Credit Information Governance Body

Compliance and Enforcement Policy

Version	Date	Owner	Author	Approved by	Document Location	Comments
1.0	September 2025	Legal Counsel			Sharepoint	
2.0	November 2025					
3.0	January 2026					Additional no. 8

Background

To ensure that the CIGB can effectively fulfil its purpose and meet its objectives, the CIGB needs to have tools at its disposal to ensure subscribers comply with its rules as well as a course of action in the case of non-compliance. As part of the CIGB remit, a policing role constitutes a key aspect in fulfilling and supporting CIGB's raison d'être. It's policing framework should:

- Enable initiation via multiple methods, including self and peer reporting.
- Allow resolution to range from privately handled to regulatory involvement, depending on the nature of the breach.
- Support appropriate consequences for breach.
- Reflect the CIGB's source of powers and account for potential breaches by FSMA subscribers as well as non-FSMA subscribers.
- Take a reactive approach in most cases, with some exceptions requiring more proactive policing by the CIGB, accounting for proportionality and resource-efficiency.

The policing model for the CIGB has been considered in detail. Policing in this context refers to the need for a level of oversight of and ensuring compliance with all of the CIGB's rules. These rules include the PoR (both as they currently stand and once they are updated following CIGB's leading of the CIMS industry-led remedies), any policies put in place in implementing the CIMS industry-led remedies or other industry changes and any policies established to govern the industry, including in terms of compliance and dispute resolution.

The power to allow CIGB to police the rules is being obtained via contract law. An oversight model has been implemented to monitor compliance with CIGB's rules as well as a non-compliance process in the event a subscriber breaches the rules.

Oversight model

As part of the proposed contracting approach for the CIGB, subscribers will be required to agree to abide by the CIGB's rules. The subscriber will then be assigned a unique identification number which will prove that they have registered with the CIGB, the subscriber's name and identification number will be published within the CIGB's public register of subscribers in due course.

CRAs, until the public register has been facilitated, will be able to request and be given this information to determine if they are able to provide shared data services to the firm. However, the CIGB would need to keep data protection obligations under review. Regardless of whether CRAs request information, the Subscriber database will be made available to CRAs on a quarterly basis until the public register has been made available. CRAs will actively be told in writing by CIGB if a Subscriber status changes or if a subscription is incomplete or lapsed.

Participants are not included in the CIGB public register nor subject to a CIGB contract. Participants may be tracked for information purposes only.

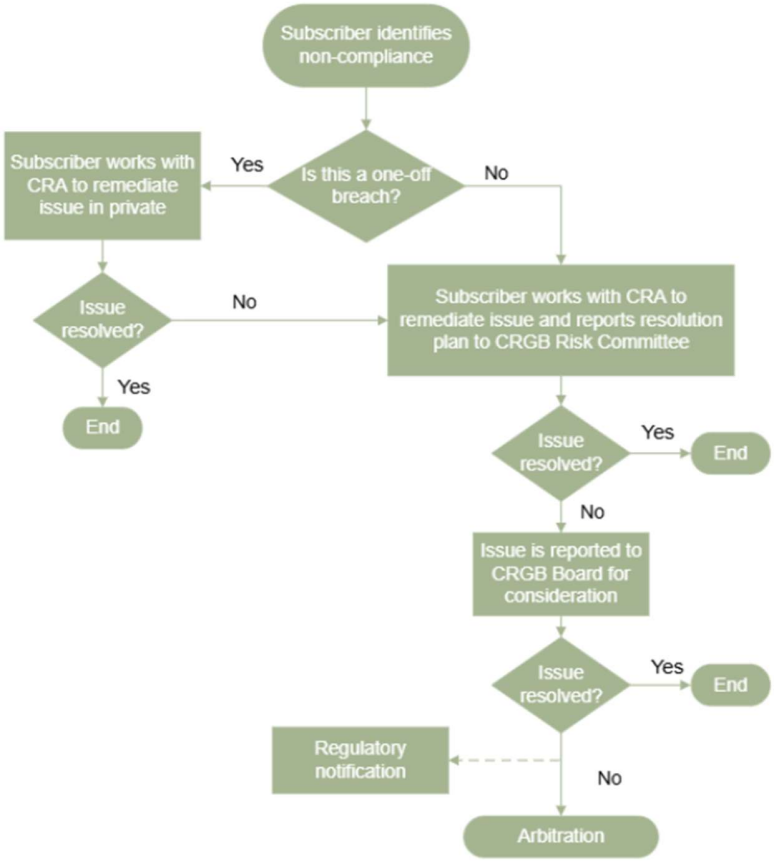
1. Annual attestation of subscribers (which shall not be required until 2027). The content of the attestation will be defined by the CIGB Board at set up and this content will be reviewed periodically to ensure it remains relevant and reflective of the industry and data being collected and shared.
2. Subscribers will provide CIGB with a named employee to ensure accountability in case of failure to comply with CIGB's oversight requirements.
3. The subscriber will be required to undertake frequent compliance self-assessments, as deemed appropriate and proportional by the CIGB Board.
4. A published self-reporting and peer reporting process will be determined by the CIGB Board. Consequences of these processes are covered under the non-compliance section of this policy.
5. A published complaint process where complaints can be made in confidence to the CIGB to address situations where the peer reporting process cannot be applied.
6. The CIGB should retain the right to undertake an audit of the subscriber or pursue the subscriber with other proportionate methods, such as a review meeting, if needed.
7. Through compliance self-assessments and attestations, the CIGB will also seek data from its subscribers regarding their contributions towards the design of industry-led remedies or the steps taken by them to implement industry-led remedies. From this data, the CIGB will produce a periodic report outlining the progress made on the design and implementation of the CIMS industry-led remedies.
8. Without prejudice to any laws or regulations that independently govern consumers and individual subscribers, the CIGB rules should not seek to override existing laws or place unnecessary limits or restrictions on a consumer's ability to authorise firms on how to use the consumer's data in the interests of the consumer. This should not override nor detriment a subscriber's commitment and obligation to adhere to CIGB's rules.

The CIGB Board may need to consider at the time of implementing if the rules around industry-led remedies need to be incorporated into the scheme rules, and therefore, subject to this oversight model. Or, if alternative oversight models need to be considered. The CIGB would need to have appropriate confidentiality and data protection frameworks to ensure the risks from such a compliance process are kept to a minimum.

Non-compliance process

CIGB requires a published process for addressing non-compliance with the CIGB's rules. It is important that the process is defined around the goal of constructive engagement to resolve any breach in private with as little business impact as possible.

CIGB's non-compliance process



CRA: When identified, any breach or non-compliance by a subscriber would be resolved by working directly with the relevant CRA. This process will be undertaken in private and via an agreed remediation plan. The CIGB will only become aware of first-time breaches if the subscriber self-reports to the CIGB or if the issue is identified as part of the attestation process. If it is a recurrent breach, the resolution plan will be reported to CIGB's Audit and Risk Committee. The CIGB Board may reserve the right to determine that certain types of one-off breaches, for example concerning particular rules, should be referred directly to the next stage of the process.

CIGB: Failure to remediate any breach will result in referral to the CIGB. It is the responsibility of the subscriber to report the issue to the CIGB. In the case of a breach by a CRA, the non-compliance process will begin at this stage.

When an issue is referred to the CIGB, as a preliminary step, the CIGB will call a CIGB Board meeting to discuss termination action before any steps are taken. The intent is that a meeting will be convened with the relevant CRA (that has a contract with the subscriber facing the sanction and this may be more than one CRA) to discuss the relevant impacts and timeline for termination of data flow. This will be a private meeting between CIGB and the CRA. An additional meeting will then be called and attendees at that meeting would be the CIGB Board, the CIGB's General Manager, and the CRA. The subscriber in question will also be present to discuss the issue.

Following the above preliminary step, the CIGB will evaluate the breach initially through its Audit and Risk Committee and then ultimately the CIGB Board. The CIGB Board will pass a decision

on non-compliance, including, wherever applicable, a remediation plan with associated timings for implementation. The issue remains private.

Regulatory notification: If the CIGB Board's decision on non-compliance and the associated remediation is not implemented by the non-compliant entity or the entity does not challenge the CIGB Board decision via arbitration within the period specified by the CIGB Board, the CIGB will notify the relevant regulator, utilising established confidential information gateways. The regulator may choose to take their own action if the breach relates to rules within their remit. For CRAs, given their systematic importance to the industry, the CIGB will not take further action until the FCA has been engaged on the issue and agrees to the proposed next steps. If the breach is considered severe or is recurrent, the CIGB could suspend the non-compliant subscriber's subscription alongside notifying the relevant regulator. Conditions of suspension depend on the type of breach.

Independent review: If the non-compliant subscriber rejects the proposed remediation plan or regulatory notification does not otherwise resolve the breach, the subscriber or the CIGB itself can refer the case for review by an independent arbitrator. An independent arbitrator would consider the evidence base and engage with all relevant parties. The arbitrator could affirm the CIGB's decision, adapt (including proposing an alternative remediation plan) or overturn it. English Law and the Arbitration Act 1996 specify that arbitration is final and binding on all parties and cannot be disputed in court, unless for procedural grounds or jurisdiction. If a subscriber does not abide by the arbitrator's decision, the CIGB can further enforce this via the courts. Generally, arbitral processes are confidential and private. However, wherever the CIGB engages in an arbitral process and the findings of the arbitrator may be useful to guide industry conduct and practices, the CIGB make appropriate disclosures regarding these findings.

Consequences of breach

A breach can result in different actions depending on the point at which it is escalated during the non-compliance process:

- A private resolution plan (between the CRA and data user) that is implemented in an agreed timeframe.
- A resolution plan, with an agreed timeframe, that is monitored by the CIGB.
- Removal of the CIGB registration number from the subscriber with the resultant exclusion from access to the shared data. The period and conditions will be agreed based on the circumstances.
- Notification to the relevant regulator of the breach which may result in separate actions by the regulator.

The ultimate sanction in this process is the right of the CIGB to temporarily suspend or terminate the subscription of the non-compliant data user, if the breach cannot be rectified in any other way. Without a subscription, the non-compliant data user may be unable to access

the shared data. The period of suspension will depend on the nature and severity of the breach. CIGB shall, in the confines of confidentiality of the arbitral process, share with the industry:

- the lessons learnt from its oversight and non-compliance processes.
- the qualitative and quantitative data regarding the type of firms pursued under its oversight model, the type of behaviour found to be frequently of issue, the remedies designed, and the costs incurred in this process by the CIGB and the firms.

This will lead to improved knowledge amongst the CIGB subscribers and enhance certainty for subscriber organisations in their operations.

The ultimate sanction for a CRA needs to take a different approach given CRAs control access to the shared data and are systematically important to the functioning of the credit information industry. If a CRA is found to be non-compliant with CIGB's rules and the breach has not been resolved earlier in the process, the CIGB will engage with the FCA on next steps. If the breach is still not resolved after regulatory engagement, arbitration proceedings will be taken against the CRA. The arbitral award might order specific performance on the part of the CRA which they would then need to comply with to ensure compliance with the CIGB's rules.

In addition, the CRAs will independently determine whether they are permitted under the CIGB's rules to provide the shared data to any given organisation. Further, the subscribers who face these consequences will have access to alternative sources of data which they can use to continue to offer their products and services.

Audits

If, during a subscriber's attestation process, information becomes known to the CIGB about that subscriber which the CIGB considers requires further investigation in relation to that subscriber's compliance with CIGB rules, that subscriber agrees to allow the CIGB or the CIGB's representatives to carry out an audit and also agrees to cooperate fully with such an audit including without limitation by providing access to relevant information, documentation and personnel.