS Application Risk Management (We noted that the Information Security Questionnaire covers 3rd party security assessments; however, it does not address an annual reassessment of the risks) These policies should continue to be reviewed as part of the annual policy review to ensure that they are in line with business requirements.
Management Comments	Management will take the following actions: 1. Document and formalize the SaaS application lifecycle management policy and procedure 2. Implement the SaaS application lifecycle management procedure
Responsible Party and timing	Mat Daley, Director, Information Technology services, Enterprise supports 6/30/2022

Appendix 1 - Internal Audit detailed scope

Specifically, the Internal Audit addressed the following areas:

Review of the controls and governance over Software-as-a-Service (SaaS) applications (April 2021):
• Review governing policies and procedures related to SaaS applications use, including but not limited to Acceptable Use policy and other relevant policies, to assess their adequacy and relevance; • Assess existing employee training and awareness initiatives related to use of SaaS applications; • Assess the current state of SaaS application (licensed and unlicensed) usage at the Corporation of the City of London; • Understand the IT Software procurement process as it relates to acquisition of SaaS applications; • Review the adequacy of management oversight and visibility over SaaS applications currently in use (approved and unapproved), including metrics for tracking, reporting and processes for decommissioning/blocking of unsanctioned applications; • Provide guidance and best practices with respect to SaaS monitoring tools to enhance management oversight and visibility over SaaS applications with the intent of decreasing the potential use of unapproved and unmanaged SaaS applications

Appendix 2 - Internal Audit rating scale

Individual observation prioritization

Internal Audit has prioritized each observation and recommendation within this report using a four point rating scale. The four point rating scale is as follows:

Description	Definition
High	Observation is high priority and should be given immediate attention due to the existence of either significant internal control risk or a potential significant operational improvement opportunity.
Medium	Observation is a moderate priority risk or operational improvement opportunity and should be addressed in the near term.
Low	Observation does not present a significant or medium control risk but should be addressed to either improve internal controls or process efficiency.
Leading Practice	Consideration should be given to implementing recommendations in order to improve the maturity of the process and align with leading practices.

Appendix 3 - Stakeholder involvement

In conducting this assessment, the following Service London management and staff were interviewed to gain an understanding of the Service London Contact Centre's processes and practices.

Stakeholder	Position	Division
Mat Daley	Director	Information Technology Services
Dean Thompson	Manager III	Information Security

Appendix 4 - Audit procedures performed

As part of The City of London's SaaS application assessment, the following procedures were performed:

- Conducted planning meeting with Director of Information Technology Services, and Manager II of Application Development
- Updated and issued finalized Project Charter and request for information
- Conducted meetings and interviews with City management and staff to obtain an understanding of the control framework and assessment criteria
- Performed interviews with key personnel on the current state of SaaS application usage
- Inspected the City's current SaaS applications processes related to: acceptable use policy, logical access management – access provisioning and deprovisioning, application acquisition, application monitoring, application reporting and applications decommissioning, SaaS applications related third party vendor management, employee IT security training and awareness, and SaaS software change management
- Responding to emails, phone calls and in-person requests, ensuring adequate process documentation (service requests), tracking and monitoring performance, compliance with applicable policy requirements, and training/onboarding of staff
- Obtained documentation regarding relevant procedures and controls to perform an inspection of:
  - SaaS application provisioning and approval
  - Risk assessments to identify key People, Processes and technologies,
  - Training and onboarding procedures for employees,
  - Relevant SaaS acquiring and change processes,
  - Workflow diagrams for SaaS lifecycle management processes, and
  - Monitoring procedures.
- Consulted with subject matter expert(s) on the City of London's current processes and compared to best practices used by industry leaders
- Using the reviewed documentation and interview narratives, assessed the effectiveness of SaaS applications program with regards to governance, oversight, visibility and accountability.
- Drafted preliminary observations and verified observations with management
- Conducted a closing meeting with key management stakeholders to validate and communicate our findings, and
- Issued this Internal Audit report with our detailed observations.

Deloitte.

www.deloitte.ca

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights and service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals—9,400 of whom are based in Canada—make an impact that matters, please connect with us on LinkedIn, Twitter or Facebook.