Business Application – Acquisition, Development & Implementation

(Chapter - 5 : DISSA Course) **IS Audit**

Arijit Chakraborty

July 31 , 2021

IS Control Weaknesses – Major Observations

- **1. Inadequate information security policies** –
- policies were out of date or did not sufficiently cover key areas of IS security.
- 2. **Ineffective management of technical vulnerabilities** – lack of appropriate SOP to patch OS software & application vulnerabilities
- **3. Inadequate access controls –**
- network & public facing systems did not require 2FA / MFA to strengthen access to systems.

- **4. Administrator privileges are not managed well –**
- limiting privileges & reducing no of privileged users = important mitigation against network & system compromise.
- 5. **Lack of data loss prevention controls –**
- no processes to detect or block unauthorised transfers of sensitive data
- 6. **Network segregation is not appropriate –**
- networks are not segregated to limit impact of compromise. Partitioning network into smaller zones & limiting communication b/w them = control.

IS Audit Report : – Government Entities : 2021

- **IS Audit report date -**
- May 30, 2021
- **Audit team:**
- *A. Morison*
- *R. Smith*
- *K. Khan*
- *F. Bakhsh*
- *S. Chowdhury*
- *M. Chow*
- *K. Wittstock*
- *R. Chettri*

Introduction .....
Conclusion .....
What we found: General computer controls.....
What we found: Capability assessments .....
Information security .....
Business continuity.....
Management of IT risks .....
IT operations .....
Change control.....
Physical security .....
Recommendations .....
Remote access.....
Recommendations .....

Cover letter

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT 2021 – STATE GOVERNMENT ENTITIES

This report has been prepared for submission to Parliament under the provisions of section 24 of the *Auditor General Act 2006*.

Information systems audits focus on the computer environments of entities to determine if these effectively support the confidentiality, integrity and availability of information they hold.

This is the 13th year we have separately reported on State government entities' general computer controls (GCCs). The objective of our GCC audits is to determine whether entities' computer controls effectively support the confidentiality, integrity and availability of information systems.

I wish to acknowledge the entities' staff for their cooperation with this audit.

Chief IS Auditor

Executive Summary Auditor General's overview

- **A. Cyber-Attacks**
- *In the context of intensifying cyber attacks on all sectors, this report contains a number of important findings and recommendations resulting from our general computer controls audits and capability maturity assessments.*
- *All public sector entities should consider how they can apply the recommendations and case studies in the report to their operations with the expectation of an increasingly demanding threat environment into the future.*
- **B. Controls performance**
- *While entities improved their controls in 4 categories and remained constant in 1, information security continues to be an area of significant weakness.*
- *It is disappointing to see only 50% of entities met our benchmark in this area, a drop of 7% from last year.*
- *Poor information security controls leave entity systems and information vulnerable to misuse and may impact critical services provided to the public.*

- **C. COVID specific IS Risks**
- *The report also includes a summary of common issues related to remote access. During the COVID-19 response periods, entities supported their workforces with flexible working from home arrangements.*
- *This transformation also brought security challenges as entities changed the way they operate, in some cases significantly.*
- **D. WFH – Remote working**
- *Remote work is stated to become more prevalent and entities may continue to operate with a mix of remote and on-site workforces. Entities should consider these findings and ensure that adequate policies, strong access controls and monitoring are in place to address the inherent risks associated with remote working arrangements. This will require them to develop plans and implement controls to manage a range of hybrid environment risks*
- **E. Changes in Audit Standards**
- *Upcoming changes to the Auditing Standards clarify and enhance the need for auditors to understand general computer controls and their impact on the financial report. In particular, auditors are required to assess controls for each aspect of the IT environment including the network, operating system, database and application layers.*

IS Audit Approach

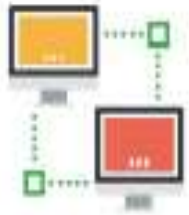
- *The model we have developed for our audits is based on accepted industry good practice.*
- *Our assessment is also influenced by various factors including the:*
- • *business objectives of the entity*
- • *level of entity dependence on IT*
- • *technological sophistication of entity computer systems*
- • *value of information managed by the entity*
- *For our capability assessments, entities improved their controls in 4 of the 6 audited categories. However, we continue to find a large number of weaknesses that could compromise the confidentiality, integrity and availability of information systems.*
- *Information security remains our biggest area of concern with only 50% of entities meeting our benchmark in this category, a drop of 7% from last year.*

Recommendations for ITGC

ITGC Categories

We focused on the following 6 categories:

Information security



IT operations

Business continuity

Change control

Management of IT risks

Physical security

Business continuity- IS Auditor comments

- *The percentage of entities that met our benchmark for this category in 2019-20 was the highest since we started benchmarking 13 years ago. This may, in part, be attributable to the need for entities to respond to COVID-19 pandemic. However, we found many still do not have adequate business continuity and disaster recovery arrangements in place.*
- *Interruptions to business can have serious impacts on the critical services entities deliver to the public. To ensure business continuity, entities should have an up-to-date BCP, DRP and incident response plan (IRP). The BCP defines and prioritises business critical operations and therefore determines the resourcing and focus areas of the DRP. The IRP needs to consider potential incidents and detail the immediate steps to ensure a timely, appropriate and effective response.*
- *Entities should test these plans on a periodic basis. Such planning and testing helps entities assess and improve their processes to recover information systems in the event of an unplanned disruption to business operations and services. Senior executives should monitor that plans are developed and tested in accordance with the risk profile and appetite of the entity*

IT operations

- *There has been steady improvement in the IT operations category since we added it to our assessment criteria in 2011. This year, entities continued to improve with 82% reaching our benchmark.*
- *Effective management of IT operations is key to maintaining data integrity and ensuring that IT infrastructure can resist and recover from errors and failures. We assessed whether entities had adequately defined their requirements for IT service levels and allocated sufficient resources to meet these requirements. We also tested whether service and support levels within entities were adequate and met good practice.*
- *Other tests included if:*
- *• policies and plans were implemented and working effectively*
- *• repeatable functions were formally defined, standardised, documented and communicated*
- *effective preventative and monitoring controls and processes had been implemented to ensure data integrity*

Common Control weaknesses

- *Without appropriate IT risk policies and practices, entities may not identify and mitigate threats within reasonable timeframes.*
- *Entities may not meet their business objectives when risks are not identified and appropriately managed.*
- ***Change control***
- *Entities' change control practices continue to improve with 85% meeting our benchmark in 2019-20.*
- *We examined if system changes are appropriately authorised, implemented, recorded and tested.*
- *We reviewed any new applications acquired or developed to evaluate if the changes were made in line with management's intentions*
- *An overarching change control framework is essential to ensuring changes are made consistently, reliably and efficiently. When examining change control, we expect entities to be following their approved change management procedures*

IS Audit of AI & RPA

1. Understand governance process of RPA;
2. Review process of identification of need, areas to be automated, KPI for automation & process of RPA tool implementation;
3. Review of system change management control, i.e., how changes identified, approved, tested, signoff of testing was given, pre and post migration review
4. Analysing robotic controller – review how instructions scheduled in RPA tool,
5. Reviewing of system blueprint & exception handling process;
6. Reviewing process of exception handling log;

- 7. Analyse periodic update & monitoring mechanism implemented by client for monitoring of BOTS.
- 8. Audit access control implemented in RPA, review:

✓ who can approve access to RPA administrator,

✓ who has access to administer BOT,

✓ who have access to manage exception,

- 9. Re-run or make changes in RPA tool, etc.
- 10. Review of RPA transaction logs.
- 11. Perform testing of edit, validation check, error check, etc., configured in RPA
- 12. Re-perform calculation & transaction reviews to ensure – results consistent.

IS Audit of AI

- **6 Elements of an AI Ecosystem**
- Artificial intelligence ethics and governance models
- Formal standards and procedures for the implementation of artificial intelligence engagements
- Data and model management, governance and privacy
- Understanding the human-machine integration, interactions, decision-support and outcome
- Third-party AI vendor management
- Cybersecurity vulnerability, risk management and business continuity
- Complementary to the notion of explainability, auditability describes the possibility to evaluate algorithms, models, and datasets; to analyse the operation, results and effects, even unexpected ones, of AI systems. This notion is made up of two parts.
- The technical part consists in measuring the performance of a system according to several criteria (reliability, accuracy of results, etc.). The ethical part consists in apprehending its individual and collective impacts, as well as checking that it does not pose a risk of breaching certain principles, such as privacy or equality.
- For example, the non-discriminatory nature of a machine learning algorithm will be tested by providing it with fictitious entry data or user profiles.

Thank You