

# Breach Reporting Policy

---

**Responsibility:** **Head of Risk and Compliance, and Compliance Manager**

## 1. Purpose

---

Australian Financial Services Licensees and responsible entities must report certain breaches and likely breaches of the *Corporations Act 2001* (Cth) (Corporations Act) and of its Australian Financial Services Licence to the Australian Securities and Investments Commission (ASIC). This Policy establishes principles and responsibilities within Cromwell for identifying, assessing, managing, and reporting where such situations occur.

## 2. Scope

---

This Policy applies to:

- all Cromwell Staff; and
- any Cromwell group entity that is or becomes an Australian Financial Services Licensee or responsible entity for a registered managed investment scheme.

## 3. Policy Statement

---

### 3.1 Compliance Commitment

- (a) Cromwell is committed to complying with the obligations it has as an Australian Financial Services Licensee and as a responsible entity. This commitment includes establishing roles and responsibilities to promote the early detection, assessment and management of Compliance Incidents and where required, reporting of Reportable Situations to ASIC.
- (b) All Staff must comply with applicable financial services laws and internal policies and procedures. If any Staff become aware of a Compliance Incident, i.e., a breach or likely breach of any of these requirements, then they must follow the procedures in this Policy relating to reporting and managing it.

### 3.2 Identifying Compliance Incidents

- (a) Compliance Incidents can be identified from numerous sources, including:
  - whilst undertaking usual business activities;
  - during compliance testing and monitoring activities;
  - resulting from investigating a customer enquiry or complaint;
  - because Staff are aware of a policy non-compliance, or a particular requirement being not followed;
  - because of completing or reviewing regular compliance checklists.
- (b) The Risk and Compliance team must provide adequate training to all Staff to ensure they are aware of:
  - the compliance obligations applicable to them for the business processes they are accountable for;

- the circumstances that may give rise to a Compliance Incident and/or a Reportable Situation; and
- what is expected of them to report, assess without delay, deal with, manage and rectify Compliance Incidents.

### 3.3 Investigating and Assessing Compliance Incidents

- (a) If any Staff member believes that they have identified an actual or potential Compliance Incident, then they must immediately notify the Risk and Compliance team either verbally or by email as soon as they become aware of the issue or potential issue.
- (b) If in doubt, Staff should report their concerns. Staff should not wait until rectification steps have been agreed upon or undertaken.
- (c) The Risk and Compliance team may require relevant Staff to complete a Compliance Incident Report (located on the Risk Hub) as part of the assessment process. These reports contain all details required for including the breach on the applicable register as well as a detailed explanation and document management system references to relevant correspondence.

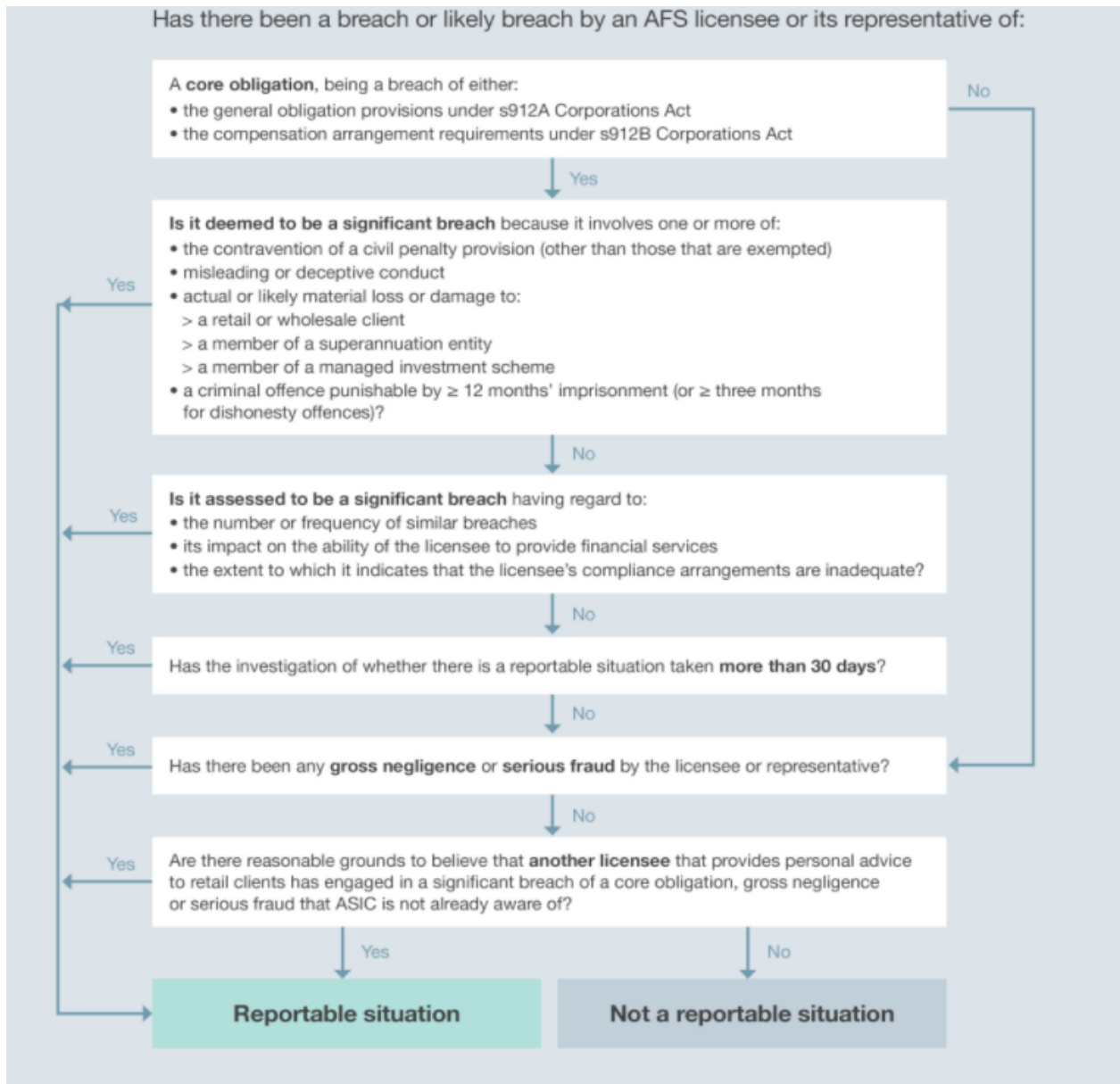
### 3.4 Documenting Compliance Incidents

- (a) Depending on the assessment of the Compliance Incident, the Risk and Compliance team must enter it on either the Non-Compliance Register or Incidents Register.
- (b) Entries on the Non-Compliance Register will include Compliance Incidents relating to:
  - scheme Compliance Plans;
  - the Corporations Act;
  - other legislation (as applicable); and
  - service provider agreements.
- (c) Compliance Incidents that do not fall into the categories in clause 4.4(b) must be recorded in the Incidents Register. The Incidents Register records matters of incident of policies and procedures that, if not appropriately managed, could result in a breach of Cromwell's obligations. If an incident continually appears on the Incidents Register, then the Compliance Manager will review the incidents and consider escalating the latest entry to the Non-Compliance Register.
- (d) The Non-Compliance Register will include all relevant information including:
  - the relevant obligation;
  - the date the Compliance Incident was identified;
  - the date the Compliance Incident occurred (or, if it is a Likely Breach, the date on which it is anticipated that Cromwell will no longer be able to comply with its obligation);
  - how long the Compliance Incident lasted;
  - how the Compliance Incident was identified;
  - the rectification plan;
  - the date of rectification;

- if the breach was reported to ASIC, why the Compliance Incident was a considered Significant Breach; and
  - when the 30 day (calendar days) reporting obligation will be reached.
- (d) The rectification plan will be agreed between the relevant manager and the Compliance Manager. The rectification plan must include appropriate measures to prevent recurrence of the Compliance Incident.
- (e) The Non-Compliance Register will also include any Compliance Incidents identified by Cromwell's service providers.

### 3.5 What must be reported to ASIC?

- (a) Cromwell must report all Reportable Situations to ASIC.
- (b) Reportable Situations (s912DAA of the Corporations Act) include:
- breaches or 'likely breaches' of Core Obligations that are significant (refer clause 4.6);
  - investigations into breaches or likely breaches of Core Obligations that are significant (refer clause 4.7(a));
  - additional Reportable Situations (refer clause 4.8); and
  - Reportable Situations about other licensees (refer clause 4.9).
- (c) Upon becoming aware of a Compliance Incident, the Risk and Compliance team must consider if the Compliance Incident is a Reportable Situation by undertaking investigations about the circumstances of the Compliance Incident to enable an assessment to be made about if there is a Reportable Situation.
- (d) The Risk and Compliance team's assessment process to determine if the Compliance Incident is a Reportable Situation is outlined below:



### 3.6 Breaches or likely breaches of Core Obligations that are significant

(a) Whether a breach or a likely breach is significant will depend upon the circumstances and impact of the individual breach or likely breach, but the following must be taken into consideration:

- the number or frequency of similar breaches (is there a continuing underlying systemic problem?);
- the impact of the breach or likely breach on Cromwell's ability to supply its financial services;
- the extent to which the breach or likely breach indicates that compliance arrangements are not adequate (how long did it take to discover the breach? Did the compliance arrangements identify the breach?);

- the actual or potential financial loss to clients (this is likely to be significant unless the breach is isolated, the amount is immaterial or only a small number of clients are affected); and
  - the materiality of the actual or potential financial loss to Cromwell.
- (b) The above factors can be considered based on the nature, scale and complexity of Cromwell's business at the time. However, if in doubt, the breach (or likely breach) should be reported to ASIC.
- (c) Examples of breaches that may be assessed as 'significant' include:
- several previously undetected compliance breaches;
  - failure to notify ASIC of changes in key persons;
  - failure to follow disclosed investment mandates;
  - recurring failure to lodge statutory reports;
  - breach of ASIC market integrity rules;
  - breach of Internal Dispute Resolution (IDR) requirements;
  - material loss or damage to clients;
  - dishonestly obtaining client funds;
  - governance failures;
  - misleading or deceptive statements in relation to a financial product or service or credit activity;
  - contravening the efficiently, honestly and fairly obligations;
  - representatives acting outside the scope of Cromwell's licence; or
  - a Representative's fraud.
- (d) The Risk and Compliance team is responsible for assessing whether the breach or likely breach is significant. This assessment is documented in the Non-Compliance Register.
- (e) Examples of when Cromwell do *not require* a 'determination of significance' before reporting to ASIC under the Reportable Situation guidance:
- Additional Reportable Situations (i.e., gross negligence or serious fraud);
  - Deemed significant breaches, which are automatically taken to be significant by operation of law; and
  - investigations that continue for more than 30 days, which require consideration of whether there may be a breach, or likely breach, of a Core Obligation that is significant.

### 3.7 Investigations

- (a) If an investigation conducted by the Risk and Compliance team under clause 4.5(d) continues for more than 30 days, then it becomes a Reportable Situation on day 31 of the investigation. If this occurs Cromwell must lodge a report with ASIC within 30 days of this date.
- (b) If an investigation into a Compliance Incident that concludes within 30 days identifies on reasonable grounds that a Reportable Situation has arisen, then Cromwell must report the Reportable Situation to ASIC within 30 calendar days.

- (c) Examples of investigations that are Reportable Situations:
- internal audit of unit pricing identifies a risk of unit pricing errors;
  - client complaints about fees for no service;
  - annual compliance audit identifies a significant breach;
  - receipt of a customer complaint regarding a breach of the law.
- (d) If an investigation commences and concludes within 30 days and there are no reasonable grounds to believe that a Reportable Situation has arisen, then the Compliance Incident is not a Reportable Situation.

### 3.8 Additional Reportable Situations?

If Cromwell or its Representatives:

- engage in conduct constituting gross negligence during providing a financial service; or
- commit serious fraud,

then Cromwell must report these as a Reportable Situation to ASIC.

### 3.9 Reportable Situations about other licensees

Cromwell may be required to lodge a breach report to ASIC in relation to a Reportable Situation about another licensee such as a financial adviser or a mortgage broker. In this situation Cromwell will follow the Reportable Situations about other licensees' guidelines.

### 3.10 Breach reporting process – within Cromwell and to ASIC

- (a) The Company Secretary, or in the Company Secretary's absence, the Head of Risk and Compliance with appropriate consultation with the Legal team, is responsible for lodging reports of any Reportable Situations to ASIC.
- (b) The Head of Risk and Compliance will notify the Responsible Managers if a Reportable Situation occurs.
- (c) The Head of Risk and Compliance and the Compliance Manager must be involved in the process of assessing Reportable Situations.
- (d) The ASIC prescribed online form must be completed and submitted to ASIC via the ASIC Regulatory Portal. The key points of the Reportable Situation include:
- Cromwell must tell ASIC in writing, within 30 calendar days after a Reportable Situation has arisen (an investigation becomes a Reportable Situation on day 31 of the investigation and Cromwell must lodge a report within 30 days of this date);
  - The reporting period starts on the day Cromwell first becomes aware, or are reckless with respect to whether, there are reasonable grounds to believe that a Reportable Situation has arisen;
  - Cromwell must report to ASIC in the prescribed form and through the ASIC Regulatory Portal;
  - Failing to report to ASIC when a Reportable Situation has arisen can attract both civil and criminal penalties.
- (e) The Reportable Situation form to ASIC should contain as much of the information included in Schedule Three as is available at the time.

- (f) The Compliance Manager provides the up-to-date Non-Compliance Register and Incidents Register to the Compliance Committee at each meeting for review and discussion. The Compliance Committee's Report to the Board annexes the Non-Compliance Register and, if required, is also provided to the Audit and Risk Committee by the Company Secretary.

## 4. Roles, Responsibilities and Delegations

| Roles   | Responsibilities   |
|---|--|
| Company Secretary or Head of Risk and Compliance in their absence | Lodging reports of any Reportable Situations to ASIC   |
| Risk and Compliance Team  | Review of Compliance Incident to determine whether it is a Reportable Situation, or a Significant Breach |
| Employees/Staff   | Know and understand the policy and understand the application of risk to their specific role             |

## 5. References

### 5.1 Documentation

| Name                       | Doc Type  |
|----------------------------|-----------|
| Breach Reporting Procedure | Procedure |
| Risk Hub                   | Reporting |

### 5.2 Legislation

- Section 912D of the *Corporations Act 2001* (Cth)
- Section 912DAA of the *Corporations Act 2001* (Cth)
- Section 601FC(1)(l) of the *Corporations Act 2001* (Cth)
- Section 1671A of the *Corporations Act 2001* (Cth)
- ASIC Regulatory Guide 78: Breach reporting by AFS licensees (last update September 2021)

## 6. Version Control

This Policy has been approved and adopted by the Board of CPS, the Board of CFM, and the Board of CRE. The Compliance Manager is responsible for reviewing the Policy at least annually and will seek Board approval for any material changes to the Policy.

The Policy was last reviewed October 2023.

## 7. Glossary

| Term  | Meaning   |
|---|---|
| <b>Board</b>  | The relevant board of directors of any Cromwell group entity that is or becomes an Australian Financial Services Licensee or responsible entity for a registered managed investment scheme.   |
| <b>Compliance Incident</b>                                | An actual, suspected, potential, likely or imminent: <ul style="list-style-type: none"> <li>(a) contravention or breach of any law, regulation, industry standard or code, internal policy or procedure; or</li> <li>(b) Reportable Situation.</li> </ul> |
| <b>Core Obligation or Obligations</b>                     | The obligations that Cromwell has under either the general obligation provisions (s912A of the Corporations Act) or the compensation arrangement requirements (s912B of the Corporations Act) more particularly described in Schedule One.                |
| <b>Cromwell / Australian Financial Services Licensees</b> | Cromwell Property Securities Limited ACN 079 147 809, AFS 238 052 (CPS)<br>Cromwell Funds Management Limited ACN 114 782 777, AFS 333 214 (CFM)<br>Cromwell Real Estate Partners Pty Ltd ACN 152 674 792, AFS 418 476 (CRE)                               |
| <b>Deemed Significant Breach</b>                          | A breach or likely breach of a Core Obligation that is taken to be significant under s912D(4) of the Corporations Act.  |
| <b>Likely Breach</b>                                      | A situation where Cromwell or a Representative is no longer able to comply with a Core Obligation and the breach, if it occurs, will be significant.  |
| <b>Reportable Situation</b>                               | Has the meaning given by s912D of the Corporations Act. It includes the types of situations required to be reported to ASIC described in RG78.25 and referred to in clause 4.5.   |
| <b>Representative</b>                                     | As defined in s910A of the Corporations Act. Representatives include authorised representatives, an employee or director or the licensee or related body corporate, or any other person acting on behalf of the licensee.                                 |
| <b>CPS &amp; CFM</b>                                      | These AFSL are also responsible entities for registered managed investment schemes  |
| <b>Significant Breach</b>                                 | Means: <ul style="list-style-type: none"> <li>(a) a Deemed Significant Breach; or</li> <li>(b) a breach or Likely Breach of a Core Obligation that is significant having regard to the factors in s912D(5) of the Corporations Act.</li> </ul>            |
| <b>Staff</b>  | All Cromwell directors, staff, Representatives, and contractors.  |



---

## Schedule One – Core Obligations

---

Cromwell's Core Obligations are those that arise under either the:

- general obligations provisions in s912A of the Corporations Act; or
- compensation arrangement requirements in s912B of the Corporations Act.

These are more fully described below as:

- a) do all things necessary to ensure that the financial services covered by each licence is provided efficiently, honestly and fairly;
- b) have in place adequate arrangements for the management of conflicts of interest;
- c) comply with the conditions of each licence;
- d) take reasonable steps to ensure that Cromwell representatives comply with financial services law;
- e) comply with ASIC reference checking and information sharing protocol;
- f) have adequate resources to provide the financial services covered by the relevant licence and to carry out supervisory arrangements;
- g) be competent to provide the financial services;
- h) have trained and competent representatives;
- i) have a dispute resolution system for retail clients;
- j) have adequate risk management systems;
- k) have compensation arrangements; and
- l) comply with any other obligations prescribed by the Corporations Regulations, including the requirement to cooperate with the Australian Financial Complaints Authority (AFCA).

The obligations under s912A(1)(c) of the Corporations Act to comply with the 'financial services laws' as defined in s761A.

All chapters and divisions set out in the Corporations Act and any other laws set out in the regulations.

In relation to traditional trustee company services provided by a licensed trustee company, the obligations under s912A(1)(c) of the Corporations Act to comply with financial services laws so far as they are Commonwealth, state or territory legislation or the common law or equity that relate to provision of financial services and traditional trustee company services.

Cromwell will be 'likely to' breach an obligation if it becomes aware that at a future time it will be unable to comply with its relevant obligations.

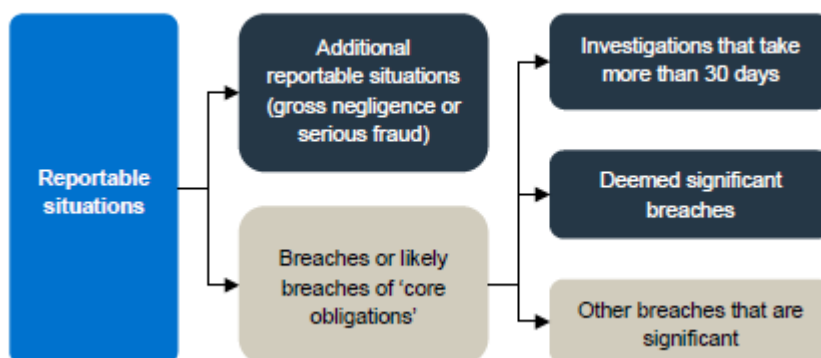
It is important to note that the financial services laws referred to above include obligations to:

- comply with a scheme's constitution;
- not make any misleading and deceptive statements about a product (whether in a product disclosure statement, information memorandum, flyer, advertisement or otherwise); and
- not allow a product disclosure statement to become out of date.

## Schedule Two – Reportable Situations

| Type of situation   | Description   | Guidance & examples   |
|---|---|-----------------------|
| <b>Breaches or 'likely' breaches of Core Obligations that are significant</b>                   | These situations include: <ul style="list-style-type: none"> <li>Any breach of a 'Core Obligation' where the breach is significant; and</li> <li>Any 'likely' breach of a 'Core Obligation' where the licensee or a representative of the licensee is no longer able to comply with a Core Obligation and the breach, if it occurs, will be significant.</li> </ul> | Ref RG78.34 - RG78.49 |
| <b>Investigations into breaches or likely breaches or Core Obligations that are significant</b> | This includes: <ul style="list-style-type: none"> <li>Investigations that continue for more than 30 days into whether there is a breach or likely breach of a core obligation that is significant; and</li> <li>The outcome of such an investigation if it discloses there is no breach or likely breach of a core obligation that is significant.</li> </ul>       | Ref RG78.50 – RG78.64 |
| <b>Additional Reportable Situations</b>   | These situations include: <ul style="list-style-type: none"> <li>Conduct constituting gross negligence;</li> <li>Conduct constituting serious fraud; and</li> <li>Other circumstances prescribed by the regulations.</li> </ul>   | Ref RG78.65 – RG78.69 |
| <b>Reportable Situations about other licensees</b>  | These situations relate to conduct in certain prescribed circumstances of individual financial advisers and mortgage brokers or other licensees.  | Ref RG78.70 – RG78.84 |

### Reportable situation, core obligations and objective determinations of 'significance'



## Schedule Three – Information provided to ASIC

### Date of the Reportable Situation

- the date that the Reportable Situation arose, or the date Cromwell anticipated that Cromwell will no longer be able to comply with its obligations; and
- the date Cromwell first knew that there were reasonable grounds to believe that a Reportable Situation had arisen.

### Nature of the Reportable Situation

- a significant breach of a core obligation;
- a likely significant breach of a core obligation;
- an additional Reportable Situation (serious fraud or gross negligence);
- an investigation into whether a breach (or likely breach) of a core obligation has occurred that has continued for more than 30 days;
- an investigation into whether a breach (or likely breach) of a core obligation has occurred that has continued for more than 30 days that discloses that no Reportable Situation has occurred; or
- a Reportable Situation about another licensee.

### Description of the Reportable Situation. Stating whether the report relates to:

- Cromwell must describe the Reportable Situation, including the section of the Corporations Act that sets out the relevant obligation, including any relevant financial services law and any relevant AFS condition.

### Why the breach is significant (if relevant). This may involve:

- Identifying that the Reportable Situation relates to a deemed significant breach; or
- Identifying that factors in s912D(5) of the Corporations Act or s50A(5) of the National Credit Act that you consider apply in determining whether the breach (or likely breach) is significant and required to be reported to ASIC.

### How the Reportable Situation was identified

- Cromwell must provide details of how Cromwell found out about the Reportable Situation. For example, via compliance arrangements, an audit or review, or as a result of an investor complaint.

### How long the breach lasted

- Cromwell will need to include details as relevant, including whether the breach is still continuing.

### Information about representatives

- If an authorised representative is involved, Cromwell must include:
  - That representatives name and number;
  - If the representatives' authorisation has been revoked or suspended; and
  - If the representatives work is being monitored or supervised.

### Whether and how the Reportable Situation has been rectified

Where relevant, Cromwell must provide details of plans to rectify the breach (or likely breach). This includes:

- When Cromwell expect to complete the rectification (or complete a plan for rectifying the breach); and
- How the rectification will be achieved.
- If ongoing steps are being taken to rectify the breach (or likely breach), indicate when Cromwell expects to send ASIC a report on the progress in rectifying it, as well as a notification that rectification is complete.

Whether and when affected clients have been compensated or remediation information

- Cromwell must provide details of any remediation program (including preventative measures) that has been or is being developed to compensate clients that have suffered a loss. Include relevant dates or expected dates for the start and conclusion of the remediation program.
- Cromwell should also provide information about completion of remediation.

Future compliance

- Cromwell must describe any steps that have been or will be taken to ensure future compliance with the obligation.