TPRM INTAKE FORM

Field	Response Type	Purpose	VENDOR	
Vendor Name	Free Text	Identify the third party	PaySure Ltd.	Score
Business Unit Requesting	Free Text	Track internal owner	HR	
Contact Person (Internal)	Free Text	Escalation / clarification	Carla James	
Contact Person (Vendor)	Free Text	Assessment follow-up	Rita Adams	
Description of Services Provided	Free Text	Understand scope of service	Payroll system	
Will the vendor access our network/systems?	Yes / No	Data/system access = High impact factor	No	1
Will the vendor process/store data?	Yes / No	If yes, triggers further classification	Yes	
What type of data is involved?	Multiple select	e.g., PII, PHI, PCI, Internal, Public	Employee PII, Financial	3
Will the vendor access sensitive data?	Yes / No	Helps determine data sensitivity score	Yes	3
Will they integrate with critical systems?	Yes / No	Vendor criticality = higher tier	No	3
Is this vendor the sole provider?	Yes / No	Supply chain dependency	No	1
Would a disruption impact business ops?	Yes / No	Business criticality	Moderate disruption	3
Is this vendor customer-facing?	Yes / No	Reputational risk	No	1
Does the vendor have known breaches/lawsuits?	Yes / No	Used to flag reputational/operational history	None	1
Are subcontractors involved?	Yes / No	Introduces supply chain/4th-party risk	No	3
Planned Contract Start Date	Date	Useful for scheduling assessment	01-May-25	
Requested Go-Live Date	Date	Prioritize by urgency	20-Sep-25	
		SCORE		19
		TIER		MEDIUM RISK

INHERENT RISK SCORING GUIDE

Question	Risk Factor	Scoring Logic
Will the vendor access our network/systems?	System Access	Yes = 3, No = 1
Will the vendor process/store data?	(Trigger only)	No score; enables data sensitivity scoring
What type of data is involved?	Data Sensitivity	PII/PHI/PCI = 3
		Internal = 2
		Public = 1
Will the vendor access sensitive data?	Data Sensitivity (New)	Yes = 3, No = 1
Will they integrate with critical systems?	Vendor Criticality	Yes = 3, No = 1
Is this vendor the sole provider?	Vendor Criticality (New)	Yes = 3, No = 1
Would a disruption impact business operations?	Business Impact	Major = 3, Moderate = 2, Minimal = 1
Is this vendor customer-facing?	Reputational Exposure	Yes = 3, No = 1
Known breaches or legal issues?	Reputational Exposure	Confirmed breach, regulatory action, lawsuit = 3
		Reputational issue / minor privacy concern = 2
		No known issues = 1
Are subcontractors involved?	4th Party/Subcontractor Risk	Yes = 3, No = 1

NEW RISK TIER LOGIC

Total Score (out of 30)	Assigned Tier	Guidance
21 – 27	High	High sensitivity, access, or criticality – requires full due diligence
13 – 20	Medium	Moderate risk – questionnaire and targeted controls review required
9 – 12	Low	Minimal exposure – minimal assessment required, standard controls acceptable

Section	Question	NIST CSF	ISO/IEC 27001:2022	Sample Responses	Score
Access Control Policy	Do you have a documented access control policy?	PR.AC-1	A.9.1.1	Yes, ISO 27001 aligned	1
	How often is your policy reviewed?	ID.GV-1	A.5.1.2	Annually	1
	How often are entitlements evaluated?	PR.AC-4	A.9.2.5	Quarterly	0.5
	Are access rights adjusted or revoked on termination?	PR.AC-4	A.9.2.6	Yes, automated via IAM	0.5
Asset Management Policy	Do you have a documented asset management policy?	ID.AM-1	A.8.1.1	Yes, but light on non-IT assets	0
	Please provide link to supporting documentation	ID.AM-1	A.8.1.2	Shared	0
	How often is your policy reviewed?	ID.GV-1	A.5.1.2	Bi-annually	0.5
Acceptable Use Policy	Do you have a documented acceptable use policy?	PR.AC-1	A.9.3.1	Yes, required for all employees	1
	Are all personnel required to sign an AUP?	PR.AT-1	A.6.2.1	Yes, but not enforced during onboarding	0.5
App Security Policy	Do you have a documented application security policy?	PR.IP-1	A.14.2.1	Yes, based on OWASP	1
	Is application input/output validated?	PR.IP-3	A.14.2.5	Partial – input validated, output not consistently	0.5
	Are app network boundaries protected by firewalls?	PR.AC-5	A.13.1.1	Yes	1
	Do you perform vulnerability assessments? How often?	DE.CM-8	A.12.6.1	Yes, quarterly scans	0.5
	Do you perform penetration testing? How often?	DE.CM-8	A.5.36	Yearly	0.5
	Is the service hosted in the cloud?	ID.AM-4	A.13.2.1	Yes – AWS	0
	Where are the data centers located?	ID.AM-4	A.13.2.1	US and EU	0
	Do you support any types of SSO?	PR.AC-1	A.9.4.2	Yes – SAML & OAuth	1
Backup Policy	Do you have a documented backup policy?	PR.IP-4	A.12.3.1	Yes	1
	How long are backups retained?	PR.IP-4	A.12.3.1	30 days	0.5
	Are backups encrypted?	PR.DS-1	A.10.1.1	Yes – AES 256	1
BCDR Policy	Do you have a documented BCDR policy?	PR.IP-9	A.17.1.1	Yes	1
	How often is your policy reviewed?	ID.GV-1	A.5.1.2	Not defined	0
	Is your infrastructure supported by redundant systems or failover capabilities? How regularly are they tested	RC.IM-1	A.5.30	Not comprehensive, every 2 years	0.5
Change Mgmt Policy	Do you have a documented change management policy?	PR.IP-3	A.12.1.2	Yes	1
	Is code validated before production deployment?	PR.IP-1	A.14.2.9	Yes – with peer review + CI/CD tests	1
	Is version control used?	PR.IP-3	A.14.2.2	Yes – GitHub enterprise	1
Code of Conduct	Do you have a documented code of conduct policy?	ID.GV-2	A.5.1.1	Yes	1
Data Deletion Policy	Do you have a documented data deletion policy?	PR.DS-3	A.8.10	Yes, includes secure deletion	1
	Will data be deleted at contract termination?	PR.DS-3	A.8.10	Only upon request	0.5
Encryption Policy	Do you have a documented encryption policy?	PR.DS-1	A.10.1.1	No, not formally defined	0
	Is data encrypted at rest?	PR.DS-1	A.10.1.1	Yes – AES 256	1
	What method is used to encrypt data in transit?	PR.DS-2	A.10.1.1	TLS 1.2 / 1.3	1
InfoSec Policy	Do you have a documented information security policy?	ID.GV-1	A.5.1.1	Yes – ISO 27001 driven	1
	Are background checks performed?	PR.AT-2	A.7.1.1	Yes – for all new hires	1
	Is annual security awareness training conducted?	PR.AT-1	A.6.3.2	Offered but not mandatory	0.5
Incident Response Policy	Do you have a documented incident response policy?	RS.RP-1	A.5.25	Yes	1
	Does the IR policy contain external communications and public relations protocols?	ID.GV-3	A.5.12	Not yet, in development	0.5
	Does the IR policy contain a data classification matrix?	RS.RP-1	A.5.25	Not yet, in development	0.5
Password Policy	Do you have a documented password policy?	PR.AC-1	A.9.4.3	Yes	1
	Do you require complex passwords?	PR.AC-1	A.9.4.3	Yes – NIST SP 800-63 compliant	1
	Is MFA required where available?	PR.AC-7	A.9.4.2	No	0
Privacy Policy	Do you have a documented privacy policy?	ID.GV-1	A.5.1.1	Yes	0
	Do you collect PHI?	ID.RA-1	A.8.1.1	No – but PII is collected	1
Compliance & Certifications	Evidence of third-party security audit in the past 12 months?	ID.RA-3	A.5.36	Yes	1
	Evidence of all relevant certifications	ID.GV-3	A.5.36	Partially	0.5
Third-Party Management	Do you have a documented third-party management policy?	ID.SC-4	A.5.19	Yes, basic vendor onboarding checklist	0.5
	Do third parties have access to customer PII?	ID.SC-4	A.5.19	Yes – but with contracts + limited access	0.5
	How do third parties comply with your security standards?	ID.SC-4	A.5.19	Through contractual obligations	0.5
				TOTAL	**31.5**

Control Effectiveness	**0.70**
Residual Risk = Inherent Risk × (1 - Control Effectiveness)	**5.70**

Residual Risk Tiering – Score-Based Model

Residual Risk Score	Tier	Treatment Guidance
>12.0	**High**	Unacceptable. Escalate for waiver, remediation, or disqualify vendor.
>5.0 – 12.0	**Medium**	Review needed. Require remediation, documentation, or risk mitigation.
0.0 – 5.0	**Low**	Acceptable. Proceed with onboarding and standard monitoring.

IDENTIFIED GAPS FROM QUESTIONNAIRE

Control Area	Gap Description
Asset Management	No formal policy in place; no defined owner — major governance deficiency.
Acceptable Use	Policy not consistently enforced during onboarding.
App Security	Partial input validation; vulnerability testing only once a year — low maturity.
BCDR	Infrequent testing (biannually); no clearly defined review process.
Infrastructure Resilience	Redundancy/failover tested only every 2 years — insufficient for high-availability services.
Data Deletion	No automation; deletion only on request at contract termination.
Incident Response	No data classification protocol; IR policy still under development.
Training	Security awareness training offered, but not mandatory.
Vendor Oversight	Only basic onboarding checklist; no formal subcontractor access review or reassessment.
Compliance & Certification	Limited evidence of formal certifications or audits (e.g., SOC 2, ISO 27001 not confirmed).

Final Risk Treatment Record for *PaySure Ltd.*

Field	Entry
Inherent Risk Score	19
Residual Risk Score	5.70
Residual Risk Tier	**Medium**
Primary Risk Areas	Asset Management: No policy or ownership; major governance deficiency.
	Incident Response: IR policy incomplete; lacks classification protocol.
	Compliance & Certification: No evidence of SOC 2, ISO 27001, or equivalent controls.
	Vendor Oversight: No subcontractor reviews; minimal onboarding diligence.
Risk Treatment Decision	**Remediate**
Justification	Multiple baseline control deficiencies that pose unacceptable regulatory and operational risks, impacting confidentiality and availability.
Risk Owner / Approver	Carla James (HR)
Required Remediation Actions	Develop and approve a formal asset management policy. Assign ownership and implement an inventory process with periodic reviews.
	Finalize the IR policy with defined roles, escalation paths, and classification-based response triggers. Conduct a tabletop incident response exercise.
	Request SOC 2 Type II, ISO 27001, or equivalent certifications. If unavailable, require a third-party audit and documented remediation roadmap before onboarding.
	Implement a formal third-party risk management lifecycle, including subcontractor assessments, continuous monitoring, and periodic reassessments.
Remediation Deadline	**Asset Management - 30 days**
	Incident Response - 30- 45 days
	Compliance & Certification - 60-90 days
	Vendor Oversight - 45-60 days
Final Status	**Conditionally Approved – Pending Remediation**