Moonstone Compliance Privacy Governance: Regulatory Risk Registers Webinar 2022

24 August 2022

Presented by **Andrea de Jongh**

Agenda

Time	Topic	Presenter
10:00 - 10:05	**Opening and Welcome**	Andrea de Jongh
10:05 – 12:00	**Regulatory Risk Registers**	Andrea de Jongh
12:00 – 12:30	**Questions and Answers**	Andrea de Jongh

CONTEXT

- **Learnings for today:**
  - Why is a Regulatory Risk Register necessary?
  - The Privacy Governance Legislative Framework and understanding risk within the context of your Compliance Universe.
  - Understanding how to mitigate risk through identifying appropriate control measures.
  - Familiarising yourself with the structure of a regulatory risk register.
  - Gaining practical experience with populating a regulatory risk register.

WHY?

- Section 19 POPIA
  - *A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking* ***appropriate, reasonable technical and organisational measures*** *to prevent loss of, damage to, or unauthorised destruction of personal information and unlawful access to or processing of personal information.*

WHY?

- Regulation 4 to POPIA

4. (1) An information officer must, in addition to the responsibilities referred to in section 55(1) of the Act, ensure that-

*(a) a **compliance framework** is developed, implemented, monitored and maintained;*

(b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

(c) a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

(d) internal measures are developed together with adequate systems to process requests for information or access thereto; and

*(e) **internal awareness sessions** are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.*

*(2) **The information officer shall upon request by any person, provide copies of the manual** to that person upon the payment of a fee to be determined by the Regulator from time to time. Application for issuing code of conduct 5…*

RISK ASSESSMENT

- Consider the nature, sensitivity, and volume of personal data affected:
  - The number of individuals affected?
  - The overall quantity of affected personal data?
  - The risk of combining the types of data breached when processed together – i.e. identity theft or fraud
- Consider whether the data can be restored after an attack, if not due to poor organisational controls, it would increase the risk if the backup files were affected by the ransomware

DATA PRIVACY PROGRAMMES

- **Legal compliance**
  - POPIA
  - PAIA
  - FSP Compliance universe
  - Cybercrimes Act

POPIA – Privacy Governance as your point of departure

Andrea de Jongh

DATA PRIVACY PROGRAMMES

a) Executive buy in
b) Know your data
c) Policy-setting
d) Training
e) Vendor & third-party management
f) Legal compliance
g) Reporting

KNOW YOUR DATA

• POPIA s17 (art 30 GDPR) read with PAIA – you need a record of processing activities, specifically, where in your operation you process personal information

• This will help your governance risk and compliance relating to data, help you take informed risks, and have a record of your processing and level of compliance

Fact finding mission:

- Know where your gaps are;
- If you know what your benchmark is, you will understand whether you are applying the required standards and principles to your processing activities;
- You can't do this if you don't have a clear understanding of where you are processing personal information; and
- What your justification ground(s) is/are

THE CRUX OF POPIA

POPIA

Protection of Personal Information Act

ACT Summary and Preamble

Chapter 1 Definitions and Purpose

Chapter 2 Application Provisions

Chapter 3 Conditions for lawful Processing

Part A Processing of personal information in general

Condition 1 Accountability

Condition 2 Processing limitation

Section 9 Lawfulness of processing

Section 10 Minimality

Section 11 Consent, justification and objection

Section 12 Collection directly from data subject

Condition 3 Purpose specification

Section 4 Lawful processing of personal information

(1) The conditions for the lawful processing of personal information by or for a responsible part are the following:

- **(a) "Accountability",** as referred to in section 8;
- **(b) "Processing limitation",** as referred to in sections 9 to 12;
- **(c) "Purpose specification",** as referred to in sections 13 to 14;
- **(d) "Further processing limitation",** as referred to in section 15;
- **(e) "Information quality",** as referred to in section 16;
- **(f) "Openness",** as referred to in sections 17 and 18;
- **(g) "Security safeguards",** as referred to in sections 19 to 22; and
- **(h) "Data subject participation",** as referred to in sections 23 to 25.

(2) The conditions, as referred to in subsection (1), are not applicable to the processing of personal information to the extent that such processing is:

- (a) excluded, in terms of section 6 to 7, from the operation of this Act; or
- (b) Exempted in terms of section 37 to 38, from one or more of the conditions concerned in relation to such processing.

POPIA'S 8 PROCESSING CONDITIONS

1. **Accountability** – the responsible party (RP) is accountable for compliance with POPIA.

2. **Processing limitation** – you may only process the minimum information needed to fulfil the purpose for which the personal information (PI) was collected. Crux, there must be a causal between the PI being processed and the purpose for which it was obtained. You may only process PI over and above the stated purpose if it meets the criteria of Further Processing Limitation.

3. **Purpose specification** – the RP must collect the PI for a specific, explicitly defined, and lawful purpose related to its function or activity.

4. **Further processing limitation** – further processing of PI must be compatible with the original purpose why the RP collected the PI.

5. **Information quality** – the RP must take reasonably practical steps to ensure the PI is complete, accurate, not misleading, and up to date, having regard to the purpose for which the PI is collected or further processed.

6. **Openness** – you must be transparent about your reasons for obtaining PI and ensure that what you do with the information is in line with the reasonable expectations of the data subject.

7. **Security safeguards** – you must secure the integrity and confidentiality of PI by taking appropriate, reasonable, technical, and organisational measures to prevent loss, damage, unauthorised destruction of, and unlawful access to, or processing of PI.

8. **Data subject participation** – the data subject has the right to request you to confirm what PI you hold and with whom you have shared it, as well as to request you to correct, update or delete their PI.

THE CRUX OF POPIA

Section 11 Consent, justification and objection

(1) Personal information may only be processed if:

a. the data subject or competent person where the data subject is a child consents to the processing;
b. Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
c. Processing companies with an obligation imposed by law on the responsible party;
d. Processing protects a legitimate interest of the data subject;
e. Processing is necessary for the proper performance of a public law duty by a public body; or
f. Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied

(2)

a. The responsible party bears the burden of proof for the data subject's or competent person's consent as referred to in subsection (1)(a).
b. The data subject or competent person may withdraw his, her or its consent, as referred to in subsection (1)(a), at any time: Provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of subsection (1)(b) to (f) will not be affected.

KNOW YOUR DATA

Identifying your processing activities and Legal Compliance

- Identify every processing activity in the organisation where personal information is collected
  - Processing activities where no personal information is collected do not fall within the ambit of POPIA.

- Identify the legal justifications for the processing of personal information within each activity (section 11).
  - If the organisation cannot justify (per the grounds provided in section 11)
  - why it is processing the personal information,
  - it must stop processing immediately.

KNOW YOUR DATA

Identifying your processing activities and Legal Compliance

- Identify every processing activity in the organisation where personal information is collected
  - Processing activities where no personal information is collected do not fall within the ambit of POPIA.

- Identify the legal justifications for the processing of personal information within each activity (section 11).
  - Where the organisation has identified any special personal information is collected within the processing activity:
    - ensure that such processing adheres to the conditions listed in sections 26 to 33, as applicable.
  - Where the organisation has identified that personal information of a child is processed is collected within the processing activity:
    - ensure that such processing adheres to the conditions listed in sections 34 and 35, as applicable.

KNOW YOUR DATA

Data mapping, forms and documenting processing activities

- Document and data map each of the processing activities
  - It is important to identify and be able to demonstrate to the Information Regulator where the personal information is collected from, with whom it is shared and how it will be stored.

- Identify the processing activities in your organisation that requires data subjects to complete or fill in a form
  - Forms include hard copies and online versions.

- Evaluate and assess each data field on the form to establish whether the organisation has a legal justification for the collection of the personal information requested in each field
  - This process will help to simplify your forms, as the organisation must refrain from requesting personal information which is not relevant to the performance of the services rendered by the organisation.

KNOW YOUR DATA

Inherent risk ratings

- Perform an inherent risk rating on each processing activity, by looking at:
  - Factors such as the volume of Personal Information processed; whether the Personal Information is valuable; will there be a disruption to the business if the Personal Information is lost; how easily can the Personal Information be recovered etc.; and
  - Risk criteria, namely the terms of reference against which the significance of risk is evaluated, e.g.
    - Risk criteria are based on organizational objectives, and external context and internal context; and
    - Risk criteria can be derived from standards, laws, policies and other requirements.

KNOW YOUR DATA

Inherent risk ratings

- Risk ratings are usually conducted according to a “likelihood” and “impact” scoring model, where the combined score provides the inherent risk rating.
- The aforementioned is done to identify which processing activities pose the highest risk for the organisation
- These are the risks that the organisation will have to address first.

KNOW YOUR DATA

Risk Criteria

Risk criteria derived from an external context refers to the external environment in which the organization seeks to achieve its objectives

- **External context can include the following:**
  - the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
  - key drivers and trends having impact on the *objectives* of the organization;
  - relationships with, and perceptions and values of, external stakeholders **.**

KNOW YOUR DATA

Risk Criteria

Risk criteria derived from an internal context refers to the internal environment in which the organization seeks to achieve its objectives

- **Internal context can include:**
  - governance, organizational structure, roles and accountabilities;
  - policies, objectives, and the strategies that are in place to achieve them;
  - the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
  - information systems, information flows and decision-making processes (both formal and informal);
  - relationships with, and perceptions and values of, internal stakeholders;
  - the organization's culture;
  - standards, guidelines and models adopted by the organization;
  - form and extent of contractual relationships.

KNOW YOUR DATA

Risk Treatment

What is it?

- Risk treatment is the process to modify risk and can involve:
  - avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
  - taking or increasing risk in order to pursue an opportunity;
  - removing the risk source;
  - changing the likelihood;
  - changing the consequences;
  - sharing the risk with another party or parties (including contracts and risk financing);
  - retaining the risk by informed choice.

- Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

- Risk treatment can create new risks or modify existing risks.

KNOW YOUR DATA

Residual Risk

What is it?

- Residual risk is the risk remaining after risk treatment
  - Residual risk can contain unidentified risk.
  - Residual risk can also be referred to as “retained risk”.

KNOW YOUR DATA

Non-conformances & Solutions (Regulatory Risk Register)

Identify which remedial steps will be implemented to address the non-conformances. There are four types of control measures:

1. Directive Control Measure

Directive controls provide guidance on how to prevent a risk or loss. It is the simplest form of an internal control system, but also the easiest to implement, e.g. Policies, Procedures and Training Sessions

2. Preventative Control Measure

Preventative controls are designed to prevent the materialisation of loss or risk before they occur, e.g. separation of duties, various sign off and approval systems, insurance measures and reporting.

3. Detective Control Measure

Detective controls are designed to discover the source of an error or irregularities and to correct it accordingly. Detective controls can assist to prevent small problems from becoming major problems, e.g. the regular reviewing and updating of systems.

4. Corrective Control Measure

Corrective controls aim to remedy problems that can be systematically corrected, e.g. additional training or gradual changes in procedures.

KNOW YOUR DATA

Non-conformances & Solutions (Regulatory Risk Register)

- The remedial steps is to:
  - ensure that the processing activity is compliant with POPIA, the non-conformances must be brought in line with the conditions for lawful processing
  - incorporate the 8 conditions for lawful processing

KNOW YOUR DATA

Non-conformances & Solutions (Regulatory Risk Register)

- Starting with the processing activities which scored the highest risk ratings during activity 10, measure each data mapped processing activity against the conditions for lawful processing stipulated in POPIA, and note the non-conformances in your Regulatory Risk Register.
  - By measuring your processing activities against the conditions for lawful processing, the organisation is establishing whether its processing activities are in fact POPIA compliant or not.
  - Processing activities with a “lower” risk rating can be dealt with after the processing activities with a “higher” risk rating have been fully addressed.
- Identify which remedial steps will be implemented to address the non-conformances.
  - To ensure that the processing activity is compliant with POPIA, the non-conformances must be brought in line with the conditions for lawful processing through the identification of remedial steps which incorporates the conditions for lawful processing.

KNOW YOUR DATA

Non-conformances & Solutions (Regulatory Risk Register)

- Starting with the processing activities which scored the highest risk ratings:
  - measure each data mapped processing activity against the conditions for lawful processing stipulated in POPIA: and
  - note the non-conformances in your Regulatory Risk Register.
- By measuring your processing activities against the conditions for lawful processing, the organisation is establishing whether its processing activities are in fact POPIA compliant or not.
- Processing activities with a “lower” risk rating can be dealt with after the processing activities with a “higher” risk rating have been fully addressed.
- Identify which remedial steps will be implemented to address the non-conformances:
  - to ensure that the processing activity is compliant with POPIA;
  - the non-conformances must be brought in line with the conditions for lawful processing;
  - through the identification of remedial steps which incorporates the conditions for lawful processing.

KNOW YOUR DATA

Non-conformances & Solutions (Regulatory Risk Register)

- Set out the remedial steps in a project timeline, according to which the proposed remedies will be implemented.
  - Assign a responsible person and a due date by which the remedial steps must be implemented.

- Monitor the effectiveness of the remedies implemented.
  - Propose and implement alternate remedies if the current remedies are inefficient

KNOW YOUR DATA

Policy Setting

- Draft and implement an Information Security Management Policy. Where there is an existing Information Security Management Policy, review the content to ensure that it is in line with
  - Refer to ISO Standards 27001 (the Requirements for setting up the information security management system (“ISMS”)) and 27002 (the Code of Good Practice for ISMS) for guidance.

  - Ensure that the Information Security Management Policy addresses the organisation’s incident management procedure, information security risk assessments, information asset registers and information security assessments.

KNOW YOUR DATA

Classic Information Security Management System (“ISMS”) Roadmap (27001)

- **Establishing the context:**
  - Initiating, scope & policy – section 4
  - Leadership – section 5
- **Planning – section 6:**
  - Risk methodology & acceptance
  - Risk assessment
  - Risk treatment & Statement of Applicability
- **Supporting Activities:**
  - Implementation – section 7
  - Training & Awareness – section 8
- **Performance Evaluation – section 9:**
  - Monitor, Review, & Internal Audit
  - Continual Improvement
  - Certification and External Audit
  - Run ISMS

BUSINESS BEST PRACTICE TO PREVENT CYBERSECURITY BREACH

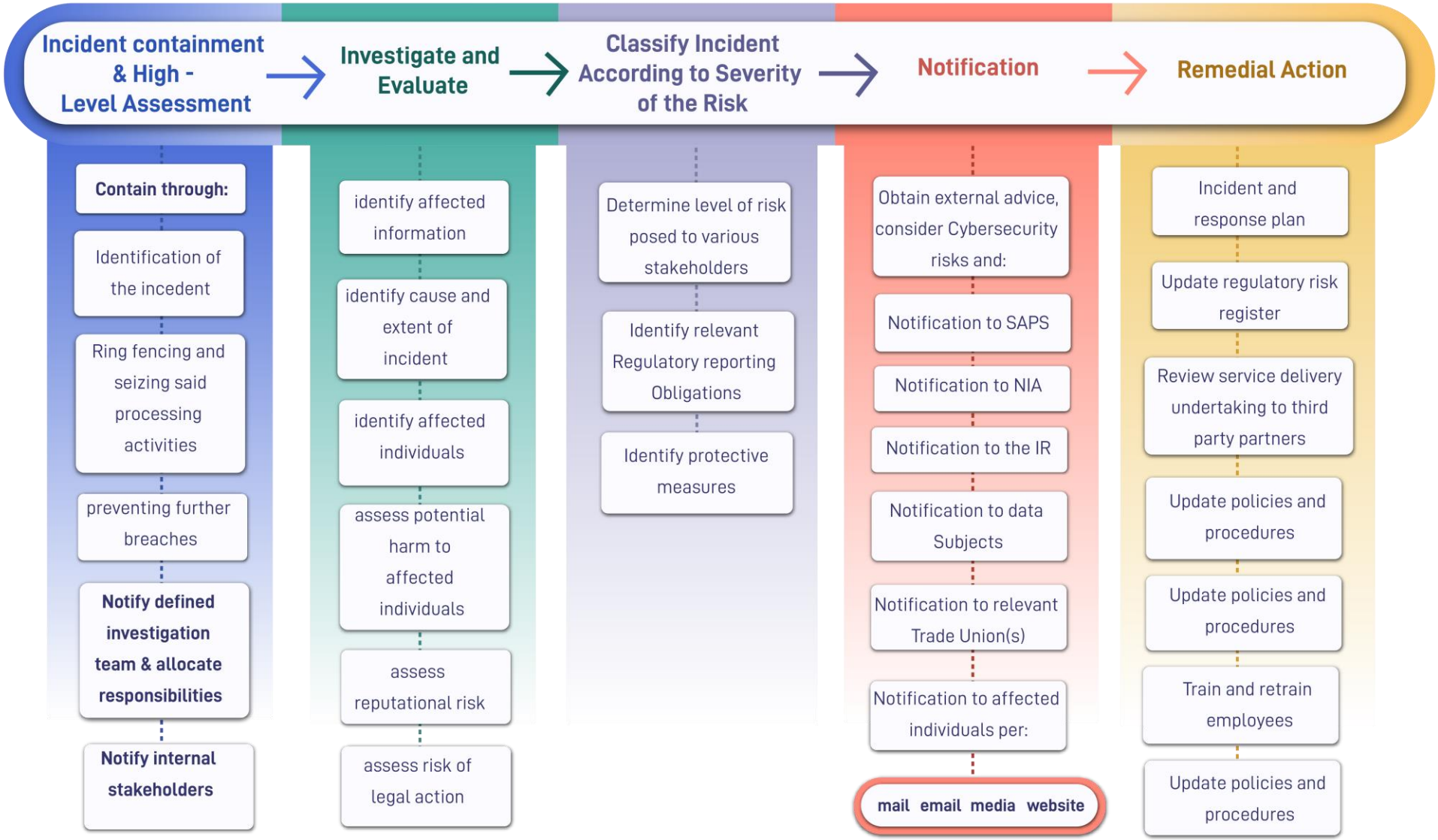
Control Measures to consider

- Build and practice good cyber hygiene (preventative measure)
- Protect access to assets (protect business value)
- Protect email domain (prevent phishing attacks)
- Build disaster recovery plan (mitigate cyber risk)
- Build culture of cybersecurity (support a protected environment)

CYBERSECURITY PRO-ACTIVE BEHAVIOUR

- Understand what your responsibilities are flowing from your Compliance Universe
  - What do you need to report to whom in the event of a breach; and
  - When does your reporting obligation arise?
- Ensure your cybersecurity programme contains sufficient controls to ensure your Compliance Universe responsibilities are integrated and can be met with ease:
  - POPIA (Information Regulator)
  - Cybercrimes Act (SAPS & NIA)
  - Scope of Financial Services Legislation (FSCA)
  - Scope of Registered Credit Providers (Credit Regulator)
  - SARS
- Train your team and colleagues
- Have your service providers in place
- Practice your process – have a Dry-run
- Update your Regulatory Risk Register

There is an Incident



THE DRY RUN

Regulatory Risk Register structure

- Risk ID number;
- Last review date;
- Exposure;
- Compliance Risk Area;
- Regulatory Reference;
- Operational Attributes;
- Provision [relevant section(s) of POPIA];
- Risk Description;
- Risk Owner;
- Likelihood Rating;
- Impact Rating;
- Risk Rating (Likelihood x Impact);
- Control Measures (Detective, Directive, Preventative, Corrective)

THE DRY RUN

Regulatory Risk Register

- **Exposure:**
  - Ongoing

THE DRY RUN

Regulatory Risk Register

- **Regulatory Reference:**
  - The Rights of the Data Subjects
  - Follows the 8 processing conditions as per POPIA
  - Processing Special PI
  - Processing PI of Children
  - Specific responsibilities of the Information Officer
  - Prior Authorisation
  - Direct Marketing
  - Directories
  - Automated Decision Making
  - Transborder Information Flow

THE DRY RUN

Regulatory Risk Register

- **Compliance Risk Areas:**
  1. GRC Function and Control Measures
  2. Ethics, Conduct and Culture
  3. Licensing & Statutory Returns
  4. Operational Ability
  5. Financial Management
  6. Human Resources & Development
  7. Information Management & Security
  8. Anti-Money Laundering & Corruption
  9. Complaints Management
  10. Marketing & Communications
  11. Third Party Management & Security

THE DRY RUN

Regulatory Risk Register

- **Organisational Attributes:**
  - Responsible Party; or
  - Operator

Closing and Questions

Andrea de Jongh

OUR POPIA Toolkit

The POPIA Toolkit is aimed at addressing essential compliance risks within the POPI Act and includes useful and customisable templates which will assist your business along its POPIA journey.

The POPIA Toolkit Provides:

- Guidance, Customisable Templates, Checklists and a comprehensive library with legislative texts

Pricing - Please contact us via events@moonstonecompliance.co.za for assistance:

- Our POPIA Toolkit is available to non-clients attending today's webinar, at last year's price of R2 900.00 (ex VAT).
- Existing Moonstone Compliance Clients may download our POPIA Toolkit for free.

Thank you for your time in viewing this presentation

Andrea de Jongh

Privacy Governance Specialist

adejongh@moonstonecompliance.co.za

MOONSTONE
COMPLIANCE AND RISK MANAGEMENT