ASF-QMS-003

Risk Management Policy

Document code	ASF-QMS-003
Version	V3.0
Status	Published — effective 2026-12-01
Approved by	Prof. Giorgi Pkhakadze, MD, MPH, PhD President, Accréditation Sans Frontières
Applies to	All ASF operations, governance processes, and the ASF Quality Management System
Related documents	ASF-QMS-001 Internal Audit Policy · ASF-QMS-002 Management Review Procedure · ASF-GOV-003 Impartiality Policy · ASF-GOV-004 Confidentiality Policy · ASF-OPS-001 Accreditation Decision Framework
Supersedes	ASF-QMS-003 V2.0 (2026-11-28)
Next review	December 2031, or earlier on trigger

Version History

Version	Date	Nature of change	Approved by
V0.1	2026-11-06	Initial draft	—
V1.0	2026-11-19	Management review	QMS Coordinator
V2.0	2026-11-28	Approved and published	Prof. G. Pkhakadze, ASF President
V3.0	2026-12-01	Expanded to full policy; 5×5 risk scoring matrix, 4-level risk rating table with colour coding, 6-category risk taxonomy, 5-step risk assessment process, risk treatment options, risk register requirements, integration with audit and management review, and 12 references	Prof. G. Pkhakadze, ASF President

© Accréditation Sans Frontières · Legally established in Paris, France, 2020 · france-asf.fr · This document is subject to version control. Unauthorised reproduction is prohibited.

1. Purpose

1.1 Risk management is the systematic identification, assessment, treatment, and monitoring of risks that could affect ASF's ability to deliver a credible, impartial, and high-quality accreditation programme. This policy establishes ASF's approach to risk management as a standing component of its quality management system, integrated with internal audit (ASF-QMS-001) and management review (ASF-QMS-002).

1.2 The risk management framework in this policy is based on ISO 31000:2018 principles and is adapted for the specific operational context of an international accreditation body. The purpose is not to eliminate all risk — that is not achievable — but to ensure that ASF's risk exposure is understood, managed to an acceptable level, and regularly reviewed.

2. Risk Categories

2.1 ASF's risk register organises risks into the following categories. Each category is assessed as part of the annual risk review cycle:

Risk category	Description	Example risks
Impartiality risk	Risks that could compromise — or appear to compromise — the independence of ASF's accreditation decisions	Undisclosed CoI; financial dependency on a single accredited organisation; surveyor relationship with an applicant
Standards quality risk	Risks to the validity, currency, and relevance of ASF's accreditation standards	Standards not updated in response to regulatory change; criteria that do not reflect current clinical evidence
Operational risk	Risks to ASF's ability to deliver surveys on time, with competent surveyors, and to agreed quality	Surveyor shortage; survey scheduling failures; loss of a key staff member
Legal and compliance risk	Risks of non-compliance with applicable law, including GDPR, French civil law, Georgian law, and contractual obligations	Data breach; breach of Accreditation Agreement; regulatory investigation
Reputational risk	Risks to ASF's credibility, standing with ISQua, and trust among applicants, accredited organisations, and regulators	A high-profile adverse event at an accredited facility; media criticism; unfair complaint upheld against a surveyor
Financial and sustainability risk	Risks to ASF's financial stability and long-term operational viability	Revenue below forecast; unpaid survey fees; unbudgeted costs

3. Risk Assessment — Likelihood and Impact Scoring

3.1 Each identified risk is assessed on two dimensions using a five-point scale:

© Accréditation Sans Frontières · Legally established in Paris, France, 2020 · france-asf.fr · This document is subject to version control. Unauthorised reproduction is prohibited.

(a) Likelihood: 1 = Rare (less than once in 10 years); 2 = Unlikely (once in 5–10 years); 3 = Possible (once in 2–5 years); 4 = Likely (once a year or more); 5 = Almost certain (multiple times per year).

(b) Impact: 1 = Negligible; 2 = Minor; 3 = Moderate; 4 = Major; 5 = Critical (threatens ASF's ability to continue operating or its ISQua EEA accreditation).

3.2 The inherent risk score is calculated as Likelihood × Impact (range 1–25). The residual risk score is calculated after applying existing controls. Both scores are recorded in the risk register.

3.3 Risk levels and the required management responses are as follows:

Risk level	Likelihood × Impact	Score range	Required action and timescale
CRITICAL	High likelihood × High impact	16–25	Immediate escalation to ASF President; treatment plan within 5 working days; extraordinary management review convened if not resolved within 15 working days
HIGH	High likelihood × Medium impact, or Medium × High	10–15	Treatment plan within 15 working days; reported at next management review; monthly monitoring
MEDIUM	Medium likelihood × Medium impact, or Low × High	6–9	Treatment plan within 30 working days; reported at annual management review; quarterly monitoring
LOW	Low likelihood × Low impact, or Low × Medium	1–5	Accepted or monitored; reviewed at annual audit; no immediate action required unless score increases

4. Risk Assessment Process — Five Steps

Step 1 — Risk Identification

4.1 Risks are identified through: review of previous internal audit findings; management review outputs; complaints and appeals data; changes in ASF's operating environment; and the professional judgement of ASF staff, committee members, and surveyors. Any ASF staff member or committee member may submit a risk identification to the QMS Coordinator at any time.

Step 2 — Risk Analysis

4.2 The QMS Coordinator analyses each identified risk, assigns it to the appropriate category, and scores its likelihood and impact (inherent score) using the scales in §3.1. Existing controls are identified and documented.

© Accréditation Sans Frontières · Legally established in Paris, France, 2020 · france-asf.fr · This document is subject to version control. Unauthorised reproduction is prohibited.

Step 3 — Risk Evaluation

4.3 The residual risk score is calculated after accounting for existing controls. The risk is rated as Critical, High, Medium, or Low using the matrix in §3.3. Risks rated Critical or High are escalated to the ASF President immediately.

Step 4 — Risk Treatment

4.4 For each risk rated Medium or above, a risk treatment plan is agreed. The four standard risk treatment options are:

- **(a)** Avoid — discontinue the activity or process that gives rise to the risk;
- **(b)** Reduce — implement additional controls to reduce the likelihood and/or impact to an acceptable residual level;
- **(c)** Transfer — transfer some or all of the risk to a third party (e.g. through insurance or contractual provisions);
- **(d)** Accept — acknowledge the risk and accept it without further action, where the cost of treatment exceeds the benefit, and the residual risk is within ASF's risk appetite.

4.5 Risks rated Critical are never accepted without a documented rationale and explicit approval by the ASF President. No Critical risk may be accepted without a compensating control that reduces the effective rating to High or below.

Step 5 — Monitoring and Review

4.6 The risk register is reviewed at the following points:

- **(a)** At each annual management review — all risks reviewed; ratings updated to reflect changes in likelihood, impact, or control effectiveness since the last review;
- **(b)** At each extraordinary management review — risks in the relevant category reviewed as part of the trigger-issue assessment;
- **(c)** Following each internal audit cycle — audit findings used to update risk ratings for the audited process area;
- **(d)** When a significant change occurs in ASF's operating environment — a new standard type launched, a new regulatory requirement, a change in surveyor pool — the QMS Coordinator conducts a targeted risk review within 20 working days.

5. Risk Register

5.1 The ASF risk register is maintained by the QMS Coordinator and approved by the ASF President. It is a living document updated at least annually and following each of the triggers in §4.6. The register records for each risk:

- **(a)** Risk ID (sequential, e.g. R-001);
- **(b)** Risk category (from §2.1);
- **(c)** Risk description — what could go wrong, and why;
- **(d)** Current controls — what is already in place to manage this risk;
- **(e)** Inherent risk score (Likelihood × Impact before controls);
- **(f)** Residual risk score (Likelihood × Impact after controls);
- **(g)** Risk rating (Critical / High / Medium / Low);
- **(h)** Risk treatment plan and target residual rating;

© Accréditation Sans Frontières · Legally established in Paris, France, 2020 · france-asf.fr · This document is subject to version control. Unauthorised reproduction is prohibited.

(i) Owner — the named person responsible for managing the risk and implementing the treatment plan;

(j) Date last reviewed and next scheduled review date.

5.2 The risk register is presented to the annual management review as a mandatory review input (ASF-QMS-002, §4.1, item 2). A summary of High and Critical risks is included in the pre-meeting documentation pack.

6. Records

6.1 The following records are maintained by the QMS Coordinator and retained for a minimum of 5 years:

(a) the risk register and all prior versions;

(b) risk treatment plans and their implementation status;

(c) risk escalation records (for Critical and High risks);

(d) the risk summary presented at each management review.

7. ISQua EEA Alignment

7.1 This policy supports ISQua EEA Principle 10 (Quality Management System), which requires accreditation bodies to have a systematic approach to identifying and managing risks to the impartiality, integrity, and performance of their accreditation programme. It also supports Principle 4 (Independence), insofar as impartiality risk management is a standing component of the risk framework. The ASF ISQua EEA Crosswalk (ASF-EV-004) maps the provisions of this policy to the applicable EEA criteria.

8. References

[1]	ISQua IAP. Principles for Standards. 6th Ed. ISQua EEA, Dublin, 2023.
[2]	International Organization for Standardization. ISO 31000:2018 — Risk Management: Guidelines. ISO, Geneva, 2018.
[3]	ISO/IEC 31010:2019 — Risk Management: Risk Assessment Techniques. ISO, Geneva, 2019.
[4]	ISO 9001:2015 — Quality Management Systems: Requirements. §6.1 Actions to Address Risks and Opportunities. ISO, Geneva, 2015.
[5]	ISO/IEC 17021-1:2015 — Conformity Assessment. §8.5 Impartiality. ISO, Geneva, 2015.
[6]	Committee of Sponsoring Organizations of the Treadway Commission (COSO). Enterprise Risk Management — Integrating with Strategy and Performance. COSO, 2017.
[7]	Accreditation Canada. Risk Management Policy. ISQua EEA Accredited Document, 2022.
[8]	HQACI. Risk Management Policy. ISQua EEA Accredited Document, 2026.
[9]	Braithwaite J et al. Complexity science in healthcare. BMJ Qual Saf. 2017;26(12):1000–1004.

© Accréditation Sans Frontières · Legally established in Paris, France, 2020 · france-asf.fr · This document is subject to version control. Unauthorised reproduction is prohibited.

[10]	Flodgren G et al. External inspection of compliance with standards for improved healthcare outcomes. Cochrane Database Syst Rev. 2016;12:CD008992.
[11]	World Health Organization. Risk Management for WHO Field Offices. WHO, Geneva, 2012.
[12]	Shaw CD et al. Profiling health-care accreditation organisations. Int J Qual Health Care. 2013;25(3):222–231.

Formal Approval

Name and title	Signature	Date
Prof. Giorgi Pkhakadze, MD, MPH, PhD President, Accréditation Sans Frontières		2026-12-01

Document code: ASF-QMS-003 · Version: V3.0 · Effective: 2026-12-01 · Next review: December 2031

© Accréditation Sans Frontières · Legally established in Paris, France, 2020 · france-asf.fr · This document is subject to version control. Unauthorised reproduction is prohibited.