Risks and Controls

CONTENTS

1. Control framework overview

🎯 Purpose

Describes how the control system in this workspace fits together: where controls are defined, how they are operated, tested and improved. Distribution-specific control operation lives in **Distribution Controls**; this document is the framework those operations follow.

🧭 The control loop

1. **Define**
   Risks are identified in the operational risk register; each material risk receives named key controls, an accountable owner and a defined evidence artefact.

2. **Operate**
   Controls operate within SOPs and work instructions. Controls that exist only in a register are not considered operationally effective.

3. **Attest**
   Control owners complete monthly control self-assessments supported by retained evidence.

4. **Verify**
   Second-line reviews sample attestations quarterly, while Internal Audit performs risk-based assurance reviews.

5. **Improve**
   Control failures, incidents and near-misses are routed into the continuous improvement pipeline for remediation and optimisation.

🛡️ Design rules

> ℹ️ **Control design requirement**
>
> Every control must define **one accountable owner, an operating frequency and an evidence artefact**. Controls missing any of these elements must not enter the control register.

- Preventive beats detective where the process allows it.
- Controls are written into the SOP step where they operate, with their register ID (for example CTRL-D-03), so procedure and register never drift apart.

🔎 Governance implementation guidance

- Reference control IDs directly within SOP activities and operational procedures.
- Retain evidence in auditable repositories aligned to records retention requirements.
- Prioritise preventive controls where process architecture allows automation or hard-stop enforcement.
- Review control effectiveness through recurring governance forums and operational metrics.

🧩 Three lines summary

Line	Who	Role here
First	Process teams and owners	Operate and attest controls
Second	Risk and Compliance	Frameworks, sampling, challenge
Third	Internal audit	Independent assurance

2. Operational risk register

🎯 Purpose

Register of the material operational risks in the processes this workspace documents, with their key controls and current assessment. Maintained by the operational risk forum; reviewed monthly at the ops review.

📋 Register (extract)

ID	Risk	Process area	Gross	Key controls	Residual	Trend
OR-01	Unlicensed or unfit intermediary activated	Intermediary onboarding	High	CTRL-D-03, CTRL-D-04, CTRL-D-07	Low	Stable
OR-02	Cover confirmed before KYC complete	Customer onboarding	High	CTRL-C-01 hard stop	Low	Stable
OR-03	Commission paid on uncollected premium	Finance cycles	Medium	Collected-basis rule in commission run	Low	Stable
OR-04	Banking detail fraud on agreements or refunds	Agreements, refunds	High	Call-back verification (CTRL-D-11 pattern)	Medium	Watch
OR-05	Underwriting authority breach	Referrals	Medium	Delegation matrix, queue monitoring	Medium	Watch
OR-06	Policy record does not match issued schedule	Policy administration	High	Endorsement four-eyes, discrepancy incident route	Medium	Improving
OR-07	Claims fraud not detected at FNOL	Claims	Medium	FNOL fraud checklist, SIU routing	Medium	Stable
OR-08	Client money unallocated beyond tolerance	Premium reconciliation	High	Monthly rec, 60-day escalation	Low	Stable

📐 Governance conventions

- Gross = risk with no controls; Residual = with controls operating as tested in the monthly self-assessment.
- A control failure in the self-assessment automatically flags the linked risk for re-assessment at the next forum.
- New risks enter through the forum with a named accountable owner from the RACI in **Roles and Responsibilities**.

🔎 Assessment and review guidance

- Review risk trends monthly through operational governance forums.
- Escalate repeated control failures into formal remediation tracking.
- Verify that residual risk ratings align with current control effectiveness evidence.
- Ensure accountable owners are assigned to every material operational risk.

2.1. Risk deep-dives

2.1.1. OR-04 Banking detail fraud

⚠️ Risk statement

A fraudster impersonating an intermediary or policyholder changes banking details on an agreement or a refund, diverting commission or refund payments. Gross rating **High**; residual **Medium**, trend **Watch**.

🧭 Attack paths seen in the industry

1. **Compromised intermediary mailbox**
   A fraudulent actor sends a banking detail change using authentic branding and credible intermediary correspondence.
2. **Insider-enabled amendment submission**
   An internal or partner contact submits fraudulent changes alongside legitimate operational amendments.
3. **Refund redirection timing attack**
   Fraudulent refund amendments are submitted immediately following policy cancellation before customer confirmation controls complete.

🛡️ Key controls

Control	Type	Evidence
Call-back verification to the number already on file (CTRL-D-11 pattern)	Preventive	Call log reference on the amendment record
Four-eyes release on refunds above threshold	Preventive	Second approver in payment run log
Confirmation letter to the OLD contact channel on every banking change	Detective	Dispatch record

> 🚫 **Banking verification control**
>
> All call-back verification activity must use the telephone number already recorded in the core system. Contact details provided in the change request must never be used for authentication.

📈 Watch rationale

Attempt volume is rising industry-wide; the control set is adequate but attempt-detection reporting is manual. Improvement candidate: automated alert on banking change + refund within 30 days.

🧾 Evidence retention expectations

- Store call recordings or call log references against the amendment transaction.
- Retain payment approval evidence within the finance workflow archive.
- Preserve outbound notification evidence for all banking detail amendments.
- Escalate failed verification attempts through operational fraud incident management procedures.