mauvlabs / advisory

FICTIONAL SAMPLE DELIVERABLE

Pentest Report Advisory - Remediation Plan

A worked example showing how six mock pentest findings become a practical remediation sequence, with accountable owners and evidence for closure.

PREPARED FOR	Example SaaS Sdn. Bhd. (fictional)
SYSTEM	Multi-tenant invoice management platform
REPORT DATE	18 July 2026
REFERENCE	MA-SAMPLE-PRA-001
CLASSIFICATION	Sample - Public

ABOUT THIS SAMPLE

Document control and use

Illustrative material only

The client, platform, report evidence, findings and decisions in this document are fictional. This is not a pentest report, formal risk acceptance, legal advice or proof that any system is secure. A real remediation plan must be based on the complete test evidence, the deployed environment and discussions with the people who own the service.

Document reference	MA-SAMPLE-PRA-001
Document owner	Mauvlabs Advisory
Prepared for	Example SaaS Sdn. Bhd. (fictional)
Report type	Pentest report advisory - remediation plan
Version	1.0
Issue date	18 July 2026
Distribution	Public sample
Source report	Mock penetration-test report dated 10 July 2026

Contents

MANAGEMENT VIEW

Executive summary

The mock report contains six valid findings. One finding requires same-day containment because the tester demonstrated access across customer tenants. Three findings should enter the current delivery window. The remaining two can be scheduled, provided the exposure assumptions recorded in this plan remain true.

6	1	3	2
findings reviewed	contain today	fix next	schedule

Consultant's conclusions

- PT-01 is the release blocker for the affected bulk-export capability. Keep the route restricted until the production check and independent retest pass.
- PT-04 was rated medium by the tester but is raised to P1 because administrator and support roles can act across customer tenants.
- PT-05 was rated high but is placed at P2 because the affected PDF function is not reachable through the tested public upload path. Reassess immediately if that assumption changes.
- No risk acceptance is recommended for PT-01 through PT-04. Short deferrals for PT-05 and PT-06 need named owners and dates.

Release recommendation

Do not restore bulk invoice export until PT-01 is verified in the deployed environment and independently retested. Unrelated releases may continue if their change risk is reviewed and they do not weaken the temporary containment.

Immediate business decisions

- Approve the temporary export restriction.
- Nominate one accountable owner for each work package.
- Reserve the original tester for focused retesting.

Incident trigger

- Review relevant access logs for cross-tenant export activity.
- Use the incident process if misuse or unexplained access is found.
- Preserve evidence before routine log retention removes it.

ADVISORY METHOD

How the report was triaged

Report severity describes the tester's assessment of a finding. Remediation priority records the action agreed for this system. The two are related, but they answer different questions.

01	Confirm evidence	Review the affected asset, route, role, proof, preconditions and stated impact.
02	Check exposure	Decide who can reach the weakness and which controls constrain the attack path.
03	Connect findings	Look for shared root causes, repeated access patterns and findings that combine into one scenario.
04	Plan treatment	Set containment, durable fix, accountable owner, target window and closure evidence.

Priority definitions used in this plan

P0	Contain now	Same working day	Credible path to material harm. Reduce exposure before completing the durable fix.
P1	Fix next	Within 10 working days	Exposed weakness or important control gap. Include it in the current delivery window.
P2	Schedule	Within 30 calendar days	Valid issue with reduced immediate exposure or an effective interim control.
P3	Planned hardening	Within 60 calendar days	Complete through normal maintenance and keep the item visible until verified.

Target windows are not a service-level promise

These windows belong to this fictional plan. In a real engagement, the client approves dates after considering release timing, operational constraints and delivery capacity.

WORKING REGISTER

Findings priority map

The original report reference remains the source for technical evidence. This register adds the delivery treatment, owner and closure route agreed during advisory triage.

REF	FINDING	REPORT	PLAN	AGREED TREATMENT	OWNER	CLOSURE
PT-01	Cross-tenant invoice export	Critical	P0	Restrict route today; correct tenant checks	Backend lead	Independent retest
PT-02	Stored script execution in attachment names	High	P1	Encode output; review shared renderer	Frontend lead	Internal check and retest
PT-03	Password reset token can be reused	High	P1	Single-use, short-lived reset tokens	Identity owner	Security review and retest
PT-04	MFA is optional for administrators	Medium	P1	Enforce MFA for privileged roles	IT operations	Configuration and access test
PT-05	Outdated PDF processing library	High	P2	Upgrade and constrain parser path	Platform lead	Version and regression evidence
PT-06	Verbose API error responses	Low	P3	Safe errors with correlation ID	API lead	Deployed response check

Why two priorities differ from report severity

PT-04 raised from medium to P1

- Privileged roles can access several tenants.
- The control protects high-impact administrative actions.
- Identity-provider enforcement is available without application redesign.

PT-05 scheduled at P2

- The vulnerable parser is not exposed to anonymous upload.
- Only authorised users can reach the document workflow.
- The priority must be reopened if either assumption changes.

Status rule

A finding is not closed because a ticket moved to Done. Closure requires deployed evidence and the verification route recorded in this register.

DELIVERY SEQUENCE

Remediation roadmap

The roadmap separates containment from durable correction. It also shows when management input, independent testing or incident handling may be needed.

0-4 hours	Contain the exposed path Restrict the affected bulk invoice export route. Keep the normal single-invoice workflow available. Preserve relevant access logs before routine expiry.	Product owner and backend lead
Same day	Check for misuse Review access logs for cross-tenant export activity. Escalate through the incident process if evidence is found. Confirm the temporary route restriction in production.	Platform lead
0-10 working days	Complete P0 and P1 work Correct tenant enforcement in API and background jobs. Fix stored script execution and password reset reuse. Enforce MFA for every privileged role.	Engineering and IT operations
11-30 calendar days	Complete scheduled remediation Upgrade the PDF processing library. Confirm parser access assumptions remain valid. Prepare the retest evidence pack.	Platform and security owners
31-60 calendar days	Close remaining hardening Replace verbose API responses with safe client errors. Verify all findings and record residual decisions. Feed root causes into engineering standards.	API lead and technical owner

Change control note

The sequence may change if containment affects customers, if log review identifies misuse, or if a proposed fix changes a trust boundary. Record any change to priority, owner or target date in the decision log.

WP-01 / PT-01 / P0

Stop cross-tenant invoice access

Accountable owner	Backend lead
Supporting roles	Product owner, platform lead, original tester
Target window	Contain same day; durable fix within 2 working days
Closure route	Independent retest required

Why this work matters

The tester demonstrated that a tenant administrator could change an identifier and export another customer's invoice data. The endpoint is internet-facing and the result crosses the main customer trust boundary.

Interim containment

- Restrict bulk export for tenant administrators while keeping the normal single-invoice workflow available.
- Confirm the restriction in production and record the deployment reference.
- Review relevant access logs and use the incident process if there is evidence of misuse.

Required correction

- Take the tenant identifier from the authenticated server-side session, never from request data.
- Apply the ownership check inside the database query and the background export job.
- Search related bulk invoice and reporting routes for the same access pattern.
- Keep the temporary restriction until production verification and retesting pass.

Evidence required for closure

- Automated negative tests using accounts from two separate tenants.
- Successful same-tenant export test.
- Production deployment reference and configuration check.
- Focused retest result from the original testing provider.

Recorded decision

The affected export capability cannot be restored until the cross-tenant tests and independent retest pass.

WP-02 / PT-02 / P1

Remove stored script execution from support views

Accountable owner	Frontend lead
Supporting roles	Support application owner, security reviewer
Target window	Within 10 working days
Closure route	Internal verification, followed by focused retest

Why this work matters

The payload runs when a support user opens an attachment record. That role can view several customers, so a successful attack can reach an account with broader access than the submitting user.

Interim containment

- Limit attachment review to the smallest practical support group until the correction is deployed.
- Tell support staff not to open unexpected attachment records from untrusted accounts.
- Do not treat staff awareness as the durable security control.

Required correction

- Encode attachment names at every HTML output point. Do not rely on input filtering as the main control.
- Review the shared attachment component, support console and notification templates.
- Add a restrictive Content Security Policy after checking application dependencies.
- Check whether the same renderer is used for comments, labels or imported metadata.

Evidence required for closure

- Unit tests for the reported payload and common encoding variants.
- Manual checks in customer and support views.
- Response header capture from the deployed environment.
- Retest of every affected renderer, not only the screenshot path.

Recorded decision

The finding stays open until every affected renderer is checked. Fixing one display path is insufficient.

WP-03 / PT-03 AND PT-04 / P1

Tighten recovery and privileged access

Accountable owner	Identity owner
Supporting roles	IT operations lead, application lead, service desk
Target window	Within 10 working days
Closure route	Security review, access test and focused retest

Why this work matters

The findings affect the same control area. A reusable reset token weakens account recovery, while optional administrator MFA increases the consequence if a privileged account is taken over.

Interim containment

- Reduce the reset-token lifetime while the single-use change is prepared.
- Enforce MFA through the identity provider for privileged users where this can be done safely.
- Prepare recovery and break-glass steps before removing exceptions.

Required correction

- Store only a hash of each reset token, use a 15-minute validity period and consume it atomically.
- Invalidate outstanding reset tokens after a password change without logging token values.
- Require MFA for administrator and support roles and remove remembered-device exceptions.
- Monitor break-glass use and alert the nominated system owner.

Evidence required for closure

- A second use of the same reset link is rejected.
- Expired and superseded reset links are rejected.
- Privileged login without MFA is blocked.
- Break-glass use creates the expected log and alert.

Recorded decision

PT-04 is raised from medium to P1 because privileged roles can view or change data across tenants.

WP-04 / PT-05 AND PT-06 / P2-P3

Complete remaining platform hardening

Accountable owner	Platform lead
Supporting roles	API lead, quality engineering, security reviewer
Target window	PT-05 within 30 days; PT-06 within 60 days
Closure route	Version evidence, regression test and production response check

Why this work matters

Both findings are valid, but neither currently provides the clearest route to material harm. The PDF parser is not exposed to anonymous upload, and detailed API errors require an authenticated user. Reassess if either assumption changes.

Interim containment

- Confirm only authorised users can submit documents to the affected parser.
- Keep the parser behind the existing authenticated workflow until the upgrade is complete.
- Restrict detailed errors at the edge where this can be done without hiding operational evidence.

Required correction

- Upgrade the PDF library, pin the corrected version and run document-processing regression tests.
- Record the parser access assumptions in the system notes and threat model.
- Return a generic API error and correlation ID to callers.
- Keep technical error detail in access-controlled server logs.

Evidence required for closure

- Dependency lockfile and deployed version evidence.
- Successful processing of the agreed document test set.
- Access test confirming the parser is not anonymously reachable.
- Production API responses contain no stack or query detail.

Recorded decision

PT-05 remains P2 only while the parser exposure assumption is true. Any architecture change reopens the priority.

CLOSURE CONTROL

Verification and retest plan

A merged change is not closure evidence. Each finding stays open until the deployed behaviour is checked and the nominated verifier records the result.

01	Deployment	The change has reached the agreed environment and the deployment reference is recorded.
02	Original behaviour	The reported behaviour can no longer be reproduced using the agreed test conditions.
03	Nearby cases	Relevant roles, tenants, methods and related routes have been checked.
04	Evidence	Test output, configuration evidence and deployment details are attached to the work item.
05	Independent view	PT-01 is verified by someone other than the person who implemented the fix.

Verification assignments

REF	VERIFIER	WHEN	MINIMUM EVIDENCE
PT-01	Original tester	Required before route restoration	Two-tenant negative and positive test set
PT-02	Internal security review, then tester	After every shared renderer is checked	Stored payload variants in support and customer views
PT-03	Internal security review, then tester	After reset flow reaches production	Reuse, expiry and superseded-token cases
PT-04	IT operations and security reviewer	After MFA enforcement	Privileged login, recovery and break-glass events
PT-05	Platform and quality engineering	After library upgrade	Deployed version and agreed document regression set
PT-06	API owner	After production deployment	Representative error paths with correlation IDs

If the finding remains

Reopen the original work item with the new evidence. Do not create a duplicate simply because the implementation changed. Record what was tested, what still works and who owns the next decision.

HANDOVER

Decision log and responsibilities

The remediation plan is a shared working record. The consultant advises and challenges; the client owns implementation, operational decisions and formal acceptance of residual risk.

ID	DECISION	STATUS	OWNER	CONDITION
D-01	Restrict bulk export immediately	Approved in sample	Product owner	Remove only after PT-01 closure
D-02	Raise administrator MFA to P1	Approved in sample	System owner	Privileged cross-tenant access
D-03	Schedule PDF library at P2	Conditional	Platform lead	Reopen if exposure changes
D-04	Use original tester for PT-01	Required	Engagement owner	Independent assurance needed

Consultant responsibilities

- Review report evidence and technical context.
- Challenge severity, exposure and proposed fixes.
- Prepare priorities, work packages and closure criteria.
- Record decisions from the advisory working session.

Client responsibilities

- Provide the complete report, architecture and system owners.
- Approve priorities, risk treatment and release decisions.
- Implement, test, deploy and operate the changes.
- Arrange retesting and incident handling where required.

Work outside this sample advisory scope

- Running the penetration test or independently retesting the fixes.
- Writing or deploying production code and configuration changes.
- Incident containment, forensic investigation, legal advice or regulatory notification.
- Formal acceptance of risk on behalf of the client or system owner.

Commercial and scheduling note

Subject to consultants' availability. A booking is confirmed only after the scope, schedule and fee are agreed in writing. The signed engagement letter takes precedence over this public sample.

End of sample report