Contract Clause Review – Internal Memo

Justification Summary for Company-Issued Agreement (PaySure Ltd.)

This memo summarizes the updates to the company's standard Agreement and the outcome of contractual clause negotiations with PaySure Ltd., a prospective vendor handling sensitive payroll and employee data. The goal was to balance security and compliance requirements with the vendor's operational constraints, while ensuring residual risk remains within acceptable thresholds.

A. Contract Gap Analysis

As part of PaySure Ltd.'s onboarding into the Company's Third-Party Risk Management (TPRM) process, a cybersecurity contract clause review was conducted to validate that the Company-issued agreement sufficiently reflects the required information security and regulatory protections.

The assessment focused on whether the agreement enforces critical risk controls, including those related to access management, incident response, data handling, and vendor accountability. While the contract includes several strong provisions—such as encryption requirements and audit rights—specific gaps were identified that require updates to strengthen the agreement before execution.

Key Observations:

- **Breach Notification Timelines** should be explicitly defined (e.g., 72 hours) to meet incident response and regulatory requirements.
- **Multi-Factor Authentication (MFA)** is not currently mandated for systems handling sensitive data and should be required for privileged access.
- **Subcontractor Controls** are not addressed, leaving supply chain risk unmanaged; clauses should require disclosure and security oversight.
- **Data Deletion and Residency Requirements** need to be added or clarified to ensure appropriate end-of-contract handling and jurisdictional compliance.
- **Cyber Liability Insurance Coverage** should be specified, including minimum coverage amounts, to support risk transfer strategy.

To ensure the agreement aligns with the Company's information security policy, regulatory expectations (e.g., GDPR, OSFI B-10), and industry frameworks (e.g., NIST CSF, ISO 27001), updates were recommended prior to issuing the Agreement to the vendor for review. These revisions ensured appropriate risk allocation and vendor accountability for protecting Company Data throughout the engagement lifecycle.

B. Negotiations

Overview of Negotiated Clauses

Clause	Vendor Objection Summary	Risk Level
Breach Notification	Could not commit to 72 hrs outright	Language revised to "within 72 hours of confirmation" to preserve urgency and legal defensibility
MFA	Not deployed org-wide	Scoped requirement to systems accessing Company Data to maintain essential control
Subcontractor Oversight	Limited disclosure due to confidentiality	Revised to require disclosure only for subcontractors with logical/data access
Data Deletion	Standard retention is 90 days	Accepted 30-day window with carveout for regulatory or audit requirements
Cyber Insurance	Coverage under $1M, renewal pending	Approved temporary $500K minimum, increasing to $1M at next renewal
Security Training	No formal annual program	Required at least basic annual training for personnel accessing Company Data

C. Risk Position

Each revised clause was reviewed and adjusted with the following principles:

- Preserve coverage of critical risk domains (access, incident response, data handling).
- Allow operational flexibility without sacrificing core security outcomes.
- Ensure enforceability and audit defensibility under OSFI B-10, GDPR, and Company policy.

D. Next Steps

- Finalize contract with updated clauses.
- Monitor vendor adherence during onboarding and periodic reassessment.
- Flag any non-compliance during contract lifecycle for risk re-evaluation.