



BERMUDA

**INSURANCE (PRUDENTIAL STANDARDS)
(INSURANCE MANAGERS ANNUAL RETURN) AMENDMENT RULES 2018**

BR 4 / 2018

TABLE OF CONTENTS

- 1 Citation
- 2 Interpretation
- 3 Annual return
- 4 Declaration

SCHEDULES

Matters to be Included in Annual Return

The Bermuda Monetary Authority, in exercise of the power conferred by section 6A of the Insurance Act 1978, makes the following Rules:

Citation

- 1 These Rules may be cited as the Insurance (Prudential Standards) (Insurance Managers Annual Return) Rules 2018.

Interpretation

- 2 In these Rules—
 - “Act” means the Insurance Act 1978;
 - “financial year” has the meaning given in section 1(1) of the Act, except that “insurer” and “insurance group” are substituted with “insurance manager”.

Annual return

- 3 (1) An insurance manager shall file with the Authority an annual return on or before 30 June of each year.

INSURANCE (PRUDENTIAL STANDARDS) (INSURANCE MANAGERS ANNUAL RETURN) RULES 2018

(2) The annual return shall contain information in respect of the matters set out in the Schedules I, II, III and IV, as such matters stood when the annual return is filed.

- (3) The annual return shall be accompanied by a copy of the insurance manager's —
- (a) management accounts for the financial year;
 - (b) business plan for the next financial year.

(4) The insurance manager shall keep a copy of the annual return at its principal office for a period of five years, beginning with the date on which the annual return was filed, and shall produce it to the Authority if so directed by the Authority on or before a date specified in the direction.

Declaration

4 An insurance manager shall, at the time of filing its annual return, file with the Authority a declaration signed by two directors, one of whom may be the chief executive, that to the best of their knowledge and belief, the information in the annual return is fair and accurate.

DRAFT

SCHEDULE I – INSURANCE MANAGERS RETURN

(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 (affiliated) or 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, 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 insurance policies have been issued to the insurance manager in respect of professional indemnity insurance, errors and omissions insurance and directors and officers insurance—
 - (i) the full legal names of the insurers who issued those policies, and their financial strength rating;

INSURANCE (PRUDENTIAL STANDARDS) (INSURANCE MANAGERS ANNUAL RETURN) RULES 2018

- (ii) the name of the agency that issued the financial strength rating referred to in clause (i);
- (iii) the excess or deductible and policy limits
- (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

DRAFT

SCHEDULE II – CYBER RISK MANAGEMENT

(paragraph 3(2))

MATTERS TO BE INCLUDED IN ANNUAL RETURN

1. Has the Board approved the Insurance Manager's cyber risk strategy? If yes, how often does the Board review the strategy?
2. Has the Insurance Manager formally adopted a cyber security standard or practice? If yes, how often does the Board review the strategy?
3. Is cyber risk considered part of the Insurance Manager's Internal Control process? If yes, provide the relevant documentation.
4. Does the Insurance Manager have a process to identify the organisation's critical functions, processes and key information assets that are exposed to cyber risk? If yes, describe how critical functions are defined and provide any relevant policy/documentation.
5. Does the Insurance Manager's Internal Audit department or third party experts conduct reviews on the organisation's cyber security systems, controls and processes? If yes, provide the latest report.
6. Does the Insurance Manager have cyber insurance? If yes, please provide limit(s), as well as deductible/excess.
7. Do you perform internal regular vulnerability testing and penetration testing? If yes, provide the latest report(s).
8. Have you engaged an external consultant to perform vulnerability/penetration testing in the last year? If yes, which vendor do you use for this? Provide the latest vendor report.
9. Are all staff provided with on-going cyber security training?
10. Has an assessment been made regarding cyber/potential contagion risk from third party service providers. If yes, provide the assessment report.
11. Does the Insurance Manager have formal policies and procedures, and controls in place to protect critical data and sensitive data such as personal identification information? If yes, please provide the policies and procedures.
12. Does the Insurance Manager have formal policies and procedures in place to ensure maintenance of software including installation of patches and updates in a timely manner? If yes, please provide the policies and procedures.
13. Does the Insurance Manager have formal policies and procedures in place to monitor its networks and detect anomalous network activity? If yes, please provide the policies and procedures.
14. Is there a documented response plan and are formal thresholds set for events and incidents to determine the appropriate response (including reporting to impacted stakeholders and regulators)?
 - If yes, provide relevant policy/documentation.
 - Does the plan include detailed Incident recovery plans?
 - Does the plan identify requirements for the remediation of any identified weaknesses and associated controls?
 - Has the Insurance Manager been subject to a cyber incident? Describe the incident and the amount of loss if applicable.
15. Where relevant, how do you ensure that outsourced functions have equivalent levels of

INSURANCE (PRUDENTIAL STANDARDS) (INSURANCE MANAGERS ANNUAL RETURN) RULES 2018

security and protection?

16. What percentage of the current year's budget is allocated to cyber security? If cyber security is part of the overall IT expenses, kindly indicate. If the Insurance Manager is unable to break down the cyber security portion within the total IT expenses, please enter the percentage of the total IT budget.

DRAFT

SCHEDULE III – AML-ATF QUESTIONNAIRE

(paragraph 3(2))

MATTERS TO BE INCLUDED IN ANNUAL RETURN

1. Section A – Client / Customer Numbers

2. Total Number of insurers managed?
3. Do you risk rate insurers for Anti-Money Laundering (“AML”) / Anti-Terrorist Financing (“TF”) risk?
4. The number of insurers in the following risk assessment category by Low Risk, Medium Risk, High Risk, Unknown.

1. Section B – Products / Services

2. Do you manage any Direct Long-Term Insurers (LTIs)?
 - 1.1 If yes, how many?
 - 1.2 List the names and classes of direct LTIs managed.
 - 1.3 Confirm the services and number of entities for each service provided to direct LTIs.
3. Confirm if the Insurance Manager has been engaged to provide outsourcing services (particular to AML/ATF activities) to any direct LTIs;
 - 2.1 If yes, provide the LTIs names.
4. Are there Corporate Service Provider specific services offered to any managed entities?
5. Delete as captured in the detailed table (service and number) Is the Insurance Manager required to file Suspicious Activity Reports (SAR) on behalf of any other BMA licensed or registered entities?

1. Section C – Delivery Channel

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

1. Section D – Geography

2. 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.
3. Is your AML/ATF policies and procedures designed to identify PEPs.
4. Confirm if the Insurance Manager performs transaction monitoring.

1. Section E – Suspicious Activity Reporting

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

1. Section F – Training / Personnel

2. Confirm if the company provides employees with training in relating to AML and ATF.

INSURANCE (PRUDENTIAL STANDARDS) (INSURANCE MANAGERS ANNUAL RETURN) RULES 2018

1.1 If yes, confirm if:

- (a) AML/ATF training is included in the induction program of new employees.
- (b) The AML/ATF 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 AML/ATF training.

3. How many persons are employed by the company or are employed by an affiliate, but work for the Insurance Manager 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.

4. 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	

5. Confirm if the Company's Senior Compliance Officer is a member of the senior management of the Company.

Section G – AML / ATF Controls

1. Has the Company got AML/ATF controls that are specific for direct LTIs.
2. Has the Company got AML/ATF controls that are specific for all other managed entities.
3. Has the Company got other specific AML/ATF controls. If yes, describe the AML/ATF controls
4. Confirm the frequency with which it rates the AML/ATF risks of its insurers. – table to be added to the model to allow a number to be added to low, medium and high risk clients
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 completed its last entity-wide AML/ATF risk assessment.
9. The date the Company last commissioned an independent audit of its AML/ATF program, provide 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.

INSURANCE (PRUDENTIAL STANDARDS) (INSURANCE MANAGERS ANNUAL RETURN) RULES 2018

11. Does the Company document the ML/TF risks associated with a new product/service prior to launch?

Section H – Company Data

1. Is the Company a part of Group? If yes, provide the name of the ultimate Parent and the Register of Company number (where it is a Bermuda entity)
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

The Insurance Manager shall complete the following information (to the best of its knowledge and belief). The responses will cover the reporting period:

	<u>Corporate Governance</u>	<u>Confirm Yes or No</u>
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 Senior Management, HR and/or Compliance when applicable or required.	
7	That the Board provides oversight to the Insurance Manager with regard to 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 internal audit functions is independent of all operational and business functions as far as practicable, and have direct lines of communication to the Board and 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	
	<u>Employee Integrity</u>	
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	

INSURANCE (PRUDENTIAL STANDARDS) (INSURANCE MANAGERS ANNUAL RETURN) RULES 2018

	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.	
	<u>Employee Knowledge</u>	
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, 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 by the Insurance Manager 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).	
	<u>Employee Compliance</u>	
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.	

SCHEDULE IV – SANCTIONS QUESTIONNAIRE

(paragraph 3(2))

MATTERS TO BE INCLUDED IN ANNUAL RETURN

1. Does the company screen insurers and beneficiaries (where relevant) 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 sanctions regime?
3. Has the Company frozen any assets in the last 12 months under the Bermuda sanctions regime?
 - 3.1 If yes, provide the number of circumstances where assets were frozen?
 - 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?

INSURANCE (PRUDENTIAL STANDARDS) (INSURANCE MANAGERS ANNUAL RETURN) RULES 2018

Made this 17th day of August 2018

Chairman
The Bermuda Monetary Authority

DRAFT