Privacy Commissioner
Bermuda

JOB DESCRIPTION FORM

POSITION (PID) #	101014					
IDENTIFYING INFORMATION			**POST CERTIFICATION**			
Post Title	Information Systems Auditor			Print Name	Signature	Date
Present Grade	35-37		Prepared By	Christopher R. Moulder	Christopher Moulder	5th Jan 2023
Department	Privacy Commissioner		Post holder Reviewed	Vacant		
Section	Investigations		Dept. Head Agreed	Alexander White		06 Jan 2023

POST STATUS				**POST TRANSFER (if applicable)**	
	New Post	Revised Post	Redefined Post	Previous Title	
				Previous Department	
Date	3rd Jan 2023			Previous Section	
Cabinet Conclusion Ref		2022-23 Budget		Previous Number	
Last Review Date		N/A			
Panel Decision	Grade	Date	Signature	Previous Grade	
		N/A		Date of Transfer	

1. SUMMARY OF MAIN DUTIES (Ideal Maximum Four)	**%**
1. PRIVACY AND SECURITY AUDIT	40
2. RESEARCH, INVESTIGATIONS & REPORTING	40
3. ADMINISTRATION	15
4. TRAINING & ADVISORY	5
	TOTAL = 100%

2. SUMMARY OF ACCOUNTABILITY

2.1 What specifically is this post accountable for?

Working in the Office of the Privacy Commissioner for Bermuda and under the direct supervision of the Assistant Commissioner (Investigations), the post holder's work will consist of a range of complex and diverse functions, including planning and conducting information security and privacy program audits and the provision of guidance on the development of recommendations and remediation plans for control deviancies and information security and privacy risks. The post holder will carry out audits of routine and complex privacy complaints, incidents and data breaches, and document and report audit results to management. As well, the postholder undertakes associated duties within the Office of the Privacy Commissioner that may be required to ensure the business unit continuously adheres to all internal policies, procedures and legislative requirements under the Personal Information Protection Act (PIPA).

2.2 Briefly describe the level of decision-making authority held by this post.

The post-holder has limited decision-making authority for the business unit, but makes recommendations that relate to the audit, risk management, investigations, reporting and related functions. All decisions requiring management input are to be referred to the Assistant Commissioner (Investigations).

2.3 To which position does this post report directly? Assistant Commissioner (Investigations)

3. ESSENTIAL KNOWLEDGE & SKILLS

List the key knowledge and skills required to fulfil the *minimum requirements* of the post under the following categories.

3.1 General Knowledge / People Skills (Soft Skills).

- A high level of integrity and ability to maintain confidentiality in all matters that come to his/her knowledge and the ability to effectively handle confidential and sensitive information
- Good interpersonal skills with a professional service orientated approach in effectively interacting with customers both internally, as a team, and externally
- Sound time management and problem-solving skills
- Excellent communication skills (written and oral)
- Good conflict management and resolution skills
- Advanced ability to multi-task and be adaptable whilst working in a fast-pace, dynamic environment
- Must be detail oriented and careful to verify documentation
- Able to learn quickly, retain and understand relevant information
- Demonstrated case management skills and the ability to prioritize and plan work effectively
- Have a flexible approach to the job and willingness to assist in other areas within the department
- Domestic and international research skills

3.2 Technical Knowledge / Position Specific Skills (Hard Skills). This includes knowledge of particular legislation, processes, specialties, etc.

- Proficient in the use of Microsoft Office Suite of Products and other common computer programmes
- Strong knowledge of audit, security, and privacy frameworks and risk management, internal controls frameworks and/or external auditing, compliance, technology and computer systems
- Strong Understanding of the data lifecycle (e.g., identification, use, access, transmission, storage and destruction of data)
- Strong knowledge of information systems, terminology, concepts and practices
- Strong ability to effectively conduct quality control reviews of audit systems & products, complex audits, privacy impact risk assessments and monitoring activities.
- Ability to analyse, prepare and present detailed and complex audit reports with respect to data obtained from audit, risk management, investigations and monitoring functions
- Ability to perform data mining and data analytics is preferably desired
- Working knowledge of the Personal Information Protection Act and relevant legislation and regulations, including the skills to apply, interpret, and explain.

4. MINIMUM EXPERIENCE REQUIRED (Tick the Appropriate Box)

Based upon the above identified knowledge and skills, what is the minimum number of years' experience required to fulfil the duties of this post?

☐ No previous experience required	☐ Minimum one (1) year	☐ Minimum two (2) years
☐ Minimum three (3) years	☒ Minimum five (5) years	☐ Minimum ten (10) years

4.1 Identify specific experience.

This post requires a minimum of five (5) years relevant experience in a similar capacity

5. MINIMUM EDUCATIONAL QUALIFICATION REQUIRED (TICK THE APPROPRIATE BOX)

☐ Secondary School Graduation Certificate	☐ Apprenticeship/College Certificate	☐ College Diploma
☐ Associates Degree	☐ Advanced or Specialist Qualification	☒ Bachelors Degree
☐ Masters Degree	☐ Professional Designation (Includes Chartered Status)	☐ Doctorate
☐ Other		

5.1 Please list the title of the academic qualification / professional designation required:

A Bachelor's Degree in Information Technology, Computer Science, Accounting, Business, Finance or a related subject

5.2 List any special licenses, registrations or certifications required for this job:

Preference will be given to those with an Internal Audit or Information Systems Auditor certification (CIA, CISA, CFSA, or CRISC) or Professional Accounting qualification (CA, CPA, ACCA)

6.0 RESOURCES UNDER MANAGEMENT

6.1 Management and Supervision of Staff

(Please ensure that the Organization Chart submitted is up to date, accurate and reflects the information listed below)

Please list the position titles (including PID) of 'All Staff' under the 'Direct Supervision' of this post.

N/A

6.2 Non-Staff Budget and Revenue Streams (FOR EACH SUB SECTION TICK THE APPROPRIATE BOX)

6.2.1 What 'Responsibility' does this post have for 'Managing Non-Staff Budget' and 'Government Revenue Collection'? (Non-Staff Budget typically applies to contracts for program delivery & capital expenditure projects)

☒ None	☐ Has Direct Management Responsibility	☐ Is the Accounting Officer

6.2.2 Please indicate the level of Non-Staff Budget and/or Revenue Streams for which this post is responsible.					
☒ None	☐ Less than $500k	☐ $500k to $2m	☐ $2m to $10m	☐ $10m to $40m	☐ Greater than $40m

6.3 Infrastructure for Vital Government Services (FOR EACH SUB SECTION TICK THE APPROPRIATE BOX)		
6.3.1 Is the post responsible for managing 'Infrastructure' critical to the delivery of 'Vital' Government Services?		
☒ No	☐ Yes. Has Direct Management Responsibility	☐ Yes. Is Ultimately Responsible
6.3.2 If 'Yes' to the above, what would be the impact of failure of this infrastructure?		
☐ Low Impact: Mainly internal to Government	☐ Medium Impact: Mainly internal to Government	☐ High Impact: Mainly internal to Government
☐ Low Impact: Bermuda-Wide	☐ Medium Impact: Bermuda-Wide	☐ High Impact: Bermuda-Wide

7. Additional Information

- Master's degree in a related field is an advantage
- Applicants who possess the following may be considered for the post in lieu of the completion of a Bachelor's or equivalent qualification: a minimum of ten (10) years of relevant experience with minimal supervision in a similar environment
- It may be necessary from time to time for the post holder to work beyond the normal working hours. The post holder must be able to act on their own initiative, and work irregular or unscheduled hours, as required, to support the unique mandate of the office
- The duties described herein provide the general nature and level of work performed by the post holder. It is not intended to be an exhaustive list of all responsibilities and skills required of this post. Actual assigned duties may differ due to the varying needs of the Office of the Privacy Commissioner
- Successful completion of an enhanced security vetting and a register of interests is a requirement for this post.

DUTIES AND RESPONSIBILITIES OF THE POST

8. DETAILED DESCRIPTION OF MAIN DUTIES AND RESPONSIBILITIES OF THE POST

(Please use the same Headings for Main Duties as Listed in Section 1.0)

8.1 Privacy and Security Audit duties:

8.1.1 Responsible for the planning and development of information system and privacy audits, including internal risk assessments, risk and approval matrixes, and related internal policies and procedures to determine degree of compliance with applicable policies, standards, procedures and controls

8.1.2 Manage the internal framework, approach, and process to audit external organizations' information security controls and privacy programs against the information security and privacy regulations.

8.1.3 Identify/recommend solutions to improve efficiency and adherence to the audit framework, policies, procedures, and legislative requirements under PIPA

8.1.4 Document information systems and privacy audit results and findings and prepare them for internal review, including recommended process enhancements and control solutions

8.1.5 Leverage past audit results to identify and remediate discrepancies in current audits

8.1.6 Maintain up-to-date professional knowledge of audit frameworks, risk management solutions, impact assessments, privacy, and data protection in order to effectively conduct audits, investigations, and evaluate organisations

8.1.7 Regularly provide briefings of audit workload, current projects, including appropriate application of the Act and presentation of a succinct list of issues for discussion and consideration of next steps.

8.1.8 Undertakes any other associated duties, as requested by the post holder's supervisor or the Privacy Commissioner.

8.2 Research, Investigations, & Reporting duties:

8.2.1 Research relevant domestic and international legislation, governance models, risk assessments, and security and privacy audit and compliance trends and best practices

8.2.2 Draft general advice regarding the development of remediation recommendations to address control deviancies and mitigate information security, systems and privacy risks

8.2.3 Provide technical expertise and advice both internally and externally during data breach incident management

8.2.4 Perform fact-finding meetings, including liaising with external organisations in order to investigate data breaches, review information systems and any other databases or security systems identified during the investigation process. Follow up with responses and inquiries as appropriate

8.2.5 Works with the Assistant Commissioner (Investigations) to determine investigation /audit next steps and may assist in the examination of witnesses under oath

8.2.6 Record, monitor, and maintain statistics and reports on audits, risk assessments, data breaches and incidents, internal information security and system policies, standards, procedures and controls. Provide reports on relevant statistics. Leverage data and data analytics to develop reports on trends and the causes of data breaches

8.2.7 Manage and perform privacy risk assessments and privacy compliance monitoring activities, and analyze results to recommend mitigation for privacy risks associated with non-compliance

8.2.8 Undertakes any other associated duties, as requested by the post holder's supervisor or the Privacy Commissioner.

8.3 Administration duties:

8.3.1 Assist the investigations unit in the development, maintenance, and use of the case management system (manual and automated)

8.3.2 Monitor relevant email mailboxes on a daily basis, identify and action emails relating audit, risk management, investigations, reporting and related functions, passes emails to the appropriate senior manager (escalating critical matters) and conducts general email housekeeping on a regular basis

8.3.3 Prioritises work in alignment with team and office objectives and long-term strategies

8.3.4 Undertakes any other associated duties, as requested by the post holder's supervisor or the Privacy Commissioner.

8.4 Training & Advisory duties:

8.4.1 Engage with external individuals and organisations with the aim to drive improvements in audit, risk management and operational standards.

8.4.2 Assist external organisations with audits, risk management techniques, data breach mitigation techniques and general advice regarding policies, procedures and best practices

8.4.3 Identify audit issues and control weaknesses and advise on corrective actions for the audit procedure. Develop recommendations to remediate control deviancies and mitigate information security and privacy risks.

8.4.4 Lead the presentation of formal reports to stakeholders and management

8.4.5 Provide relevant technical training and guidance internal and external stakeholders. Identify audit training needs within PrivCom and lead the development and delivery of audit training ensuring the appropriate input from the relevant stakeholders

8.4.6 Engage with business units to assist with developing best practice procedures that are balanced to meet the needs of PrivCom, service users, and other regulators

8.4.7 Provide guidance and advice to senior management in developing appropriate tone from the top. Provide technical regulatory advice and support to the business units in understanding their responsibilities and obligations under PrivCom audit policies and regulatory requirements

8.4.8 Undertakes any other associated duties, as requested by the post holder's supervisor or the Privacy Commissioner