

FICTIONAL SAMPLE DELIVERABLE

# Security Partner - Monthly Assurance Pack

A working assurance pack for an active product team: release challenge, architecture positions, risk ownership and a forward security plan.

|                |                                           |
|----------------|-------------------------------------------|
| PACKAGE        | Security Partner                          |
| PREPARED FOR   | MeridianPay Systems Sdn. Bhd. (fictional) |
| SAMPLE PERIOD  | July 2026                                 |
| REFERENCE      | MA-SAMPLE-SP-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-SP-001                                                              |
| Prepared for       | MeridianPay Systems Sdn. Bhd. (fictional)                                     |
| Scenario           | Payment operations platform with weekly releases and several technical owners |
| Package allocation | Up to 20 advisory hours per month                                             |
| Working rhythm     | Weekly working session when needed                                            |
| Response target    | Initial response within 1 business day                                        |
| 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 ASSURANCE

# Security position for July

The programme can continue its planned release sequence, but the new partner API should not move to production until replay protection and operational ownership are demonstrated.

|                                            |                                       |                                            |
|--------------------------------------------|---------------------------------------|--------------------------------------------|
| <div>4</div> <div>active workstreams</div> | <div>7</div> <div>risks tracked</div> | <div>2</div> <div>release conditions</div> |
|--------------------------------------------|---------------------------------------|--------------------------------------------|

## Release position

CONDITIONAL. The customer portal release may proceed. The partner API remains blocked pending nonce enforcement, alert ownership and a tested credential revocation path.

|                                                                                                                                                                                                  |                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>Security movement this month</div> <div><div>- Portal session fix verified</div><div>- Partner API threat model completed</div><div>- Production access review has named owners</div></div> | <div>Management attention</div> <div><div>- Partner go-live date assumes two open controls</div><div>- One accepted vendor risk expires in August</div><div>- On-call ownership for API abuse alerts is unresolved</div></div> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

PORTFOLIO DASHBOARD

# Workstreams, posture and next decision

The dashboard is a decision aid, not a security score. Red means an agreed decision or control is needed; it does not mean the whole system is insecure.

Use of colour

Green means no current management intervention is needed within this sample period. It is not a guarantee that the workstream is secure or complete.

| WORKSTREAM          | CURRENT POSITION | MOVEMENT              | NEXT DECISION                  | OWNER            |
|---------------------|------------------|-----------------------|--------------------------------|------------------|
| Partner API         | RED              | Threat model complete | Go-live after two conditions   | Product director |
| Customer portal     | AMBER            | Session fix verified  | Close remaining logging action | Engineering lead |
| AWS hardening       | AMBER            | Admin roles reduced   | Approve service role split     | Platform lead    |
| Pentest remediation | GREEN            | Critical item closed  | Retest high items              | Application lead |

RELEASE CHALLENGE

# Partner API go-live conditions

The advisor challenged the release against the abuse cases most likely to create a material operational or customer impact.

|                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Consultant position</b> <ul style="list-style-type: none"><li>- Do not waive replay protection for schedule</li><li>- Manual revocation is acceptable for the first release only if tested</li><li>- Operational ownership is part of the control</li></ul> | <b>Client decision</b> <ul style="list-style-type: none"><li>- Product director owns the go-live call</li><li>- Engineering owns implementation and test evidence</li><li>- Operations owns the alert and revocation procedure</li></ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| CONTROL QUESTION                             | EVIDENCE SEEN                       | POSITION    | REQUIRED BEFORE GO-LIVE                       |
|----------------------------------------------|-------------------------------------|-------------|-----------------------------------------------|
| Can signed requests be replayed?             | Timestamp checked; nonce not stored | NOT READY   | Reject duplicate nonce within validity window |
| Can a partner credential be revoked quickly? | Manual database update documented   | CONDITIONAL | Named operator and tested procedure           |
| Who receives abuse alerts?                   | Alert exists without rota ownership | NOT READY   | Assign on-call owner and escalation path      |
| Is tenant scope enforced?                    | Negative integration tests reviewed | READY       | Keep tests in release evidence                |

## ARCHITECTURE ASSURANCE

# Trust boundaries and hardening decisions

The review focused on changes that affect isolation, privilege and failure handling. It did not attempt to document the entire platform.

## Partner request boundary

**Context**

Signed partner requests enter through the same gateway used by the customer portal.

**Consultant's advice**

Separate policy and rate limits even if the gateway remains shared. Partner trust assumptions are different.

**Agreed action**

Platform lead to create a partner policy set and evidence the deployed rules.

## Asynchronous settlement worker

**Context**

One worker role can read all tenants and write settlement status.

**Consultant's advice**

Split read and write permissions where practical; at minimum restrict resources and record denied-access tests.

**Agreed action**

Cloud engineer to propose the narrower role for review.

## Failure and retry path

**Context**

Retries are automatic but duplicate business actions rely on application checks.

**Consultant's advice**

Use idempotency at the business operation, not only the queue message. Alert on repeated conflict.

**Agreed action**

Application lead to add an idempotency test to release evidence.

RISK AND REMEDIATION

# Maintained risk tracker

The tracker records live technical exposure and the decision around it. Engineering tickets remain in the client's own delivery system.

| ID    | RISK                              | PRIORIT<br>Y | TREATMENT               | OWNER         | DUE OR TRIGGER    |
|-------|-----------------------------------|--------------|-------------------------|---------------|-------------------|
| SP-01 | Partner request replay            | P0           | Mitigate before go-live | API lead      | Before production |
| SP-02 | Alert without on-call owner       | P0           | Assign and test         | Ops manager   | Before production |
| SP-03 | Settlement worker over-privileged | P1           | Restrict role           | Platform lead | 31 Jul            |
| SP-04 | Vendor SSO does not support MFA   | P1           | Accept with expiry      | CIO           | 15 Aug            |
| SP-05 | Portal audit event gaps           | P2           | Add events              | App lead      | 09 Aug            |
| SP-06 | Legacy API error detail           | P3           | Backlog                 | API lead      | Next maintenance  |

QUARTERLY WORKING SESSION

# Identity and production access decisions

The two-hour quarterly session used live access maps to settle ownership and remove ambiguity around privileged access.

### Decision carried forward

The advisor will sample the August privileged review. The client remains responsible for operating the process and correcting access.

| DECISION                  | AGREED POSITION                                            | OWNER         | EVIDENCE                           |
|---------------------------|------------------------------------------------------------|---------------|------------------------------------|
| Production administration | Named roles only; no shared human accounts                 | Platform lead | Role membership export             |
| Break-glass access        | Two sealed identities; quarterly access test               | CIO           | Test record and credential custody |
| Vendor support access     | Time-bound approval per case                               | Ops manager   | Ticket and access log              |
| Review rhythm             | Monthly for privileged roles; quarterly for broader access | System owners | Signed review record               |

FORWARD PLAN

# 30 / 60 / 90 day advisory roadmap

The roadmap keeps the advisor on the decisions that matter instead of letting the retainer become a queue for miscellaneous security requests.

|                                                                                                                                                                                                                               |                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Advisor will concentrate on</b> <ul style="list-style-type: none"><li>- Material releases and architecture changes</li><li>- Priority risks and closure evidence</li><li>- Decisions that cross technical owners</li></ul> | <b>Separately scoped if needed</b> <ul style="list-style-type: none"><li>- Penetration testing</li><li>- Full cloud or code audit</li><li>- Emergency incident response</li><li>- Large compliance evidence programme</li></ul> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| WINDOW     | OUTCOME SOUGHT                | PLANNED WORK                                        | DECISION POINT          |
|------------|-------------------------------|-----------------------------------------------------|-------------------------|
| 0-30 days  | Safe partner API release      | Close replay, alert and revocation conditions       | Go-live position        |
| 31-60 days | Narrower production privilege | Review service roles and privileged access evidence | Approve role changes    |
| 61-90 days | Repeatable release assurance  | Define minimum evidence for material releases       | Adopt release checklist |

ACTIVITY AND GOVERNANCE

# Advisory time, forums and ownership

This sample month used the full allocation. If the decision load stays at this level, the package remains a reasonable fit.

|                                                                                                                                                                                                    |                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Regular forums</b> <ul style="list-style-type: none"><li>- Weekly working session when needed</li><li>- Release challenge for material changes</li><li>- Quarterly two-hour deep dive</li></ul> | <b>Decision ownership</b> <ul style="list-style-type: none"><li>- Advisor states the technical position</li><li>- Named client owner makes the business decision</li><li>- Engineering implements and tests</li></ul> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| ACTIVITY                           | TIME  | PRIMARY OUTPUT               |
|------------------------------------|-------|------------------------------|
| Weekly working sessions            | 4.0 h | Decisions and risk movement  |
| Partner API release challenge      | 4.0 h | Go-live conditions           |
| Architecture and role review       | 3.5 h | Hardening positions          |
| Quarterly working session          | 2.0 h | Identity decisions           |
| Evidence and closure review        | 2.0 h | Tracker updates              |
| Preparation, reporting and replies | 4.5 h | Assurance pack and follow-up |

## NEXT PERIOD

# August agenda and working conditions

The next period begins with the partner API conditions, then moves to privilege and repeatable release evidence.

## Commercial boundary

Subject to consultants' availability. New workstreams, emergency response, testing and implementation are separately scoped. The signed engagement letter takes precedence over this sample.

## Planned advisory work

- Review partner API closure evidence
- Challenge the settlement role design
- Sample the first privileged access review
- Draft minimum evidence for material releases

## Inputs due from client

- Revised API implementation and test results
- Service role policy proposal
- Access review export
- August release calendar