

VENDOR SECURITY AUDIT

version 2026.1

This checklist should be used to help evaluate the risk for using a new vendor/product or service. If you dont know the answer mark is as no, general rule is scoring below 50% their is too much risk, 50-80% the business needs to make a decision, 80% or above safe to approve.. Important to remember any new vendor/product or service should meet all internal business requirements.



OVERVIEW

Vendor/Product/Service			
Person Requesting Access			
Date of Request		Date Required	
What is the intended use			
What Information will it store			
Why do you need this			

OUTCOME

Outcome: (Approved / Declined)			
Completed By		Approved By	
Score (Count No of Yes + N/A)		Percentage	
Reason Approved / Declined			
Comment			

VENDOR SECURITY AUDIT



VENDOR BUSINESS CONTINUITY / DISASTER RECOVERY	Yes	No	N/A
Vendor has a business continuity / disaster recovery plan .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor incorporates Denial-of-Service & other cyber-attacks as part of their business continuity plan. <i>(Important for SaaS)</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor has checked / updated the plan in the last 12 months .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comment			

VENDOR ORGANIZATIONAL SECURITY	Yes	No	N/A
Employees of vendor complete routine cybersecurity training.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor has a formal change control process for IT.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor is able to provide a company security rating .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor is able to provide a history of data breaches (if any).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor has an adequate password policy (MFA Required)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comment			

VENDOR SECURITY AUDIT



VENDOR GENERAL SECURITY	Yes	No	N/A
Vendor installs antivirus software on systems & endpoints.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor routinely patches systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor invests in data protection & security controls .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor restricts physical access to core processing systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor has a process for secure disposal of equipment.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Employees have unique login ID's when accessing data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor continuously monitors security controls to protect cybersecurity incidents.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor has a process to remediate newly found risks .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comment			

VENDOR SECURITY AUDIT



VENDOR NETWORK SECURITY	Yes	No	N/A
Vendor protects network boundaries using firewalls .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor regularly performs network vulnerability scans .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor uses an IDS or IPS on their network.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor's remote users are required to use VPNs when accessing vendor's systems.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor protects wireless networks (if applicable).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comment			

VENDOR SYSTEM SECURITY	Yes	No	N/A
Vendor has verified backup & recovery process .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor uses access control (Ex: RBAC).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor restricts systems that contain sensitive data to only authorized users.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor securely collects, stores, or transmits PII (if applicable).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor has mitigations in place for web application exploits such as SQL Injection & XSS scripting attacks (if applicable).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comment			

VENDOR SECURITY AUDIT



VENDOR AUDITING / REPORTING / REGULATIONS	Yes	No	N/A
Vendor Company is registered in an approved country	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data is stored in SA / Europe or other approved location	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor has had an IT audit in the past 12 months.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor is able to provide IT Audit test results .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor has had a penetration test in the past 12 months.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor is able to provide penetration test results .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor is able to provide an IT system outline .	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor complies with any necessary governmental regulations (POPIA/GDPR HIPAA, PCI-DSS, etc. if applicable).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vendor has industry standard certifications (if applicable).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comment			



