ENDPOINT ASSURANCE GROUP

Sample Executive Assurance Summary

Sanitized example of the leadership deliverable produced after technical validation and human review.

PREPARED FOR
Sample Client

PREPARED BY
John Jankowski

ORGANIZATION
[Client Organization]

EMAIL
john@endpointassurancegroup.com

DATE
[Month Day, Year]

VERSION
1.0

Sample only: All organizations, tenant identifiers, counts, findings, and decisions in this document are fictional. This sample demonstrates delivery structure—not a real assessment result.

Executive conclusion

Sample Client has established a functional Intune management foundation, but inconsistent policy ownership, application lifecycle debt, and incomplete device-access enforcement increase operational and security risk. The environment is suitable for controlled optimization; priority actions should focus on ownership, high-impact access controls, deployment reliability, and policy consolidation.

Overall posture	Critical	High	Medium	Low
Managed—improvement required	0	4	11	8

Leadership priorities

Priority	Business significance	Recommended decision
Strengthen managed-device access requirements	Reduces the likelihood that unmanaged or noncompliant endpoints reach sensitive cloud resources	Approve design validation and staged Conditional Access pilot
Establish application lifecycle ownership	Reduces deployment failures, obsolete packages, and unclear remediation accountability	Assign application owners and approve lifecycle standard
Consolidate conflicting and duplicate policy intent	Reduces unpredictable endpoint behavior and support cost	Approve policy rationalization workshop and pilot
Formalize quarterly governance and drift review	Prevents configuration debt from reappearing after remediation	Adopt quarterly assurance cadence with risk ownership

Illustrative top findings

ID	Severity	Finding	Business impact	Recommended action
EAG-001	High	Managed-device access coverage is incomplete	Unmanaged endpoints may retain access paths to business data	Validate exclusions and pilot compliant-device access controls
EAG-002	High	Required application deployments show persistent failure patterns	Users may be unable to perform business processes or receive security tooling	Correct detection/dependency logic and pilot revised packages
EAG-003	High	Overlapping policy settings express conflicting intent	Devices may receive unpredictable effective configuration	Consolidate owners, assignments and settings into governed baselines
EAG-004	High	Administrative role review is not formally evidenced	Excess privilege can persist without accountable recertification	Establish quarterly RBAC review with named approvers

30/90/180-day roadmap

Horizon	Focus	Illustrative actions	Exit evidence
0–30 days	Contain highest risk and establish ownership	Validate CA exclusions; assign finding and application owners; correct critical deployment evidence; preserve rollback	Approved owners, pilot plans, closed critical/high quick wins
31–90 days	Standardize and optimize	Consolidate policies; improve application lifecycle; formalize RBAC and exception review; clean duplicate devices	Pilot results, change records, reduced conflict and failure counts
91–180 days	Sustain and measure	Quarterly drift assessment; KPI review; roadmap refresh; operational knowledge transfer	Baseline comparison, governance minutes, updated risk register

Evidence and qualification

- Technical collection is tenant-bound and read-only.
- Collection limitations and manual validations are explicitly recorded.
- Framework mappings are evidence alignment, not certification.
- Findings require consultant interpretation and client ownership.
- Implementation is separate from assessment and requires approved change control.

Recommended next engagement

Conduct a two-hour remediation planning workshop to confirm owners, dependencies, sequencing, pilot groups, rollback requirements, and the first 30-day change backlog.