mauvlabs / advisory

FICTIONAL SAMPLE DELIVERABLE

Retained Advisor - Monthly Advisory Report

A monthly management and engineering record covering technical decisions, artefact reviews, remediation priorities and the next work plan.

PACKAGE	Retained Advisor
PREPARED FOR	RimbaOps Software Sdn. Bhd. (fictional)
SAMPLE PERIOD	July 2026
REFERENCE	MA-SAMPLE-RA-001
CLASSIFICATION	Sample - Public

This sample is fictional. It shows the type of written advisory output a client may receive; the actual contents depend on the agreed scope, information supplied and time used.

DOCUMENT CONTROL

How to read this sample

This is a worked example, not a promise that every month will produce every page shown here. Advisory effort follows the live decisions and artefacts that need attention.

CONTROL	SAMPLE DETAIL
Document reference	MA-SAMPLE-RA-001
Prepared for	RimbaOps Software Sdn. Bhd. (fictional)
Scenario	Malaysian SaaS team operating a customer portal and AWS platform
Package allocation	Up to 10 advisory hours per month
Working rhythm	Up to two scheduled sessions each month
Response target	Initial response within 2 business days
Classification	Sample - Public

What the fee buys

Reserved access to senior technical judgement, preparation, review time and concise written follow-through. Meetings, research, document review, notes and between-session replies all use the monthly allocation.

Consultant provides

- Advice based on the agreed systems and information made available.
- Clear recommendations, assumptions and points requiring a client decision.
- A practical record of priorities, owners and follow-up where the work warrants it.

Client remains responsible for

- Supplying accurate context, access and relevant technical artefacts.
- Business decisions, implementation, change approval and production testing.
- Escalating material changes, incidents or deadlines that affect the advice.

EXECUTIVE SUMMARY

July advisory position

The team is preparing a new document upload service while closing findings from an earlier application test. The immediate concern is release discipline, not the number of open tickets.

2	4	6
artefacts reviewed	risks tracked	owned actions

Management decision required

Approve a two-week release condition for the upload service: malware scanning must be active, the processing role must be restricted, and the rollback owner must be named. The medium-risk logging debt may follow after release.

Position improved this month

- Upload design has a defined trust boundary
- Critical pentest item has closure evidence
- Owners accepted for all current P0 and P1 actions

Still exposed

- Production log access is broader than needed
- Admin MFA exception remains for one service operator
- Rollback evidence has not yet been exercised

DECISION REGISTER

Decisions made and conditions attached

A retained advisor should reduce repeated debate. This register records what was decided, the basis for it and when the decision must be revisited.

Consultant's note

D-09 is an accepted operating exception, not a completed control. If it remains open after 31 July, the CTO should either correct it or record a new decision with a revised basis.

ID	DECISION	POSITION	OWNER	REVIEW TRIGGER
D-07	Release upload service with conditions	APPROVED	Product owner	Any control misses the release date
D-08	Keep signed URLs at 10 minutes	APPROVED	Platform lead	External sharing is introduced
D-09	Accept temporary log-reader group	TIME-BOUND	CTO	31 July or new engineer joins
D-10	Defer low-risk error wording fix	DEFERRED	Engineering lead	Next API maintenance release

ARTEFACT REVIEW 01

Document upload service design review

The review covered one architecture diagram and the associated data flow. It was not a penetration test or a full cloud configuration audit.

Trust boundary

Context
Files move from an authenticated user into object storage before asynchronous processing.

Consultant's advice
Use a quarantine bucket and a processing role that cannot read unrelated customer objects.

Agreed action
Platform lead to update the design and IAM policy before release review.

Content handling

Context
The first draft relied on file extension and MIME type checks at the API.

Consultant's advice
Treat both as hints. Scan the stored object, enforce size limits and render user downloads with a safe content disposition.

Agreed action
Backend lead to add scan-state handling and failure paths.

Recovery

Context
The design described deployment but not how to disable processing safely.

Consultant's advice
Add a queue pause switch, a documented rollback owner and a test that leaves quarantined files unavailable.

Agreed action
Product owner to include rollback evidence in the release record.

ARTEFACT REVIEW 02

AWS access baseline review

The second focused review checked the team's proposed access baseline against current operating needs. It did not inspect every account or resource.

Accepted for now

- One offline break-glass identity
- Manual evidence for the July release only

Not accepted

- Shared administrator credentials
- Permanent broad deployment rights
- Access review without a named owner

CONTROL AREA	OBSERVED POSITION	ADVICE	OWNER
Human administrator access	MFA required except one break-glass user	Store credentials offline and test access quarterly	Platform lead
Production log readers	Shared group has six members	Reduce to named on-call engineers and review monthly	CTO
CI deployment role	Broad write permission in two accounts	Split production role and restrict resource patterns	DevOps lead
Access evidence	Manual screenshots	Export identity and policy records into the release folder	DevOps lead

REMEDIATION TRACKER

Priority work kept in one place

The tracker combines pentest work and advisory actions where they affect the same release decision. It is not a replacement for the team's engineering backlog.

ID	RISK OR FINDING	PRIORITY	OWNER	TARGET	CLOSURE EVIDENCE
R-12	Cross-tenant invoice export	P0	Backend lead	CLOSED	Negative authorisation tests reviewed
R-14	Upload processing role too broad	P1	Platform lead	23 Jul	IAM policy and access simulation
R-15	Malware scan failure path missing	P1	Backend lead	23 Jul	Integration test and queue state
R-16	Production log group over-populated	P2	CTO	31 Jul	Membership export and approval
R-17	Verbose API error wording	P3	Engineering lead	08 Aug	Response sample

MONTHLY PRIORITIES

What the team should do next

The plan is intentionally short. It separates release conditions from useful work that can wait, so the team does not turn every advisory comment into an emergency.

Release authority

The consultant gives a technical position. The client decides whether to release and remains responsible for implementation, testing and operational approval.

Before upload release

- Restrict the processing role
- Implement malware scan failure handling
- Record rollback owner and exercise the pause path

After release

- Reduce production log readers
- Split the CI deployment role
- Improve the API error wording

CHECKPOINT	DECISION OWNER	REQUIRED INPUT	CONSULTANT INVOLVEMENT
Design update	Platform lead	Revised diagram and IAM policy	Focused review
Release readiness	Product owner	Control evidence and rollback record	Challenge session
Post-release review	CTO	Open exceptions and incident signals	Prioritisation advice

ACTIVITY AND ALLOCATION

Where the ten hours went

Transparent time use helps the client decide whether the package still matches the decision load.

Scope control

A full AWS assessment, penetration test, code audit or production change is separately scoped. Extra advisory time starts only after written approval.

ACTIVITY	TIME	WRITTEN OR WORKING OUTPUT
Two working sessions	2.0 h	Decisions, owners and release conditions
Upload design review	2.0 h	Three design observations and follow-up
AWS baseline review	1.5 h	Focused control advice
Pentest closure review	1.0 h	R-12 closure position
Preparation and written report	2.5 h	Monthly advisory report
Between-session replies	0.5 h	Clarifications on upload controls
Remaining allocation	0.5 h	Held for approved July follow-up

NEXT MONTH

Proposed August agenda and responsibilities

The next plan is provisional. It changes if a material incident, deadline or new system enters the agreed scope.

Consultant

- Prepare and challenge the agreed items
- State assumptions and unanswered questions
- Keep decisions and priorities concise

Client

- Send artefacts at least two business days before review
- Name decision owners
- Implement and test approved changes

PROPOSED ITEM	WHY NOW	INPUT NEEDED FROM CLIENT	EXPECTED ADVISORY OUTPUT
Post-release upload review	Confirm controls held in operation	Metrics, incidents and exceptions	Short assurance note
CI deployment role	Broad permission remains open	Current policy and pipeline flow	Focused recommendation
Customer questionnaire pattern	Repeated sales requests	Two recent questionnaires	Answering guide and evidence list

Subject to consultants' availability. The signed engagement letter and agreed monthly scope take precedence over this public sample.