AVENLOFT SYSTEMS GROUP

Governance, Risk & Compliance

LABLIST CASE FILE | PROJECT 1

BUILD A CYBERSECURITY RISK REGISTER

CASE ID

GRC-RISK-001

ASSIGNED BY

Aaron Bell, Director - Governance, Risk & Compliance

ISSUED

September 7, 2026

YOUR ASSIGNMENT

Identify and document cybersecurity risk scenarios using the evidence in this packet. Build a prioritized risk register and a one-page executive summary for leadership.

DELIVERABLES

- Cybersecurity risk register
- Top-five risk prioritization
- Executive risk summary

Fiction notice: Avenloft Systems Group, its employees, systems, events, and identifiers are fictional. Reserved example domains are used where applicable.

Assignment Brief

To: Junior GRC Analyst

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

Subject: Initial Cybersecurity Risk Register for FY2027 Planning

Due: September 18, 2026

Avenloft is preparing its FY2027 security plan and Q4 executive risk review. Leadership wants a concise cybersecurity risk register that connects technical conditions to business impact and shows which issues need treatment first. Your job is to review the evidence in this case file, identify credible risk scenarios, score them using Avenloft's supplied methodology, and recommend an appropriate treatment path.

The packet is intentionally imperfect. Some evidence is incomplete, some controls reduce risk without eliminating it, and several observations may contribute to the same underlying risk. Do not create one register entry per bullet simply because a bullet exists. Think like an analyst.

Analyst rule	Do not invent missing facts. If information is not available, record the assumption or mark the item as Needs validation. A defensible uncertainty is better than a confident guess.

Required Deliverables

- Cybersecurity risk register: 8-12 well-formed risk entries using the supplied fields and scoring model.
- Top-five prioritization: identify the five residual risks you believe deserve the most immediate management attention.
- Executive risk summary: one page explaining the major themes, immediate actions, and any important information gaps.

Assessment Boundaries

- Use only the information supplied in this packet and the authoritative references linked at the end.
- Assess cybersecurity risk to Avenloft Systems Group and its business objectives. Do not perform legal analysis or invent regulatory obligations.
- Treat named commercial products as part of the fictional company environment. The company, people, events, metrics, and internal records are synthetic.
- You are not expected to find a single “correct” score. Your reasoning and consistency matter.

Company Profile

Avenloft Systems Group, Inc. is a fictional U.S.-based B2B software company. Its flagship SaaS platform, Avenloft Relay, helps mid-market manufacturers and distributors coordinate warehouse scheduling, supplier handoffs, inventory workflows, and shipment status.

Company attribute	Case fact
Employees	Approximately 640; hybrid and remote workforce across the United States
Customers	185 business customers; approximately 22,000 customer user accounts
Revenue profile	Approximately $84M annual recurring revenue
Primary service	Avenloft Relay - cloud-hosted logistics and warehouse workflow SaaS
Customer data	Business contact information, warehouse locations, purchase-order identifiers, inventory quantities, shipment schedules, support attachments
Excluded data	Avenloft does not intentionally process payment-card PAN data or protected health information in Relay
Assurance posture	Current SOC 2 Type II report; next examination period begins in Q4 2026
Operating model	Cloud-first; no customer-facing on-premises production environment

Business Objectives for FY2027

- Protect customer trust: avoid unauthorized disclosure of customer data and preserve contractual security commitments.
- Maintain service reliability: keep Avenloft Relay available and recover quickly from disruptive events.
- Win larger enterprise customers: demonstrate mature risk management, audit readiness, and predictable control operation.
- Scale responsibly: adopt automation and AI where they improve productivity without creating unmanaged customer-data or decision risk.
- Reduce friction: make security reviews, access decisions, and vendor onboarding more consistent as the company grows.

Risk Appetite and Tolerance

Leadership has provided the following directional guidance. It is not a substitute for scoring each scenario, but it should influence your treatment recommendations.

Area	Leadership direction
Customer data confidentiality	Low tolerance for unauthorized disclosure or uncontrolled third-party use of customer information.
Privileged access	Low tolerance for weak authentication, stale privileged accounts, or untraceable administrative activity.
Production availability	Low tolerance for outages exceeding four hours during business operations; recovery capability is considered business-critical.
Critical vulnerabilities	No acceptance of known critical internet-facing vulnerabilities beyond 30 days without a current written exception and compensating controls.
Internal productivity	Moderate tolerance for short, reversible productivity interruptions that do not affect customers or material financial reporting.
Experimentation / AI	Moderate appetite for controlled pilots; low tolerance for customer or confidential data entering unapproved tools.

Organization and Governance Context

Name	Role	Why this role matters to the case
Maya Chen	Chief Information Security Officer (CISO)	Executive owner for the security program and escalation point for High / Very High cyber risk.
Aaron Bell	Director, Governance, Risk & Compliance	Owns the cybersecurity risk register, policy governance, assurance coordination, and GRC reporting.
Priya Nair	VP, Engineering	Accountable for product engineering, cloud production, software delivery, and remediation of engineering-owned risks.
Marcus Holloway	Director, IT & Workplace Technology	Owns workforce identity, endpoints, corporate infrastructure, and administrative access.
Elena Ruiz	VP, Finance & Operations	Executive stakeholder for business continuity, financial operations, and enterprise risk reporting.
Lena Ortiz	VP, Customer Success	Owns customer support operations and several customer-data workflows.
Hannah Kim	General Counsel & Privacy Lead	Advises on contracts, privacy, and data-handling obligations.
Noah Grant	Director, Procurement	Owns procurement workflow and coordinates vendor onboarding.
Jared Cole	Head of People Operations	Owns employee lifecycle data; employee offboarding integrates with IT, contractor offboarding currently does not.

Current Governance Cadence

- Security Steering Committee meets monthly. High and above residual risks are expected to have a named owner and treatment plan.
- The GRC team maintains policies, customer assurance responses, the risk register, audit evidence coordination, and third-party security review.
- Security risks may be accepted by the accountable business owner only within delegated authority. High and Very High residual risks require CISO review; acceptance of Very High residual risk requires executive leadership approval.
- The risk register is reviewed quarterly and before major executive planning cycles.

Technology Environment

Use this inventory to understand where business processes and evidence connect. It is not intended to be a complete CMDB.

Environment / service	Purpose	Security notes
Avenloft Relay production (AWS)	Customer-facing SaaS application and APIs	Production is hosted in AWS. Customer data is stored in managed databases and object storage.
Okta	Workforce identity and SSO	MFA is required for standard workforce SSO applications.
Microsoft 365	Email, collaboration, document storage	SSO through Okta; managed endpoints required for standard employee access.
GitHub Enterprise Cloud	Source code and software collaboration	Employee SSO is automated; contractor access is managed manually by engineering sponsors.
Salesforce	CRM and enterprise customer records	Administrative audit logs retained through standard platform settings; detailed exports are retained 30 days.
Jira / Confluence	Engineering and corporate work tracking	Contains internal technical documentation and remediation tickets.
Workday	Employee system of record	Employee termination events trigger automated deprovisioning through the identity workflow.
Corporate endpoints	Laptops for employees	Full-disk encryption and EDR are required; fleet coverage is approximately 98%.
Legacy remote admin gateway	Restricted administrative access to two legacy network appliances	Uses local accounts and passwords; limited to six IT administrators and source-IP allowlisting.

Current Security Baseline

Control area	Current baseline
Identity	Okta SSO and MFA for standard workforce applications; role-based access is used for major SaaS systems.
Endpoint security	EDR and full-disk encryption required on managed endpoints; coverage measured at 98%.
Vulnerability management	Weekly external and internal scanning; policy target is 30 days for critical internet-facing findings.
Backups	Daily production backups with protected copies; operations performs restore testing periodically.
Logging	AWS production security logs are centralized; SaaS-platform audit-log retention varies by service.
Awareness	Annual security-awareness training and periodic phishing simulations.
Incident response	Documented incident-response plan with named technical and business contacts.
Third-party risk	Security review is required for vendors classified as high risk by the current procurement workflow; classification is heavily influenced by annual spend.
Access reviews	Quarterly certification for selected high-risk employee access; contractor access is reviewed separately by system owners.

Evidence Set: Security and Control Observations

The following items were collected during interviews, control reviews, open remediation tracking, and the September Security Steering Committee preparation. Treat them as evidence, not prewritten risks. Several observations may combine into one risk scenario, and one observation may support more than one scenario.

OBS-01 Recovery testing lag	Source: IT Operations interview
Observation	Production database backups run daily and protected copies are maintained. The last documented full application-and-database restore exercise occurred 14 months ago. The recovery runbook still references the pre-migration network layout used before the company moved the final production services into its current AWS architecture.
Existing context / controls	Backups exist and operations monitors job completion. No evidence of a failed backup was identified in this review.

OBS-02 Critical Partner Portal vulnerability	Source: Vulnerability remediation tracker
Observation	A critical vulnerability (CVSS 9.1) remains open on the internet-facing Partner Portal after 32 days. Engineering delayed the vendor patch because regression testing caused partner-session failures. A web-application firewall rule was added as temporary mitigation. The formal risk exception expired five days ago and has not been renewed.
Existing context / controls	Weekly scanning is operating. WAF mitigation is documented, but the exception is no longer current.

OBS-03 Contractor offboarding delay	Source: Quarterly access review
Observation	Three engineering contractors retained GitHub access after their contract end dates for 4, 6, and 9 days. No unauthorized activity was found in the sampled logs. Employee departures are automatically deprovisioned from Workday through Okta, but contractor offboarding depends on the engineering sponsor submitting a ticket.
Existing context / controls	All three accounts are now disabled. GitHub requires SSO for workforce identities.

OBS-04 Legacy administrative gateway without MFA	Source: IT architecture note
Observation	Six IT administrators use a legacy remote administration gateway to manage two network appliances. The gateway does not support Okta or MFA and uses local username/password authentication. Access is restricted to company VPN source addresses.
Existing context / controls	The gateway is not exposed to arbitrary internet sources, only six administrators are authorized, and password rotation is performed through the team vault.

Evidence Set: Security and Control Observations (continued)

OBS-05 Vendor review classification gap	Source: Procurement process review
Observation	The procurement workflow automatically requires security review for vendors above a spend threshold. Data sensitivity is not a mandatory classification field. During the review, GRC identified a customer-support analytics vendor receiving periodic ticket exports even though the vendor did not receive a security assessment before onboarding because annual spend was below the threshold.
Existing context / controls	The vendor contract includes confidentiality language. No security questionnaire, architecture review, or formal risk rating is on file.

OBS-06 Awareness and phishing results	Source: Security awareness dashboard
Observation	Annual training completion is 91%; 56 employees are overdue. The most recent phishing simulation had a 6% company-wide click rate. Customer Success recorded a 14% click rate. Repeat simulation failures do not currently trigger mandatory remedial training.
Existing context / controls	Email filtering and endpoint protection are in place. Training reminders are sent automatically.

OBS-07 SaaS audit-log retention gap	Source: Logging standard review
Observation	The security logging standard calls for 180 days of searchable administrative logs for high-value systems. AWS production logging meets the standard. Detailed administrative exports from Salesforce and GitHub are currently retained for 30 days because extended retention was not included in the original implementation.
Existing context / controls	Native audit logging is enabled in both services. Security can retrieve the retained 30-day window when needed.

OBS-08 Customer-support download workflow	Source: Customer Success interview
Observation	Support agents sometimes download customer ticket attachments to local laptops to reproduce product issues. Approximately 18 such downloads occur in a typical month. Managed laptops use disk encryption and EDR, but there is no DLP rule preventing local copies or requiring deletion after the case closes.
Existing context / controls	Access to support tickets is role-based. Customer Success managers review unusual export volumes when alerted.

Evidence Set: Security and Control Observations (continued)

OBS-09 Incident-response exercise is stale	Source: Incident response program review
Observation	The incident-response plan was reviewed six months ago, but the last ransomware tabletop exercise occurred 22 months ago. The tabletop predates the final AWS migration and did not test loss of the primary identity provider.
Existing context / controls	The incident plan contains current contact information and an executive escalation tree.

OBS-10 Shared appliance administrator identity	Source: IT control walkthrough
Observation	Two legacy network appliances are administered through a shared account named netadmin because the appliances do not support individual administrator identities. The password is stored in the privileged credential vault and check-out activity is logged. Device audit logs record netadmin rather than the individual who made the change.
Existing context / controls	Vault check-out records provide partial attribution outside the appliance itself. Only the network administration team can retrieve the credential.

OBS-11 Asset ownership gaps	Source: Asset inventory review
Observation	The asset inventory covers approximately 93% of known computing assets. Eighteen Linux build servers discovered during a cloud-cost review do not have a documented business owner in the inventory. Engineering states that the servers support non-production software builds and are patched through the standard image pipeline.
Existing context / controls	The servers are not customer-facing and are managed through the engineering cloud account.

OBS-12 Unmanaged AI experimentation	Source: Security Steering Committee notes
Observation	Marketing has permitted employees to use consumer generative-AI accounts for low-sensitivity drafting. Customer Success has separately requested approval for a SaaS AI tool that would summarize customer calls and support tickets. Avenloft does not yet maintain a formal AI use-case inventory or a standard AI-risk intake process.
Existing context / controls	Leadership has told teams not to place customer-confidential information into unapproved AI tools. The Customer Success request is paused pending GRC review.

Supplemental Stakeholder Notes

These excerpts provide business context that may change how you interpret the observations. They are intentionally brief.

Aaron Bell - GRC	"The register needs to be usable by leadership, not just security. If the risk statement does not explain what happens to the business, rewrite it."
Priya Nair - Engineering	"The Partner Portal patch is not being ignored. We tried the vendor fix twice and it broke partner sessions. The WAF rule buys time, but I agree the current exception should not have lapsed."
Marcus Holloway - IT	"The old admin gateway is one of the last systems we have not moved behind modern SSO. Replacing the two appliances is already proposed for next fiscal year."
Lena Ortiz - Customer Success	"Support downloads are usually screenshots, logs, or customer-provided files needed to reproduce a problem. We do not have a good workflow for proving the local copy was deleted afterward."
Noah Grant - Procurement	"Our vendor workflow grew out of finance controls, so spend still drives most of the routing. I can see why that misses inexpensive services that touch sensitive data."
Maya Chen - CISO	"Do not rank everything High. I need to know which risks deserve scarce time and budget first, what is already reducing the risk, and where the uncertainty itself is material."

Facts You Should Not Assume

- An observation is not automatically a control failure, and a control gap is not automatically a high risk.
- The absence of evidence in this packet does not prove that a control does not exist. Record unknowns when they matter.
- A vulnerability score is not the same as a business risk score.
- A risk owner should normally be accountable for the affected business or technology outcome; GRC facilitates and monitors the risk rather than owning every risk.

Avenloft Risk Assessment Method

For this exercise, Avenloft uses the qualitative risk-level matrix published in NIST SP 800-30 Rev. 1, Appendix I, Table I-2. NIST presents the table as an exemplary assessment scale that organizations may tailor; Avenloft uses the published five-level matrix directly so you can practice with a real, publicly available risk-assessment model rather than an invented scoring grid.

1. Write the Risk Scenario

Use a cause-and-impact structure that connects a plausible threat event or failure condition to a business consequence. A useful pattern is:

Risk statement pattern	If [threat event or failure] exploits / occurs alongside [condition or weakness], then [asset, process, or objective] may experience [business impact].

Avoid statements such as “MFA risk,” “outdated policy,” or “critical CVE.” Those describe a technology or condition, not the risk to the business.

2. Rate Inherent Risk

Estimate the risk before giving credit to the listed controls. Use the scenario and business context to assign an inherent overall likelihood and level of impact, then use the NIST matrix to determine the inherent risk level. This is an analytical estimate, not a prediction.

3. Evaluate Existing Controls

Record the safeguards already in place and decide whether they materially reduce the likelihood, the impact, or both. Do not give a control full credit simply because it exists; consider the evidence about how it is operating.

4. Rate Residual Risk

Reassess overall likelihood and impact after considering the current controls, then use the same NIST matrix to determine the residual risk level. Residual risk is the risk that remains and is the primary rating you will use for prioritization in this case.

Overall Likelihood Scale

NIST value	Working guidance for this case
Very Low	The threat event occurring and resulting in adverse impact is highly unlikely based on the available evidence.
Low	The scenario is unlikely to produce adverse impact, although it remains plausible.
Moderate	The scenario is somewhat likely to occur and result in adverse impact.
High	The scenario is highly likely to occur and result in adverse impact.
Very High	The scenario is almost certain to occur and result in adverse impact.

Impact Scale

NIST value	NIST concept applied to Avenloft
Very Low	Negligible adverse effect; little meaningful effect on operations, assets, customers, or objectives.
Low	Limited adverse effect that can be handled through normal operations.
Moderate	Serious adverse effect requiring management attention, such as meaningful service, customer, financial, or assurance impact.
High	Severe or catastrophic adverse effect, such as major service loss, customer harm, or significant contractual or financial consequence.
Very High	Multiple severe or catastrophic adverse effects with broad or sustained consequences for Avenloft and its stakeholders.

Risk Determination, Prioritization, and Treatment

Use the matrix below to combine overall likelihood and level of impact. This reproduces the qualitative risk determination in NIST SP 800-30 Rev. 1, Appendix I, Table I-2. Do not multiply ordinal labels together; the published matrix determines the risk level.

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 control ownership.
Low	Monitor; treatment may still be appropriate when the risk conflicts with a stated tolerance.
Moderate	Assign an accountable owner and document a treatment decision or rationale.
High	Document a treatment plan and target date; escalate to the CISO for review.
Very High	Immediate executive visibility and formal treatment; acceptance requires executive leadership approval.

Risk Response Options

Response	Use when...
Mitigate	Additional controls or process changes can reduce likelihood and/or impact.
Avoid	The activity creating the risk can be stopped or redesigned so the scenario no longer exists.
Transfer / Share	A contract, insurance arrangement, service provider, or other mechanism shifts or shares part of the consequence; accountability is not magically eliminated.
Accept	The accountable authority explicitly agrees to retain the residual risk within delegated tolerance, with rationale and review date.

Important

The matrix supports prioritization; it does not make the management decision for you. A Moderate risk can still require prompt action if it conflicts with a stated tolerance or strategic objective.

Required Risk Register Fields

Field	What to record
Risk ID	Use a simple identifier such as R-001.
Risk title	Short, business-readable name.
Risk statement	Scenario linking threat/failure, condition, affected asset/process, and business impact.
Business objective / asset	What Avenloft objective, process, data, system, or service is exposed.
Evidence / source	Observation IDs or stakeholder notes that support the scenario.
Inherent likelihood / impact / risk	Qualitative ratings before existing controls; use the NIST matrix to determine inherent risk.
Existing controls	Safeguards already operating or temporarily mitigating the condition.
Residual likelihood / impact / risk	Qualitative ratings after considering controls; use the NIST matrix to determine residual risk.
Residual risk level	Very Low, Low, Moderate, High, or Very High based on the NIST matrix.
Treatment recommendation	Mitigate, Avoid, Transfer/Share, or Accept, with a concise rationale.
Risk owner	Accountable business or technology leader based on the scenario.
Target action / due date	Practical next step and proposed timing.
Status / uncertainty	Open, In Treatment, Accepted, Needs Validation, etc.; note material unknowns.

Blank Register Layout

ID	Title	Risk statement	Evidence	Inherent L/I/R	Controls	Residual L/I/R	Risk	Treatment / Owner

You may build the working register in Excel, Google Sheets, LibreOffice Calc, or another tool. The layout above is only the minimum information Avenloft expects.

Executive Summary Structure

- Overall risk posture: 2-4 sentences describing the dominant risk themes you found.
- Top five residual risks: list them in priority order and explain why each matters to Avenloft.
- Immediate actions: identify 3-5 actions leadership should fund, assign, or escalate first.
- Important unknowns: note missing information that could materially change a rating or treatment decision.
- Management message: keep the summary to one page and write for leaders who may not know the technical details.

Quality Bar for the Analyst

A strong submission does more than fill cells. It shows that you can distinguish a technical condition from a business risk, use evidence, account for existing controls, prioritize, and communicate uncertainty.

Strong analyst behavior	Weak analyst behavior
Writes risk scenarios with a clear business consequence.	Copies observation text into the risk-title column.
Uses evidence IDs and states assumptions.	Invents facts to make scoring easier.
Distinguishes inherent from residual risk.	Scores the vulnerability itself without considering controls.
Explains why a risk owner is accountable.	Assigns every risk to GRC or “IT.”
Prioritizes based on residual risk, appetite, and business objectives.	Marks nearly every issue High or Very High.
Makes practical treatment recommendations.	Writes “fix it” without an owner, action, or target date.

Authoritative Reference Material

You do not need to read every publication before completing the exercise. These sources support the concepts used in the case and are useful for cross-reference:

- NIST IR 8286 Rev. 1 - Integrating Cybersecurity and Enterprise Risk Management (ERM)
- NIST IR 8286A Rev. 1 - Identifying and Estimating Cybersecurity Risk for ERM
- NIST IR 8286B - Prioritizing Cybersecurity Risk for Enterprise Risk Management
- NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments
- NIST Cybersecurity Framework (CSF) 2.0 Resource Center

Methodology note	The likelihood-impact matrix in this case is based directly on NIST SP 800-30 Rev. 1, Appendix I, Table I-2. Avenloft's business context, risk appetite, escalation expectations, use of the matrix for inherent and residual ratings, and due-date expectations are fictional company rules for this exercise. NIST presents its assessment scales as examples that organizations may tailor.

Fiction and Safety Notice

Avenloft Systems Group, Inc., Avenloft Relay, all employees, internal records, observations, metrics, and events in this packet are fictional and created for training. Commercial products named in the technology inventory are real products used only to make the fictional environment recognizable. The domain avenloft.example uses the reserved .example namespace and is not intended to identify a real organization.

This packet contains no credentials, malware, personal data, or active infrastructure. It is safe to use as a documentation and analysis exercise.