INFORMATION SECURITY STUDY

OF

EXCOTRACK:
CABINET DOCUMENT MANAGEMENT SOLUTION

2013 - 2016

Office of the Auditor General
Brades
Montserrat
January 2019

EXCOTRACK: CABINET DOCUMENT MANAGEMENT SOLUTION

This is the Report of an Information Security Study conducted by the Office of the Auditor General under the Montserrat Constitution Order 2010.

Florence A Lee
Auditor General
Office of the Auditor General
January 2019

INTENTIONALLY LEFT BLANK

PREAMBLE

Vision Statement

"To be a proactive Supreme Audit Institution that helps the nation make good use of its resources."

Mission Statement

"The O.A.G is the national authority on public sector auditing issues and is focused on assessing performance and promoting accountability, transparency and improved stewardship in managing public resources by conducting independent and objective reviews of the accounts and operations of central government and statutory agencies; providing advice; and submitting timely Reports to Accounting Officers and the Legislative Assembly."

The Goal

"To promote staff development, enhance productivity, and maintain a high standard of auditing and accounting in the public sector, thereby contributing to the general efficiency and effectiveness of public finance management."

AUDITOR GENERAL'S OVERVIEW

As technology advances, the Government of Montserrat's (GoM) Ministries and Departments have become increasingly dependent on computerised information systems to carry out their operations to process, maintain, and report essential information. The manual system to monitor/track the decisions of the Executive Council (EXCO, now Cabinet), proved inadequate and unsecured and was protracted. In an effort to provide efficient ways to monitor GoM's decisions and policies this system was replaced with a computerised bespoke virtual document management web application, ExcoTrack software which was developed by a former government employee.

Our review that covered the period July 2013 to July 2016 revealed that the ExcoTrack software is user friendly and accessible from any electronic device and no security breach or issues have arisen to date. However, we found that ExcoTrack's automated alert function does not always work sometimes causing significant delays and there is no formally signed agreement or contract between the GoM and Rovika Inc. which outlines clear ownership or operational parameters. Rovika Inc. retains all business knowledge and ownership of ExcoTrack which poses a high risk to GoM should Rovika Inc. fold, fail to maintain the software, or becomes insolvent. It is our recommendation that the Office of the Premier (OotP) take steps to ensure that a contract or service level agreement be developed and signed by the two parties.

We also noted that neither the vendor nor the GoM has a Business Continuity Plan, Disaster Recovery, IT Security Plan or Policies in place should there be a security breach to ExcoTrack. We have recommended the development of a BCP which describes the immediate steps to be taken during any disruption(s) and the action(s) required to recover.

As with this and other similar reviews, the GoM must desist from entering into software arrangements without having the necessary documented agreements or contracts in place. We have highlighted other findings and made a number of recommendations and the acceptance and implementation of these will improve the overall governance and management of ExcoTrack.

Subsequent to our audit of the software application ExcoTrack in 2017, it has come to the attention of the Office of the Auditor General that the GoM and the ExcoTrack software developer, Rovika are now engaged in legal proceedings surrounding contractual payments, data access and ownership, and the issue of overall ownership rights to the software. The OAG will revisit this matter at the conclusion of the court proceedings.

We wish to record our thanks to Staff of the Office of the Premier and Rovika Inc. and others who provided valuable information, clarifications or extended courtesies during the course of this review.

Florence A. Lee, CPA, BSc, MSc
Auditor General
January 29, 2019

CONTENTS

ABBREVIATIONS

AWS	Amazon Web Services
BCP	Business Continuity Plan
CabSec	Cabinet Secretariat
CIA	Confidentiality, Integrity, and Availability
CoC	Clerk of Council
DITES	Department of Information Technology e-Services
DRP	Disaster Recovery Plan
EXCO	Executive Council
FS	Financial Secretary
GoM	Government of Montserrat
HoD	Head of Department
IS	Information Security
ISAE	International Standard on Assurance Engagements
ISSAI	International Standards of Supreme Audit Institutions
I.T./IT	Information Technology
OAG	Office of the Auditor General
ODG	Office of the Deputy Governor
OotP	Office of the Premier
RBAC	Role-based Access Control
SAP	Security Access Protocol
SCO	Senior Clerical Officer
SLA	Service Level Agreement
SQL	Structured Query Language
SSL	Secure Sockets Layer

EXECUTIVE SUMMARY

The previous manual Cabinet Documentation System, proved inadequate and insecure. Consequently in 2012, a computerised version of the Cabinet documentation monitoring/tracking process, ExcoTrack, was developed in an effort to provide efficient ways to monitor/track the GoM's decisions and policies.

The main purpose of this Information Security review, is to assess and determine if ExcoTrack is self-sufficient, secure, and robust, with adequate application controls in place to ensure the integrity, completeness, accuracy, and security, of the (i) user information and (ii) Cabinet-related confidential information that is inputted, processed, and outputted, by the application software, and in a timely manner.

Main Findings

1. **Overall Achievement**. The Cabinet Secretariat had achieved its objective of having an automated Cabinet documentation monitoring/tracking software that is efficient and secured. The vendor, Rovika Inc., developed a very secure and robust application software that is user-friendly and accessible from any electronic and/or data-enabled device that has access to the Internet. To date, there has not been any internal or external security breach or issues, associated with ExcoTrack.
2. **Weaknesses identified**. However, the automated alert function does not always work and this causes delays in the decision-making process. Neither the vendor, nor Office of the Premier (OotP), has a Business Continuity Plan (BCP) or IT Plan or Policies in the event of a security breach to ExcoTrack. There is also the serious issue of not having a formally signed contract/agreement between the two entities, in addition to the nonexistence of a Service Level Agreement that clearly outlined who retains all business knowledge and ownership of ExcoTrack's data and process (es).

Key Recommendations

1. **Business Continuity.** The Office of the Premier (OotP) should request the establishment of a detailed contingency strategy documentation from Rovika Inc., that is, a Business Continuity Plan, or Risk Register. OotP should also devise their own contingency plan pertaining to ExcoTrack either separate from, or established on, Rovika Inc.'s contingency strategies. A Business Impact Analysis (BIA) and a Risk Assessment, have to be conducted before the BCP can be developed at the Risk Management stage.
2. **Outsourcing.** Develop a Service Level Agreement (SLA) that defines what the future I.T. services vendors/contractors will be expected to accomplish and the technical parameters for those services. For future outsourcing of IT service providers, create an outsourcing service contract with proper security management processes in place to protect the Office of the Premier's data, and to mitigate any security risks associated with outsourced IT projects and/or services.

Prepare a post-contract/agreement, to be signed by OotP and Rovika Inc. that clearly state and affirm OotP's ownership of the data stored by, or on, the service provider's system and specifies their rights to the data/information (intellectual property rights).

In terms of risk of supplier failure, assess the feasibility of purchasing the software and maintaining it in-house, at the Department of Information Technology & e-Services (DITES); or request that the software be lodged in an escrow agreement.

3. **Information Security.** Devise and distribute/circulate an Information Security (IS) policy to the various government departments in relation to ExcoTrack; for example, non-disclosure agreements, enforce and check strong passwords (authorise), and user account creation/deactivation process.

Audit Conclusion

The Office of the Auditor General (OAG) has determined that ExcoTrack is self-sufficient, secure, and robust, with adequate application controls in place. These controls ensure the integrity, completeness, accuracy, and security, of the user information and Cabinet-related confidential information by the application software. However, ExcoTrack's automated alert function does not always work sometimes causing significant delays.

We also established that OotP has not made any provisions to ensure continuance of service if person(s) and/or entity maintaining the application software should leave, fold, or have their services terminated; or in the event of a security breach or other mishaps. As with this and other similar information systems reviews, the GoM must desist from entering into software arrangements without having the necessary documented agreements or contracts in place.

Subsequent Events

Subsequent to our audit of the software application ExcoTrack in 2017, it has come to the attention of the Office of the Auditor General (OAG) that the Government of Montserrat (GoM) and the ExcoTrack software developer, Rovika are now engaged in legal proceedings surrounding contractual payments, data access and ownership, and the issue of overall ownership rights to the software. It is important to note that some of the issues highlighted in the audit have manifested themselves and led to the GoM no longer being able to use the software for its regular Cabinet data management operations. It is our understanding that GoM now has 'read only' access to the data in ExcoTrack, and is seeking an alternative solution for document management for the Cabinet Office. The OAG will revisit this matter at the conclusion of the court proceedings.

CHAPTER 1 INTRODUCTION

BACKGROUND

The Cabinet Secretariat (Cab Sec) Unit was established in 2012 by the previous government to coordinate, monitor, and evaluate the implementation of the whole of the Government Policy and Planning and provide technical support through the Cabinet Secretary (now the Director of Policy and Planning) - to the Governor, the Premier, Ministers of Government, and their Ministries. This division no longer exists and the functions have since reverted to the Office of the Premier (OotP). The OotP now manages the Cabinet decision-making process and works closely with the Governor, the Premier, and other Cabinet members to ensure that Cabinet receives accurate information and documentation to support its decision making process.

The Clerk of Council previously managed and disseminated Executive Council (EXCO) (now Cabinet) documentation, manually. In addition, a Microsoft Access Database was used by the Office of the Deputy Governor (ODG) for the monitoring of Cabinet Decisions. This manual monitoring process proved to be protracted, inadequate, and insecure for EXCO’s (now Cabinet) documentation; subsequently, the need arose for a more modernised and secure virtual document management system. Consequently, the web-based application (web-app) ExcoTrack was created by a government employee - Programmer to provide accurate, relevant, and timely information and documentation.

MANAGEMENT’S RESPONSIBILITY

Management is responsible for ensuring that appropriate policies and effective controls exist. More specifically, management must ensure that policies and controls exist to facilitate IT Operations, Development & Acquisition, Outsourcing, Information Security, and to guide the development of Business Continuity Plan and/or Disaster Recovery Plan. Management is also responsible for establishing appropriate Application Controls and for ensuring that they function effectively.

AUDITOR’S RESPONSIBILITY

Our responsibility is to independently express a conclusion on IT Operations, Development & Acquisition, Outsourcing, Information Security, Business Continuity, Disaster Recovery, and Application Controls, for the Cabinet Secretariat based on our audit. Our work was conducted in accordance with International Standards of Supreme Audit Institutions (ISSAI) 100, 5300, and International Standard on Assurance Engagements (ISAE) 3000. These principles require that we comply with ethical requirements and plan and perform the audit in order to obtain reasonable assurance whether tried and true policies, plans, procedures, and internal controls exist and are functioning effectively, proper records have been and are being kept, and all the necessary information and explanations for the purpose of our audit, has been obtained.

AUDIT MANDATE

The Office of the Auditor General (OAG) is mandated through the Montserrat Constitution Order 2010 to perform the audit. This mandate is supported by ISSAI 1, 200, 300, 400, and strengthened by the Public Finance Management and Accountability Act (PFMAA) 2008 and the Public Finance Management and Accountability Regulations (PFMAR) 2009.

AUDIT STANDARDS & GUIDELINES

The standards and guidelines used to assess the IT Operations, Development & Acquisition, Outsourcing, Information Security, Business Continuity, Disaster Recovery, and Application Controls and assessments included the use of ISSAI 1, 100, 3100, 4100, 5310, COBIT 4.1, FISCAM, and NIST, together with the IDI Handbook for IT Audits.

AUDIT OBJECTIVES

The main purpose of this Information Security review is to assess and determine whether:

A. ExcoTrack is self-sufficient, secure, and robust, with adequate application controls in place to ensure the integrity, completeness, accuracy, and security, of the (i) user information and (ii) Cabinet-related confidential information that is inputted, processed, and outputted, by the application software, and in a timely manner.

B. Provisions were made by either Cab Sec or Office of the Premier (OotP) to ensure continuance of the service if person(s) and/or the entity maintaining the application and system should leave, fold, or have their services terminated; or if there was a security breach of the application software.

AUDIT SCOPE AND METHODOLOGY

The study will cover the period July 2013 to July 2016 and will focus on the examination of the policies, procedures, and controls that guide development, operations, outsourcing, access, security, business continuity, and disaster recovery of the Cabinet Document Management Solution - ExcoTrack, designed and maintained by Rovika Inc.

A combination of techniques were utilised to gather information and assess whether relevant controls existed, were implemented, and if they were effective in ensuring that OotP's confidential data is protected and there is continuance of service. These included, but were not limited to, interviewing of the Clerk of Council, Clerk of Cabinet and other relevant GoM staff, inspection of documents and assets, and issuance of questionnaires to the key stakeholders in order to gather in-depth information about the application software ExcoTrack.

CHAPTER 2 CABINET DOCUMENT MONITORING SYSTEM PAST & PRESENT

Clerk of Council

1. Initially, the Clerk of Council (CoC) was in charge of monitoring/tracking of the decisions made, and policies put in place, by the Executive Council (EXCO) (now Cabinet). This original monitoring system was a manual and paper-based one comprised of several types of EXCO documents:

    - **Memorandums** - used to present a request, proposal, or policy that EXCO is to consider.
    - **Information papers** - used to notify Cabinet only, it does not need a decision for action.
    - **Round Robins** - used for urgent, straightforward, matters that requires immediate action and noncontroversial.
    - **Decisions** - to include Policy, Statutory, Financial, and Resource Decisions. They are generated from the Information Papers, Memorandums, and Round Robins, and/or Other Business that has been submitted orally.
    - **Minutes** - are records of proceedings in Cabinet meetings, done manually by the CoC. These minutes have to be confirmed as accurate records of the proceedings by Ministers of Government, the Governor (President of Cabinet), Attorney General (AG), Financial Secretary (FS) and the Deputy Governor (DG).[1]

2. Whenever there was an matter or an opinion that the various Ministries/Departments or outside agencies and Statutory Bodies required EXCO to consider, hard copies of either a Memorandum, Round Robin, or Information Paper were drafted, and submitted to the Attorney General (AG) and Financial Secretary (FS) for their legal or fiscal remarks.
3. Once these officials annotated and returned them to the originating Ministry/Department, the commentaries were typewritten into the documents, signed by The Head of Department (HoD) and of the Minister of the submitting Ministry/Department, before eight (8) copies to the CoC for processing.
4. At the CoC, these papers were logged and numbered sequentially in a book and proof-read for accuracy before being sent out to all the members of EXCO for the next scheduled meeting. An Agenda would also be created and delivered with the documents.
5. However, before a date could be set for EXCO to convene, the CoC had to confirm that there would be at least a quorum of four (4) members present (for e.g., 2 Ministers, AG, & FS). Once a quorum was confirmed, the EXCO document package would be sent out to the Governor, 4 Ministers of Government, the AG, the FS, and the CoC who has to keep a copy.

[1] *Cabinet Guidelines and Procedure, Montserrat Cabinet Secretariat 2014 Edition*

6. The CoC typed up the Minutes and circulated it to EXCO members, for them to confirm if the information chronicled by the CoC was accurate.

7. Once the Minutes were confirmed as correct at the next EXCO meeting, they were used to create the Decisions. These Decisions were signed and hand delivered with a pink slip to the relevant Ministry's Permanent Secretary (PS)/HoD, to be actioned. Carbon-copies (without the pink slip), were also distributed to the Governor, AG, FS, Auditor General and the Deputy Governor's Office (after it was established).

Office of the Deputy Governor (ODG)

8. When the Office of the Deputy Governor (ODG), formerly the Chief Establishment Office, was instituted in 2007, one of its functions was to keep track of the Decisions/Policy agreed upon or put into place by the members of EXCO. The ODG used a document register that was developed by a staff member of DITES, in Microsoft Access Database called EXCOTRACK, to log and track these Decisions/Policies.

9. After receiving a copy of EXCO's Decisions/Policy from the CoC, the ODG sent out a form to the relevant Ministries with a 2 week deadline to report on the status of the actions that were being effected (ongoing or completed). This information was inputted back into the MS Access database so that quarterly reports could be generated and presented to EXCO. This task was later relinquished to the Cabinet Secretariat in 2012.

Cabinet Secretariat (now Office of the Premier)

10. The department was established in 2012, to coordinate, monitor, and evaluate the implementation of whole of Government Policy and Planning and provide technical support through the Cabinet Secretary - to the Governor, Premier, Ministers of Government and their Ministries. This division is no longer in existence and its functions have reverted to the OotP.

11. OotP coordinates the Cabinet Decision making process and worked closely with the Governor, the Premier, and the other Cabinet members to ensure that Cabinet received accurate information and documentation to support its decision-making process. Therefore, as a supporting role to Cabinet, the Office of the Premier performs the following functions:

    - Provide administrative and secretariat support for Cabinet and its committees
    - Control the quality and context of information reaching Cabinet
    - Produce and circulate the Decision of Cabinet
    - Work closely with Ministries to ensure that the Decisions of Cabinet were conveyed and implemented

- Initiate where necessary, and participate in, key meetings leading up to the formulation of policy.[2]

Cabinet Secretary (now Director of Policy and Planning)

12. The role of the Cabinet Secretary, now Director of Policy and Planning, includes the coordination of all policy functions, servicing Cabinet, Information and Communications, and Department for Information Technology and E-Government Services (DITES),[3] as follows:

    - Coordinate the Cabinet Decision making process and work closely with the Governor, the Premier, the Ministers, the Attorney General, the Financial Secretary and their Ministries to ensure that the Cabinet received all the information and documentation for decision making.
    - Develop the Cabinet agenda in consultation with the Premier and the Governor well in advance of meetings.
    - Report to the Governor and the Premier and was responsible for servicing the operations of the Cabinet including providing technical support to the Governor and the Premier as the Cabinet may have required.
    - Convey the decisions of the Cabinet to the relevant parties.
    - Oversee the Policy process within the Government and ensured that Policy submissions were consistent with the overall Government Policy.
    - Ensure the effectiveness of the Cabinet process and also track the implementation of all Cabinet Decisions.[4]

Clerk of Cabinet

13. The Clerk of Cabinet coordinates the Cabinet Decision making process and works closely the Governor, the Premier, the Ministers, the Attorney General, the Financial Secretary, and their Ministries to ensure that the Cabinet receives all the information and documentation for the decision-making.

14. In addition, to developing the Cabinet agenda in consultation with the Premier and the Governor well in advance of meetings, the role of the Clerk of Cabinet includes the following:

    - Reporting directly to the Governor and the Premier
    - Responsible for servicing the operations of the Cabinet including providing technical support to the Governor and the Premier, as the Cabinet may require
    - Conveys the decisions of the Cabinet to the relevant parties
    - Oversees the Policy process within Government and ensures that Policy submissions are consistent with the overall Government Policy

[2] *Cabinet Guidelines and Procedure, Montserrat Cabinet Secretariat 2014 Edition*

[3] *http://www.gov.ms/2011/09/29/government-of-montserrats-ministries-reorganised/*

[4 & 5] *Cabinet Guidelines and Procedure, Montserrat Cabinet Secretariat 2014 Edition*

- Ensures the effectiveness of the Cabinet process and tracks the implementation of all Cabinet Decisions.[5]

15. Each department submits the papers that they want to be considered. From these papers the Decisions are directives of Cabinet (they have to agree to recommendations). Once confirmed, the Governor signs it off; then and then only can the decisions can be issued.

16. Agendas and Calendars have to be prepared, signed, and circulated two (2) days ahead of the scheduled meeting by the CoC; Other Business can be submitted orally and are not issued to the Ministries/Departments unless Cabinet specifies that it is to be circulated.

Rovika Inc.

17. Rovika Inc. is a small local software development company that was established in 2013, and is co-owned and managed by two software programmers. Both are the Directors and the sole personnel who develop customised software to realise the needs of their local and regional clientele.

ExcoTrack

18. In 2012, the then Cabinet Secretary, approached a government employee – Programmer (who is currently one of the co-owners of Rovika Inc.), to develop a computerised version of the Cabinet documentation monitoring/tracking process in an effort to provide efficient ways to monitor/track the GoM's decisions and policies.

19. The computerised bespoke virtual software ExcoTrack is designed and developed to be a fully self-sufficient and secure virtual document management web application. It is used for the creation, circulation, commentary and approval, and tracking, of Cabinet documentation. ExcoTrack is also used for the preparation of Cabinet minutes, agendas, and/or third party attachments all of which, can be accessed from any electronic device (desktop, cellular phone, laptop, or IPad) once there is Internet access and/or data-enabled device. The first version of ExcoTrack was launched in mid-July 2013, although it was still in its developmental stages. The initial cost for the development and design of, and training for, ExcoTrack was XCD$22,000.

20. Authorised users login to ExcoTrack from any device at the URL (Uniform Resource Locator) https://ExcoTrack.rovika.net/users/sign_in. A dashboard page opens up with the various menu options and page indexes where each task at the different stages in the Cabinet document management process, is performed.

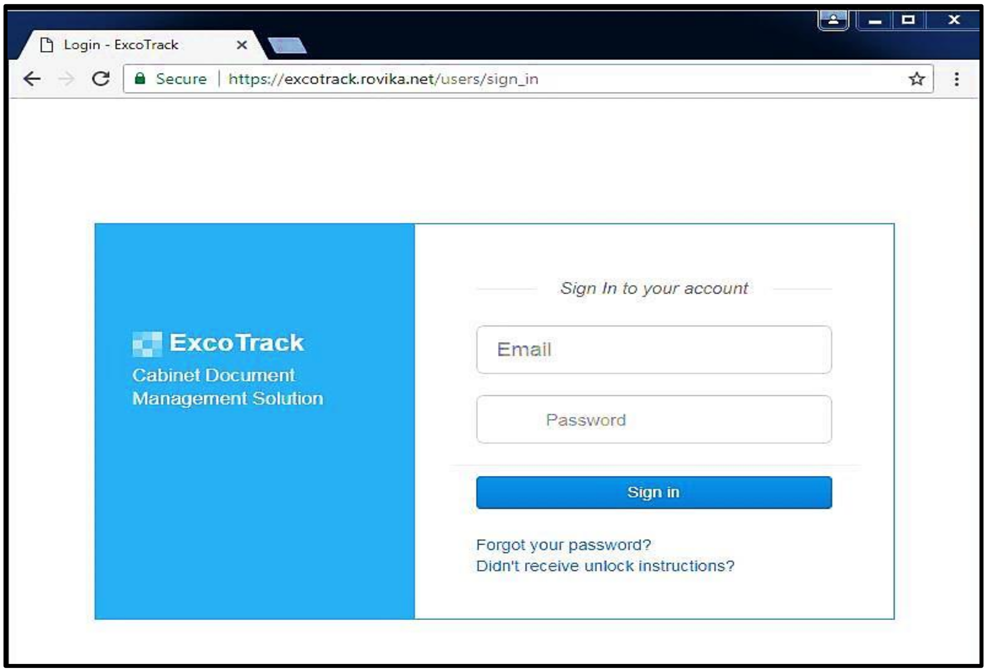

Login - ExcoTrack
Secure | https://excotrack.rovika.net/users/sign_in
ExcoTrack
Cabinet Document Management Solution
Sign In to your account
Email
Password
Sign in
Forgot your password?
Didn't receive unlock instructions?

Figure I – ExcoTrack Dashboard Page

Observations

21. ExcoTrack was designed to send automatic alerts to relevant participants when their written input is required to facilitate completion of the Decision, etc., and submission to Cabinet for sign off or otherwise. The function does not always provide the relevant alert(s) causing significant delays in documents reaching Cabinet for decision-making.

22. When Decisions require input by relevant participants, if any grammatical errors or mistakes were made in the information being keyed in, these errors/mistakes cannot be corrected once the comment has been submitted. Therefore, a new comment will have to be created to insert the corrections; consequently, sometimes there could be several comments under a particular Decision from a single participant.

CHAPTER 3 OUTSOURCING

Outsourcing Policy

23. OotP has no formal and/or documented outsourcing policy, or any list highlighting the services that could be outsourced or any clear approval process for the outsourcing of a function/service. There are no documents to record that OotP has identified the risks associated with different modes of outsourcing or to verify that the organisation is aware of the risks associated with the possibility of takeover, closure or withdrawal of Rovika Inc.'s services.

Solicitation

24. No formal solicitation process was followed in terms of advertising a solicitation package for bid/tenders from software developing companies and selecting the best proposal. After Cab Sec took over the monitoring of the EXCO Decisions/Policy documentation from the ODG, the document register in use proved to be inadequate and insecure for the additional functions that the then newly formed department had to undertake.

25. Consequently, the Cabinet Secretary in 2012 approached the same individual (now a co-owner of a local software company, Rovika Inc.) and informally commissioned the development of a more robust, self-contained, electronic solution to provide accurate, relevant, timely, information and document management.

Service Level Agreement (SLA)/Contract

26. There was no signed Service Level Agreement (SLA) and/or contract between the Cabinet Secretariat and Rovika Inc., outlining the parameters and/or other arrangements in regards to ExcoTrack. The contractor's services were retained via a verbal collaborative agreement by the former Cabinet Secretary. Typical areas covered in an SLA, but not restricted to, may include:

- types of service to be provided
- times available and locations covered
- measurement of service delivery
- change control
- liaison
- charges and penalties.

27. A SLA should define the services the vendor is expected to perform as well as the technical parameters for those services since it is a legally binding agreement between the vendor and the organisation.[6]

[6] *WGITA-IDI Handbook on IT Audit for Supreme Audit Institutions (February 2014)*

Vendor or Contractor Monitoring

28. After Cab Sec was presented with the demos of ExcoTrack during the development phase and the software was fully launched, there was no monitoring of the contractor.

Retaining Business Knowledge/Ownership of Business Process

29. There is an inherent risk of loss of business knowledge, which resides within the developers of applications. In the event that the vendor for some reason is unable to provide this service, Government IT organisations must be ready to assume this duty again. Also, as the development of the application would happen outside the organisation, the organisation also runs the risk of abdicating or losing the ownership of the business process, which may be claimed by the service provider as their intellectual property. Organisations need to address this issue at the time of entering into contract, and ensure that they have complete documentation of the system development process as well as the system designs. This will also help the organisation to switch service providers, if required.[7]

30. There is no SLA/contract that delineates and documents ExcoTrack's process(es) ownership. Rovika Inc. retains all business knowledge and ownership of ExcoTrack's process (es).

31. The OotP pays Rovika Inc., an annual hosting and maintenance fee of XCD$6,792.00 for unlimited users' licence.

Data Rights

32. There is no SLA/contract between the two entities that identifies (i) ownership of ExcoTrack data and (ii) the organisation's data protection requirements and access rights or (iii) delineates the mechanism in place to ensure that the data protection and security requirements as per the Service Level Agreement are being adopted and implemented by Rovika Inc.

Observations

33. The contractor's services were retained via a verbal collaborative agreement by the then Cabinet Secretary, and not via a formally signed SLA or contract, this makes the arrangement an "expressed" or verbal contract.

34. OotP does not retain ownership of the business process(es), or data, and this can pose as a high risk factor, if Rovika Inc.:

    - goes out of business
    - fails to maintain the software
    - becomes insolvent/admits insolvency or is unable to pay off their debt
    - files for bankruptcy or

[7] *WGITA-IDI Handbook on IT Audit for Supreme Audit Institutions (February 2014)*

- is controlled by a rival customer

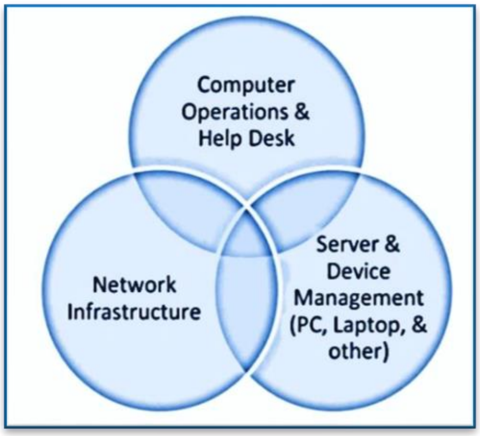
35. Although ExcoTrack is in currently in operational use, the software's source code is still held and owned by Rovika Inc. and only they can make adjustments to it. This may appear on the surface as a good control mechanism, however, this may pose high risks associated with the developer maintaining control over the software:

- There is the risk of delays in processing the Cabinet documentation when difficulties with the functionality of the software are encountered.
- There is a risk of continued availability of support or supplier failure that would lead to loss of software use and negatively impact the creation, circulation, commentary and approval, and tracking, of Cabinet documentation.
- There is an inherent risk of loss of data which resides with the developers of ExcoTrack.

CHAPTER 4 IT OPERATIONS

IT Operations

36. IT operations are typically the day-to-day running of the IT infrastructure to support business needs. Properly managed IT operations make it possible to identify bottlenecks and plan for anticipated capacity changes (additional hardware, or network resources), measures performance to ensure it meets the agreed-upon needs of the business owners, and provides help desk and incident management support to the users of IT resources.[8]


Computer Operations & Help Desk
Network Infrastructure
Server & Device Management (PC, Laptop, & other)

37. There is no formal Contract or SLA outlining parameters but flexible helpdesk service is provided by Rovika Inc. to OotP. Any user complaint, inquiry, or change request is communicated to them by the Clerk of Cabinet, via an email or phone call. The contractor can also review user problems from the built-in incident report feature.

38. Other services provided by the contractor includes basic maintenance and hosting, for an annual fee of XCD$6,792.00; upgrades, updates, creation and/or improvements to the modules and protocols, and miscellaneous requests from the Clerk of Cabinet. These improvement or corrections are charged according to the task(s) that were effected.

Service Management

39. Rovika Inc. actively monitors the IT operations of ExcoTrack although there is no signed internal SLA or Contract outlining the allocation of responsibilities between the entity and OotP, documented network management business objectives, service offerings and metrics, definition for problem types, help desk responsibilities.

40. The OotP does not have any BCP/DRP standards for data back-up and recovery practices. However, the cloud computing service provider that Rovika Inc. utilises, performs a weekly backup for disaster recovery purposes.

[8] *WGITA-IDI Handbook on IT Audit for Supreme Audit Institutions (February 2014)*

Problem and Incident Management

41. There is a built-in report feature (incident management tool) that monitors ExcoTrack and its usage. Each user profile generates activity logs that includes, for example, IP address, browser connection, status of action (successful/error), etc. The data collected is usually reviewed on a daily basis, but if there is a specific inquiry from the Clerk of Cabinet the activity logs will be inspected.

Change Management

42. In IT organisations, the change management process is normally used to manage and control changes to assets, such as software, hardware, and related documentation. Change controls are needed to ensure that all changes to system configurations are authorised, tested, documented and controlled so that the systems continue to support business operations in the manner planned, and that there is an adequate trail/record of changes.[9]

43. There is no change control board charter only the co-owners conferring and collaborating with each other before any changes are made to ExcoTrack. User feedback is taken into consideration when improvements are being designed and implemented.

44. ExcoTrack is constantly being updated by Rovika Inc. They utilise a Version Control Software to implement any fixes to, or creating new features for, the application before they rollout a newer version of ExcoTrack. Full rollbacks are not the most desirable course of action for editing source code, as it can cause some of the features, or information, etc., stored at database level, to be lost during the process. With Version Control Software, any adjustments made to the code are tracked and stored in a special database which enables the developer(s) to evaluate earlier versions of the code and/or to do rollbacks to specific point(s) in the source code. This aids with minimising any disruptions during the debugging process. For example, if any weaknesses in access controls are identified, Rovika Inc. will perform a seamless system update that does not require users to exit ExcoTrack; they would just do a Refresh/reload of the page.

45. Security technology is incorporated into the application to ensure that all ExcoTrack data is secure includes: SSL (Secure Sockets Layer) and the opensource and security database industry standard solution, PostgreSQL.

46. There are no change documents or user training manuals, as the system is not designed to rely on manuals or documentation. Training for new users of the ExcoTrack application is done by Rovika Inc., when notified by the Clerk of Cabinet. Likewise, whenever changes/updates to the system are effected, they are not that drastic to require supplementary user instructions or for the users to receive additional training.

[9] *WGITA-IDI Handbook on IT Audit for Supreme Audit Institutions (February 2014)*

Observations

47. Although there is no signed contractual agreement between the two parties the operation of ExcoTrack is in full effect. Service reports, maintenance and user/application response time is adequately maintained by Rovika Inc.

48. Any changes or upgrades executed by Rovika Inc. are done seamlessly with minimal to zero disruptions or errors.

49. No helpdesk documentation is/was being provided by the contractor, Rovika Inc. (helpdesk logs, emails, etc.).

CHAPTER 5 INFORMATION SECURITY

Information Security

50. Information Security processes and methodologies typically involve measures designed to protect print, electronic, or any other form of confidential, private, and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.[10]

51. The following three major requirements, CIA, are essential to the security of ExcoTrack's information as follows:

- **Confidentiality** - ensures that ExcoTrack is accessed only by authorised parties. Only those who should have access to ExcoTrack and the Cabinet documentation will actually get that access. "Access" includes not only reading but also viewing, printing. Confidentiality is sometimes called secrecy or privacy.
- **Integrity** - means that Cabinet documentation stored on ExcoTrack can be modified only by authorised parties or only in authorised ways. In this context, modification includes writing, changing, changing status, deleting, and creating.
- **Availability** - means that Cabinet documentation stored on ExcoTrack are accessible to authorised parties at appropriate times.[11]

Security Policy

52. To be meaningful, laws, rules, and practices must provide individuals with a reasonable ability to determine whether their actions violate or comply with the policy.[12]

53. Neither OotP, nor the contractor, has a formal/written Information Security policy or plan.

Risk Assessment

54. Risk assessment is identifying, analysis, and evaluating risks in the IT Security infrastructure. It is the process of assessing security-related risks from internal and external threats to an entity, its assets, and personnel.[13]

[10] *https://www.sans.org/information-security/*

[11] *http://www.informit.com/articles/article.aspx?p=680830&seqNum=3*

[12,13] *WGITA-IDI Handbook on IT Audit for Supreme Audit Institutions*

55. Since Rovika Inc. does not have a physical office space or server room, but instead utilises the services of cloud computing, as a result they do not have a risk register that contains significant risks that were identified and assessed, i.e. internal and external risks, possible effects and impact of Information Security breaches assessed.

56. They also do not generate incident handling reports.

Access Controls

57. In a government environment, access control is important as many government entities process sensitive data and privacy concerns limit who should view various parts of the information. Access control ensures that only users with the process credentials have access to sensitive data.[14]

Physical Security Controls

58. Security inevitably incurs costs and, in reality, it can never be perfect or complete – in other words, security can reduce but cannot entirely eliminate risks. Given that controls are imperfect, strong physical security applies the principle of defense in depth using appropriate combinations of overlapping and complementary controls. [15]

59. Rovika Inc. does not have a physical office space or building with a traditional server room that houses hardwired computer equipment dedicated to the storage and running of ExcoTrack.

Logical Access Control

60. Logical access controls are protection mechanisms that limit users' access to information and restrict the modes of access on the system to only what is appropriate for them.[16]

61. The matters that are discussed in Cabinet are confidential in nature. Therefore, the security of the information contained in Cabinet documentation is of utmost importance, especially when there are over 100 users of ExcoTrack consisting of Ministers, PS's, Directors, and SCO's from the relevant departments.

62. The Clerk of Cabinet is responsible for creating or adding new ExcoTrack user accounts. A request to add a new user is in the form of an email is sent to the Clerk of Cabinet from the various Ministries/Departments. After the requested new user account is created and activated, a notification email is automatically generated and sent by the system to the new user. User accounts are rendered 'inactive' and not deleted, when user access to ExcoTrack is no longer necessary.

[14,15,] *WGITA-IDI Handbook on IT Audit for Supreme Audit Institutions (February 2014)*

[16] *http://securityv.isu.edu/isl/hk_acces.html*

63. ExcoTrack uses the Security Access Protocol (SAP) for user-level restriction and password protection access that cannot be changed or modified. Authorised users login to ExcoTrack online from https://ExcoTrack.rovika.net/users/sign_in with a unique username and masked password that contains alphanumeric characters 6 - 128 characters long. These passwords are also 'salted' (cryptography) to make them more secure; the system generates random secure passwords and sends them to the users.

64. ExcoTrack has multiple tiers of access and restrictions; consequently, once login is successful the users can only perform specific tasks/actions in accordance with their respective job responsibilities or Role-based Access control (RBAC).

65. Other security measures include:

(i) the user accounts are set to automatically log out after 30 minutes of inactivity.

(ii) user's account will be locked for duration of six (6) hours after three (3) unsuccessful login attempts; this lockout period cannot be overridden.

(iii) if the user forgets their password, it can be changed/reset via a password link.

(iv) when users login to ExcoTrack from smart phones and electronic devices, passwords expire after 30 seconds.

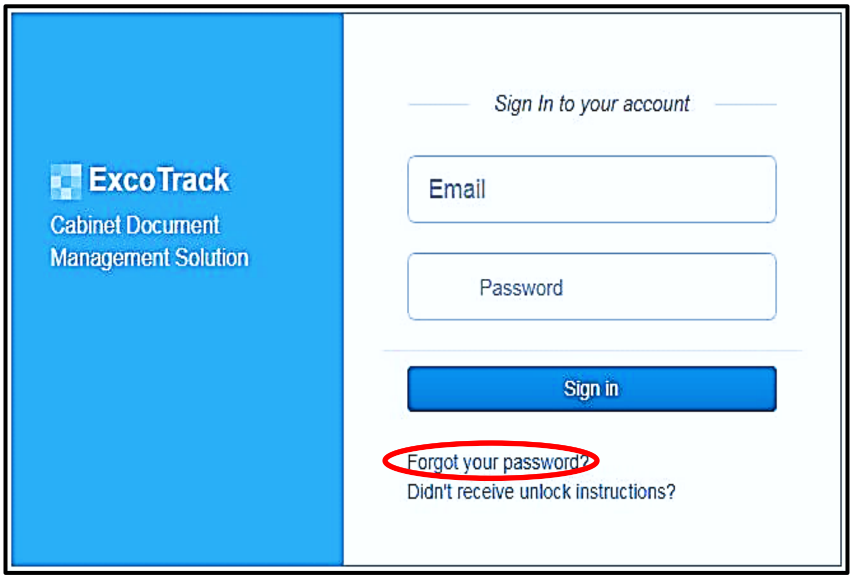


Figure II – Password Link

Observations

66. ExcoTrack is not run from a physical server. Rovika Inc., opted to run ExcoTrack on rented servers with Cloud platforms from the USA-based companies Amazon Web Services (AWS), Digital Ocean Private Network, and New Relic for some of the following benefits:

- **Collaboration Efficiency** - Cloud computing enables users of ExcoTrack to access the files simultaneously and the ability to communicate and share more easily outside of the traditional methods.
- **Flexibility** - Cloud-based service can provide more bandwidth instantly to meet the demand. In addition, it is enables users to access ExcoTrack at anytime and anywhere from any type of device such as smart phones, tablets, etc.
- **Scalability** - Cloud computing allows Rovika Inc. to scale up (expand) or down (reduce) rapidly according to their operation and storage requirements whenever the need arises. So rather than purchasing and installing expensive upgrades, the service provider handles it.
- **Security** - The security of ExcoTrack's data is of utmost importance. Security improves in the Cloud environment as security policy is easier to enforce, and threats to ExcoTrack and its data are easier to detect and address. Since Cloud data and apps are centralised in a data center, it is actually easier to establish effective security policy, monitor compliance, and intervene quickly and often preventatively when there are issues. The data is not stored on end-user devices, if a device fails or is lost or stolen; the data remains safe and secure.[17,18]

67. ExcoTrack is monitored by Amazon Cloud and New Relic.

68. ExcoTrack has built-in functions that store any manipulations of the dataset data and the cumulative database. Since no ExcoTrack data is stored on end-user devices, if a device fails or is lost or stolen, the will data remain safe and secure.

69. The Security Access Protocol (SAP) utilised for access control for ExcoTrack, is very effective. ExcoTrack has never had a security breach on the system side (hacking), or security concerns from the user end; it is a very secure application software.

70. Activity logs of all user account activities and by location (for example, successful login/log outs, failed login attempts, security related events, and or security violations), are generated. These logs function as an Intrusion Detection System. None was provided for us to review.

71. There is no set protocol to deactivate user accounts. No formal emails are sent to Clerk of Cabinet. She uses her own initiative in instances when she is aware that a user has left the department and/or no longer works with the GoM.

72. The 6-hour lockout period for failed log-in attempts, which cannot be overridden, is excessive and impractical.

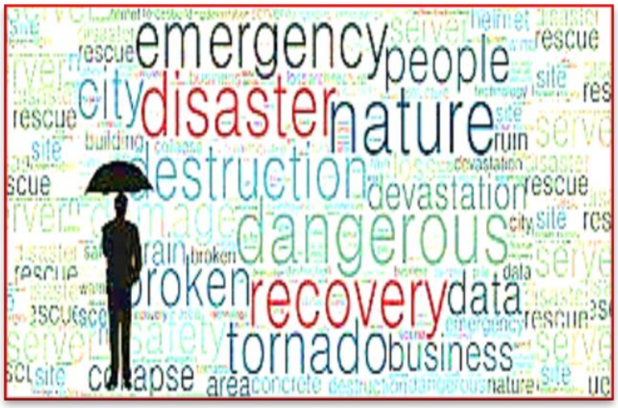
73. No documentation provided by the contractor Rovika Inc. for OAG to verify authorised security parameters (password management, authorisation, automatic log out, failed log-in attempts, auditing of access events)

[17] *https://www.slideshare.net/grazitti/advantages-of-cloud-computing-090513*
[18] *https://aws.amazon.com/solutions/*

CHAPTER 6 BUSINESS CONTINUITY AND DISASTER RECOVERY

Business Continuity and Disaster Recovery Plans

74. In essence, a business continuity plan (BCP) addresses an organisation's ability to continue functioning when normal operations are disrupted. This plan incorporates the policies, procedures, and practices that allow an organization to recover and resume manual and automated mission-critical processes after a disaster or crisis.



75. Besides stating the practices that must be followed in the event of an interruption, some BCPs include other components such as disaster recovery, emergency response, user recovery, and contingency and crisis management activities. Therefore, in these organizations, business continuity is seen as an all-encompassing term that covers both disaster recovery and the resumption of business activities.[19]

76. Neither OotP, nor Rovika Inc., have any formal BC or DR plan, which outlines the backup and recovery plans for the ExcoTrack software itself, ExcoTrack data, computer hardware, and a data centre (recovery).

Observations

77. Rovika Inc. utilises the cloud platform services of Amazon secure cloud computing instead of the traditional physical server and network infrastructure for business continuity and disaster recovery purposes for the following reasons:

- **Fast Performance** - Cloud computing enables fast disk-based storage and retrieval of files so that data can be recovered within 24 hrs and also minimises any downtime and loss of productivity.
- **No Tape** - Eliminate costs associated with transporting, storing, and retrieving tape media and associated tape backup software.
- **Elasticity** - Add any amount of data, quickly. Easily expire and delete without handling media.
- **Secure** - Secure and durable cloud disaster recovery platform. The cloud ensures it is backed up and protected.[20]

[19] *http://www.theiia.org/intAuditor/itaudit/archives/2008/january/the-it-auditors-role-in-business-continuity-management*

[20] *https://aws.amazon.com/disaster-recovery/?hp=tile*

78. Rovika Inc. performs warm backups of the application. However, frequent cloud based backups are performed every 10 - 15 minutes by the Amazon Web Services (AWS) Cloud, from where ExcoTrack is stored and run from.

79. The Cloud cumulative database backups are retained for as far back as Rovika Inc. requires, for either disaster recovery or analysis purposes (i.e. functionality and development).

80. It has not been necessary to effect recovery procedures since ExcoTrack was been launched in 2013, as the application is being continually developed and tested.

81. Data collected by incident management tool (built-in report) is reviewed on a daily basis. Specific inquires would prompt a review of the activity logs.

CHAPTER 7 FINDINGS AND RECOMMENDATIONS

Findings

82. Overall, ExcoTrack has met the objectives that were initially outlined by Cab Sec in 2012. A government employee - Programmer (now a co-owner of a local software company, Rovika Inc.), was approached by the then Cabinet Secretary via a verbal agreement to provide an expert service independent of GoM's Information Technology Dept. (DITES).

83. The contractor developed a very secure, robust, application software that is user-friendly and accessible from any electronic device that has access to the Internet, and/or from any data-enabled device. Rovika Inc. continues to seamlessly maintain ExcoTrack. It constantly upgrades, updates, and very quickly and proficiently performs any requested amendments to the application with minimal downtime.

84. Frequent and cumulative back-ups are performed both locally and by the Amazon Cloud computing platform, on which they elected to have ExcoTrack run and stored. These backups are for recovery purposes. Most importantly, to date, there have not been any internal or external, security breaches or issues associated with ExcoTrack.

85. However, among other things, it was found in terms of contingency neither the vendor nor OotP have a Business Continuity Plan (BCP) or IT Security Plan or Policies in the event of a security breach of ExcoTrack. There is also the serious issue of not having a formally signed contract between the two entities, in addition to the nonexistence of a Service Level Agreement that clearly outlines who retains all business knowledge and ownership of ExcoTrack's process (es).

86. Consequently, listed below are the post-software development issues and/or recommendations and future IT outsourced projects concentrations that we pinpointed and propose that OotP addresses:

Recommendations

A. Background

87. Considerable effort should be made to rectify the automatic alerts glitch, quickly, in order to reduce the delay time in the Cabinet decision-making process.

88. The issue of not being able to modify errors and mistakes, once a comment is submitted, should be corrected in order to eliminate the unnecessary and inefficient option of creating more than one comment under a particular Decision.

B. Outsourcing

89. OotP should develop a Service Level Agreement (SLA) that defines what the future IT services vendors/contractors will be expected to accomplish, and the technical parameters for those services. Whatever items are critical to OotP must be included in the SLA. Typical areas to include and but not limited to are:

- The types of services that will be performed by the vendor
- Allocation of responsibilities between the organisation and the vendor
- Services that will be measured, the measurement period, duration, location, and reporting timelines (defect rates, response time, help desk staffing hours, etc.)
- Time to implement new functionality, rework levels
- Type of documentation required for applications developed by the vendor
- Location where services are to be performed
- Frequency of back-up, data recovery parameters
- Termination and data delivery methods and formats
- Incentive and penalty clauses

90. OotP should consider developing a clear outsourcing policy that documents the functions that can be outsourced. They should identify and define all the roles and responsibilities between them and the IT services vendors/contractors.

91. If or when outsourcing any IT service provider, proper security management processes must be put in place to protect OotP's data, as well as to mitigate any security risks associated with outsourced IT projects and/or services.

92. The following areas should be considered:

(i) When preparing an outsourcing service contract, the organisation should clearly define the security requirements of the IT systems to be outsourced, such as how all personal and sensitive data should be handled throughout the contract. These requirements should form the basis of the tendering process and become an integral part of the performance metrics.

(ii) The outsourcing contract should include requirements for all staff of service providers/and vendors to sign non-disclosure agreements to protect sensitive data in the systems.

(iii) When engaging IT service providers, OotP should ensure that the vendor employs adequate security controls.

(iv) OotP should monitor and review actively and periodically, the security control compliance of service provider and users. The Department must reserve the right to audit responsibilities defined in the service level agreement, and have those audits carried out by an independent third party.

(v) OotP should ensure the adequacy of contingency plans and back-up processes provided by the service provider in the aftermath of a natural disaster, or in the event of service failure or security breach.

(vi) The security roles and responsibilities of the service provider, internal staff and end-users pertaining to the outsourced IT system should be clearly defined and documented.

(vii) It is essential to ensure that all data to be handled by the outsourcing party are clearly and properly classified, and security privileges for access should only be assigned on an as-needed basis for the performance of their work or the discharging of contractual obligations.[21]

93. OotP's confidential data is inputted into ExcoTrack, and the application software is itself stored and run from Amazon Cloud computing. There was, and still is, no signed contract between the entities stating ownership of ExcoTrack's data.

94. Therefore we strongly recommend that OotP makes it a priority to prepare a post-agreement, to be signed by them and Rovika Inc. This belated contract or agreement must clearly state and affirm OotP's ownership of the data stored by, or on, the service provider's system, and specifies their rights to the data/information (intellectual property rights). It should ensure that the following matters/areas, but not necessarily limited to, are addressed:

- Retention of business process ownership is to be well delineated and documented
- Loss of business knowledge, due to outsourcing, does not occur
- There is capacity to conduct the outsourced services in-house
- Business continuity must be ensured if the vendor/contractor is unable to provide services at any point or in future (supplier failure).
- Data protection and access rights.

95. This document can be applied to and be utilised as the standard for any future outsourced ventures.

96. With respect to risk of supplier failure, we recommend that OotP should assess the feasibility of purchasing the software and maintaining it, in-house at the Department of Information Technology & e-Services (DITES).

97. Should this option not be accepted by Rovika Inc., then OotP should ask for the software to be lodged in an escrow agreement where the source code is stored with an independent third party. Therefore, if Rovika Inc. goes out of business or withdraws its services (for whatever reason) then OotP would have access to the source code enabling it to continue using ExcoTrack.

[21] *https://www.infosec.gov.hk/english/technical/files/itos.pdf*

C. Information Security (IS)

98. We recommend that OotP devises and distributes/circulates an Information Security (IS) policy to the various government departments in relation to ExcoTrack. The following can be included in the IS policy, but not necessarily limited to the examples outlined below:

- **Non-disclosure agreements** - All ExcoTrack users should be asked to sign a nondisclosure agreement for confidentiality purposes.
- **Enforce and check strong passwords (authorise)** - Strong passwords can be requested and changed after a given time frame has expired.
- **User account creation/deactivation process** - Aside from the requests/authorisation in the form of email, the same should be enforced for the deactivation of user accounts, which is currently not the case.

99. The 6-hour hard lockout period for failed log-in attempts, which cannot be overridden, is excessive and impractical. Therefore, steps should be taken as to reduce the time-based lock-out period from 6-hours to perhaps 30 minutes or less. One alternative is to utilise a time-based incrementing approach. For example, the first time it locks out after 3 incorrect passwords it locks for 10 minutes. If it is locked again it locks for 20 minutes. The third time 40 minutes, and so on. This incrementing time makes it time consuming for automated brute force attempts and will give significant time to the system administrators to identify an attack.

100. Aside from both of ExcoTrack's system administrators having the ability to override the lockout security setting, another consideration is to equip the Clerk of Cabinet with the capability of overriding the lock-out setting as well.

D. Business Continuity

101. We recommend that OotP request a BCP from Rovika Inc. detailing the contingency strategies that they have in place for such an eventuality. Therefore, we advise that OotP poses to the software company that they furnish the department with:

- A document listing the risks they identified and assessed (Risk Register).
- Business Continuity strategies that they conceived and intend to implement in the event of a security breach of ExcoTrack.

102. OotP should also devise its own contingency plan for ExcoTrack. The BCP can either be separate and apart from, or based on, Rovika Inc.'s contingency strategies.

103. A well-written BCP should describe the immediate steps to be taken during an event in order to minimise the damage from a disruption, as well as the action necessary to recover. Thus, business continuity planning should be focused on the OotP's operations after a disruption. Specific scenarios should include (once applicable) how the entity would respond if:

- Critical personnel are not available

- Critical buildings, facilities, or geographic regions are not accessible
- Equipment malfunctions (hardware, telecommunications, operational equipment)
- ExcoTrack and the data are not accessible or are corrupted
- Vendor assistance or service provider is not available (Rovika Inc.)
- Utilities are not available (power, telecommunications) and
- Critical documentation and/or records are not available.[22]

104. Two important preliminary stages have to be conducted before the BCP is generated, in the third and final phase:

(A) **Business Impact Analysis** - this is the first step in developing a BCP. It should include:

- Identification of the potential impact of uncontrolled, non-specific events on OotP's documentation processes and the users of ExcoTrack.
- Estimation of maximum allowable downtime (i.e. interruption) and acceptable levels of data loss.

(B) **Risk Assessment** - this is the second step in developing a BCP. It should include:

- A prioritising of potential disruptions to the Cabinet documentation process based upon severity and likelihood of occurrence.
- An analysis of threats based upon the impact on OotP and ExcoTrack users, not just the nature of the threat.

(C) **Risk Management** - is the third and final phase where there is the development of a written BCP. OotP should ensure that the BCP is:

- Written and disseminated so that various departments/users of ExcoTrack can implement it in a timely manner.
- Specific regarding what conditions should prompt implementation of the plan and the process for invoking the BCP.
- Specific regarding what immediate steps should be taken during a disruption.
- Flexible to respond to unanticipated threat scenarios and changing internal conditions.
- Focused on the impact of various threats that could potentially disrupt operations rather than on specific events.
- Developed based on valid assumptions and an analysis of interdependencies.

[22] *https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum06/bcp.pdf*

- Effective in minimising disruptions to the creation, circulation, commentary and approval, and tracking, of Cabinet documentation through the implementation of tailored mitigation strategies.

CHAPTER 8 CONCLUSION

105. The Office of the Auditor General determined that ExcoTrack is self-sufficient, secure, and robust, with adequate and suitable application controls in place to ensure the integrity, completeness, accuracy, and security, of the user information and Cabinet-related confidential information by the application software.

106. However, from the findings of the review, we also established that first Cab Sec, and now the Office of the Premier (OotP), did not make any provisions to ensure continuance of service if person(s) and/or entity maintaining the application software should leave, fold, or have their services terminated; or in the event of security breaches or other mishaps.

107. The most pressing concerns that were realised are as follows:

108. The OotP does not have, and did not provide Rovika Inc., with a Service Level Agreement (SLA). A SLA is important as it contains the specific requirements and operational parameters of an entity that solicits the services of external service providers, and can be a key tool to managing these vendors. It defines day-to-day technical parameters that the vendor/contractor is to adhere to, or the services it expected to provide, at that level.

109. Another major concern was that there was, and still is, no signed contract between OotP and Rovika Inc. A contract defines the overall requirements for the effort and any associated security or other requirements to be followed.

110. Both aforementioned documents are legally binding agreements between the outsourced entity and the soliciting organisation. The vendor/contractor can be managed and held accountable to the terms of service agreed upon in the signed contract and/or service level agreement.

111. The OotP should take the initiative to have the source code ownership issue, resolved as soon as possible to avoid the possible loss of ExcoTrack's business process(es). The software's source code is being held and owned by the developers, Rovika Inc. Measures should be taken to purchase the application software and maintaining it, in-house, or request that the software be lodged in escrow where the source code would be stored with an independent third party, such as DITES.

112. Finally, we also noted the absence of Business Continuity, Disaster Recovery and IT Security polices and guidelines. The lack of these policy documents can lead to the weakening of governance and management of the application software, ExcoTrack.

CHAPTER 9 MANAGEMENT RESPONSE

No management response received from the Office of the Premier, despite several requests for their response.

REFERENCES

Websites

https://aws.amazon.com/disaster-recovery/?hp=tile

https://www.atlassian.com/git/tutorials/what-is-version-control

https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum06/bcp.pdf

http://www.informit.com/articles/article.aspx?p=680830&seqNum=3

https://www.infosec.gov.hk/english/technical/files/itos.pdf

http://intosaiitaudit.org/India_GeneralPrinciples.pdf

https://ithandbook.ffiec.gov/it-booklets/information-security.aspx

http://www.questsys.com/files/Challenges-Benefits-Cloud-Computing.pdf

http://mitigationguide.org/task-6/the-mitigation-strategy-goals-actions-action-plan/

https://security.stackexchange.com/questions/31901/account-lockout-with-human-interaction-required-to-unlock

http://www.theiia.org/intAuditor/itaudit/archives/2008/january/the-it-auditors-role-in-business-continuity-management

Publications

Cabinet Guidelines and Procedure, Montserrat Cabinet Secretariat, 2014 Edition

GAO Federal Information Systems Control Audit Manual (FISCAM), February 2009

ISSAI 5310 Information Security System Review, October 1995

WGITA-IDI IT Audit Handbook, 2014

Books

Chris Davis et al (2011), *IT Auditing: Using Controls to Protect Information Assets (Second Edition)*, McGraw Hill, ISBN 978-0-07-174238-2