CONTROL FRAMEWORK · VERSION 1.5

Risk Management Protocol

Exposure limits, incident triggers and the recovery process for inference and task funding.

> Pool-side controls are the proposed operating protocol for eligible tasks. Limits, trigger thresholds, responsibilities and escalation windows require approval before use.
>
> A pool settlement must be tied to reconciled cash and an identifiable statement. Losses, idle capacity and delayed acceptance can reduce or eliminate distributions. A payout with an ambiguous processor response requires reconciliation before any new submission.

Contents

Position limits and owners 02

Emergency Pause 03

Recovery and residual risk 04

CHAPTER 01

Position limits and owners

Set task-wide and per-operation limits before an agent spends. A task's remaining budget accounts for posted costs and unsettled commitments. Additional limits can apply to a vendor, model, settlement currency or collection exposure.

Limit	Control	Suggested owner
Operation	Evaluate each proposed purchase against its approved maximum. Record overruns as exceptions.	Task owner
Task	Evaluate posted costs plus open commitments against the authorized task limit.	Operations
Vendor or provider	Limit concentration and review service dependencies before raising exposure.	Risk owner
Account access	Scope credentials by integration and revoke exposed keys.	Account owner
Customer exposure	Track unpaid invoices and concentration before authorizing more work.	Finance reviewer

Worked control example

A task has $40 approved, $18 posted and $9 committed. It has $13 remaining and a $10 limit per operation. A $12 operation exceeds the per-operation approval. Record the decision and request approval or reduce the scope.

Exception record

Chat and generation enforce request-rate and concurrency limits. Uploads have type and size checks, private storage and owner-only access. PDF extraction has time and memory limits. An uncertain generation keeps its reservation pending reconciliation and is not automatically submitted again.

Attach the task and operation references, proposed amount, reason, intended duration, and approval role (spending controller or on-call operator). Reassess limits when the service, customer, delivery deadline or spending assumptions change.

CHAPTER 02

Emergency Pause

The framework calls for an automatic pause on new affected operations once approved monitoring confirms a configured severe trigger, such as an increase in model provider tariffs above the approved threshold. Operators can also initiate a pause in response to a material reconciliation or security issue. Approve the tariff increase threshold together with budget limits.

Event	First action	Check before restarting
Model provider tariff change	Recalculate open task reserves at the new tariffs. If the increase exceeds the threshold, pause approval of new budgets.	Verify the tariff source and applicable threshold.
Provider or processor failure	Pause the affected route and track accepted requests.	Reconcile metering, confirmations, and payments.
Ledger discrepancy	Stop new relevant commitments and isolate the entries.	Match charges to approved spend and supporting records.
Security event	Disable affected credentials, notify operators, and review usage.	Verify key rotation and remediation of the incident.

During the pause

- Record the trigger, timestamp in UTC, affected services and owner.
- Stop new commitments within the affected scope. Continue recording evidence and receiving status updates for open obligations.
- Classify in-flight items as completed, failed, unsettled or ambiguous. Verify potential duplicates before retrying.
- Preserve the record of decisions through closure and reconciliation.

CHAPTER 03

Recovery and residual risk

Criteria for reopening

1. Verify the data, provider health, credential state or tariff source that triggered the pause.
2. Reconcile open authorizations, payments and provider charges. Assign an owner to every unresolved item.
3. Approve the restart scope and capacity. Resume with a limited set of operations and monitor for recurrence.
4. Document incident impact, verified charges, corrections, decisions and follow-up owners.

Residual exposures

Validation and operational limits can reduce new exposure. They do not reverse an irreversible chain transfer, compel customer payment or guarantee a provider response. Funds can be lost through wrong-network transfers, higher resource costs, service failures or counterparty nonpayment.

Customer action

Verify your checkout invoice before sending crypto, keep payment and response references, and revoke exposed API keys. Check the workspace before resubmitting a request whose outcome you cannot determine.

Review the online risk register and support guide for what to send when an issue arises.