Vendor Risk Assessment Framework

NMFTA™ National Motor Freight Traffic Association, Inc. | CYBER

Introduction to Vendor Risk Management

Third-party vendors play a critical role in the success and resilience of trucking operations. However, poor visibility into vendor security practices exposes fleets to cyber-enabled cargo theft, data breaches, platform impersonation, and operational disruption. This framework is designed for use by carriers and logistics providers at all levels of cybersecurity maturity—whether they are just getting started or maintaining a structured security program.

Rooted in the principles of the National Motor Freight Traffic Association, Inc.'s (NMFTA)™ cybersecurity guidance and aligned with industry best practices (National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), Center for Internet Security Controls (CIS Controls), Standardized Information Gathering questionnaire (SIG)), this framework provides a structured approach to evaluate, onboard, and monitor vendors. It includes a customizable checklist and scoring model to streamline risk-based decisions.

Core Objectives of Vendor Cybersecurity Oversight

- Ensure third-party services do not introduce undue cyber or operational risk.
- Require visibility into vendors' identity validation, access control, and network segregation.
- Vet vendors' ability to respond to incidents affecting your fleet's systems or data.
- Enforce contractual controls aligned with operational needs and threat exposure.
- Prioritize vendors handling sensitive cargo, telematics, driver comms, or brokerage roles.

Pre-Contract Risk Screening

1) Is there an individual responsible for cybersecurity within your organization?
Having an individual designated *in writing* as responsible for the cybersecurity of the organization demonstrates that the organization prioritizes cybersecurity.

Compliant	Clearly assigned and documented.
At Risk	Understood but not documented.
Non-Compliant	No clear assignment.

2) Do you have an executive leadership role responsible for cybersecurity strategy?
Having a Chief Information Security Officer (CISO), or an equivalent executive role, demonstrates that cybersecurity is not just operationally managed but is prioritized at the strategic and leadership level.

Compliant	Executive-level role is formally assigned and documented.
At Risk	Role exists but is informal or unclear.
Non-Compliant	No executive cybersecurity leadership.

3) Have you experienced a major cybersecurity incident? If so, how was it handled?
A major cybersecurity incident could include things like a ransomware attack, data breach, or unauthorized access to sensitive systems. Whether or not an incident has occurred, what's most important is how the organization detects, responds to, and recovers from such events.

Compliant	Incident handled via documented response plan; lesson applied **OR** If no incidents have occurred: Documented preparedness
At Risk	Response occurred but was informal or undocumented **OR** *If no incidents:* Undocumented preparedness to respond.
Non-Compliant	No process in place or visibility into incident handling or incident handling preparedness.

4) Do you use any subcontractors or fourth-party service providers? What access do they have?
Subcontractors (third parties) and fourth-party service providers (vendors your vendors use) can introduce risk if they have access to sensitive systems, data, or credentials. Knowing who they are and what access they have is essential for managing cybersecurity risk beyond an organization's walls.

Compliant	All access is limited, monitored and contractually controlled.
At Risk	Access controls exist but are loosely managed or inconsistent.
Non-Compliant	No oversight or control over external access.

5) When was your last external cybersecurity assessment or penetration test?
An external cybersecurity assessment or penetration test helps to identify vulnerabilities before attackers can exploit them. Regular testing and documented remediation of identity vulnerabilities shows that an organization takes cybersecurity seriously.

Compliant	Completed within 12 months with complete documentation; findings addressed.
At Risk	Outdated, follow-up incomplete, or insufficiently documented.
Non-Compliant	Not performed, or unknown **OR** Reported as performed, but no supporting documentation of findings or remediations.

Contractual Safeguards

1) Do your service agreements include breach notification terms, access limitations, and audit rights?
Service agreements should clearly state how security incidents are reported (breach notification), who can access systems and data (access limitations), and whether the customer or a third-party can verify compliance (audit rights). These terms help protect both parties and clarify expectations.

Compliant	All terms included in current contracts.
At Risk	Terms vary between contracts or are incomplete.
Non-Compliant	No relevant terms included.

2) What controls are in place to secure, or out-of-band communications (email, portals, other)?
Out-of-band communications—such as emails, secure messaging apps, or web portals—are often used to send sensitive information. Without protections, this information could be intercepted or misused.

Compliant	Encrypted channels used; access is secured.
At Risk	Partial protections; inconsistent use.
Non-Compliant	No secure channels or defined procedures.

3) Are service termination or liability clauses included for cybersecurity non-compliance?
Contracts should include explicit consequences for failing to meet cybersecurity obligations. This helps ensure accountability and provide options if contractual obligations are not met.

Compliant	Clauses are standard and enforceable.
At Risk	Terms exist but lack clarity or consistency.
Non-Compliant	No such clauses are present.

4) Do you maintain a removable media policy?
A removable media policy sets rules for how things like USB drives and external devices can be used. It helps prevent malware infections and data loss.

Compliant	Documented policy exits; use is restricted, policy is enforced.
At Risk	Some controls exist, but no formal policy or inconsistent enforcement.
Non-Compliant	No policy or controls in place.

5) Are your contractual terms reviewed by legal and security jointly?
A joint review of contracts by both legal and security teams ensures that cybersecurity requirements are not just legally sound but also technically enforceable.

Compliant	Legal and security review contracts before approval.
At Risk	One party reviews; the other is informed but not involved in approval.
Non-Compliant	Contracts are reviewed without input from security or legal.

Vendor Categorization & Prioritization

1) What systems or data will your services interact with?
   Understanding which systems and types of data a vendor will access is essential for assessing risk. This includes whether they'll interact with production environments, customer information, financial records, or internal tools. The more sensitive the system or data, the more security oversight is required. Clear documentation of this interaction supports appropriate access controls, monitoring, and contract terms.

Compliant	Systems and data types are clearly defined and documented.
At Risk	General access is understood but not formally documented.
Non-Compliant	No clarity or documentation on systems or data involved.

2) Would an outage in your systems impact our operations?
   Understanding whether a vendor's service is critical to your operations helps define the level of risk and response planning needed. If an outage would interrupt core business processes, then uptime, recovery processes, and communication procedures become essential. Even if the impact is minimal, it should be clearly assessed and documented to guide expectations.

Compliant	Impact has been clearly evaluated and communicated.
At Risk	Impact is assumed or partially understood but not fully documented.
Non-Compliant	No analysis of operational impact from an outage.

3) How do you classify sensitive data, and what protections are in place?
   Classifying data means identifying what information is sensitive—like personal data, financial records, or proprietary business details—and labeling it accordingly (e.g., public, internal, confidential). This ensures that the most sensitive data receives the strongest protections.

Compliant	Data is classified by type and sensitivity, labeled accordingly, and appropriate protections enforced.
At Risk	Some sensitive data is protected, but classification or controls are inconsistent.
Non-Compliant	No formal data classification or protection standards in place.

4) What critical infrastructure or cloud dependencies do you rely on?
Knowing which underlying services a vendor depends on—such as public cloud providers, hosting platforms, internet service providers (ISPs), or third-party application programming interfaces (APIs)—is essential for understanding availability, risk concentration, and potential points of failure. These dependencies can impact uptime, data security, and recovery if not properly managed. Transparency around these components supports better planning, contractual protections, and incident response coordination.

Compliant	All critical dependencies are identified, documented, and monitored.
At Risk	Some dependencies are known, but documentation or visibility is incomplete.
Non-Compliant	No clear understanding or disclosure of critical infrastructure or cloud reliance.

5) Are your systems integrated into our network or isolated?
Whether a vendor's systems are integrated into your network or kept separate affects your security posture. Integrated systems may introduce more risk but can offer efficiency. Isolated systems may reduce exposure but may require extra coordination. Knowing the integration model helps define access controls, monitoring requirements, and incident response planning.

Compliant	Integration model is clearly defined, documented, and access is appropriately secured.
At Risk	Integration exists but is not fully documented or access boundaries are unclear.
Non-Compliant	No visibility into whether systems are integrated or isolated.

Onboarding & Technical Integration

1) What access will your personnel or tools require?
   Vendors should clearly define what level of access their staff or automated tools will need—whether it's read-only access to data, admin rights to systems, or integration with internal platforms. This helps enforce the principles of least privilege, Role-Based Access Control (RBAC), and Attribute Based Access Control (ABAC). It also ensures sensitive areas are protected and allows access to be properly monitored and revoked when no longer required.

Compliant	Access needs are clearly defined, limited, and documented.
At Risk	Access is requested only as needed but not consistently defined or documented.
Non-Compliant	No clear understanding or control of access requirements.

2) How do you implement least privilege access?
   Lease privilege means giving users and systems only the access they need to do their jobs—nothing more. This reduces the risk of accidental or malicious misuse of sensitive data or systems. Least privilege is implemented through RBAC, regular access reviews and restrictions on administrative rights. This is a key control for limiting the blast radius of any potential breach.

Compliant	Access is role-based, minimized by default, and regularly reviewed.
At Risk	Least privilege is practiced informally, with limited review or enforcement.
Non-Compliant	Broad access is granted without restriction or oversight.

3) Do you use secure credential vaulting or SSO integration?
   Protecting login credentials is critical to preventing unauthorized access. Secure credential vaulting stores passwords in encrypted vaults instead of local files or spreadsheets. Multi-Factor Authentication (MFA) adds an extra step to confirm identity. Single Sign-On (SSO) allows users to access multiple systems with one login reducing password fatigue and improving oversight of access.

Compliant	Credential vaulting, MFA, and SSO are implemented and enforced.
At Risk	Some controls are in place but not consistently used or fully integrated.
Non-Compliant	Credentials are not security managed, MFA and/or SSO are not in use.

4) Who will serve as our technical point of contact?
A technical point of contact (POC) is the primary person responsible for handling technical questions, coordinating integrations, and assisting with troubleshooting. Having a designated POC ensures clear communication, faster problem resolution, and accountability throughout the engagement.

Compliant	A dedicated technical POC is assigned and documented.
At Risk	A POC exists but is not formally assigned or may change without notice.
Non-Compliant	No designated technical contact.

5) Do you inventory and document third-party access by role?
Documenting and tracking what third parties can access—and aligning that access to specific roles—helps to ensure that external users only have the permissions they need. This improves oversight, simplifies audits, and makes it easier to revoke access quickly when it's no longer required.

Compliant	All third-party access is documented, role-based, and regularly reviewed.
At Risk	Some tracking exists but is incomplete or not reviewed regularly.
Non-Compliant	No inventory or documentation of third-party access.

Monitoring & Ongoing Review

1) What cybersecurity certifications or attestations do you maintain (e.g., SOC 2)? Cybersecurity certifications and attestations—such as System and Organization Controls 2 (SOC 2), International Organization for Standardization (ISO 27001), Payment Card Industry Data Security Standard (PCI DSS), or Federal Risk and Authorization Management Program (FedRAMP)—demonstrate that an organization's security practices have been independently assessed against recognized standards. Maintaining these certifications provides assurance to customers that security controls are in place and regularly evaluated.

Compliant	Current, valid certifications or attestations are maintained and fully documented.
At Risk	Some certifications exist but are outdated, limited in scope, or are in progress.
Non-Compliant	No recognized cybersecurity certifications or attestations.

2) How do you monitor for suspicious behavior across endpoints or networks? Monitoring for suspicious activity helps to detect potential security incidents early. This is typically done with tools like endpoint detection and response (EDR), intrusion detection systems (IDS), and security information and event management (SIEM) platforms. Continuous monitoring allows faster investigation and response to threats.

Compliant	Continuous monitoring is in place with alerts, logging, and defined response processes.
At Risk	Some monitoring exists but is limited in scope, frequency, or response capabilities.
Non-Compliant	No monitoring for suspicious activity across endpoints or networks.

3) Do you conduct regular internal/external vulnerability scans or red team exercises? Vulnerability scans identify weaknesses in systems before attackers can exploit them. Internal scans focus on the organization's own network, while external scans test internet-facing systems. Red team exercises go further by simulating real-world attacks to tete defenses, detections, and responses. Regular testing ensures vulnerabilities are found and addressed proactively.

Compliant	Internal and external scans are performed regularly; red team exercises are conducted as appropriate. Comprehensive documentation is maintained.
At Risk	Some testing is done, but is irregular, incomplete, or findings and remediations are not consistently documented.
Non-Compliant	No regular vulnerability scans or red team activities.

4) How will you notify us of a breach affecting our data?
A clear breach notification process ensures you're informed quickly if your data is compromised. This should include how you'll be contacted, what details will be provided, and the timeline for notification. Prompt communication allows you to take immediate action to contain damage and meet your own legal or contractual obligations.

Compliant	Formal breach notification process exists with defined timelines and communication methods.
At Risk	Notification is promised, but process or timelines are vague.
Non-Compliant	No defined breach notification process.

5) Do you have an external security monitoring service (CyHy or other)?
External security monitoring services, such as the U.S. Department of Homeland Security's Cyber Hygiene (CyHy) program or commercial equivalents, scan and monitor internet-facing systems for vulnerabilities or misconfigurations. These services provide early warnings and help reduce the risk of an external attack.

Compliant	External monitoring service is in place and actively used. Findings are remediated and documentation is maintained.
At Risk	Some monitoring exists but is limited in scope or frequency; Findings and remediations are not fully documented.
Non-Compliant	No external security monitoring service in place.

6) Can we schedule annual or event-driven reviews of your cybersecurity program?
Regular reviews—whether scheduled annually or triggered by major changes or incidents—help ensure a vendor's cybersecurity program remains effective and aligned with your requirements. These reviews provide transparency, allow discussions of improvements, and confirm that agreed-upon controls are still in place.

Compliant	Annual and event driven reviews are allowed and supported.
At Risk	Reviews are possible but only under limited circumstances or with restrictions.
Non-Compliant	Reviews are not permitted or not addressed.

Implementation Tips for Fleets of Varying Maturity

- **New or Small Fleets:** Focus on critical vendors only. Use a simplified checklist. Partner with cybersecurity-minded brokers.
- **Growing Fleets:** Develop a vendor inventory and classify by risk. Assign roles for contract review and technical integration.
- **Large or Cyber-Mature Fleets:** Integrate vendor risk scoring with Governance, Risk, and Compliance (GRC) or ticketing platforms. Automate reassessments and link with legal for streamlined contract review and execution.

By implementing vendor oversight practices, fleets can disrupt the pathways cybercriminals use to hijack credentials, steal data, steal freight, or otherwise inflict financial, reputational and operational damage.

VENDOR RISK ASSESSMENT CHECKLIST

Section	Question	Vendor Response	Compliance Level	Follow-Up Action Req	Reviewer Notes
Pre-Contract	Is there an individual responsible for cybersecurity within your organization?				
Pre-Contract	Do you have a CISO or equivalent leadership role?				
Pre-Contract	Have you experienced a major cybersecurity incident? If so, how was it handled?				
Pre-Contract	Do you use any subcontractors or fourth-party service providers (MSP or MSSP, Others)?				
Pre-Contract	When was your last external cybersecurity assessment or penetration test?				
Contractual Safeguards	Do your service agreements include breach notification terms, access limitations, and audit rights?				
Contractual Safeguards	What controls are in place to secure, or out-of-band communications (email, portals, other)?				
Contractual Safeguards	Are service termination or liability clauses included for cybersecurity non-compliance?				

Section	Question	Vendor Response	Compliance Level	Follow-Up Action Req	Reviewer Notes
Contractual Safeguards	Do you maintain a removable media policy?				
Contractual Safeguards	Are your contractual terms reviewed by legal and security jointly?				
Vendor Categorization	What systems or data will your services interact with?				
Vendor Categorization	Would an outage in your systems impact our operations?				
Vendor Categorization	How do you classify sensitive data, and what protections are in place?				
Vendor Categorization	What critical infrastructure or cloud dependencies do you rely on (AWS, Azure, GCP)?				
Vendor Categorization	Are your systems integrated into our network or isolated?				
Onboarding & Integration	What access will your personnel or tools require?				
Onboarding & Integration	How do you implement least privilege access?				
Onboarding & Integration	Do you use secure credential vaulting, MFA, or SSO integration?				
Onboarding & Integration	Who will serve as our technical point of contact?				
Onboarding & Integration	Do you inventory and document third-party access by role?				

Section	Question	Vendor Response	Compliance Level	Follow-Up Action Req	Reviewer Notes
Monitoring & Ongoing Review	How do you monitor for suspicious behavior across endpoints or networks?				
Monitoring & Ongoing Review	Do you conduct regular internal/external vulnerability scans or red team exercises?				
Monitoring & Ongoing Review	How will you notify us of a breach affecting our data?				
Monitoring & Ongoing Review	Do you have an external security monitoring service (CyHy or other)?				
Monitoring & Ongoing Review	Can we schedule annual or event-driven reviews of your cybersecurity program?				

NOTES