SCHEDULE I – INSURANCE MARKET PLACE PROVIDER RETURN

MATTERS TO BE INCLUDED IN ANNUAL RETURN

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

Section A – All insurance marketplace providers are required to complete the questions below:

(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 marketplace provider;

(b) the organisational structure of the Insurance Marketplace Provider, including but not limited to —

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

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

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

(c) details of the services provided by the Insurance Marketplace Provider;

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

(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;

(iv) the number of local employees (residing in Bermuda);

(v) confirmation if the outsource services provide board of director services to the insurance marketplace provider;

(vi) confirmation if the outsource services provide senior management services to the insurance marketplace provider;

(e) where policies have been issued to the Insurance Marketplace Provider in respect of professional indemnity insurance, directors and officers insurance, and errors and omissions insurance—

(i) the full legal names of the entity 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

(f) a statement that the Insurance Marketplace Provider has met all of the requirements of the minimum criteria for registration in accordance with the Act;

(g) where an Insurance Marketplace Provider has not met the minimum criteria for registration, a description of the non-compliance and any remedial action taken, if any;

(h) the names, registration numbers, insurance classes of all clients and their roles within the insurance marketplace platform; whether or not the entity is an affiliate of the insurance marketplace provider; information as to the number of transactions, gross premium volume and statutory lines of business facilitated by the insurance marketplace provider in the last 12 months; and,

(i) confirmation if the Insurance Marketplace Provider has conflicts of interest policy.

2. **CYBER RISK MANAGEMENT**

SECTION A - BUSINESS SUMMARY QUESTIONS

Geographical details

1. Is the company headquartered in Bermuda?
2. Number of users located in Bermuda.
3. Number of users Globally
4. Do you have a data centre in Bermuda to host your servers?
5. Do you utilise a cloud hosting company to host your servers?
6. Does the organisation have cybersecurity insurance coverage (i.e. to cover internal risk from security incidents)?

Is the following data type stored/processed

7. Personal data of customers
8. Payment card data (i.e. credit/debit card)
9. Is customer personal data stored/processed on behalf of other entities

Are the following internet facing services in place?

10. Brochureware (static content only)
11. Web applications
12. Web applications that process (query, reference, capture, store, transmit) personal data or payment card data

Roles & Responsibilities

13. Is there a dedicated IT Risk Manager, if not which job title holds this responsibility
14. Is there a dedicated IT Security Manager, if not which job title holds this responsibility
15. Is there a dedicated IT Disaster Recovery Manager, if not which job title holds this responsibility
16. Is there a dedicated Business Continuity Manager (BCP) in place, if not which job title holds this responsibility
17. Does the organisation have a designated Data Privacy Officer
18. Is there an annual IT audit plan in place i.e. detailing any IT audit activity for the year

SECTION B - NIST CONTROL SUMMARY

Identify

1. Is there a Cyber Risk Management Programme in place (i.e. assessing all IT risk to include IT Security Risk)
2. Is the status of the Cyber Risk Management Programme communicated to the Senior Mgt. team & the Board of Directors on a regular basis
3. Has a Cyber Risk Policy (or Cyber Security Policy) been approved by the Board and is annually updated?

4. Are the roles and responsibilities of each of the three lines of defence clearly defined
5. Has the organisation performed an assessment of compliance against Data Protection regulatory requirements
6. Asset Management - are physical devices, information systems, and data within the organization inventoried
7. Has the organisation classified all data
8. Has a third party security risk assessment been completed during the past year? i.e. to assess IT risks arising from third parties

Protect

9. Is data that is classified as critical, encrypted in transit and at rest
10. Is there a formal process to ensure maintenance of software and hardware i.e. patching & managing end of life technologies
11. Is there a Logical Access Management Standard defining how systems access is verified, managed, revoked, and audited
12. Do all staff complete cybersecurity training annually
13. Has a penetration test been completed in the last year
14. Has the company segregated the enterprise network into multiple, separate trust zones
15. Is there a process detailing IT service management controls i.e. change, release & configuration management
16. Does the company document and enforce security configuration standards of all network devices

Detect

17. Is there a process enabling the review of threat intelligence & vulnerability alerting data
18. Is there a process in place to monitor information systems and assets to identify cybersecurity events
19. Does the company store & archive security event logs centrally

Respond

20. Is there a documented security incident response plan in place, including internal & external communications & crisis management
21. In the event of a major incident, is the company contracted to a "4th line" IT security expert service (for example a Managed Security Services Provider - MSSP)

Recover

22. Has a test of the Business Continuity and IT Disaster Recovery plans been performed during the past 12 months
23. Has the organisation been subject to a significant cyber incident during the past 12 months

SECTION C - Technical Security Controls

Technical controls summary

1. Antivirus software is installed on all Microsoft Operating System endpoints
2. Is there an endpoint Advanced Persistent Threat (APT) control in place
3. "Are Data Loss Prevention (DLP) controls in place i.e.: to prevent unauthorised data leaving the enterprise"
4. Is INTERNAL vulnerability scanning conducted (& what is the frequency)
5. Is EXTERNAL vulnerability scanning conducted (& what is the frequency)
6. Are there regular (6 monthly minimum) firewall ruleset reviews
7. Is there a network perimeter Intrusion Detection or Prevention (IDS/IPS) control
8. Is there a DDOS defence in place for internet gateways

3. **AML-ATF QUESTIONNAIRE (Except for Section I or J on Corporate Governance which are required for all insurance marketplace providers, the rest of the sections in this schedule are required only where the insurance marketplace provider is an AML/ATF Regulated Financial Institution under Proceeds of Crime Act 1997.)**

Section A – Client / Customer Numbers

1. Total Number of clients served?

2. Do you risk rate clients for Money Laundering (ML) / Terrorist Financing (TF) risk?

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

Section B – Products / Services

1. Do you transact with any client dealing with Direct Long-Term Insurance (LTIs)?

   1.1 If yes, how many?

   1.2 List the names and classes of clients dealing with direct LTIs served.

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

2. Confirm if your company has been engaged to provide outsourcing services (particular to AML/ATF activities) on behalf of any clients dealing with direct LTIs?;

   2.1 If yes, provide entity names.

3. Does your company file Suspicious Activity Reports (SAR) on behalf of any other BMA licensed or registered entities?

   3.1 If yes, how many?

Section C – Delivery Channel

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

2. Do you identify PEPs.

3. Confirm if the company performs transaction monitoring.

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 Virigina
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. Is your company registered with GoAML at www.fia.bm.
   1.1 If yes, under what name and when?
   1.2 If you answered no to 1., do you have access to GoAML through another registration?
   1.3 Under what name and how are you connected?
   1.4 If you answered no to 1. and 1.2 who would file a SAR on your behalf?

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

Section F – Training / Personnel

1. Confirm if the company provides employees with training in relating to ML and TF.
   1.1 If yes, 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 insurer or is of general application.
   (c) The frequency that employees must undertake ML/TF training.

2. How many persons are employed by the company on a full time and part time basis?
   2.1 Confirm the work arrangement of 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 if the Company's Senior Compliance Officer is a member of the senior management of the Company.

Section G – AML / ATF Controls

1. The Company has AML/ATF controls that are specific for its business.

2. The Company has AML/ATF controls that are specific for all other services entities.

3. The Company has other specific AML/ATF controls. If yes, describe the AML/ATF controls

4. Confirm the frequency with which it rates the AML/ATF risks.

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

6. If 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 company relating to AML/ATF are in line with all applicable laws and regulations
   7.1 Confirm the frequency for which the Company'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 Company last performed an entity-wide AML/ATF risk assessment.

9. The date the Company last conducted an independent audit of its AML/ATF programme 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. Does the Company document the ML/TF risks associated with a product/service prior to launch?

Section H – Company Data

1. Is the Company a Part of Group? If yes, provide the name of the group and Registrar of Company number (where relevant)

2. Is the company listed on a stock exchange? If yes, 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

SCHEDULE I – INSURANCE MARKETPLACE PROVIDER RETURN

If the Insurance marketplace provider is a company, complete this section. Otherwise, proceed to Section J.

The Insurance Marketplace Provider 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 marketplace provider (Board) and senior management are clearly defined, segregated and understood.	
2	That the Insurance Marketplace Provider 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 Marketplace Provider'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 Marketplace Provider's system of internal controls.	
5	Whether the Board ensures that the Insurance Marketplace Provider 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 Marketplace Provider 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 Marketplace Provider's policies and procedures.	
9	Whether the Board sets and enforces clear lines of responsibility and accountability throughout the organisation.	
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 Marketplace Provider 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 Marketplace Provider 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 Marketplace Provider'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 Marketplace Provider 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 Marketplace Provider	
21	Whether the Insurance Marketplace Provider has an appropriate number of suitably trained employees and other resources necessary to implement and operate its AML/ATF programme.	
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 Marketplace Provider'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 marketplace provider operates in on a regular basis (at least annually).	
	Employee Compliance	
28	Whether the Insurance Marketplace Provider 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 Marketplace Provider'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.	

Section J – Corporate Governance

The section is to be completed by Insurance Marketplace Provider who are partnerships, sole proprietorships or individuals

The Insurance Marketplace Provider 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	The Insurance Marketplace Provider reviews and monitors its structure, size and composition and recommends improvements to ensure its compliance to the applicable laws, regulations and policies.	
2	The Insurance Marketplace Provider has an effective 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 control and information technology security.	
3	The Insurance Marketplace Provider complies with all relevant laws and regulations and endeavours to adopt accepted best business practices.	
4	A qualified party provides oversight with regard to enterprise risk management and identifies key risk areas and key performance indicators and monitor these factors with due diligence.	
5	The compliance and audit function are independent of all operational and business functions as far as practicable.	
	Employee Integrity	
6	The Insurance Marketplace Provider establishes, maintains and operates appropriate procedures in order to be satisfied of the integrity of any new employees.	
7	There are appropriate mechanisms that ensure the protection of the Insurance Marketplace Provider's staff for reporting suspicious transactions and their other actions to comply with AML/ATF obligations.	

8	There are adequate procedures or management information systems in place to provide relevant staff with timely information that might include any information on any connected accounts or relationships.	
9	There are adequate procedures or management information systems in place to ensure relevant legal obligations are well understood by staff and adequate guidance and training is provided.	
10	The incidence of integrity failure (e.g. theft, fraud) involving the Insurance marketplace provider's staff is low	
	Employee Knowledge	
11	All staff know who the AML/ATF Compliance Officer is and report all suspicious activities.	
12	Training programmes are designed to cover the AML/ATF risks of the Insurance Marketplace Provider in order to ensure that all appropriate staff members are trained.	
13	The Insurance Marketplace Provider has an appropriate number of suitably trained staff and other resources necessary to implement and operate its AML/ATF programme.	
14	Staff comply fully with all Anti-Money Laundering procedures in respect of customer identification, account monitoring, record keeping and reporting.	
15	Staff remain vigilant to the possibility of ML/TF.	
16	Staff who violate any of the AML/ATF regulations or the policies and procedures outlined in the handbook will be subject to disciplinary action.	
17	All staff members are required to undergo refresher training to ensure that their knowledge of AML/ATF laws, policies and procedure is current (at least annually).	
18	Staff are updated on ML/TF schemes and typologies on a regular basis.	
19	Staff are required to declare their personal dealings on a regular basis (at least annually).	
	Employee Compliance	
20	The Insurance Marketplace Provider ensures that the Compliance Officer is the focal point for the oversight of all activities relating to the prevention and detection of ML/TF.	
21	The Compliance Officer is fully conversant in regulatory requirements and AML/ATF risks arising from your business.	
22	The Insurance Marketplace Provider monitors compliance with corporate governance regulations and guidelines.	

4. SANCTIONS QUESTIONNAIRE (Applicable to all Insurance Marketplace Providers)

1. Does the company screen clients, to determine if they are subject to measures imposed under Bermuda sanctions regime?

2. Does the company screen employees to determine if they are subject to measures imposed under Bermuda's sanctions regime?

3. Has the company frozen any assets in the last 12 months under the Bermuda sanctions regime?

   3.1 If yes, how many?

   3.2 provide the following details for those assets freezes from the consolidated list:

	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?
