Protection and Retention of Client Data

Presenter: **Lettie Janse van Vuuren** CA(SA)

28 OCTOBER 2021

Issued by IRBA as a staff alert in September 2021…..
to provide guidance and considerations to auditors with respect to the protection and retention of client data

Presenter

Lettie Janse van Vuuren CA(SA)

- Lettie joined SA Accounting Academy in November 2017 as Head of Technical. She is a Chartered Accountant, Qualified Auditor, Assessor and Moderator.
- She is a **professional trainer and webinar host**, and with her relaxed and humorous presentation style, she is able to hold the attention of an audience. She has a unique ability to communicate with delegates at their respective levels of knowledge and experience. Over the last 20 years, she has trained thousands of partners, managers, trainee accountants and other professionals.
- She is responsible for our MCLU (Monthly Compliance and Legislation Updates).
- She was the Professional Development Manager at SAICA for 4 years and in charge of accrediting new training offices and monitoring existing ones (including the moderation of training offices and trainee assessments).
- Lettie is passionate about improving the efficiency and standardisation at practices. She has extensive experience on a variety of technical and practical topics which she consults on, including: SAICA re-accreditation assistance and preparation, IRBA inspection assistance and preparation, audit file reviews (post-issuance monitoring and EQCR), Quality control implementation, other office-specific manuals, and FASSET skills development facilitation.

WHAT'S ON THE AGENDA?

Contents

- **Introduction**: More on Cybersecurity
- **How does digital processing link to the following laws, regulations and pronouncements:** POPIA, ISQM 1, IRBA Code
- **Contents of the IRBA Staff Practice Alert, including:**
  - Possible implications on the audit firm if the confidentiality of client data is compromised;
  - Possible threats to the protection and retention of client data;
  - Possible developments and improvements of the control environment that can be implemented by an audit firm to protect and retain client data; and
- **Some key questions for the firm's leadership to consider when processing client data.**
- **In closing…**

Quotes

THEY WANT WHAT YOU'VE GOT. DON'T GIVE IT TO THEM.

INTRODUCTION

Abbreviations used

- **IRBA** = Independent Regulatory Board for Auditors
- **POPIA** = Protection of Personal Information Act
- **ISQM** = International Standard on Quality Management

Recent changes in our world…

- With digitisation and protection of information the new buzzwords of the decade, the digital processing of data is increasing on a daily basis.
- Reeling from the effects of the COVID-19 pandemic, clients and firms are working remotely.
- This means that 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.

➢ *Refer to IRBA Staff Alert 6 which is available to you as a Source Document*

Effects on Auditors

- 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 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

"I know a lot of highly-confidential company secrets, so my boss made me get a firewall installed."

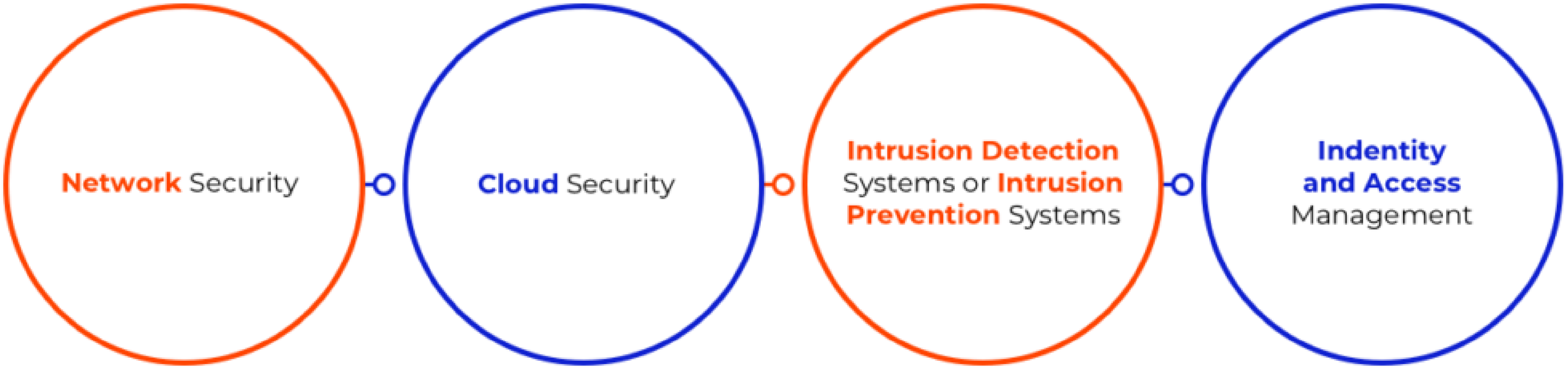
Cybersecurity

- We cannot ignore cybersecurity when talking about POPIA.
- Part of information security is cybersecurity, which refers to the practice of ensuring the integrity, confidentiality, and availability of information.

Why is cybersecurity important?

- The world relies on technology more than ever before. As a result, digital data is created at a pace never thought possible.
- Today, businesses and governments store a great deal of that data on computers and transmit it across networks to other computers and countries. The major cybersecurity risks to your business.

Common types of Cybersecurity



Is Cybersecurity changing?

- YES! Cybersecurity is constantly evolving
- Traditional cybersecurity is centered on the implementation of defensive measures around a defined perimeter.
- Recent enablement initiatives like remote workers and Bring Your Own Device policies have dissolved the perimeter, reduced visibility into cyber activity, and expanded the attack surface.
- Ultimately, your company must be empowered to prioritise the most serious threats to data privacy by reducing investigation, and threat detection times.

Data Breaches

- 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
- Data breaches can be caused by employees
- Data breaches can be caused by hackers
- Remember that data breaches must be reported to the Information Regulator of SA (in terms of POPIA)
- Links to articles on recent incidents in SA

➢ *Refer to page 4 of Staff Alert 6*

How does Digital Processing link to Laws, Regulations & Pronouncements?

Link to other authoritative items

Digital processing links to the following laws, regulations and pronouncements:

- **POPIA** (The Protection of Personal Information Act) – definitions = NB
  - ➢ *Refer to page 2 of Staff Alert 6*
- **ISQM 1**, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*
  - ➢ *Refer to page 3 of Staff Alert 6*
- The **IRBA Code** of Professional Conduct for Registered Auditors (Revised November 2018)
  - ➢ *Refer to page 3 of Staff Alert 6*

CONTENTS OF THE IRBA STAFF PRACTICE ALERT 6

Where will we focus?

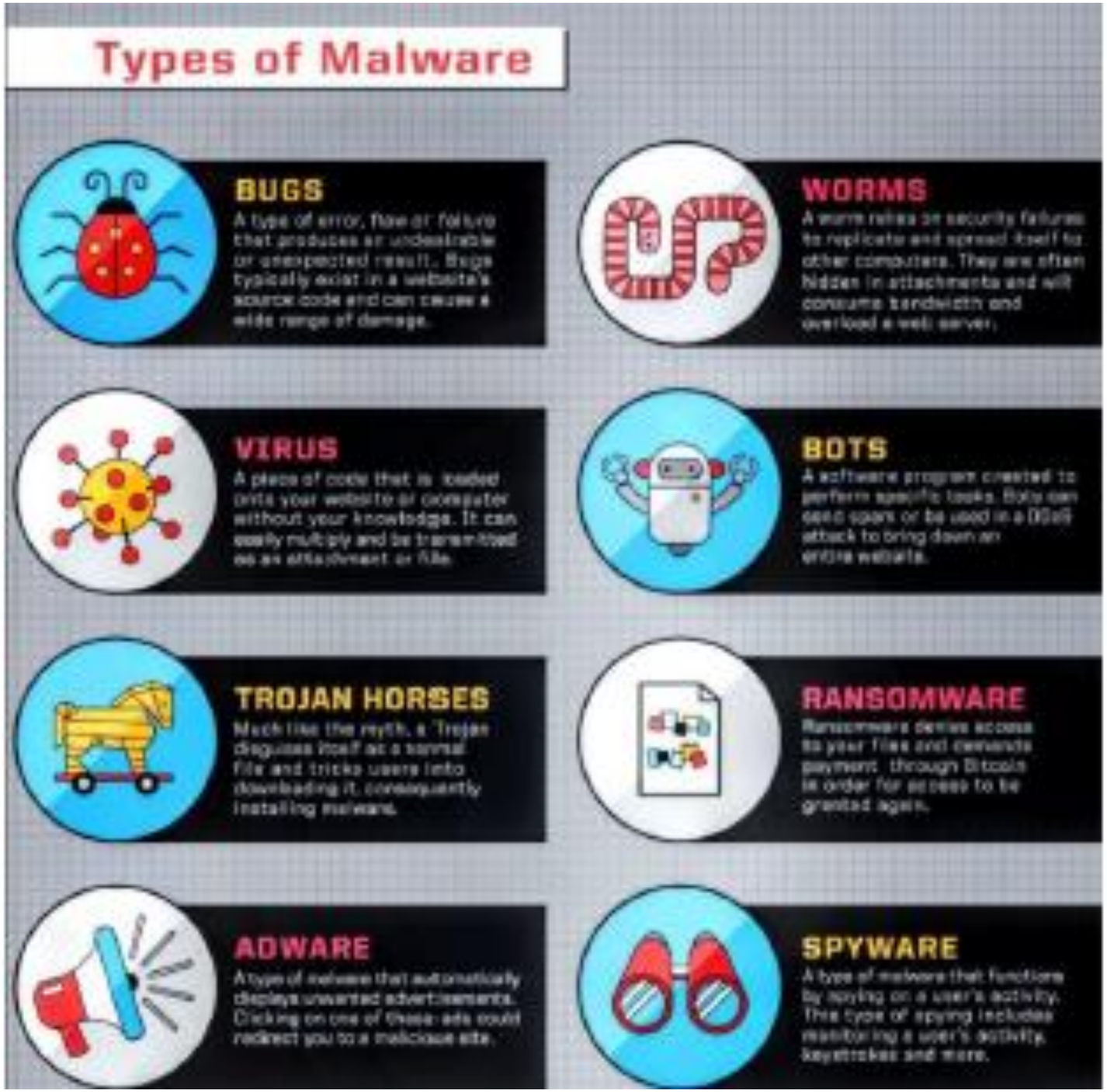
- An overview of this staff alert to help practitioners and firms successfully plan and implement the standards by the effective date, and will also provide some examples for illustrative purposes:
  - Possible implications on the audit firm if the confidentiality of client data is compromised;
  - Possible **threats** to the protection and retention of client data;
  - Possible developments and improvements of the **control environment** that can be implemented by an audit firm to protect and retain client data;

➢ *Refer to Source Document available to you*

Threats

- **Possible Threats**
  - Data breaches
  - Malware

➢ *TYPES OF MALWARE: Refer to page 6 of Staff Alert 6*

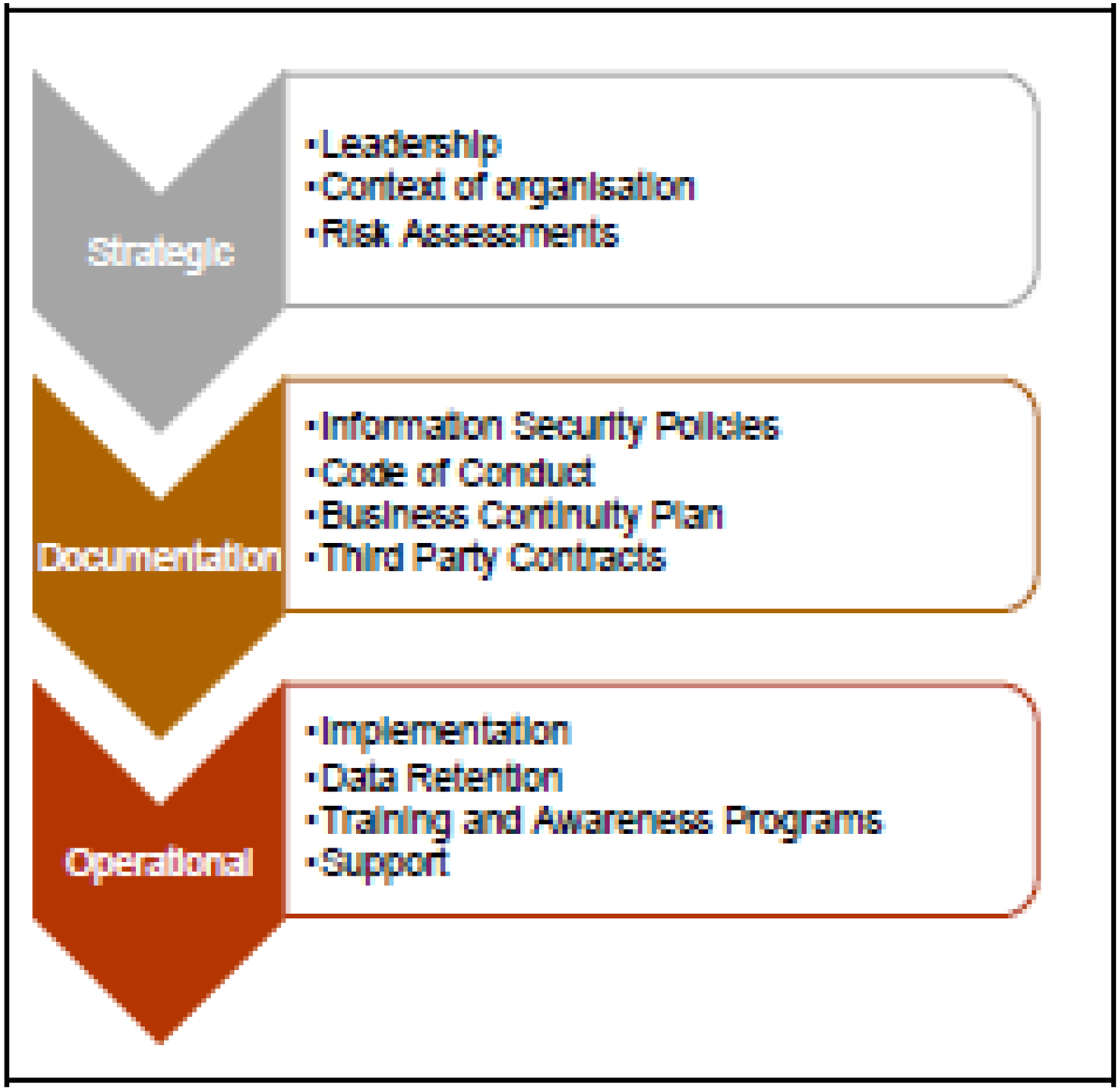


Types of Malware

The Control Environment

- **The Control Environment**
  - Strategic
  - Documentation
  - Operational

➢ *Refer to pages 7 of Staff Alert 6*



What to consider…

Key Questions for the Firm's Leadership to Consider When Processing Client Data

What to ask yourself

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?

➢ *Refer to page 10 of IRBA Staff Alert 6 – available to you as a Source Document*

Source & Bonus Documents

The following SOURCE Documents are available to you:

1. IRBA Communique 66_Protection-and-Retention-of-Client-Data-Practice-Alert
2. IRBA Staff Audit Practice Alert 6_Protection and Retention of Client Data
3. Staff Alert with Lettie's highlights…

The following BONUS Documents are available to you:

1. SAICA_Retention_of_Records_Guide_updated_2021

- *Watch your emails for upcoming webinars on Cybercrime presented by Lettie*

These are uploaded to your profiles & should be available immediately after the webinar

In closing…

- Info
  - Info
  - Info
- Info

Important INFO

Knowledge = Power!

- **Technical Alerts published daily**
  - **Follow SA Accounting Academy on LinkedIN**
- **Technical Summary Videos**
  - **Short summaries that you access when you want to**
- **Webinars-on-Demand**
  - **Wide variety of topics – not always a “live” event…**
  - All our webinars are available as individual recordings – which you can listen to at your leisure
  - Please refer to the SAAA website
- **MCLU subscription**
  - Stay up-to-date on all the latest developments in our field by attending the **Monthly Compliance & Legislation Update**
  - Please refer to the SAAA website for subscription options

QUESTIONS

for your participation!