AVENLOFT SYSTEMS GROUP

Governance, Risk & Compliance

LABLIST CASE FILE | PROJECT 3

CONDUCT A THIRD-PARTY VENDOR RISK ASSESSMENT

CASE ID

GRC-TPRM-003

ASSIGNED BY

Aaron Bell, Director - Governance, Risk & Compliance

ISSUED

October 12, 2026

YOUR ASSIGNMENT

Review an existing SaaS vendor before contract renewal. Assess the relationship, evidence, gaps, and conditions for continued use.

DELIVERABLES

- Vendor risk assessment
- Findings / remediation tracker
- Vendor decision memo

Fiction notice: Avenloft, CobaltCedar, all people, records, terms, metrics, reports, and events in this packet are fictional. Reserved example domains are used where applicable.

Assignment Brief

To: Junior GRC Analyst

From: Aaron Bell, Director - Governance, Risk & Compliance

Business owner: Lena Ortiz, VP, Customer Success

Procurement: Noah Grant, Director, Procurement

Subject: Third-Party Security Review - CobaltCedar SupportLens Renewal

Due: October 23, 2026

During the September risk review, GRC identified that an inexpensive Customer Success analytics service had been receiving periodic support-ticket exports without a formal security assessment. The vendor was originally routed outside security review because annual spend fell below the procurement threshold. Its contract renews on November 1.

Leadership wants a documented third-party risk assessment before renewal. Your task is to understand what Avenloft sends to the vendor, determine the vendor relationship's criticality, evaluate the evidence provided, identify material gaps, rate the risks using Avenloft's established method, and recommend whether the relationship should continue.

Analyst rule	A questionnaire answer is not automatically evidence, and a SOC 2 report is not a blanket statement that a vendor is “secure.” Use each artifact for what it actually supports, note what remains unknown, and connect gaps to Avenloft's specific exposure.

Required Deliverables

- Vendor risk assessment: relationship profile, criticality, evidence review, material risks, controls, and residual risk.
- Findings and remediation tracker: gaps, required actions, owners, target dates, and status.
- Vendor decision memo: Renew, Renew with Conditions, Pause / Remediate, or Exit, with monitoring and reassessment expectations.

Assessment Boundaries

- Assess the existing CobaltCedar SupportLens relationship, not every product or service the vendor may offer.
- Use supplied evidence and authoritative NIST references. Do not invent certifications, breaches, legal duties, or contract rights.
- You are not performing legal review. Contract and privacy issues that require counsel should be identified for Hannah Kim.
- More than one final recommendation can be defensible if the evidence, risk ratings, and conditions support it.

Why This Review Exists

Avenloft's September risk assessment recorded OBS-05 - Vendor review classification gap. The procurement workflow required security review primarily when annual spend exceeded a threshold. That allowed a lower-cost analytics vendor to receive customer-support data without the questionnaire, architecture review, or formal risk rating normally expected for sensitive-data vendors.

Noah Grant has now routed the relationship to GRC before renewal. The case is deliberately retrospective: the service is already in use, so your recommendation has to account for both current exposure and the practical cost of changing the relationship.

Avenloft fact	Current case context
Service owner	Customer Success - Lena Ortiz
Vendor spend	$18,600 annually; below the old spend-based security-review threshold
Renewal date	November 1, 2026
Business use	Analyze closed support cases for product themes, response trends, escalation patterns, and account-level support volume
Data sensitivity	Customer business contact information and support-case content; ticket text can contain customer-provided technical details
System access	No direct access to Avenloft production, endpoints, or Salesforce; data is exported and uploaded to the vendor
Operational dependency	Useful for reporting and planning, but Avenloft Relay and frontline support can operate without the service

People Already Established in the Avenloft Environment

Name	Role in this review
Aaron Bell - Director, GRC	Coordinates assessment, challenges evidence, records residual risk, and prepares the recommendation.
Lena Ortiz - VP, Customer Success	Business owner for the support workflow and relationship.
Noah Grant - Director, Procurement	Owns renewal workflow and vendor onboarding process.
Hannah Kim - General Counsel & Privacy Lead	Reviews contract, privacy, notification, and data-handling terms when needed.
Maya Chen - CISO	Escalation point for High / Very High residual cybersecurity risk.

How Avenloft Classifies Third Parties

The old procurement rule relied too heavily on annual spend. For this review, Avenloft is using a risk-based classification approach informed by the supplier-criticality and due-diligence outcomes in the NIST Cybersecurity Framework 2.0 supply-chain category.

NIST CSF 2.0 calls for suppliers to be known and prioritized by criticality, for due diligence before formal relationships, and for supplier risks to be understood, recorded, assessed, responded to, and monitored over the relationship lifecycle. The implementation examples emphasize factors such as data sensitivity, access to systems, and importance of the service to the organization.

Factor	Questions to consider
Data	What Avenloft information does the third party receive, store, transmit, or derive? How sensitive would disclosure or misuse be?
Access	Does the vendor have credentials, integrations, privileged access, network connectivity, or only data provided through a controlled transfer?
Business criticality	Could vendor outage or failure materially interrupt Avenloft Relay, customer support, financial operations, or another important objective?
Concentration / dependency	How difficult would replacement be? Is Avenloft dependent on one provider, proprietary format, or long migration timeline?
Security evidence	What evidence supports the vendor's claims, and how current is it?
Contract / lifecycle	Are security requirements, incident expectations, data deletion, subprocessor handling, and termination activities addressed?

Your classification

Do not classify the vendor by spend alone. Decide whether this relationship is Low, Moderate, or Elevated review priority based on the exposure described in the packet, and explain which factors drove the classification.

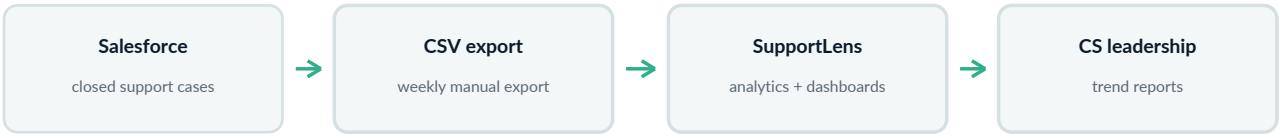
NIST Sources Used in This Case

- NIST CSF 2.0 - GV.SC: supplier criticality, contractual requirements, due diligence, ongoing assessment, incident integration, monitoring, and termination.
- NIST SP 1305: practical use of CSF 2.0 for cybersecurity supply-chain risk management and supplier requirements.
- NIST SP 1326: due diligence as an investigative process for informed supplier and acquisition decisions.
- NIST SP 800-161 Rev. 1: broader cybersecurity supply-chain risk management guidance.

Vendor and Service Profile

Vendor attribute	Case fact
Vendor	CobaltCedar Analytics, Inc. - fictional U.S.-based SaaS company
Product	CobaltCedar SupportLens
Employees	Approximately 76
Customers	Approximately 420 organizations
Avenloft relationship	Customer since February 2026
Annual spend	$18,600
Hosting	Multi-tenant SaaS hosted in AWS U.S. regions
Primary use	Support analytics dashboards and trend reporting from closed-case exports
Avenloft users	8 Customer Success managers and operations analysts
Authentication	Local account login; TOTP MFA available. SAML SSO requires Enterprise tier.
Assurance	Fictional SOC 2 Type II report and independent penetration-test summary supplied for review

Current Data Flow



Attachments are excluded by process, but ticket free text may contain customer-provided logs, identifiers, or troubleshooting details.

Every Friday, Customer Success Operations exports the prior week's closed Salesforce support cases to CSV and uploads the file to SupportLens through the vendor's authenticated web portal. SupportLens produces trend dashboards and account-level reporting. The vendor has no direct Salesforce integration and no credentials into Avenloft systems.

Fields Included in the Export

Included	Excluded by current process
Customer company name	Ticket attachments
Business contact name and email	Authentication secrets by design
Ticket subject and free-text body	Payment-card data by design
Severity, product area, timestamps	Avenloft source code
Case owner and resolution code	Direct production database records

Important limitation	“Excluded by design” does not guarantee that free-text support tickets never contain sensitive technical details. Customers sometimes paste log excerpts, hostnames, identifiers, or troubleshooting data into ticket bodies.

Vendor Security Overview

Area	Vendor statement / supplied evidence
Hosting and isolation	AWS U.S. regions; multi-tenant logical isolation. Vendor states production administrative access is restricted to approved engineering and operations personnel.
Encryption	TLS 1.2 or higher in transit; AES-256 encryption at rest for application databases, object storage, and backups.
Vendor workforce identity	Central SSO and MFA required for vendor employees; privileged access requires separate elevated roles.
Customer authentication	Local username/password accounts. TOTP MFA is available but not enforced by the vendor on the Standard plan. SAML SSO is available on the Enterprise tier.
Vulnerability management	Weekly external scanning, monthly authenticated infrastructure scanning, annual independent penetration test. Vendor target: Critical 15 days, High 30 days.
Logging	Administrative actions and data-export events logged. Standard customers can view 30 days of activity; vendor retains security logs for 180 days.
Incident response	Written incident plan; annual tabletop; 24/7 engineering on-call. Contract language requires notice “without undue delay” after a confirmed security incident affecting customer data.
Business continuity	Nightly backups; stated RPO 24 hours and RTO 8 hours. Restore exercise completed February 2026.
Data retention	Support-case records retained 180 days by default. Contract termination deletion begins within 30 days; backups age out on a 35-day cycle.
Subprocessors	AWS (hosting), Datadog (monitoring), SendGrid (transactional email). Vendor says all production data remains in U.S. regions.

Current Avenloft Account State

Control	Observed state
Named accounts	8 individual Avenloft user accounts; no shared accounts identified
MFA enrollment	5 of 8 accounts have TOTP MFA enabled
SSO / SCIM	Not available on Avenloft's current Standard plan
Access review	Customer Success manager informally reviews active users during quarterly operations review; no documented certification retained
Export permissions	4 of 8 Avenloft accounts can export vendor analytics results; all 8 can view uploaded support data

Vendor Security Questionnaire - Part 1

ID	Question	Vendor response	Evidence status
Q-01	Do you maintain a documented information-security program?	Yes. Security program approved annually by executive management.	Policy index supplied; full policies not provided.
Q-02	Do workforce users authenticate with MFA?	Yes. SSO and MFA are mandatory for CobaltCedar workforce users.	SOC 2 summary references identity controls.
Q-03	Can customers enforce MFA or SSO?	TOTP MFA is available. SAML SSO is Enterprise-tier only.	Product admin guide excerpt supplied.
Q-04	How is Avenloft data encrypted?	TLS 1.2+ in transit and AES-256 at rest.	Architecture statement; SOC 2 summary covers encryption controls.
Q-05	How is tenant separation implemented?	Tenant ID enforced in application and database access layer; access tested in SDLC.	Architecture narrative only; no test evidence supplied.
Q-06	How is privileged access controlled?	Separate privileged roles, MFA, approval, and quarterly review.	SOC 2 summary; one access-review exception noted in report period.
Q-07	How are vulnerabilities identified and remediated?	Weekly scanning, monthly authenticated scans, annual pen test; SLA by severity.	Pen-test summary and remediation tracker supplied.
Q-08	Do you operate a secure development lifecycle?	Peer review, automated dependency scanning, SAST in CI, production change approval.	SOC 2 summary; no SDLC procedure supplied.
Q-09	Do you maintain security logs?	Yes. Security logs retained 180 days; customer-facing activity 30 days on Standard plan.	Questionnaire response and product documentation.
Q-10	Have you had a security incident affecting customer accounts in the last 24 months?	Yes. March 2026 credential-stuffing incident affected several customers.	Incident summary supplied.

Vendor Security Questionnaire - Part 2

ID	Question	Vendor response	Evidence status
Q-11	What is your customer-data retention period?	180 days by default. Shorter retention can be configured on Enterprise tier.	Contract and product guide excerpt.
Q-12	How is data deleted after termination?	Active data deletion begins within 30 days; encrypted backups expire within 35 additional days.	Contract excerpt; no deletion certificate example supplied.
Q-13	Do you use subprocessors?	Yes. Current list: AWS, Datadog, SendGrid.	Subprocessor list dated May 2026.
Q-14	How are subprocessor changes communicated?	Customers may subscribe to Trust Center updates. Contract does not specify advance notice.	Trust Center excerpt and contract.
Q-15	What is your incident-notification commitment?	Contract: without undue delay after confirmation. Internal target is within 72 hours of confirming customer-data impact.	IR summary and contract excerpt.
Q-16	Do you test business continuity and restoration?	Yes. Restore test completed February 2026.	Exercise summary supplied.
Q-17	What are your recovery objectives?	RTO 8 hours; RPO 24 hours.	BCP summary supplied.
Q-18	Do you have independent assurance?	SOC 2 Type II report issued August 2026; annual external penetration testing.	Report summary and pen-test summary supplied.
Q-19	Do you permit customers to retrieve audit activity?	Standard plan exposes 30 days of user/admin events through SupportLens.	Product guide excerpt.
Q-20	Will you notify customers of material changes to your security program?	Material changes communicated through customer notices when they affect contracted services.	Self-attestation only; no contract clause located.

Evidence discipline

A self-attested questionnaire answer can be useful, but it is not equivalent to independent evidence. Your assessment should distinguish what is stated, what is supported, and what still needs follow-up.

Evidence Review: Independent Assurance

Synthetic SOC 2 Type II Summary

Report item	Case fact
Service organization	CobaltCedar Analytics, Inc. - SupportLens
Report period	July 1, 2025 through June 30, 2026
Report issued	August 21, 2026
Opinion	Unmodified opinion in this fictional training report
Scope summary	Logical access, change management, security monitoring, incident response, availability, and selected data-protection controls were described as in scope.
Noted exception	Two of 25 sampled terminated vendor workforce accounts were disabled after 36 and 44 hours; the vendor's stated target was within 24 hours.
Management response	Vendor states an HR-to-identity workflow was changed in July 2026. The corrective action occurred after the report period and is not independently tested by the supplied report.
Customer responsibility note	Customers remain responsible for controlling their own SupportLens user access and enabling available authentication settings.

This is a synthetic report summary created for the exercise. It does not reproduce AICPA Trust Services Criteria or a real auditor's report. Treat it as one piece of vendor evidence, not a substitute for your own relationship-specific assessment.

Synthetic Penetration-Test Summary

Item	Case fact
Test date	May 11-22, 2026
Scope	Internet-facing SupportLens web application and API endpoints
Findings at issue	0 Critical, 0 High, 3 Medium, 4 Low
Remediation status	Two Medium findings marked remediated in July 2026. One Medium finding remains open: insufficient rate limiting on a bulk-export endpoint.
Open-finding context	Vendor states exploitation requires an authenticated account with export permission; target remediation date is October 30, 2026.
Retest evidence	No independent retest letter for the remaining Medium finding is supplied.

Evidence Review: March 2026 Account Incident

CobaltCedar disclosed the following synthetic incident summary in response to Q-10. Avenloft was not identified as an affected customer.

Item	Vendor-provided incident summary
Date	March 14-15, 2026
Event	Credential-stuffing activity targeted SupportLens customer login accounts using credentials obtained outside CobaltCedar.
Affected customers	Nine customer user accounts across four customer organizations authenticated successfully.
Data access	Two compromised accounts had export permissions and exported SupportLens analytics data. Vendor states no administrative or production infrastructure was accessed.
Detection	Vendor detected abnormal login volume and export activity through account-risk and audit-log monitoring.
Response	Sessions revoked, impacted users reset, IP ranges blocked, affected customers notified, additional impossible-travel and high-volume export alerts enabled.
Root cause statement	Vendor found no evidence that CobaltCedar systems were the source of the stolen credentials.
Control change	Vendor increased MFA enrollment prompts but did not make TOTP mandatory for Standard-plan customer accounts. SAML SSO remains Enterprise-tier only.

What This Evidence Does - and Does Not - Tell You

The incident provides real context for evaluating Avenloft's current account configuration. It does not prove that CobaltCedar is unsafe, nor does the absence of Avenloft impact prove the relationship is low risk. Consider the event alongside current MFA enrollment, export permissions, the open rate-limiting finding, and the sensitivity of the data being stored.

Do not double-count blindly	Several facts may contribute to the same underlying risk scenario. Avoid creating separate risk entries for “MFA optional,” “credential stuffing,” and “bulk export” if they are better analyzed together as one relationship risk.

Contract and Data-Handling Excerpts

The following synthetic excerpts summarize the current commercial agreement. They are included to support a security-risk review, not a legal analysis.

Topic	Current agreement / case evidence
Confidentiality	Vendor must protect Avenloft confidential information using reasonable administrative, technical, and physical safeguards.
Security incident notice	Vendor will notify Avenloft without undue delay after confirming a security incident affecting Avenloft customer data. No specific hour-based deadline is stated.
Security assurance	Vendor will maintain an information-security program appropriate to the service. No explicit obligation to maintain SOC 2 is written into the current order form.
Subprocessors	Vendor may use subprocessors to provide the service. Current contract does not specify advance notice or objection rights for changes.
Data retention	SupportLens retains uploaded case data for 180 days by default. Standard plan does not expose shorter retention configuration.
Termination deletion	Vendor will begin deletion of active customer data within 30 days after termination; backup copies expire within the vendor's normal 35-day backup lifecycle.
Customer authentication	Current order form does not require SSO or customer MFA. Enterprise tier includes SAML SSO and configurable retention.
Right to assess	Avenloft may request then-current security documentation once annually. No on-site audit right is included.

Business Owner Request

Lena Ortiz would like to renew on the current Standard plan because SupportLens is useful and replacing the reporting workflow before Q4 planning would create several weeks of manual work. She is open to additional controls but wants to understand which requirements are actually necessary.

Procurement Note

Noah Grant confirms the Enterprise tier would increase annual cost from $18,600 to approximately $24,600. It would add SAML SSO, configurable data retention, and 180-day customer-visible audit history. Commercial negotiation has not started.

Supplemental Stakeholder Notes

Stakeholder	Case note
Aaron Bell - GRC	"We missed this vendor because the old workflow treated spend as a proxy for risk. I want the review to show what the relationship actually exposes and which evidence supports the conclusion."
Lena Ortiz - Customer Success	"SupportLens saves us time every week, but it is reporting, not a system Relay depends on. If we lose it tomorrow, we can go back to Salesforce reports while we replace it."
Noah Grant - Procurement	"I can negotiate security terms at renewal, but I need a short list of requirements. If everything is mandatory, nothing is prioritized."
Hannah Kim - Legal / Privacy	"Please flag notification, retention, deletion, and subprocessor terms that security believes are important. I will handle the legal language and any privacy analysis."
Maya Chen - CISO	"A current SOC 2 report helps, but I care about the Avenloft-specific exposure. What data do they hold, how do our users authenticate, and what happens if an account is compromised?"

Open Questions in the Evidence Set

- No evidence is supplied showing that the July 2026 vendor offboarding fix has been independently tested.
- The remaining Medium penetration-test finding has not yet been independently retested.
- The subprocessor list is dated May 2026; the packet does not establish whether it is current as of renewal.
- The contract does not define a specific incident-notification deadline.
- The packet does not establish whether Avenloft can reduce ticket fields before export without breaking SupportLens reporting.
- No formal evidence shows that Avenloft's current quarterly user review is consistently performed or retained.

Needs validation	If an unknown could materially change your decision or rating, record it as a follow-up item. Do not quietly assume the answer in whichever direction makes the assessment easier.

Avenloft Vendor Risk Assessment Method

Avenloft uses the same qualitative likelihood-and-impact method established in the September cybersecurity risk case. The matrix below reproduces the NIST SP 800-30 Rev. 1 Appendix I qualitative risk determination so the company uses consistent risk language across internal and third-party assessments.

How to Apply It Here

- Write relationship-specific risk scenarios. Example categories may involve unauthorized data access, account compromise, inadequate incident notification, excessive retention, third-party dependency, or another issue supported by the evidence. Do not create a risk merely because a questionnaire answer is imperfect.
- Estimate inherent likelihood and impact before giving credit to current controls.
- Evaluate current controls and evidence. Distinguish vendor controls, Avenloft controls, contractual safeguards, and proposed future conditions.
- Reassess residual likelihood and impact using only controls that actually exist today. Proposed renewal conditions belong in the remediation plan, not the current-control column.

NIST Qualitative Risk Matrix

Likelihood \ Impact	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Residual risk	Expected handling in this case
Very Low	Monitor through normal relationship ownership.
Low	Monitor; treatment may still be appropriate if the relationship conflicts with stated tolerance.
Moderate	Document treatment decision, owner, and follow-up.
High	Document treatment plan and target date; escalate to CISO review.
Very High	Immediate executive visibility and formal treatment; acceptance requires executive leadership approval.

Required Vendor Assessment Fields

Field	What to record
Vendor / service	CobaltCedar Analytics, Inc. / SupportLens
Business owner	Accountable Avenloft relationship owner
Purpose	What business process the service supports
Data / access profile	Data types, transfer method, system access, authentication, and export capability
Criticality classification	Low, Moderate, or Elevated review priority with rationale
Evidence reviewed	Questionnaire, SOC 2 summary, pen-test summary, incident summary, contract, BCP, and other supplied artifacts
Material risk scenarios	Relationship-specific scenarios supported by evidence
Inherent L / I / risk	Qualitative rating before current controls
Current controls	Vendor, Avenloft, and contractual safeguards that exist now
Residual L / I / risk	Qualitative rating after current controls
Finding / gap	Specific weakness, uncertainty, or missing requirement
Required action	Practical remediation or contractual condition
Owner / target date	Who is accountable and when action should be completed
Monitoring / reassessment	What should be checked after renewal and what triggers a new review

Decision Options

Decision	Use when...
Renew	Current evidence and controls support continued use without material new conditions.
Renew with Conditions	Continued use is acceptable if defined security, contract, configuration, or monitoring requirements are completed by stated dates.
Pause / Remediate	Current exposure is not acceptable for continued data transfer until one or more gating issues are resolved.
Exit	The relationship cannot be brought within Avenloft's risk tolerance on a reasonable basis.

Decision Memo Structure

- Relationship and business purpose
- Criticality classification and why it matters
- Most important residual risks
- Required conditions or remediation
- Renewal recommendation
- Monitoring and reassessment triggers
- Material unknowns requiring follow-up

Quality Bar for the Analyst

Strong analyst behavior	Weak analyst behavior
Classifies the relationship using data, access, criticality, and dependency.	Treats annual spend as the risk rating.
Separates questionnaire claims from independently supported evidence.	Marks every “Yes” answer as proof of an effective control.
Uses the SOC 2 and pen-test summaries for their actual scope and limitations.	Writes “SOC 2 = secure” and stops reviewing the relationship.
Combines related facts into meaningful vendor-risk scenarios.	Creates one risk per questionnaire gap.
Rates residual risk using current controls only.	Counts proposed renewal conditions as if they already exist.
Prioritizes a short list of contractual and technical requirements.	Sends Procurement a long list where every item is “critical.”
Defines monitoring and reassessment triggers.	Treats approval as permanent and never revisits the vendor.

Authoritative Reference Material

- NIST Cybersecurity Framework (CSF) 2.0
- NIST SP 1305 - CSF 2.0 Quick-Start Guide for C-SCRM
- NIST SP 1326 - C-SCRM Due Diligence Assessment Quick-Start Guide
- NIST SP 800-161 Rev. 1 - Cybersecurity Supply Chain Risk Management Practices
- NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments

Framework note	NIST CSF 2.0 supplier outcomes and the NIST C-SCRM quick-start guides inform the assessment lens in this case. Avenloft's classification labels, renewal decision options, contract expectations, due dates, and business-specific tolerances are fictional internal rules for training.

Fiction and Safety Notice

Avenloft Systems Group, Inc., Avenloft Relay, CobaltCedar Analytics, Inc., CobaltCedar SupportLens, all vendor personnel, internal records, questionnaire responses, assurance summaries, incidents, contract excerpts, metrics, and events in this packet are fictional and created for training. Commercial products named in background technology references are real products used only to make the environment recognizable. The domains avenloft.example and cobaltcedar.example use the reserved .example namespace and do not identify real organizations.

The SOC 2 and penetration-test material in this packet is synthetic. It does not reproduce a real audit report, a real vendor report, or AICPA Trust Services Criteria.