Corrective Action Form

Appendix 1 to ISMS-DOC-07 Procedure for Corrective Actions

Document code	TPL-024
Document name	Corrective Action Form (Appendix 1 to ISMS-DOC-07)
Type	Form / Record
Used by	Originator of the corrective action; CISO; Action owner; Verifier
When to use	One form per corrective action — opened within 5 business days of identification per ISMS-DOC-07 §5 Step 1, completed through the lifecycle, closed at verification.
Mandatory under	ISO/IEC 27001:2022 clauses 10.1 and 10.2
Retention	5 years from closure of the corrective action
Compliance scope	Records the lifecycle of one corrective action — from identification through verification. Operationalises ISMS-DOC-07. Aggregate metrics across all forms feed Management Review.

1. Identification

Action ID	[CA-YYYY-NNN]
Date opened	[DD/MM/YYYY]
Originator	[Name, role]
Source of the action	[PIR / Internal audit / External audit / Management Review / Monitoring / Risk assessment / Supplier review / Other — specify]
Source reference	[e.g. PIR-2025-001, Audit-2025-Q3, RA-2025, etc.]
Type	[Corrective / Preventive / Improvement]
Priority	[High / Medium / Low — based on risk and urgency]
Action owner	[Name, role — assigned by CISO]
Target deadline	[DD/MM/YYYY]
Status	[Open / In progress / Pending verification / Closed effective / Closed not effective — re-opened]

2. Description of the gap

What is the gap, the nonconformity, or the improvement opportunity? Where was it observed? When? Who observed it? Be factual and specific — the description must be sufficient for a third party to understand without further context.

[Enter response here…]

3. Root cause analysis

Use the 5-Whys or equivalent. Distinguish: immediate cause (what triggered the gap); contributing factors (conditions that allowed the gap to exist or persist); systemic factors (policy, training, design, supplier). State explicitly which findings are conclusions vs. hypotheses.

[Enter response here…]

4. Action plan

List the specific corrective measures to address the root cause(s). Each measure has a sub-owner and a deadline. Plans for systemic root causes typically include more than one measure (e.g. revise procedure + deliver training + update monitoring).

#	Measure	Sub-owner	Deadline	Status
1	[Measure description]	[Name, role]	[DD/MM/YYYY]	[Status]
2	[Measure description]	[Name, role]	[DD/MM/YYYY]	[Status]
3	[Measure description]	[Name, role]	[DD/MM/YYYY]	[Status]
4	[Measure description]	[Name, role]	[DD/MM/YYYY]	[Status]

5. Plan approval

The CISO approves the action plan. For high-impact actions the Executive Sponsor approves. Approval criteria: action addresses the root cause; deadline is realistic; owner has authority to execute.

Role	Name	Signature	Date
Approved by	[Name, role — CISO]	[Signature]	[DD/MM/YYYY]

6. Execution evidence

Summarise the evidence that the planned measures have been completed. Reference attached evidence (revised document codes, training records, configuration screenshots, audit logs). Distinguish completed measures from those still in progress.

[Enter response here…]

7. Verification of effectiveness

Independent verification by the CISO or a designated peer (not by the action owner). The verifier answers two questions explicitly: was the action completed? Is the gap genuinely addressed?

Verification question	Answer + evidence
(a) Was the planned action actually completed?	[Yes / No / Partially — explain]
(b) Is the gap genuinely addressed?	[Yes / No / Partially — explain]

Verifier: [Name, role — CISO or designated peer]
Verification date: [DD/MM/YYYY]
Conclusion: [Closed effective / Closed not effective — re-open]

8. Lessons learned and follow-up

Summary of what the organisation has learned from this gap. Reference any related actions or system changes triggered (e.g. training updates per PLA-008, policy revisions, risk assessment updates, monitoring changes). Where a finding has implications across the management system, escalate to the Management Review.

[Enter response here…]