

To: [Name of Management Representative]

From: [Name of Auditor/Security Lead]

Date: [Current Date]

Subject: Management Letter Regarding Third-Party Vendor IT Security Controls

Dear [Name],

We have completed our assessment of the IT security controls governing our third-party vendor relationships. The objective of this review was to ensure that external partners handling [Company Name] data adhere to our security standards and regulatory requirements.

During our review, we identified the following areas that require management's attention:

1. Deficiency in Vendor Due Diligence

It was noted that [percentage/number] of high-risk vendors have not provided updated SOC 2 reports or independent security certifications within the last 12 months.

2. Lack of Right-to-Audit Clause Enforcement

Several contracts lack specific language regarding our right to audit the vendor's physical and digital security infrastructure in the event of a breach.

3. Insufficient Access Revocation Procedures

There is currently no formal automated process to revoke vendor access to internal systems immediately upon contract termination or project completion.

Recommendations:

- Implement a mandatory annual review cycle for all Tier 1 vendor security documentation.
- Update the standard procurement contract template to include robust security and audit requirements.
- Integrate the Vendor Access Management list with Human Resources exit protocols.

We request that management provides a formal response and an action plan to address these findings by [Date].

Sincerely,

[Your Signature]

[Your Title]