1 PURPOSE AND SCOPE

1.1 The Incident Handling Procedure outlines the process for receiving/gathering, appraising, prioritizing and responding to Incidents.

1.2 This procedure applies to Incidents related to the activities of ASI applicants and accredited/approved Conformity Assessment Bodies (CABs) and their applicant and certified Certificate Holders (CHs).

1.3 This procedure does not apply to Challenges/Appeals and Complaints as defined in their respective ASI procedures (ASI-PRO-20-103-Challenges & Appeals and ASI-PRO-20-104-Complaints).

2 CHANGE HISTORY

Version number	Date of approval	Effective Date	Description of changes
1.0	14 July 2014		First publication
2.0	24 June 2019		Major Revision: changing from internal to public document including QMS document from 10 to 20 series, update of processes, inclusion of fraud and Whistleblower policies.
2.1	15 October 2022		Minor revision to add terms “approval/approved” in line with the ASI Two-Tier Assurance Program (TTAP). ASI Logo update.
3.0	31 May 2023	01 July 2023	Major Revision: Removal of internal definitions and processes. Addition of new definitions (Appraisal, Incident Response, Rapid Response and Show Cause Notice). Modifications of definitions (i.e., Incident, Integrity Threat, Incident Investigation, Incident Whistleblower, Fraud). Investigation section changed to “Response”. Amendment of table 2, priority scoring. Extra Assessments conditions have changed. Clarity of Incident Investigation process and ASI communications including parties involved.

3 TERMS AND DEFINITIONS

3.1 All terms and definitions, where not defined below, are provided in the ASI Glossary (ASI-INF-20-100).

3.2 ***Incident:*** Any reported suspected or actual wrongdoing that threatens the reputation and/or integrity of the ASI assurance program and/or its associated “Scheme Owner” and cannot be considered under the relevant ASI procedures for Complaints and Appeals.

NOTE 1: Incidents differ from Complaints in that they are not reported following the ASI Complaints Procedure and/or can be reported anonymously. The need for a response from ASI varies according to the priority, as opposed to Complaints where a response is always required.

NOTE 2: Incidents differ from Challenges & Appeals in that anyone can report an Incident, whereas Challenges & Appeals are only available to CABs in relation to Nonconformities (NCs) or Accreditation/Approval Decisions.

3.3 ***Integrity Threat:*** Any situation, action, potential action, or inaction that could impede ASI and associated schemes in achieving their assurance objectives (including their credibility, reputation and the correctness of accreditation and certification decisions).

3.4 ***Incident Appraisal:*** An initial review of the Incident, including the prioritization of the Incident and the proposed Incident Response(s).

3.5 ***Incident Reporter:*** An individual reporting an Incident on behalf of an organization or as a private person.

3.6 ***Incident Response:*** Any agreed action to address or not to address the reported incident.

3.7 ***Incident Investigation:*** An ASI evaluation of one or more Incidents pertaining to the same topic, CAB, CH or region. An Incident Investigation culminates in an investigation report with recommendations to minimize, mitigate or prevent further threats to the credibility of ASI and/or the Scheme Owner.

3.8 ***Rapid Response:*** A prompt ASI intervention to address Integrity Threats that may negatively impact the credibility of ASI or the associated Scheme Owner.

3.9 ***Fraud***: Any intentional misrepresentation, concealment of information, or provision of false information to a relevant interested party, resulting in the deliberate violation of accreditation/approval or certification rules (adapted from International Accrediation Forum - IAF ID15:2023).

NOTE 1: The terms "fraud," "fraudulent behavior," or similar expressions in this procedure shall be understood and interpreted in alignment with the ISO and IAF normative landscape, explicitly excluding any reference to criminal offenses.

3.10 ***Fraud Assessment:*** A review of an Incident report, an allegation, and evidence to determine if there is sufficient justification to undertake a Fraud Examination.

3.11 ***Fraud Examination:*** Methodology of identifying signs or allegations of fraud. It follows a uniform, timely, and forensic process, where forensic implies suitability for use in courts of law.

3.12 ***Incident Whistleblower (hereinafter referred to as "Whistleblower"):*** A person who reports an Incident regarding any kind of information or activity, where they fear and may face risk of retaliation by coming forward. They can report anonymously to ASI through this Incident Handling Procedure.

3.13 ***Show Cause Notice:*** An order issued by ASI which requires an entity about which an allegation has been made, which can be a CAB or a CH, to provide evidence in writing to contest allegations of fraud, within a specific timeline, otherwise Sanctions may be recommended.

4 ASSOCIATED DOCUMENTATION

4.1	Procedures, Information Documents	ASI-PRO-20-103-Challenges & Appeals ASI-PRO-20-104-Complaints ASI-POL-20-255-Whistleblowing ASI-INF-20-100-ASI Glossary ISO 37002:2021- Whistleblowing
4.2	Checklists, Templates, etc.	Incident record and files – ASI System

5 GENERAL

5.1 Incidents reported to ASI are pursuant to the following steps: reporting, appraisal, response, closure and communication (See Figure 1- Incident Process Flow at the end of this procedure).

6 REPORTING

6.1 Incidents may be reported to ASI through various channels including, but not limited to:

a) Reporting by a Scheme Owner via their ASI Connect Portal;
b) Reporting by stakeholders, Scheme Owners, CABs, and other parties via the ASI website (www.asi-assurance.org/Incidents) or by email to integrity@asi-assurance.org, or any other means suitable to the reporter;
c) Anonymous reports through any of the above mentioned channels;
d) Confidential reports through any of the above mentioned channels;
e) Reports from media, NGOs or civil society organizations;
f) ASI personnel.

NOTE: Anonymous reports are always considered confidential. Confidential reports are not considered anonymous unless the reporter clearly states so. The reporter's name and organization are known in the case of a confidential report.

6.2 The grounds for Incident reports related to certification and/or Accreditation/Approval processes, include, but are not limited to:

a) Allegations of fraud and corruption;
b) Concerns regarding irresponsible business practices;
c) Warnings about Integrity Threats to Scheme Owners and/or ASI;
d) NCs or perceived NCs observed related to applicable certification or Accreditation/Approval Requirements.

6.3 ASI implements safeguarding measures for the protection of Whistleblowers through the following steps:

6.3.1 All information provided by Whistleblowers shall be handled confidentially, to ensure that persons who report Incidents are safeguarded from retaliation.

6.3.2 All possible steps shall be taken to ensure that information provided does not reveal the person's identity, while acknowledging that complete anonymity may not be guaranteed in all cases. ASI shall inform the Whistleblower about the process and corresponding risks of retaliation before the initiation of the Incident Handling process.

6.3.3 ASI shall not use the evidence provided by Whistleblowers directly if there is a risk of revealing their identity. In all possible instances, ASI shall collect the evidence again

through other means, to avoid linking the evidence with the Whistleblower. If that is not possible, ASI shall not reveal the evidence in the respective record or any subsequent reports and findings unless it is vital to do so. In such cases, ASI shall inform the Whistleblower and ask for permission to use the evidence, if their identity is known, prior to sharing information.

6.3.4 Any information that could reveal or suggest the Whistleblower's identity shall be removed from the Incident Report and records along with any attachments, and saved in a password protected folder with limited access permissions.

6.3.5 If the Incident is an allegation of deliberate criminal or illegal activity, ASI shall advise Whistleblowers to seek legal counsel.

6.4 For all Incidents where the reporter provides contact information, ASI shall acknowledge receipt when the Incident is logged. This is an automated service that indicates that the Incident has been recorded in the ASI System.

6.5 If the Incident was detected following a report from the media or/and civil society organization or NGO, ASI may reach out to the respective author of the media report for further information.

7 APPRAISAL

7.1 The Incident Appraisal shall start with a review of the Incident to confirm if it complies with the requirements of this procedure or if it should be treated as a Complaint or Challenge/Appeal as per the relevant ASI procedures.

7.1.1 If the Incident is a suspected or actual wrongdoing about a Scheme Owner, ASI shall inform the Reporter that they need to contact the Scheme Owner directly.

7.1.2 If the Incident is a suspected or actual wrongdoing of a CAB and the Reporter has not raised a Complaint with the CAB, ASI shall inform the Reporter about the CAB Complaint process.

7.1.3 If the Incident constitutes a Complaint, ASI shall advise the Reporter to submit a Complaint following the relevant ASI procedure, if this is considered more adequate.

7.2 If an Incident is eligible for further processing, ASI shall appraise the Incident using the guiding questions in Table 1. This rubric is designed to determine the severity of the Incident and direct ASI's response.

Table 1: Appraisal questions

1. Is the Incident credible? *2- Very credible, no question of the Incident's occurrence* *1- Somewhat credible, requires further validation* *0- Credibility is questionable*
2. Does the Incident pose an **immediate** threat to impartiality, integrity, reputation, or safety of ASI and its team? *2- Immediate threat to ASI* *1- Potential threat to ASI* *0- Threat localized or no threat exists*
3. Does the Incident pose an **immediate** threat to the credibility of a Scheme Owner? *2- Immediate threat to scheme* *1- Potential threat to scheme* *0- Threat is localized or no threat exists*
4. Has the Incident been reported by an internal or external source? *2- An external source that may communicate negatively about the Incident*

1- An external source that is not likely to communicate negatively about the Incident *0- An internal source* Note: An external source also involves the detection of Incidents by the ASI team through for instance media reports.
5. Has the Incident been reported by a trustworthy and known source? *This question is answered by assessing the reporter of the Incident. If the reporter is reporting on behalf of another entity, or reporting from a published source then the original source should be assessed for this indicator. If the original source is not known, then the score should be 0.* *2- Very trustworthy, no question* *1- Somewhat trustworthy, requires validation* *0- Trustworthiness is questionable*
6. Is this a systemic issue? *This question is answered by assessing whether the Incident is isolated or systemic* *2- Other Complaints, Challenges/Appeals, or Incidents report similar or same issue e.g. according to a particular CAB and/or a particular certification that indicate a systemic problem* *1- Some evidence that the Incident could be repeating, but not systemic* *0- Evidence suggests that this is an isolated Incident*
7. Does the Incident involve illegal acts? *This question is answered by assessing if the allegations, if proven, would constitute a breach of any binding legal framework relevant to the Incident* *2- The Incident is an allegation of deliberate criminal or illegal activity* *1- Some evidence that criminal or illegal activity may be occurring* *0- Incident does not suggest any form of criminal or illegal activity*

7.3 Once all the questions from Table 1 have been answered, ASI shall take the sum of the indicators in Table 1 and allocate a priority using Table 2, to design a suitable response.

Table 2: Priority scoring and Incident Response

Score	Priority	Incident Responses
0-3	Minor	The Incident is negligible and an Incident Response may not be required. Routine procedures for monitoring are applied.
4-7	Normal	The Incident is moderate and a response timeline shall be suitable to the Incident topic. Multiple normal and minor Incidents may be combined into one single Incident Response.
8 - 11	Major	The Incident is a significant Integrity Threat and requires additional control. The Incident Response shall begin within three months of the agreed Response. A major Incident may combine other Incidents into one Response if deemed appropriate.
12 - 14	Critical	The Incident is a serious Integrity Threat and requires immediate attention and response. Rapid Response shall be deployed.

7.4 Scheme Owners have access to the ASI Connect Portal and can monitor the status of all Incidents in real time. ASI shall, however, inform the Scheme Owners upon receipt of an Incident that is classified as “Critical”.

7.5 Conditions for Fraud Assessment

7.5.1 A Fraud Assessment shall always be triggered if Question 7 in Table 1 (above) has an answer of 1 or 2.

7.5.2 A Fraud Assessment may also be triggered if Fraud is suspected but nothing illegal is alleged.

7.5.3 Where a Fraud Assessment finds sufficient predication for further investigation, and where the Incident priority is major or critical, a Fraud Examination shall be part of the investigation plan.

7.6 Incidents with similar subjects covering the same geographical scope, CAB or CH may be grouped together for Incident Response.

NOTE: This is particularly relevant for minor Incidents that are logged for future reference and normal Incidents that can be gathered over a longer period of time for a suitable response.

7.7 If the Incident concerns an entity that is not certified or a CAB that is not accredited/ approved by ASI, the entity in question may be contacted by ASI to clarify and/or correct the matter if appropriate (e.g. in the case of an entity making incorrect claims about ASI).

7.8 If new information is reported after an Appraisal is completed, an Appraisal may be updated to reflect the new information. This may include upgrading or downgrading the priority of the Incident and/or changing the planned Incident Response(s).

8 RESPONSE

8.1 The Incident Response depends on the nature and the priority of the Incident being reported and can result in one or multiple responses. An Incident Response can also cover different CABs or Schemes simultaneously, if relevant to multiple parties.

8.2 ASI may highlight the need for any additional evidence to the Incident Reporter to ensure that any Incident Response can be effectively undertaken.

8.3 The types of Incident Responses include, but are not limited to the following activities:

a) Requesting a CAB for further investigation, including sending a Show Cause Notice;
b) Conducting additional research;
c) Conducting an Incident Investigation;
d) Conducting an ASI Assessment of CABs;
e) Performing Fraud Examination;
f) No further action (no response).

8.4 ASI Assessments of CABs

8.4.1 ASI reserves the right not to inform CABs and CHs about the Incident in question, to avoid disrupting further information gathering or compromising the objective of the evaluation.

8.4.2 ASI shall attempt to cover the costs as part of the Annual Service Fee (ASF) and part of the regular Assessment plan to avoid incurring extra cost to the CAB and CH (if applicable). If CAB performance issues become apparent as a result of an ASI Incident Response (e.g. NC or Sanction issued by ASI to the CAB), then ASI reserves the right to invoice the CAB for such extra assurance activities in addition to the ASF. Further,

ASI may ask CABs that pay the Regular Service Fee (RSF) to cover the costs incurred from the Incident Response.

8.5 In some instances no further action may be required, such as in the case of a minor Incident or when the content of the Incident is outside ASI's remit.

8.6 CAB request for further investigation and /or information

8.6.1 ASI may, at their discretion, request the CAB to investigate a reported Incident.
8.6.2 If ASI requests a CAB to investigate an Incident, ASI shall provide all relevant details (subject to confidentiality) including a timeline for reporting back to ASI.
8.6.3 If the Incident constitutes an allegation against a CH, the CAB shall provide ASI with a summary of how and when they plan to investigate.
8.6.4 The CAB shall inform ASI about the outcome within the requested time frame.
8.6.5 In the case of an immediate threat (see Table 1 points 2 and 3) and the Incident has a Major or Critical grade, ASI may request a response within a short time frame (usually 10 days). If the immediate threat is due to alleged illegal or fraudulent activity, then ASI may request a response via Show Cause Notice.

8.7 Incident Investigations

8.7.1 An Incident Investigation can be used to investigate more than one Incident at the same time – that means more than one CAB or CH can be involved in an Incident Investigation.
8.7.2 The investigation report may be shared with the relevant Scheme Owner.
8.7.3 ASI reserves the right to publish a summary of the final Incident Investigation report on the ASI website.

8.7.3.1 In case of publication, the draft public summary report shall be shared with the Parties involved prior to publication so that the parties can confirm, within seven (7) days, that all confidential information has been omitted.
8.7.3.2 Parties to an Incident Investigation are normally the reporter, ASI and the CAB. ASI is not required to share draft summary reports with CHs or other entities but shall ensure that all confidential information has been omitted.

8.8 If an Incident Response results in important information about the severity of the Incident and concludes that further response is necessary, the Incident record can be updated to reflect the new information. This may include upgrading or downgrading the priority of the Incident and/or agreeing on a new Incident Response(s).

9 CLOSURE AND COMMUNICATION

9.1 An Incident can be closed when the Incident Response(s) has(ve) been completed or when no Incident Response was needed.

NOTE: If the Incident Response was a CAB Assessment, ASI shall close the Incident if the Assessment resulted in an NC that addresses the Incident, even though the NCs may not be closed at the time of Incident closure.

9.2 Closed Incidents remain part of ASI's intelligence and conclusions may be used for future reference.

9.3 Communicating with the Incident Reporter

9.3.1 The Incident Reporter shall be informed when an Incident is closed, if the Incident Reporter is known to ASI.

9.3.2 The Incident Reporter may request the outcome of the Incident Response from ASI. ASI may provide such outcome, provided and in the form that shall not breach any existing confidentiality obligations of ASI. More information about ASI assessment reports is available here.

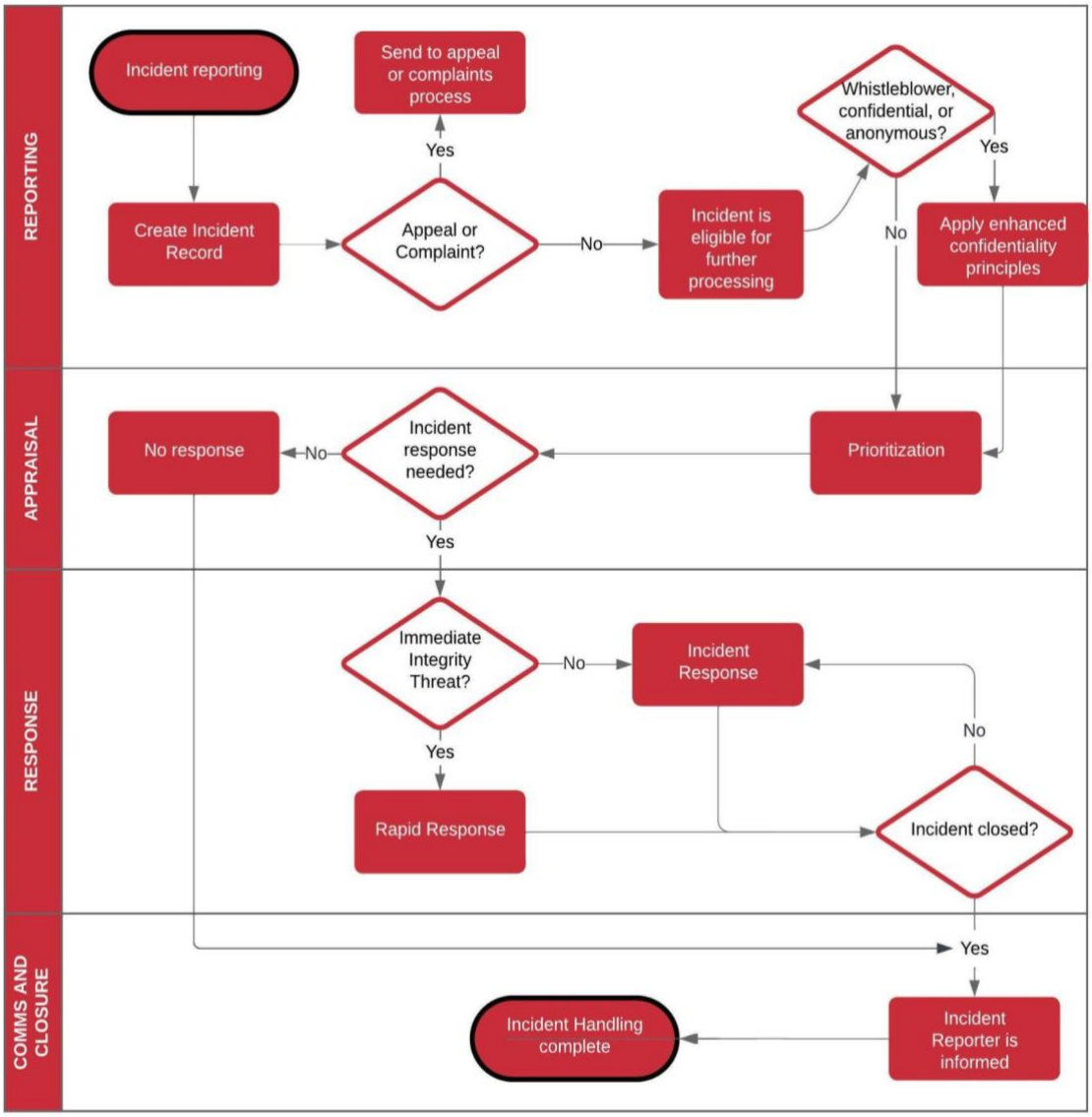
9.3.3 ASI reserves the right not to report fully to the Incident Reporter in cases where such communication with the reporter may compromise confidentiality.

9.4 If the Incident, following the response, still poses an Integrity Threat, which cannot be further addressed by ASI or is outside ASI's remit, ASI may decide to review and develop recommendations for relevant parties to minimize or mitigate such Integrity Threats. In such an event, the Incident shall be considered closed.

9.5 CABs may request information about an Incident that concerns the CAB or its clients. ASI reserves the right to determine the level and type of information shared with the CAB on a case-by-case basis or to deny information related to the Incident if it would reveal a Whistleblower's identity, compromise confidentiality and/or the success of ASI activity to respond to the Incident.

9.6 All Incidents, related responses and outcomes are available to the relevant Scheme Owner. Confidential information about Whistleblowers shall not be disclosed.

Figure 1. Incident Handling Process Flow Chart



---------- End of Document ----------