STAFF AUDIT PRACTICE ALERT 6

September 2021

PROTECTION AND RETENTION OF AUDIT CLIENT DATA

This publication has been prepared by the Protection and Retention of Client Data Task Group of the Independent Regulatory Board for Auditors' (IRBA) Committee for Auditing Standards (CFAS). It does not constitute an authoritative pronouncement from the IRBA, nor does it amend or override the International Standards on Auditing, South African Standards on Auditing, South African Auditing Practice Statements or South African Guides (collectively called pronouncements).

This publication is not meant to be exhaustive. Reading this publication is not a substitute for reading the above-mentioned pronouncements, as they are the authoritative texts.

South Africa, in 2019, had the third-highest number of cybercrime incidents in the world, despite ranking 25th in population size, as indicated in a report by a consultancy firm[1]. Firms that perform audits and reviews of financial statements, and other assurance and related services engagements could be more susceptible to data security threats than other professions as they process[2] valuable financial and non-financial information, confidential data, and personal identifiable data. Data is processed from the preliminary activities up to the expiration of the retention period of the engagement for prospective, current and previous clients.

This IRBA Staff Audit Practice Alert, serves to provide guidance and considerations to auditors with respect to the protection and retention of client data.

INTRODUCTION

1. The audit industry is experiencing a wave of digitisation, with an increase in the digital processing of data. The unprecedented challenges arising from the Covid-19 pandemic have demanded that clients and firms work remotely, and resulting in more client data is being exchanged on technological platforms (some of which are unsecure). As a result, these new ways of working are creating more threats of data security breaches.

[1] Article by BusinessInsider.
[2] Refer to paragraph 4 of this document.

2. The damage caused by a data breach is unpredictable and depends on the:
   - Nature and extent of the breach;
   - Nature and quantity of the data that is compromised; and
   - Effectiveness of containment and recovery of the compromised data.

3. A firm may incur losses from one or more of the following:
   - Business interruption;
   - Ransom payments;
   - Reputational harm;
   - Technical and forensic investigations;
   - Security and other IT improvements and repairs;
   - Loss of intellectual property;
   - Third party and regulatory claims; and/or
   - Legal fees.

4. For the purpose of understanding this Staff Audit Practice Alert, the terms “process”, “processing” and “processed” mean any operation, activity or set of operations, whether or not by automatic means, concerning data, including:
   a) the collection, receipt, recording, organisation, collation, retention, updating or modification, retrieval, alteration, consultation or use;
   b) dissemination by means of transmission, distribution or making available in any other form; or
   c) merging, linking, restriction, degradation, erasure or destruction of the data.

5. Firms are strongly encouraged to protect the data they process. This may be accomplished through appropriate data protection policies, standards, procedures, guidelines, technological and administrative controls, as well as monitoring, ongoing training and awareness efforts.

MATTERS NOT WITHIN THE SCOPE

6. The following matters are not within the scope of this Staff Audit Practice Alert:
   - Protection and retention of data by the audit client;
   - The firm’s protection and retention of data that is unrelated to assurance engagements;
   - The evaluation of the quality of data that is obtained and retained by the firm;
   - Guidance on compliance with the provisions of legislation such as the Protection of Personal Information Act, 2013 and the General Data Protection Regulation 2016/679; and
   - The endorsement of any service providers.

Therefore, firms are advised to consider other guidance and resources as it relates to these matters.

INTERNATIONAL STANDARD ON QUALITY CONTROL OR MANAGEMENT

7. International Standard on Quality Control 1 (ISQC 1), *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements*, paragraph 46, states that the firm shall establish policies and procedures that are designed to maintain the confidentiality, safe custody, integrity, accessibility and retrievability of engagement documentation.

8. International Standard on Quality Management 1 (ISQM 1), *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*[3], paragraph 31, states that the firm shall establish the following quality objective that addresses the performance of quality engagements:

    (f) Engagement documentation is assembled on a timely basis after the date of the engagement report and is appropriately maintained and retained to meet the needs of the firm and comply with law, regulation, relevant ethical requirements, or professional standards.

    Paragraph A84 of ISQM 1 states that the retention and maintenance of engagement documentation may include managing the safe custody, integrity, accessibility or retrievability of the underlying data and the related technology. The retention and maintenance of engagement documentation may involve the use of IT applications. The integrity of engagement documentation may be compromised if it is altered, supplemented or deleted without authorisation to do so, or if it is permanently lost or damaged.

IRBA CODE OF PROFESSIONAL CONDUCT FOR REGISTERED AUDITORS

9. The *IRBA Code of Professional Conduct for Registered Auditors (Revised November 2018),* subsection 114, requires a registered auditor to comply with the principle of confidentiality, and this includes the responsibility to respect the confidentiality of information acquired as a result of professional and business relationships.

[3] Effective date:
- Systems of quality management in compliance with ISQM 1 are required to be designed and implemented by 15 December 2022; and
- The evaluation of the system of quality management required by paragraphs 53-54 of ISQM 1 is required to be performed within one year following 15 December 2022.

POSSIBLE THREATS

10. Firms that have inadequate policies, processes and controls over data protection and retention may:
    - be vulnerable as the data that is processed is not secure;
    - have instances where employees, intentionally or unintentionally, do not act in the best interests of the firm; and
    - have attacks that take advantage of the weaknesses in the processes and controls.

11. Below are some possible threats to the protection and retention of client data:
    - **Outdated software** – The firm's business systems (operating systems and applications) may be more vulnerable to data breaches, if the software is outdated. Also, outdated software could result in a systems failure, leading to processed data being permanently lost.
    - **Data breaches caused by employees** – Many firms currently make use of remote access auditing tools to enable employees to access auditing software from different devices and various locations. Firms may even allow employees to use their personal devices for business purposes. These personal devices, though, might lack the security features and software updates required to keep the data safe.
    - **Unauthorised software and applications** – Employees might download unauthorised software and applications onto firm and personal devices that are used for work purposes. Unauthorised software and applications might have security features that are weaker than what the firm's security policies require.
    - **Weak passwords** – A common mistake that employees make is setting up weak passwords to access their accounts and using the same password for multiple access points. Consequently, if an attacker obtains one password, they may gain access to multiple data sources.
    - **IT asset disposal breaches** – Firms continuously update their hardware devices to meet their storage and performance needs. As a result, decommissioned IT assets could still be

Links to articles on recent incidents in South Africa:

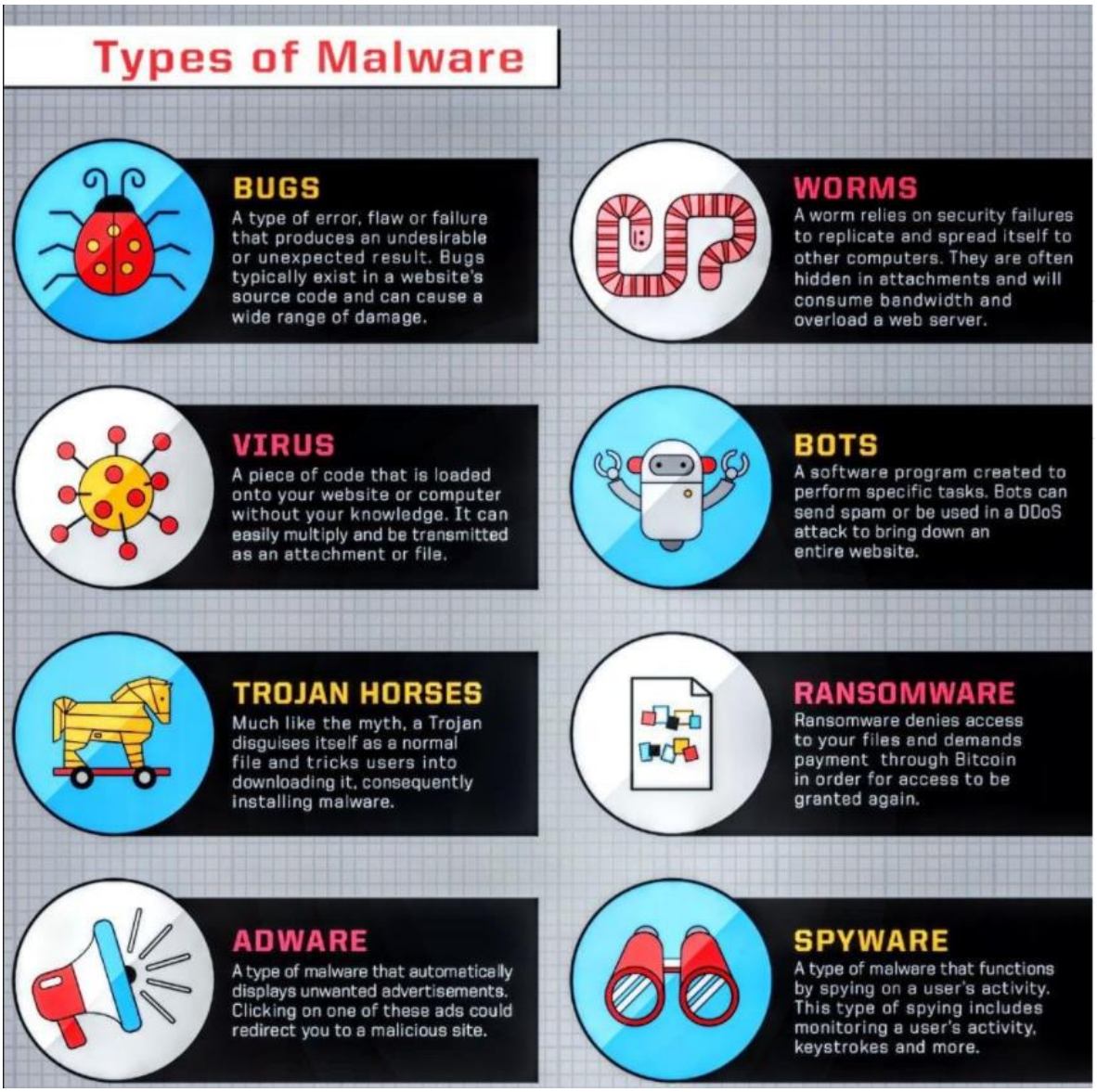
- Data breach hits major SA insurance player – Qsure
- Rain hit by security breach – Rain
- Personal information of South Africans posted online after major data breach - Experian
- Transnet cyber-attack confirmed: Port terminals division declares force majeure - Transnet
- Serious data breach rocks Absa Group – ABSA Group

in good working order and can be repurposed for resale or reuse. Unfortunately, it is possible to retrieve information from old assets, if it has only been removed through the standard delete commands. This can then lead to unauthorised access to confidential client data.

- **Employees who leave the firm** – Employees may still have access to confidential client data that is not retrieved when they leave the firm. This confidential client data could be stored at the employee's home, in external storage devices, and/or in the employee's personal email accounts, and it could be accessed easily by unauthorised users or be lost permanently.
- **Data exchange** – Firms communicate externally and internally through multiple channels. They also communicate with clients over email and might even exchange files such as bank statements, tax documents, and similar sensitive data via email attachments. The exchange of sensitive data might expose the firm to malware attacks such as ransomware to steal sensitive financial data that is in transit.
- **Data access** – Firms may use cloud-based computing to enable employees to access audit software and client data remotely over the internet or internal networks and this may increase the risk of security data breaches. In addition, intentional or unintentional destruction of physical data storage facilities or the use of malicious software (malware) could result in data loss/breaches.

Types of malware:

There are various types of malware and understanding them is one way to help to protect your data and devices. The diagram[4] below highlights some of these types of malware.

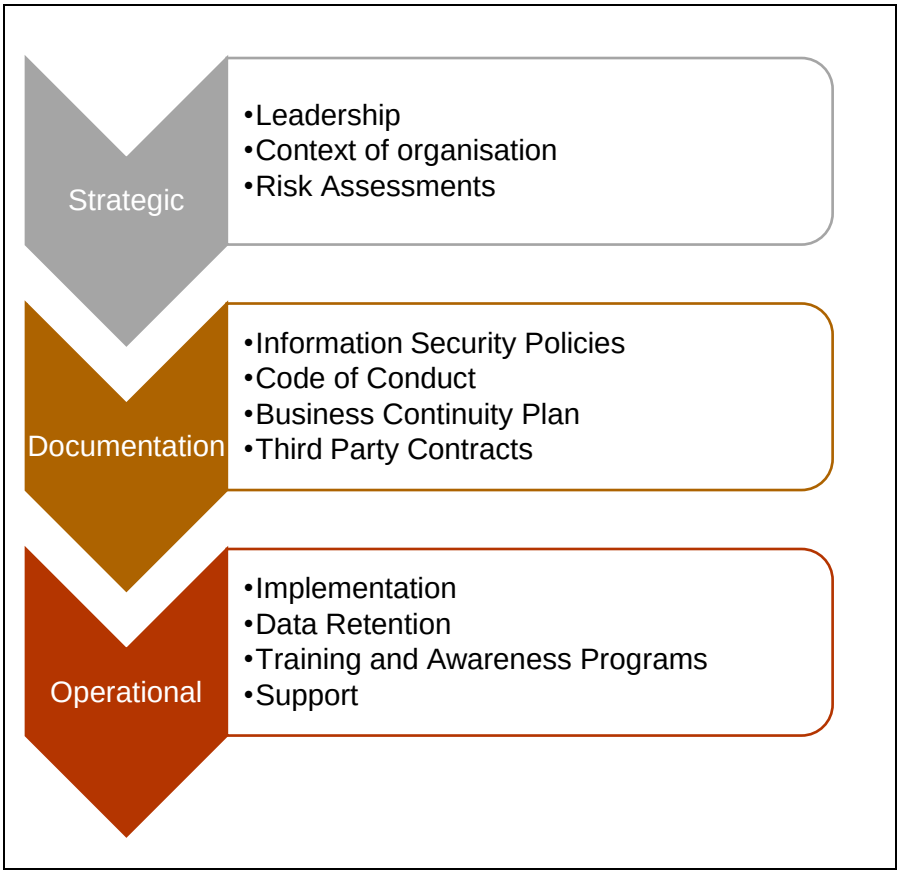


[4] The graphic is from the USCybersecurity magazine (https://web.facebook.com/USCyberMag/photos/a.832859663452332/3387773061294300/?type=3&theater).

THE CONTROL ENVIRONMENT

12. Mitigating the threats relating to the protection and retention of data can be complex. Therefore, firms are encouraged to establish quality objectives that consider recognised frameworks in developing their policies and procedures on data protection and retention.

13. In developing the policies and procedures relating to data protection and retention, the following elements may be taken into consideration:



Strategic

- **Leadership**: The commitment of the firm's leadership sets the tone at the top. Additionally, information security is a firm-wide project. Therefore, roles and responsibilities must be allocated to and understood by all parties that are responsible for processing data for the firm.
- **Context of the Organisation**: Understanding the internal and external factors that impact the data processed by the firm is important. Internal factors are under the control of the firm and include the organisational structure, organisational drivers, availability of resources or contractual relationships. External factors are not under the control of the firm, but the firm

can anticipate and adapt to them. Such external factors include applicable laws and regulations, technological innovations as well as political and economic conditions.

- **Continuous Risk Assessments**: These allow the firm to identify its risks and vulnerabilities and to then put controls in place to respond to them effectively.

Documentation

- **Information Security Policies**: A set of policies for information security that are defined, approved by the firm's leadership, published and communicated to employees and relevant external parties. Mandatory and recommended policy statements can include, but are not limited to:
  - Access control;
  - Asset management: classification and control;
  - Communications and operations security;
  - Human resources security: personnel;
  - Information systems acquisition, development and maintenance;
  - Physical and environmental security; and
  - Risk assessment.

  Additional technical security controls include, but are not limited to:
  - Desktop and laptop full disk encryption;
  - Read only USB ports;
  - Removable media encryption tools;
  - Desktop and laptop firewalls;
  - Antivirus and anti-malware software;
  - Multifactor authentication solutions;
  - Automated patching and security vulnerability assessments;
  - Intrusion detection and prevention technologies; and
  - Monitoring and detection systems.

- **Code of Conduct**: The firm's Code of Conduct guides the daily decisions made by the firm's employees, regardless of their individual role or position and it holds the employees accountable to the applicable professional and technical standards.
- **Business Continuity Plan**: This provides continuity of information security during a disruptive situation. A management structure and relevant escalation trigger points are to be identified to ensure that when an event increases in severity, the relevant escalation to the appropriate authority is made effectively and in a timely manner.
- **Third Party Contracts**: Where the firm engages third parties to process data, the contracts are to contain provisions that are commensurate with the firm's own policies, practices and

controls to ensure that its audit clients data is processed properly and securely, in accordance with legal and regulatory requirements.

Operational

- **Implementation**: Processes and controls are to be planned, implemented, controlled, monitored and maintained to operationalise information security.
- **Data Retention**: Data has to be retained for a certain number of years as defined by the applicable legislation and for an intended purpose. Where legislation refers to the retention of the same data, the firm has to consider adhering to the most stringent of the legislative requirements.
- **Training and Awareness Programmes**: Raising awareness about threats to information security is an ongoing and dynamic process that includes regular mandatory training for employees as well as other activities to drive awareness within the entire firm.
- **Support**: The availability of resources, the competence of employees, awareness, and communication are key factors that support information security.

The above, though, is not an exhaustive list of elements that could be included in a control environment framework. Therefore, it should not detract the firm and registered auditors from exercising their professional judgement and due care in protecting and retaining client data.

14. Below are key questions for the firm's leadership to consider when processing client data (this is not an exhaustive list):

1. Do engagement letters, terms and conditions and other contracting documents contain the relevant clauses regarding data protection and security?
2. Are the tools and technology used for the processing of data secure and compliant with the standards and legislation?
3. Can the processes and controls that are in place be demonstrated to regulators, authorities and clients?
4. Are there adequate policies and procedures in place to ensure the protection of data from the point of collection to destruction?
5. Are the processes, controls, and procedures frequently reviewed and tested?
6. Has training been provided to all employees regarding the protection and retention of client data?
7. Is there a response plan if a data breach were to occur?
8. Are third parties/service providers aware of and have sufficient data protection controls?
9. Are there adequate resources engaged by the firm to proactively monitor and maintain data security processes and controls?