SaaS Vendor Vetting Checklist

A lightweight, mandatory checkpoint for every new SaaS application, cloud service, or open-source tool — completed before it touches production data.

SUPPORTS	OWNER	COMPLETED BY	TIME TO COMPLETE
Ch. 7 (§7.1), Ch. 8 (Template 1B), Days 11–20 of the 90-Day Roadmap	IT Lead / Operations Lead	Business sponsor requesting the tool	About 20–40 minutes per vendor

How to use this checklist

Architecture Drift starts when technology changes faster than governance. This checklist keeps every new tool visible, owned, and governed from day one — without slowing the business down.

1. **Part 1 –** The business sponsor describes the tool and the data it will hold.
2. **Part 2 –** Answer the Four Essential Questions. These are required for every tool, every time.
3. **Part 3 –** Complete vendor assurance checks only if the tool will hold Internal or Confidential data.
4. **Parts 4–5 –** Record the risk decision, then complete onboarding so the tool enters the governance lifecycle.

Scaling down: a solo practice or very small team can complete this alone — one person, one checklist, four questions — as long as it happens before the tool is used with real customer or client data.

PART 1 REQUEST DETAILS

Completed by the business sponsor.

Vendor / SaaS name		**Product / plan tier**	
Vendor website		**Request date**	
Business sponsor		**Department**	
Estimated users		**Annual cost**	
Billing owner		**Target go-live**	

Business case justification	*What problem does this solve, and what happens if we don't adopt it?*
Existing alternative?	☐ No approved tool does this ☐ An approved tool could do this: _____
Replaces an existing tool?	☐ No ☐ Yes — tool being retired: _____ (add to offboarding plan)
Deployment type	☐ Vendor-hosted SaaS ☐ Self-hosted / on-premises ☐ Open-source (self-managed)

Data types ingested	☐ None / public only ☐ Customer personal data (PII) ☐ Employee / HR records
	☐ Financial / payment data ☐ Health information (PHI) ☐ Intellectual property
	☐ Passwords / credentials / API keys ☐ Other: _____

Highest data classification	☐ **Public** ☐ **Internal** ☐ **Confidential**
Integrations / access	*What other systems will this connect to, and what access will it be granted (read, write, admin)?*

PART 2 THE FOUR ESSENTIAL QUESTIONS

Required for every tool. Any "No" must be resolved, or documented as an exception with compensating controls in Part 4.

#	Check	Response	Evidence / Notes
2.1	**Encryption Verification — at rest** Does the provider encrypt stored data (e.g., AES-256)? Check the vendor's security page, trust center, or SOC 2 report.	☐ Yes ☐ No ☐ N/A	
2.2	**Encryption Verification — in transit** Is all traffic encrypted (TLS 1.2 or higher), including APIs and mobile apps?	☐ Yes ☐ No ☐ N/A	
2.3	**Identity Integration (SSO)** Does the platform integrate with our central identity provider (e.g., Microsoft 365 / Entra ID or Google Workspace)? Separate accounts complicate offboarding and create orphaned access. Note if SSO requires a higher-priced plan.	☐ Yes ☐ No ☐ N/A	
2.4	**Multi-Factor Authentication (MFA)** Can MFA be enforced for all users — not just offered as optional? Password-only access weakens our overall security posture.	☐ Yes ☐ No ☐ N/A	
2.5	**Patch Management** Hosted SaaS: does the vendor automatically apply security updates? Self-hosted or open-source: who is our named internal owner for patching and maintenance?	☐ Vendor-managed ☐ Internal owner ☐ Unassigned	

Internal patch owner (if self-hosted / open-source): _____

PART 3 VENDOR ASSURANCE

Required when the highest data classification is Internal or Confidential. Skip for Public-only tools.

#	Check	Response	Evidence / Notes
3.1	**Independent security attestation** SOC 2 Type II (or ISO/IEC 27001) report available and dated within the last 12 months? Record the report date and any noted exceptions.	☐ SOC 2 Type II ☐ ISO 27001 ☐ None	
3.2	**Breach notification window** How quickly does the contract or terms require the vendor to notify us of a security incident? Record the commitment (e.g., 72 hours).	_____ hours	

#	Check	Response	Evidence / Notes
3.3	**Sub-processors** Does the vendor publish its sub-processors (third parties that handle our data)? Are any in high-risk locations?	☐ Yes ☐ No ☐ N/A	
3.4	**Data location** Where is our data stored and processed? Does this meet customer contracts or regulatory requirements?	☐ U.S. ☐ EU ☐ Other	
3.5	**Data ownership & exit** Do we retain ownership of our data? Can we export it in a usable format and have it deleted (with confirmation) when we leave?	☐ Yes ☐ No ☐ N/A	
3.6	**Required agreements** Health data (PHI) → signed Business Associate Agreement (BAA). Personal data subject to privacy laws → Data Processing Agreement (DPA). Confirm exact requirements with qualified counsel.	☐ BAA ☐ DPA ☐ N/A	
3.7	**Administrative control** Is at least one admin / owner account held by our company (not solely by the vendor, a contractor, or the MSP)? Can we assign role-based permissions?	☐ Yes ☐ No ☐ N/A	
3.8	**Audit logging** Does the platform log user sign-ins, admin changes, and data exports — and can we access those logs?	☐ Yes ☐ No ☐ N/A	
3.9	**Availability & backup** Is there an uptime commitment (SLA) and a documented backup / recovery approach that fits how critical this tool will be?	☐ Yes ☐ No ☐ N/A	

PART 4 RISK DECISION & SIGN-OFF

Completed by the IT Lead / Operations Lead with the Business Owner.

Risk tier	☐ **Low** — Public data only; all Part 2 answers are "Yes". ☐ **Moderate** — Internal data; Part 2 complete; Part 3 has no material gaps. ☐ **High** — Confidential data, write/admin access to core systems, or any unresolved "No". **Complete a Vendor Risk Assessment (Template 2D) and add an entry to the Enterprise Risk Register.**
Decision	☐ Approved ☐ Approved with conditions ☐ Rejected ☐ Deferred pending information
Conditions / compensating controls	
Exception expiry / re-review date	

Enterprise Risk Register ID (if High)	

Role	Name	Signature	Date
Business Sponsor			
IT Lead / Operations Lead			
Business Owner (risk sign-off)			

PART 5 POST-APPROVAL ONBOARDING

Approval is the beginning of the tool's governance lifecycle, not the end. Complete before go-live.

	Action	Owner	Date Done
☐	**Add to the Master Asset Register (Template 1A)** Record Asset ID, Asset Type (SaaS / Cloud / On-Prem), assigned owner, and data classification.		
☐	**Assign a named business owner** The person accountable for the tool's use, cost, and access reviews.		
☐	**Document admin access and store credentials securely** Record who holds admin / root access; store break-glass credentials in the company password manager.		
☐	**Connect SSO and enforce MFA for all users** Provision users through the identity provider rather than local accounts wherever possible.		
☐	**Add to the employee offboarding checklist** So access is revoked when someone leaves — no orphaned accounts.		
☐	**Update affected Living Documents** Unified System Security Plan if controls change; Enterprise Risk Register if a risk or exception was recorded.		
☐	**Add to the Monthly GRC Heartbeat review** Confirm the tool is still secure, necessary, and properly governed.		
☐	**Set the renewal / re-vetting date** Re-vet at renewal, at least annually, or when data types or access scope change.		

REGISTER SUMMARY LINE

Carry this one-line summary into your vendor log or Master Asset Register notes.

Vendor / SaaS Name	Business Case Justification	Data Types Ingested	SOC 2 Type II	MFA / SSO Support	Risk Sign-off Status
			☐ Yes ☐ No	☐ Yes ☐ No	

Monthly GRC Heartbeat: catch unvetted tools

Once a month, the IT Lead / Operations Lead audits corporate expense reports, card statements, and single-sign-on (SSO) integration logs. Any SaaS subscription or connected app that does not appear in the Master Asset Register goes through this checklist — or gets shut off.

Generative AI accelerator

Prompt: *"Analyze the attached privacy policy and security documentation for [Insert Vendor Name]. Identify their data encryption mechanisms, sub-processor profiles, and breach notification windows. Populate the SaaS Vendor Vetting Checklist with your findings, and flag any item you could not verify from the documents."*

Use public vendor documents only. Redact sensitive internal details first, and have a person verify every AI-generated answer before sign-off.

Automation option: trigger this prompt automatically when a new software purchase request is submitted in your ticketing or project management system.

This checklist is a practical governance tool, not legal advice. Regulatory and contractual requirements vary by industry and jurisdiction; confirm exact obligations with qualified counsel. Adapt this template freely to fit your organization's approval process.