

Mirae Asset Investment Managers (India) Private
Limited IFSC Branch

INTERNAL EVENTS POLICY

Executive Summary

Brief Overview	Mirae Asset Investment Managers (India) Private Limited IFSC Branch and its officers, directors and employees (Collectively the “Company”) are committed to full compliance with all applicable laws and regulations with regards to internal Event Policy.
Objective	<p>The objective of the policy is to set out the requirements for identification, collection and reporting of Internal Events.</p> <p>The Company maintains high standards of internal governance and a sound system of internal control processes and procedures. This policy sets out the controls standards and procedures that should exist. It is the responsibility of all departments, including front, middle and back offices to achieve the objectives of this Policy.</p>
Policy Owner	Compliance
Version	1.0

Approval Details

Authority	Version	Approval Date
Board of Directors	1.0	_____, 2026

Change Matrix

Sr. No	Type of Information	Document Data
1.	Document Title	Internal Events Policy
2.	Date of Release	February 2026
3.	Document Revision No	Version 1
4.	Document Author	Mr. Akash S Srivastava
5.	Document Reviewer	Ms. Rimmi Jain
6.	Approved by the Board	Approved by the Board of Directors of Mirae Asset Investment Managers (India) Pvt. Ltd. in its meeting held on _____
7.	Change description	Policy reviewed pursuant to Annual Review. No changes observed

INDEX

Sr No.	Name of the Topic	Page No.
1	Introduction	4
2	Purpose	4
3	Scope of Application	4
4	Classification of Internal Event	5
5	Identifying, Handling and Reporting an Internal Event	5
6	Remediation Plan	7
7	Handling Event Which Incurred Financial Loss or Compensation to Client	7
8	Internal Event Register	8
9	Assessment criteria for making regulatory reporting	8
10	Governance and on-going monitoring	9

I. Introduction

1. This Policy sets out the requirements for identification, collection and reporting of Internal Events.
2. An Internal Event is defined as an incident or issue (or undesirable risk exposure / situation) caused by human error, failure / poor control of process(es) or system(s) which result in, is likely to result in or potentially have resulted in:
 - A financial impact (with or without monetary loss or gain);
 - A (negative) reputational impact in the eyes of potential or existing clients/ investors; or
 - A regulatory impact (where an event may potentially require reporting to a regulator).
 - An operational impact (disruption of process or system)
3. All staff are expected to take a proactive approach with respect to the identification, management and reporting of such Internal Events, or suspected Internal Events.
4. An Internal Event identified should be reported with respect to this Policy.
5. This Policy is aligned with the requirements of the International Financial Services Centres Authority (IFSCA) and incorporates governance, reporting, and risk-management expectations applicable to all regulated entities under IFSCA's regulatory framework, including the Capital Market Intermediaries Regulations, 2025 and relevant Master Circulars."

II. Purpose

This policy has been designed to ensure that:

- Timely and complete information exists to allow management to respond constructively to these incidents and minimize the likelihood of their recurrence through the implementation of mitigation action plans;
- There is a consistent approach to identifying Internal Events where compensation may be necessary; and
- Critical information can be obtained to identify those breaches that should be reported by local compliance team to the concern team and Senior Management of Mirae Asset Global Investments (Hong Kong) Limited

III. Scope

This policy applies to employees of Mirae Asset Investment Managers (India) Private Limited IFSC Branch

IV. Classification of Internal Events

Local Compliance team determine whether the Internal Event is classified as an incident and/or a breach and/or a complaint. Internal Event can be constituted by following factors, including but not limited to:

- Incident or issue identified internally; or
- Breach of internal policies, procedures or guidelines; or
- Near miss case which could have occurred if not for a last-minute catch (outside of normal controls); or
- Event occurred where an external party or service provider is willingness to forego its claims; or
- Error or wrongdoing which may result in exposure of control gaps; or Internal Event Policy
- Other incident or issue or potential complaint not being classified as complaint
- Internal Events shall also include cybersecurity incidents, technology disruptions, or third-party/vendor failures that impact confidentiality, integrity, or availability of systems or data, consistent with IFSCA's Cyber Security and Cyber Resilience Guidelines for Regulated Entities.

V. Identifying, Handling and Reporting an Internal Event

Where a potential Internal Event has been identified by a staff, he/she should follow the steps outlined below to ensure proper handling and reporting:

1. The staff should raise the matter with their team leader/ line manager.

2. The team leader/ line manager should investigate the event and report it to the local Compliance team as soon as practicable after becoming aware of the event;
3. If there is an incident or breach which has an open financial exposure(s) or position(s) that may have a material financial impact, the responsible team leader should immediately escalate to concern team and senior management of Mirae Asset Global Investments (Hong Kong) Limited to take appropriate action immediately. Any compliance and regulatory related matter should be referred to Compliance and / or Legal for further review.
4. The relevant staff/team shall complete a preliminary incident report with the realised financial impact or an estimation of any potential financial impact (if any), and
 - Submit the draft report to Compliance team within 5 business days of becoming aware of the Internal Event in normal circumstances;
 - Final report should be submitted within 1 month unless otherwise agreed with Compliance team.
5. An Internal Event report shall be prepared which encompass all the details. Any cybersecurity incident (including system intrusion, data breach, cyber fraud, or critical system outage) must be immediately escalated to the CISO / designated officer and reported to IFSCA within *6 hours* of detection as mandated under IFSCA Cyber Security and Cyber Resilience Guidelines.
6. Upon receipt of the incident report, local compliance team shall forward it to the Compliance team of Mirae Asset Global Investments (Hong Kong) Limited for their review the incident and /or perform investigation, where appropriate, in relation to any matter which affects, or may affect the operations, responsibilities, and reputation of the Company.
7. The concern team or senior management of Mirae Asset Global Investments (Hong Kong) Limited will consider whether compensation to the clients is necessary as a result of the Internal Event.
8. Compliance team of Mirae Asset Global Investments (Hong Kong) Limited will finalize the incident report with the responsible department head or the delegated person, and get ROs or senior management, and relevant control parties to sign-off the report.
9. Breaches are classified as active breaches or passive breaches to our internal policies, internal procedures or investment guidelines.
10. **Active breaches** result from

- portfolio management decisions taken by the investment team which triggers an investment guideline breach, or
- errors (human error / operational errors) of internal parties (front, middle or back office) or external stakeholders in carrying out their duties which leading to a breach of investment guideline. Examples are elaborated in Appendix B.

All active breaches are required to file an incident report with an indication of a breach together with a thorough impact analysis, and shall be rectified immediately with a consideration of any improvement plan to mitigate the reoccurrence risk.

11. **Passive breaches** result from unavoidably external factors without active intervention by the investment team, such as market value fluctuations and settlement cycle for redemptions or subscriptions (except for SICAV funds, under the CSSF regulations, the regulator expects cash to be managed pro-actively by considering all projected cash flows. As such, timing issues/mismatches in settlements are not regarded as a justification for a passive classification.)
12. The investment manager should take as a priority objective all steps as are necessary within a reasonable period of time to remedy the situation, taking due account of the investors' interests. Passive breaches are not required to file an incident report. Compliance team would perform daily post-trade monitoring to identify any potential passive breaches, and notify relevant investment managers with details for their attention once confirming those passive breaches. All passive breaches should be rectified within 15 business days.
13. ALL breaches must be evaluated to determine whether they constitute a material compliance failure requiring immediate notification to IFSCA, in line with the materiality criteria and reporting obligations applicable to IFSCA-regulated entities
14. Local Compliance team shall ensure the relevant documents have been properly documented and provide it to the Compliance Team of Mirae Asset Global Investments (Hong Kong) Limited, to discuss with RO / senior management on whether reporting to relevant regulator(s) and management is required based on the criteria set out in this Policy.

VI. Remediation Plan

Once an Internal Event has been identified, the relevant department and staff must:

1. Review the incident to determine when, why, how it occurred and how it was discovered;
2. Analyse and determine the root cause of the incident;
3. Conduct an impact analysis due to such incident including operational, regulatory, financial and client impact;
4. Recommend immediate rectification (if needed) and corrective action to be taken, and implement the corrective actions decided upon;
5. Consider, make recommendations on, and implement as necessary, changes to practices or procedures intended to prevent similar event from recurring; and
6. Assist in ensuring that all relevant parties are advised of the corrective actions and any procedural changes are undertaken within a reasonable timeframe.
7. For cybersecurity or technology-related events, remediation must align with IFSCA-mandated cyber resilience requirements, including root-cause analysis, impact assessment, security hardening measures, third-party/vendor review where applicable, and updates to Information Security and Cyber Resilience frameworks.

VII. Handling Event Which Incurred Financial Loss or Compensation to Client

1. If the incident or breach or complaint has a financial exposure(s) that may have a potential financial impact, the responsible team head is required to provide a proposed rectification or compensation plan with sufficient details, justifications or calculations and a potential loss amount. Please also refer to above section “Identifying, Handling and Reporting an Internal Event” on escalation details.
2. The responsible team head shall seek consult local compliance team, Compliance team of Mirae Asset Global Investments (Hong Kong) Limited, Risk and Legal (if needed) departments for any advice. Other related departments should also be involved for discussion.
3. The responsible team head will work with the with local Compliance team and Compliance team of Mirae Asset Global Investments (Hong Kong) Limited and/or other relevant teams to

recommend solution and/or compensation plan for ROs/ senior management' consideration/decision and approval.

4. Under normal circumstances, the responsible team shall prepare the incident report with financial impact (e.g. trading, order placing error) and shall seek approval from Compliance, ROs/ senior management Mirae Asset Global Investments (Hong Kong) Limited through the local compliance

team. The Internal Event report will be passed to Finance Department for approval and further processing. Accordingly, to the nature and amount of the loss, Finance will arrange further sign off to release payment.

5. In addition, the responsible team head shall work with local Compliance team and Compliance team of Mirae Asset Global Investments (Hong Kong) Limited and other relevant parties to remediate and/ or compensate the client as soon as practicable.
6. In cases where a financial loss arises from a cyber incident or technology failure, the compensation decision shall also consider obligations under IFSCA Cyber Security Guidelines, including accountability for cybersecurity lapses and third-party risk management failures.

VIII. Internal Event Register

Local Compliance team will keep a central register of all internal events. All detailed of internal events should be correctly recorded. Any material or significant Internal Event will be reported and updated to the ROs and/or senior management of Mirae Asset Global Investments (Hong Kong) Limited until it has been resolved. The Internal Event Register shall include a mandatory field indicating whether the event is reportable to IFSCA and the specific regulation or circular under which reporting is triggered

IX. Assessment criteria for making regulatory reporting

IFSCA requires immediate reporting of material breaches, regulatory violations, cyber incidents, unauthorized activities, and other significant compliance failures. All Internal Events must therefore be evaluated against IFSCA's regulatory expectations for mandatory reporting

Pursuant to the notification requirement in Code of Conduct, SFC licensed corporation should report to the Commission immediately upon the happening of any material breach, infringement of or non-compliance with any law, rules, regulations and codes administered by the SFC.

The SFC Circular has identified several non-compliance incidents that require intermediaries to report promptly after the occurrence of the breaches, including:

- Suspected unlicensed dealing activities;
- Suspected unauthorized trading activities;
- Non-compliance with the suitability requirements under paragraph 5.2 of the Code of Conduct as supplemented by the corresponding frequently asked questions;
- Breaches of the Securities and Futures (Keeping of Records) Rules;
- Breaches of the Securities and Futures (Contract Notes, Statements of Account and Receipts) Rules; and
- Non-compliance with the order recording requirements under paragraph 3.9 of the Code of Conduct.

Other than the breaches identified above, The Company will assess the materiality of each incident case by case based on the assessment criteria listed below:

- Is it an isolated incident;
- Is it intentional /fraud related;
- Does it jeopardize any client's interest;
- Any fit and proper issue for the concerned staff;
- Is it breach of the regulations / SFC rules (e.g. Code of Conduct, UT Code, Fund Manager Code of Conduct);
- What is the financial impact to the client;
- What is the financial impact to the firm;
- Any impacts to market;
- Is management involved in the wrong doings;
- Any mitigation measure taken to prevent the re-occurrence of the incident;
- Is the non-compliance incident being ascertained

If the incidents are identified to be material after assessment, The Company will have to report the incident to SFC or other relevant regulator (where applicable), subject to the review and approval from corresponding ROs/ senior management of Mirae Asset Global Investments (Hong Kong) Limited

X. Governance and on-going monitoring

Local Compliance team is responsible to produce Internal Event and provide the data to Compliance team of Mirae Asset Global Investments (Hong Kong) Limited for reporting and perform analysis (or any trend analysis) on all Internal Events on a quarterly basis during the Internal Control Committee. The Compliance function shall ensure ongoing alignment with IFSCA's governance requirements, including maintenance of a designated Principal Officer and Compliance Officer, and adherence to oversight mechanisms described under the IFSCA Master Circulars and Cyber Security Guidelines.”

Compliance team shall review and update this policy at **least once a year**.

Appendix B – Examples of Active Breaches

Portfolio Management decisions / actions

- Out-of-limit exposure due to trade initiation

Operational errors that resulting in an investment restriction breach

- Input and process inaccurate trade initiation details such as buy/sell side, fat finger (price, quantity), allocation ratio to different accounts
- Input and process inaccurate subscription or redemption instructions such as incorrect account, price, quantity, trade date, settlement date, bank account
- System issue due to human mistakes
- Insufficient process or process failure including human errors sss