



SAMPLE VENDOR REVIEW

Vendor Security Review

A sample vendor-security assessment showing business context, data handling, control review, gaps, risk decision, approval, and review triggers.

Vendor Security Review

A documented, proportionate review of a fictional SaaS provider that processes company and customer information.

Vendor profile	Vendor: Northstar Support Cloud (fictional) • Service: customer support and knowledge-base SaaS • Business owner: Customer Operations • Review type: initial onboarding
----------------	---

Review snapshot

Business criticality High Used for customer support	Data sensitivity Moderate Customer contact + ticket data	Overall residual risk Medium Approval with actions	Next review 12 months Or material change
--	---	---	---

Service and data profile

Area	Assessment
Business purpose	Central platform for customer tickets, support history, and knowledge-base content.
Data handled	Customer names, business email addresses, ticket content, product-usage context, and internal support notes. No payment-card data approved for storage.
Access model	SSO preferred; role-based support access; named administrator accounts; least-privilege review required.
Hosting / processing	Vendor states that service is cloud hosted in the United States; subprocessors listed in vendor documentation.
Business dependency	High. Loss of availability would delay customer support and reduce service visibility.

Security control review

Control area	Vendor response / evidence	Assessment	Follow-up
Authentication	Supports SSO and MFA for administrative users; customer to configure.	Acceptable	Enable SSO/MFA before production use
Encryption	Vendor documentation states encryption in transit and at rest.	Acceptable	Record supporting documentation
Access control	Role-based roles available; customer admin controls access.	Acceptable	Complete quarterly access review
Incident notification	Contractual notification commitment: without undue delay after confirmed incident.	Needs clarification	Confirm defined notification window
Subprocessors	List published; includes cloud hosting and email delivery providers.	Acceptable	Review annually and upon material change
Availability / recovery	Service status page and recovery documentation available.	Needs clarification	Confirm recovery objectives for critical support operations

Control area	Vendor response / evidence	Assessment	Follow-up
Data retention / deletion	Deletion process documented; customer configuration options available.	Acceptable	Confirm retention setting before launch

Identified gaps and risk decision

Gap	Risk	Decision / compensating control	Owner	Due
No explicit maximum breach-notification period in standard terms	Delayed awareness may affect response and customer obligations	Obtain contractual clarification or document acceptance based on data sensitivity and use case	Operations Lead	Oct 28
Recovery objectives not confirmed	Support disruption could last longer than operationally acceptable	Obtain RTO/RPO statement; document alternate support process	Customer Operations	Oct 28
SSO not enabled at onboarding	Unauthorized or unmanaged access to vendor account	Enable SSO/MFA and document admin access owners before go-live	IT / Security	Oct 14

Approval decision

Approved with conditions. The vendor may be used after SSO/MFA is enabled and the designated owners resolve or formally accept the identified notification and recovery gaps. No payment-card or highly sensitive regulated data may be placed in the service without a new review.

Approval and evidence

Record	Value
Business owner approval	Customer Operations Director — approved subject to conditions
Security review	Security Owner — medium residual risk accepted with treatment plan
Evidence retained	Security questionnaire, vendor trust documentation, subprocessors, contract notes, approval record, and follow-up actions
Next review trigger	Annual review, material change in data processing, material incident, or major contract/service change