SCHEDULE TO THE INSURANCE (PRUDENTIAL STANDARDS) (INSURANCE MANAGERS ANNUAL RETURN) RULES 2017

Schedule 1 paragraph 3(2)

MATTERS TO BE INCLUDED IN ANNUAL RETURN

1. The following information is required in an annual return—

(a) the names of the directors, types of directors (whether executive, non- executive (service provider), non-executive (affiliate), independent), residences of the directors, professional qualifications, experience of the directors and years employed by the insurance manager;

(b) the organizational structure of the insurance manager, including but not limited to —

(i) the names, roles, residences, professional qualifications, experience and years employed by the insurance manager of the managers and officers;

(ii) the names, roles, residences, professional qualifications, experience and years employed by the insurance manager of the staff and employees;

(iii) whether the staff and employees referred to in clause (ii) are employed by an affiliate of the insurance manager;

(c) details of the services provided by the insurance manager;

(d) where the services referred to in subparagraph (c) are out-sourced to service providers or affiliates of the insurance manager—

(i) the names of those service providers or affiliates;

(ii) the services provided by those service providers or affiliates; and

(iii) the jurisdictions where the service providers or affiliates perform the services;

(e) the names, registration numbers, insurance classes, and whether the entity is a affiliate or non-affiliate of all insurers that are managed by the insurance manager or to whom services are provided;

(f) where any of the insurers referred to in subparagraph (e) have, to the best of the knowledge of the insurance manager, breached or been non- compliant or potentially non-compliant with the Act and the relevant Rules and Regulations—

(i) the names and registration numbers of those insurers;

(ii) a description of the breach, non-compliance, or potential non- compliance;

(g) where policies have been issued to the insurance manager in respect of professional indemnity insurance, directors and officers insurance, and errors and omissions insurance —

(i) the full legal names of the insurers who issued those policies, and their financial strength rating;

(ii) the name of the agency that issued the financial strength rating referred to in clause (i);

(iii) the policy limits;

(iv) Excess/Deductible

(h) a statement that the insurance manager has met all of the requirements of the minimum criteria for registration in accordance with the Act;

(i) where an insurance manager has not met the minimum criteria for registration, a description of the non-compliance and any remedial action taken, if any

2. CYBER RISK MANAGEMENT

Every insurance manager shall provide the following information in relation to management of its cyber risks—

(a) whether the insurance manager's board has approved the cyber risk strategy, and if the answer is in the affirmative the insurance manager shall state how often the board reviews the strategy;

(b) whether the insurance manager has formally adopted a cyber-security standard or practice, and if the answer is in the affirmative the insurance manager shall state how often the board reviews the strategy;

(c) Whether cyber risk is considered part of the insurance manager's internal management control process, and if the answer is in the affirmative the insurance manager shall provide the relevant documentation;

(d) whether the insurance manager has a process in place to identify the organisation's critical functions, processes and key information assets that are exposed to cyber risk, and if the answer is in the affirmative the insurance manager shall describe how critical functions are defined and provide any relevant policies or documentation;

(e) whether the insurance manager's internal audit department conducts reviews of the organisation's cyber security systems, controls and processes, and if the answer is in the affirmative the insurance manager shall provide the latest report;

(f) whether the insurance manager has cyber insurance, and if the answer is in the affirmative the insurance manager shall provide the applicable limits;

(g) whether the insurance manager performs internal regular vulnerability testing and penetration testing, and if the answer is in the affirmative the insurance manager shall provide the latest reports;

(h) whether the insurance manager has engaged an external consultant to perform vulnerability or penetration testing in the last year, and if the answer is in the affirmative the insurance manager shall provide the name and address of the vendor engaged and provide the latest vendor report;

(i) whether all employees of the insurance manager are provided with on-going cyber security training;

(j) whether an assessment has been made regarding cyber and potential contagion risk from third party service providers of the insurance manager, and if the answer is in the affirmative the insurance manager shall provide the assessment report;

(k) whether the insurance manager has formal policies and procedures in place to protect critical data and sensitive data such as personal identification information, and if the answer is in the affirmative the insurance manager shall provide the policies and procedures;

(l) whether the insurance manager has formal policies and procedures in place to ensure maintenance of its software including installation of patches and updates to software in a timely manner, and if the answer is in the affirmative the insurance manager shall provide the policies and procedures;

(m) whether the insurance manager has formal policies and procedures in place to monitor its networks and to detect internal and external adverse network activity, and if the answer is in the affirmative the insurance manager shall provide the policies and procedures.

(n) whether a documented response plan has been implemented and whether formal thresholds are set for events and incidents to determine the appropriate response (including reporting to impacted stakeholders and regulators), and the answer to this query shall include information on the following—

(i) if the answer is in the affirmative the insurance manager shall provide relevant policies or supporting documentation;

(ii) the insurance manager shall state whether the plan shall include detailed incident recovery process;

(iii) the insurance manager shall state whether the plan shall identify requirements for the remediation of any identified weaknesses and associated controls;

(iv) the insurance manager shall state whether he has been subject to a cyber-incident , and if so, he shall describe the incident and the amount of loss if applicable.

(o) the insurance manager shall state where he ensures that outsourced functions have equivalent levels of security and protection;

(p) the insurance manager shall state the percentage of the current year's budget he allocates to cyber security.

3. AML-ATF QUESTIONNAIRE

Every insurance manager shall provide the following information in relation to its AML/ATF processes and policies --

Section A – Client / Customer Numbers

1. The total Number of insurers managed.

2. Whether the insurance manager risk rate insurers for Money Laundering ("ML") / Terrorist Financing ("TF") risk.

3. The number of insurers in the following risk assessment category by Low Risk, Medium Risk, High Risk, Unknown.

Section B – Products / Services

1. whether the insurance manager manages any Direct Long-Term Insurers (LTIs).

1.1 If the answer is in the affirmative, state how many.

1.2 List the names and classes of direct LTIs managed.

1.3 Confirm the services and number of entities provided to direct LTIs.

2. Confirm if the insurance manager has been engaged to provide outsourcing services (particular to AML/ATF activities) on behalf of any direct LTIs.

2.1 I If the answer is in the affirmative, provide entity names.

3. Confirm if there are Corporate Service Provider specific services offered to any managed entities.

3.1 If the answer is in the affirmative, state what they are.

4. Confirm whether the insurance manager files Suspicious Activity Reports (SAR) on behalf of any other BMA licensed or registered entities.

4.1 If the answer is in the affirmative, list all entities on behalf of which the insurance manager can file a SAR.

Section C – Delivery Channel

1. The number of business relationships onboarded for the last 12 months by face to face with clients, via intermediary, by phone, email, fax or post, or other.

Section D – Geography

1. The country of residence of Ultimate Beneficial Owners (UBOs) of managed entities by direct LTIs, all other managed entities and Politically Exposed Persons (PEP) allocated by geographic zone as outlined in Table 1.

2. Whether the insurance manager identifies Politically Exposed Persons (PEPs).

3. Confirm if the insurance manager performs transaction monitoring.

4. Confirm if claims handling services are provided for direct LTIs, and if the answer is in the affirmative, provide the value of claims paid (in United States Dollar) and number of policies by geographic zone as outlined in Table 1.

Table 1 Geographic Zone

Geographic Zone	Countries
Zone 1 - Central & Western Asia	Armenia, Azerbaijan, Bahrain, Georgia, Iraq, Israel, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Lebanon, Oman, Palestinian, Qatar, Saudi Arabia, Saudi Arab Republic, Tajikistan, Turkey, Turkmenistan, United Arab Emirates, Uzbekistan, Yemen
Zone 2 - Eastern Asia	China, Hong Kong, Japan, Macao, Mongolia, North Korea, South Korea, Taiwan
Zone 3 - South and South-Eastern Asia	Afghanistan, Bangladesh, Bhutan, Brunei Darussalam, Cambodia, India, Indonesia, Iran, Lao PDR, Malaysia, Maldives, Myanmar, Nepal, Pakistan, Philippines, Singapore, Sri Lanka, Thailand, Timor-Leste, Vietnam

Zone 4 - Oceania	American Samoa, Australia, Cook Islands, Fiji, French Polynesia, Guam, Kiribati, Marshall Islands, Micronesia, Nauru, New Caledonia, New Zealand, Niue, Norfolk Island, N. Mariana Islands, Palau, Papua New Guinea, Pitcairn, Samoa, Solomon Islands, Tokelau, Tonga, Tuvalu, Vanuatu, Wallis & Futuna Islands
Zone 5 - Northern Africa	Algeria, Benin, Burkina Faso, Cameroon, Cape Verde, Central African Republic, Chad, Cote d' Ivoire, Egypt, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Libya, Mali, Mauritania, Morocco, Niger, Nigeria, Saint Helena, Senegal, Sierra Leone, Sudan, Togo, Tunisia, Western Sahara
Zone 6 - Southern Africa	Angola, Botswana, Burundi, Democratic Republic of Congo, Comoros, Djibouti, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Kenya, Lesotho, Madagascar, Malawi, Mauritius, Mayotte, Mozambique, Namibia, Republic of Congo, Reunion, Rwanda, Sao Tome & Principe, Seychelles, Somalia, South Africa, Swaziland, Uganda, United Republic of Tanzania, Zambia, Zimbabwe
Zone 7 - Eastern Europe	Belarus, Bulgaria, Czech Republic, Hungary, Moldova, Poland, Romania, Russian Federation, Slovakia, Ukraine
Zone 8 - Northern Europe	Aland Islands, Channel Islands, Denmark, Estonia, Faeroe Islands, Finland, Guernsey, Iceland, Republic of Ireland, Isle of Man, Jersey, Latvia, Lithuania, Norway, Svalbard Jan Mayen, Sweden, United Kingdom
Zone 9 - Southern Europe	Albania, Andorra, Bosnia, Croatia, Cyprus, Gibraltar, Greece, Italy, fYR of Macedonia, Malta, Montenegro, Portugal, San Marino, Serbia, Slovenia, Spain, Vatican City,
Zone 10 - Western Europe	Austria, Belgium, France, Germany, Liechtenstein, Luxembourg, Monaco, Netherlands, Switzerland
Zone 11 - Northern America (Excluding USA)	Canada, Greenland, St Pierre & Miquelon
Zone 12 - Caribbean	Anguilla, Antigua & Barbuda, Aruba, Bahamas, Barbados, British Virgin Islands, Cayman Islands, Cuba, Dominica, Dominican Republic, El Salvador, Grenada, Guadeloupe, Haiti, Montserrat, Netherlands Antilles, Puerto Rico, St-Barthelemy, St Kitts & Nevis, St Lucia, St Martin, St Vincent, Trinidad & Tobago, Turks & Caicos Islands, US Virgin Islands, Jamaica
Zone 13 - Eastern South America	Brazil, Falkland Islands, French Guiana, Guyana, Paraguay, Suriname, Uruguay
Zone 14 - Northern, Southern and Western South America	Argentina, Bolivia, Chile, Colombia, Ecuador, Peru, Venezuela
Zone 15 - North-East United States	Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, Vermont
Zone 16 - South-East United States	Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Puerto Rico, South Carolina, Tennessee, Virginia, West Virginia
Zone 17 - Mid-West United States	Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, Oklahoma, South Dakota, Wisconsin
Zone 18 - Western United States	Alaska, Arizona, California, Colorado, Hawaii, Idaho, Montana, Nevada, New Mexico, Oregon, Texas, Utah, Washington, Wyoming
Zone 19 - Central America	Belize, Costa Rica, Guatemala, Honduras, Mexico, Nicaragua, Panama,
Zone 20 - Bermuda	Bermuda

Section E – Reporting

1. Confirm whether the insurance manager is registered with GoAML at www.fia.bm?

1.1 I If the answer is in the affirmative, under what name and when was this done.

1.2 If the answer is in the negative to 1. whether the insurance manager has access to GoAML through another registration.

1.3 Under what name and how the insurance manager is connected to that name.

1.4 I If the answer is in the negative to 1. and 1.2 who state would file a SAR on behalf of the insurance manager.

2. How many Suspicious Activity Reports (SAR) have been filed within the last 4 years?

Section F – Training / Personnel

1. Confirm if the insurance manager provides employees with training in relating to ML and TF.

1.1 If the answer is in the affirmative, confirm if:

(a) ML/TF training is included in the induction program of new employees.
(b) The ML/TF training provided is specific to the business of insurance conducted by the insurance manager or is of general application.
(c) The frequency that employees must undertake ML/TF training.

2.Confirm how many persons are employed by the insurance manager on a full time and part time basis?

2.1 Confirm the work arrangement of the your Compliance Officer.
2.2 Confirm the work arrangement of your Reporting Officer.

3. Indicate what actions are undertaken when recruiting staff.

Verify name	
Verify residential address	
Check if the individual should be considered as PEP	
Check individual against sanctions lists	
Check for any negative press against the individual	
Confirm employment history	
Confirm references	
Request details on any regulatory action taken against the individual	

4. Confirm whether the insurance manager's Senior Compliance Officer is a member of the senior management of the Company.

Section G – AML / ATF Controls

Every insurance manager shall provide the following information--

1. Whether the insurance manager has AML/ATF controls that are specific for direct LTIs.

2. Whether the insurance manager has AML/ATF controls that are specific for all other managed entities.

3. Whether the insurance manager has other specific AML/ATF controls. If the answer is in the affirmative describe the AML/ATF controls.

4. Confirm the frequency with which the insurance manager rates the AML/ATF risks of its insurers.

5. Whether senior management approval is required to approve new business, if the client has been risk rated as Low, Medium or High.

6. Whether senior management approval is required to retain an existing client, if the client's risk rating has changed to Low, Medium or High.

7. Confirm if the policies and procedure manuals of the insurance manager relating to AML/ATF are in line with all applicable laws and regulations.

7.1 Confirm the frequency for which the insurance manager's AML/ATF policies and procedures are reviewed. Provide a copy of the AML/ATF policies and procedures if they have been updated in the last 12 months.

8. The date the insurance manager last performed an entity-wide AML/ATF risk assessment.

9. The date the insurance manager last conducted an independent audit of its AML/ATF program along with a copy of the report.

10. The date of the last Compliance/ Reporting Officer report on the operation and effectiveness of the Company AML/ATF policies, procedures and controls.

11. Whether the insurance manager documents the ML/TF risks associated with a product/service prior to launch?

Section H – Company Data

1. Confirm whether the insurance manager is a Part of Group. If the answer is in the affirmative provide the name of the group and Register of Company number (ROC) where relevant.

2. Whether the insurance manager is listed on a stock exchange. If the answer is in the affirmative list the name of the exchange:

3. Include any additional information/comments which you think might be relevant to this exercise.

Section I – Corporate Governance

The Insurance Manager shall confirm the following information (to the best of its knowledge and belief) as at the reporting period

	Corporate Governance	Confirm Yes or No
1	Whether the powers, roles, responsibilities and accountabilities between the board of directors of the Insurance Manager (Board) and senior management are clearly defined, segregated and understood.	
2	That the Insurance Manager reviews and monitors the structure, size and composition of the Board and recommends improvements to ensure its compliance with the applicable laws, regulations, listing rules and Insurance Manager's policies.	
3	That the Audit and Risk Management Committee of the Board or any related Board committee, assists the Board in fulfilling its oversight function through the review and evaluation of the financial reporting process and adequacy and effectiveness of the system of internal controls; including financial reporting and information technology security controls.	
4	Confirmation that the Board receives sufficient AML/ATF information to assess and understand the senior executive's process for evaluating the Insurance Manager's system of internal controls.	
5	Whether the Board ensures that the Insurance Manager complies with all relevant laws and regulations and endeavours to adopt accepted best business practices.	
6	That the Board and senior management declare any personal dealings to HR and the Compliance department when applicable or required.	
7	That the Board provides oversight to the Insurance Manager with regard to enterprise risk management and identifies key risk areas and key performance indicators and monitor these factors with due diligence.	
8	Whether Board members ensure there is appropriate oversight by the senior management that is consistent with the Insurance Manager's policies and procedures.	

9	Whether the Board sets and enforces clear lines of responsibility and accountability throughout the organization.	
10	That at least annually the Board monitors the senior management's compliance with policies set by the Board and its performance based on approved targets and objectives.	
11	That the Board receives advice on all major financing transactions, principal agreements and capitalisation requiring Board approval and makes appropriate recommendations for their consideration	
12	Whether the compliance and audit function are independent of all operational and business functions as far as practicable and have direct lines of communication to the senior management.	
13	That the Insurance Manager has instituted policies or procedures to provide for the Senior Compliance Officer to have regular contact with and direct access to, the senior management	
	Employee Integrity	
14	Whether the Insurance Manager has established and, maintains and operates appropriate procedures in order to be satisfied of the integrity of new employees.	
15	That appropriate mechanisms have been established to ensure the protection of the Insurance Manager's relevant employee to report suspicious transactions and other actions to comply with AML/ATF obligations.	
16	That adequate procedures or management information systems are in place to provide relevant employees with timely information which may include information regarding connected accounts or relationships.	
17	Whether adequate procedures or document information systems are in place to ensure relevant legal obligations are understood and practiced by relevant employees and adequate guidance and training is provided by the Insurance Manager to employees.	
18	Whether the incidences of financial crime committed by relevant employees (e.g. theft, fraud) is low.	
	Employee Knowledge	
19	That all relevant employees are aware of the identity of the Reporting Officer and how to report suspicious activity.	
20	Confirm whether training programs are designed to cover the AML/ATF risks of the Insurance Manager	
21	Whether the Insurance Manager has an appropriate number of suitably trained employees and other resources necessary to implement and operate its AML/ATF program.	
22	Whether relevant employees fully comply with all AML/ATF procedures in respect of customer identification, account monitoring, record keeping and reporting.	
23	That relevant employees are expected to remain vigilant to the possibility of ML/TF.	
24	Whether relevant employees who violate any of the AML/ATF regulations and or policies and procedures outlined in the Insurance Manager's handbook will be subject to disciplinary action.	
25	That all relevant employees are required to (at least annually) undertake training to ensure that their knowledge of AML/ATF laws, policies and procedure is current.	
26	Whether relevant employees are updated on ML/TF schemes and typologies on a regular basis.	
27	That employees are required to declare personal dealings relevant in the jurisdictions that the Insurance Manager operates in on a regular basis (at least annually).	
	Employee Compliance	
28	Whether the Insurance Manager ensures that the Senior Compliance Officer is the focal point for the oversight of all activities relating to the prevention and detection of ML/TF.	
29	That the Senior Compliance Officer is fully conversant and trained in up to date regulatory requirements and ML/TF risks arising from the Insurance Manager's business.	
30	That the Board monitors compliance with corporate governance regulations and guidelines.	
31	Whether the Board supports the senior management's scope of AML/ATF internal control assessment and receives regular (at least annually) reports from the senior management.	

4. INTERNATIONAL SANCTIONS QUESTIONNAIRE

Confirm the following information:

(a) whether the insurance manager screens policyholders and beneficiaries (where relevant) to determine whether they are subject to measures imposed under the International Sanctions Act 2003 and related regulations ("Bermuda sanctions regime");

(b) whether the insurance manager screen employees to determine whether they are subject to measures imposed under the Bermuda sanctions regime;

(c) the insurance manager shall state if they have frozen any client assets in the last 12 months pursuant to enforcement action taken under the Bermuda sanctions regime;

(d) if the answer to the query in paragraph (c) is in the affirmative, the insurance manager shall state how many asset freezes there have been;

(e) the insurance manager shall provide the following details for assets freezes from the consolidated list: as published by the United Kingdom's Office of Financial Sanctions Implementation (OFSI)—

	Group ID	Name of the designated person as given on the consolidated list	Name of the person/entity if owned/controlled by a designated person.	Value of Assets
1				
2				
3				
4				

Include any additional information/comments which you think might be relevant to this exercise.
