MANAGED SECURITY / FICTIONAL EXAMPLE

Monthly security review

Example Operations LLC — synthetic reporting period

This mock management report demonstrates the format of a recurring security review for a hypothetical 25-device environment. The metrics, issues and operational activities below are fabricated illustrations and should not be understood as actual KITAU service performance.

Coverage snapshot

Measure	Illustrative value	Interpretation
Devices in agreed scope	25	Example inventory baseline
Devices with expected protection	24 of 25	One device requires investigation
Patch baseline compliance	92%	Exceptions remain for planned remediation
High-risk issues open	4	Customer actions or acceptance required
Cloud identity review	Completed	Privileged account changes examined

Executive assessment

The synthetic environment improved patch coverage while one endpoint remains outside the desired protection state. The priority is to investigate the unmanaged device and confirm responsibility for four high-risk exceptions. None of these sample metrics proves that a security control is effective without verification.

Management actions

Illustrative month-end discussion: approve high-risk remediation owners, verify the device inventory with the IT provider and review whether backup restore validation should be scoped as a separate engagement.

OPEN ISSUES / ACTION REGISTER

Track and close the important work

Reference	Severity / status	Owner & next step
MS-014	High / Open	IT owner to enforce MFA on remaining privileged account
MS-018	High / In progress	System owner to approve update window
MS-020	High / Open	IT team to investigate unmanaged endpoint
MS-022	High / Planned	Network owner to review remote-access policy
MS-024	Medium / Accepted	Manager to document exception rationale

Illustrative activity log

Review area	Example activity
Vulnerability management	Reviewed new scanner findings; re-checked known exceptions
Identity protection	Compared privileged access list with approved baseline
Endpoint coverage	Reconciled the 25-device inventory with the management console
Risk reporting	Updated the action register and highlighted overdue decisions

Client-side responsibilities

This format distinguishes observed status from action owners. Unless specifically delegated, KITAU may report and coordinate while customer IT owners authorise and execute patching, account changes, backup restores or emergency containment.

NEXT STEPS / SERVICE BOUNDARIES

Priorities for the next reporting cycle

Proposed 30-day focus

1. Confirm endpoint MS-020 inventory and endpoint protection status. 2. Agree a change window for MS-018. 3. Decide whether MS-024 is an accepted risk. 4. Review MFA exceptions and access restrictions. 5. Evaluate a separately scoped backup restore exercise.

Coverage and escalation boundaries

The proposed starting managed-security service assumes business-hours coordination and periodic review of agreed systems. This example does not represent 24/7 SOC, guaranteed alert triage times, hands-on containment, forensic investigation or a disaster recovery service. Any such commitment must be explicitly documented and supported.

Report quality checklist

Deliverable component	Why it matters
Inventory and coverage	Shows what was and was not monitored
Exceptions and evidence	Explains where unresolved risk remains
Owners and target dates	Turns findings into accountable work
Trends and decisions	Connects monthly activity with business priorities
Service boundary notes	Prevents ambiguity around emergency response

Important disclaimer

This is a template-style fictional sample and not a verified customer report, client testimonial or representation of an existing live monitoring service. The actual cadence, tooling, deliverables and service levels require confirmation in a signed agreement.