SAMPLE DELIVERABLE

Technology Due Diligence

Findings Register & Deal-Model Impact

PREPARED FOR
Illustrative Sponsor, L.P.

TARGET
Meridian Packaging Holdings
Composite; not a real company

ENGAGEMENT
Pre-LOI technology assessment

TIMELINE
3–4 weeks

VERTEX CIO ADVISORY

vertexcio.com
hello@vertexcio.com

SECTION 01

Executive summary

Vertex CIO Advisory was engaged to assess the technology estate of Meridian Packaging Holdings ahead of a proposed acquisition. The assessment covered infrastructure, security posture, identity and access, licensing, vendor relationships, and continuity capability across three facilities and approximately 170 users.

The environment is functional and the business is running. That is not the same as the environment being sound. Ten findings were identified, two of them Critical. The aggregate first-year remediation cost falls in a range of $142,000 to $242,000, of which approximately $95,000 to $150,000 should be treated as non-discretionary within the first 180 days post-close.

None of the two Critical findings appear in the quality of earnings analysis, and neither would be visible from financial statements or a management presentation. Both were identified through direct inspection of the environment.

65 / 100

TECHNOLOGY RISK SCORE · ELEVATED

Material remediation required. Deal proceedable with price or escrow adjustment and a funded 100-day plan. Scoring begins at 100 with per-finding deductions (Critical -8, High -4, Medium -2, Low -0.5) and a 20-point ceiling per category. Scores below 70 indicate remediation cost material to the deal model. Reconciles: 100 - (2×8) - (3×4) - (3×2) - (2×0.5) = 65.

CRITICAL	HIGH	MEDIUM	LOW
2	3	3	2

SECTION 02

Scope & method

The assessment was conducted over three weeks with read-only access to the production environment and interviews with internal IT and the incumbent managed services provider. No changes were made to any system. All collection was performed under signed NDA with material non-public information protocols in place before access began.

In scope

- Active Directory: domain and forest configuration, privileged group membership, account hygiene, password policy, Group Policy inventory
- Server and endpoint estate: hardware age, operating system versions, patch currency, and support status
- Security controls: endpoint protection deployment and configuration, exclusion sets, email security posture, external attack surface
- Identity: M365 tenant configuration, conditional access, MFA coverage across remote access and privileged accounts
- Continuity: backup configuration, retention, offsite replication, documented and tested recovery capability
- Licensing: server, database, and productivity licensing reconciled against available purchase records
- Vendor: managed services agreement terms, SLA definition and measurement, exit provisions
- Documentation: network diagrams, asset inventory, credential management, change history

Out of scope

Application-level code review, ERP business process assessment, and penetration testing were excluded from this engagement. Where findings indicate the need for deeper review, that is stated in the finding.

Method

Collection was performed using a proprietary assessment toolset run from a domain-joined host with a read-only service account, supplemented by external attack-surface testing from outside the network perimeter. Findings were normalized to a common schema — severity, category, finding, evidence — then reviewed manually. Automated collection identifies conditions; severity and deal-model impact are assigned by the assessor, not by the tool.

SECTION 03

Findings register

Ten findings, ordered by severity. Each carries an estimated remediation cost and timeline. Cost ranges reflect third-party labor and hardware at Dallas–Fort Worth market rates and exclude internal staff time.

CRITICAL F-01 INFRASTRUCTURE

Domain controller consolidated with file, print, and ERP database roles

OBSERVED

A single physical host (2016 vintage, out of manufacturer hardware support) runs Active Directory, the primary file share, print services, and the SQL instance backing the ERP. Loss of this host halts all operations. Restore has not been tested against the current backup set since 2024.

IMPACT

Single point of failure for the entire operating environment. A hardware failure or ransomware event produces an outage of days, not hours, with no verified recovery path.

REMEDIATION

Separate roles across virtualized hosts; establish and test a documented restore. 4–6 weeks.

Est. cost: $38,000 – $52,000

CRITICAL F-02 CYBER INSURANCE

Cyber policy renewal contingent on MFA coverage the company cannot evidence

OBSERVED

The current policy application attests to multi-factor authentication on all remote access and privileged accounts. MFA is enforced on the M365 tenant but not on VPN, not on the ERP application, and not on four domain administrator accounts.

IMPACT

Attestation gap exposes the buyer to policy rescission in the event of a claim — the coverage is effectively unpriced. Remediation cost pulls forward into the deal model.

REMEDIATION

Enforce MFA across remote access and privileged accounts; re-attest before renewal. 2–3 weeks.

Est. cost: $6,000 – $11,000

HIGH F-03 ENDPOINT SECURITY

Endpoint protection exclusions applied at drive root

OBSERVED

Antivirus exclusions are configured at the root of the data volume on eleven servers, disabling scanning across the accounting and engineering file shares. The exclusion set predates the current MSP relationship and no documented business justification exists.

IMPACT

The most valuable data in the environment is unmonitored. Standard ransomware tradecraft targets exactly these paths.

REMEDIATION

Scope exclusions to specific process and file paths with documented justification. 1–2 weeks.

Est. cost: $3,000 – $6,000

HIGH F-04 KEY PERSON RISK

Undocumented environment with single-person institutional knowledge

OBSERVED

No current network diagram, no asset inventory, no documented change history. Credentials for the firewall, the ERP database, and three line-of-business applications are held by one internal administrator with no documented handoff.

IMPACT

Departure of one employee converts a manageable environment into a forensic exercise. Materially raises integration cost and timeline.

REMEDIATION

Full environment documentation, credential vaulting, and knowledge transfer. 3–5 weeks.

Est. cost: $14,000 – $22,000

HIGH F-05 LICENSING

Server and database licensing not reconcilable to purchase records

OBSERVED

Nine Windows Server instances and two SQL Server instances are in production. Purchase documentation was located for six server licenses and one SQL license. No Software Assurance and no volume licensing agreement of record.

IMPACT

True-up exposure on audit. Licensing is commonly excluded from QoE scope and lands on the buyer post-close.

REMEDIATION

License reconciliation and remediation purchase. 2–4 weeks.

Est. cost: $25,000 – $60,000

MEDIUM F-06 VENDOR RISK

MSP agreement auto-renews with no termination-for-convenience clause

OBSERVED

The managed services agreement renews annually with 90-day notice and no convenience termination. Response-time SLAs are defined but not measured or reported. No exit or data-return provisions.

IMPACT

Constrains post-close vendor consolidation and removes leverage in renegotiation.

REMEDIATION

Renegotiate at renewal or serve notice. Timing-dependent.

Est. cost: Negotiation-dependent

MEDIUM F-07 INFRASTRUCTURE

Network equipment past end-of-support

OBSERVED

The core switch stack and both edge firewalls reached vendor end-of-support in 2024. No firmware updates or security patches are available. Wireless infrastructure is consumer-grade across two of three facilities.

IMPACT

Unpatchable devices at the network perimeter. Refresh is a capital requirement in year one, not a discretionary upgrade.

REMEDIATION

Network refresh across three sites. 6–8 weeks.

Est. cost: $45,000 – $70,000

MEDIUM F-08 IDENTITY

Stale privileged accounts and oversized administrator groups

OBSERVED

Domain Admins contains fourteen members against an IT headcount of two. Six enabled accounts have not authenticated in over 180 days, including two belonging to former employees. No periodic access review.

IMPACT

Expands the attack surface and complicates identity migration during integration.

REMEDIATION

Privileged access review and account cleanup. 1–2 weeks.

Est. cost: $4,000 – $8,000

LOW F-09 EMAIL SECURITY

SPF configured; DKIM and DMARC absent

OBSERVED

The sending domain publishes an SPF record ending in a soft fail. No DKIM signing and no DMARC policy are published.

IMPACT

Domain is spoofable for business email compromise against customers and vendors.

REMEDIATION

Publish DKIM and staged DMARC. 1–2 weeks.

Est. cost: $2,000 – $4,000

LOW F-10 CONTINUITY

Backup retention below stated recovery objectives

OBSERVED

Local backups retain 14 days; offsite replication retains 30. Management stated a 90-day recovery objective. No documented RTO or RPO exists.

IMPACT

Actual recovery capability is narrower than management believes. Relevant to any ransomware scenario with delayed detection.

REMEDIATION

Extend retention and document RTO/RPO. 2 weeks.

Est. cost: $5,000 – $9,000

SECTION 04

Deal-model impact

The findings translate into three categories of financial consequence. Only the first is typically visible in a quality of earnings analysis.

One-time remediation — year one

Category	Low	High
Infrastructure remediation & network refresh	$83,000	$122,000
Licensing true-up	$25,000	$60,000
Security & identity remediation	$13,000	$25,000
Documentation & knowledge transfer	$14,000	$22,000
Continuity & email security	$7,000	$13,000
Total	$142,000	$242,000

Recurring cost normalization

Current IT operating spend understates a sustainable run rate. The environment carries no budget line for hardware refresh, licensing is under-provisioned, and the MSP agreement is priced below the service level the business actually consumes. A normalized run rate is approximately $85,000 to $110,000 per year above current spend. This is an EBITDA adjustment, not a one-time cost.

Contingent exposure

The cyber insurance attestation gap (F-02) is not a cost until it is a claim, at which point it is the full uninsured loss. The licensing position (F-05) is not a cost until audit. Neither belongs in the base case; both belong in the risk section of the investment committee memo.

RECOMMENDED DEAL TREATMENT

- Price adjustment or indemnity escrow sized to the non-discretionary remediation range of $95,000 to $150,000.
- EBITDA normalization of $85,000 to $110,000 annually for sustainable IT run rate.
- Close condition: MFA remediation (F-02) completed or contractually committed prior to cyber policy renewal.
- Funded 100-day plan with named accountability for F-01 and F-04. These two findings drive integration timeline more than any other factor in the estate.

SECTION 05

100-day remediation sequence

Sequencing is driven by risk reduction per week, not by cost. The order below closes the largest exposures first and defers work that can safely wait.

WINDOW	WORKSTREAM	FINDINGS
Days 1–15	MFA enforcement across remote access and privileged accounts; privileged group cleanup; disable stale accounts	F-02, F-08
Days 1–30	Scope endpoint protection exclusions; verify coverage across all servers	F-03
Days 15–45	Environment documentation, asset inventory, credential vaulting, knowledge transfer	F-04
Days 30–75	Role separation off the consolidated host; virtualization; tested restore	F-01, F-10
Days 45–90	Network refresh across three sites	F-07
Days 60–100	Licensing reconciliation and remediation purchase; DKIM and DMARC publication	F-05, F-09
Day 90+	MSP agreement renegotiation at renewal window	F-06

About this engagement

Vertex CIO Advisory delivers pre-close technology due diligence for private equity sponsors and mid-market strategics acquiring platform and add-on assets between $10M and $250M in enterprise value. Every engagement is fixed-fee and delivered in three to four weeks from data-room access to findings readout. Findings translate directly into deal-model adjustments, escrow language, and funded post-close remediation plans.

Vertex CIO Advisory · vertexcio.com · hello@vertexcio.com