NRF Center for Digital Risk & Innovation

A Guide to Developing a Retail Supply Chain Cybersecurity Risk Management Plan

PREPARED BY

The Chertoff Group

Overview

A standard aspect of running a retail business is procuring supplies and services from third-party suppliers. This dependency can create added supply chain cybersecurity risks. For example, malicious actors have repeatedly leveraged compromised supplier credentials as part of a cyber attack. This guide identifies supply chain-related cybersecurity risks and offers a framework and practices that can enable retailers to proactively address cybersecurity risks with partners. This model supply chain cybersecurity risk management framework includes a risk categorization of in-scope suppliers, cybersecurity due diligence of these suppliers, contractual requirements based on regulations and risk, access controls where relevant, ongoing monitoring elements, and offers guidance for each.

Supply Chain Vendor Types

A precondition to managing supply chain risk is to define and categorize it. According to the MITRE Corporation's System of Trust Framework, supply chain risk falls into three basic categories:

Risk Type	Description
Supplier Risks	Risks related to characteristics of a supplier of products or services, including their supply chain, that may potentially impact consumers of those products or services.
Supply Risks	Risks related to characteristics of a product, including their supply chain provenance and pedigree, that may potentially impact consumers of that product. *Note: "Products" includes software.*
Service Risks	Risks related to characteristics of a service, including their supply chain provenance and pedigree, that may potentially impact consumers of that service.

Risk types for each of these categories are summarized in Appendix A. The scope of this framework includes managing cybersecurity risks from suppliers (of both technology and non-technology-based supplies and services). It is not intended to address other risks beyond cybersecurity.

Inherent Risk Considerations – Criticality and Impact

Not all suppliers entail the same level of risk. Resources should be prioritized for suppliers whose supplies or services are either particularly critical to business operations or scenarios where an incident would cause a severe operational, legal or compliance, or reputational impact.

Criticality criteria may include:

	Software	Service Provider
High Value Asset (HVA)	Software meeting the Cybersecurity and Infrastructure Security Agency's (CISA) definition of a High Value Asset	Service providers providing outsourced IT managed services supporting HVAs
NIST Definition of Critical Software	Software meeting the National Institute of Standards & Technology's (NIST) definition of Critical Software	Service providers providing outsourced IT managed services supporting NIST Critical Software
Regulatory Considerations	Software storing, accessing or processing Payment Card Information (PCI) or Protected Health Information (PHI) records	Service providers providing outsourced support for regulated systems (PCI, Health Insurance Portability and Accountability Act [HIPAA])
Support to Critical Retail Functions (if not addressed above)	Make/move/sell software Store operations software	Make/move/sell services Store operations technology services
Use of Artificial Intelligence (AI)	AI software, particularly that impacts safety or rights (e.g., interactions with employees or consumers)	AI-driven services, particularly that impact safety or rights (e.g., interactions with employees or consumers)

Impact criteria may include:

Supply and Service-Related Impacts	Considerations and Examples
Operational Impacts	**Service-related impact example:** Corruption or incapacitation of a service can have significant downstream operational impacts on retailers. A February 2022 ransomware attack on logistics provider Expeditors International led to significant disruption of the logistics supply chain across the United States.
AI-Related Safety Impacts	**Supply-related impact example:** While studies have found that the use of AI-enabled automation (e.g., robotics) can reduce safety risks, such technologies can also entail potentially serious safety consequences. In November 2023, a worker at a South Korean food processing plant was reportedly crushed to death in a robot-related accident.

Loss of Information Impacts	**Supply-related impact example:** Exploitation of software can lead to significant operational impacts on retailers. Hundreds of organizations (and their customers) suffered data loss in 2023 when ransomware threat actors exploited a software vulnerability in MOVEit, a popular file transfer software.
Legal & Compliance Impacts	**Supply-related impact example:** In December 2021, cloud-based human capital management solution provider Kronos disclosed that it had suffered a ransomware incident. This incident caused massive and extended disruption in customers' ability to process payrolls, including multiple organizations in the retail sector. Impacted employees sued their employers, alleging they were improperly paid due to the outage. More generally, compliance risk arises when supplier operations are not in line with U.S. or foreign laws, regulations, or industry standards through a failure to implement appropriate security controls. Data protection and data breach notification laws have emerged across U.S. states and foreign jurisdictions, including the European Union's (EU) General Data Protection Regulation (GDPR), the EU's Digital Operational Resilience Act (DORA), the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), and the Brazilian General Data Protection Law (LGPD). These regulations are increasingly including supplier risk management as part of their related controls and standards.
Reputational Impacts	**Supply-related impact example:** The 2017 notPetya incident resulted in widespread operational disruption. For some companies, the resulting impact includes a loss of revenues because customers substituted away from the victim's service to a competitor. Corrupted Ukrainian tax accounting software was the initial access vector.
Concentration Risk	Concentration risk creates impacts where a retailer has no redundancy in the event of the incapacitation of a primary service provider or software supplier.

Risk Management and Due Diligence

Before entering supplier relationships, retailers should consider the extent to which a supplier's controls mitigate supply or service risk to an appropriate level. This section will cover some elements that should be considered when performing due diligence assessments of suppliers. The level of due diligence performed on the supplier is facts-and-circumstances-dependent and will change depending on the exact service or product being supplied in the relationship.

Supplier Business Background and Reputation

When vetting suppliers, it is helpful to start with high-level assessments of the business and its reputation. Making this determination can weed out less mature suppliers earlier in the process. Assessing suppliers' business background and reputation may include:

1. **Assessing its history of security incidents, complaints or legal compliance** using public records databases (including crosschecks with organizations like the Federal Trade Commission (FTC) and state Attorneys General (for data privacy/security enforcement actions, and media reporting);
2. **Determining length of time in business** and how significantly / rapidly the business model has changed;
3. **Researching senior leadership backgrounds**;
4. **Requesting references and/or discussing past performance**; and
5. **Reviewing third-party standing** with companies like Forrester and Gartner.

Financial Condition

Depending on the importance of the relationship from either a security or business continuity perspective, it may be useful to attempt to evaluate the supplier's financial condition and stability. Considerations could include the company's growth, income, profits, liabilities, and anything else that may impact the stability of the company and its ability to secure itself.

Geographic Location

Legislation and regulations are increasingly imposing restrictions based on geography – for example, location of data, the domicile of the supplier, and location of teams either providing services or developing software supplies. This is particularly true for suppliers that may have access to personally identifiable information. For example, in March 2024, the U.S. Department of Justice (DOJ) released an Advance Notice of Proposed Rulemaking (ANPRM) that defines regulations to prohibit or restrict transactions that may enable "countries of concern" or "covered persons" to access bulk sensitive personal data or data on U.S. government personnel. The DOJ proposed rule has broad implications across U.S. industry: It potentially impacts any company that handles more than de minimis amounts of U.S. personally identifiable information (PII), with significant considerations for global enterprises that maintain a presence or personnel in China or other "countries of concern." Retailers should consider inquiring as to the geographic location of suppliers and their staff who may have access to sensitive data.

Hiring Practices

Threat actors are increasingly targeting suppliers of technology products and services as stepping stones into supplier organizations. Moreover, remote hiring practices combined with advancements in

deepfake technologies increase risks of imposters being hired into technology roles. For example, as described by the U.S. DOJ, the North Korean government has repeatedly dispatched thousands of skilled IT workers to live abroad, with the aim of deceiving U.S. and other businesses worldwide into hiring them as freelance IT workers, to generate revenue for its weapons of mass destruction (WMD) programs. Retailers should consider inquiring about identity validation and verification practices implemented as part of supplier hiring practices.

"Nth Party" Risk Illumination

Companies are increasingly at risk from their suppliers' own supply chains – that is, a supplier's own subcontractors and software. This is also known as a supplier's fourth party, fifth party, or "n^{th} party" relationships. Resources permitting, retailers may wish to undertake efforts to illuminate a critical supplier's own supply chain. Luckily, a number of commercial illumination tools have entered the marketplace to assist in doing so. These tools collect and document supplier data and can increase transparency of the connections and dependencies of the supply chain as well as provide continuous monitoring capabilities. The tools can be used to document and analyze various types of supplier data, such as manufacturing locations, subsidiaries, ownership, leadership and their nationalities, and partner and business relationships.

Illuminating Security Performance

Understanding the level of security performance is an increasingly important part of supply chain due diligence, and yet the process can quickly become unmanageable for both retailers and suppliers. Five elements are key to making this a workable approach in practice:

1. **Inquiry:** Focused question sets and evaluation, supported by the use of authoritative security frameworks.
2. **Attestation:** Selective use of attestation and independent validation.
3. **Observability:** Selective use of continuous diagnostics.
4. **Application of (1), (2) and (3)** based on the criticality and associated risk as relate to the supplier.
5. **Automation of (1), (2), (3) and (4)** where at all possible.

Inquiry Through the Use of Authoritative Security Frameworks-Service Providers

Retailers should evaluate the extent to which a third-party service provider maintains a risk-appropriate security and business continuity program, including both policies and controls. In turn, "risk appropriate" should be framed in the context of the data or system access the third-party will have. Where data exchanged is governed by regulatory regimes such as PCI or HIPAA, compliance with those regimes essentially defines a minimum standard. See Appendix E for examples of key regulatory regimes.

More generally, the use of authoritative frameworks is recommended to support repeatability and auditability. Appendix B lists a representative set. *Some of these frameworks also include subcategorizations based on risk – for example the Center for Internet Security's Critical Security Controls subdivides controls into Implementation Groups 1, 2 and 3.*

Where the primary risk is a supplier's handling of sensitive data, retailers may also wish to consider NIST Special Publication 800-171, Protecting Controlled Unclassified Information on Non-Federal Systems and Organizations. While this guidance is intended for federal contractors, the underlying principles behind it are more broadly applicable across industry sectors.

Inquiry Through the Use of Authoritative Security Frameworks-Software

In May 2021, the Biden administration issued Executive Order (EO) 14028 "Improving the Nation's Cybersecurity" requiring federal software suppliers to conform to software security best practices defined in the NIST Secure Software Development Framework (SSDF) and attest to conformance. While this guidance is technically directed at federal suppliers, it is also instructive for supplier-purchaser relationships in the commercial sector, including retail, and is thus referenced here.

In addition, CISA and 17 U.S. and international partners released software Secure By Design guidance (originally released by CISA in 2023) intended for enterprise software providers. This guidance provides best practices on application hardening, application security features, and secure-by-default settings. In August 2024, CISA released two additional guidance documents specifically intended for software purchasers: (1) a Secure By Demand general purpose guide, which includes questions and resources that organizations buying software can use to better understand a software manufacturer's approach to cybersecurity and ensure that the manufacturer makes secure by design a core consideration; and (2) a more detailed Software Acquisition Guide for Government Enterprise Consumers.

Retailers should consider asking software providers whether they have aligned their software security programs to the SSDF and Secure By Design/Secure By Demand guidance.

For additional question sets, retailers can also consider using:

- Minimum Viable Secure Product considerations; and
- Guidance from the Australian Signals Directorate on choosing secure and verifiable software products.

As noted above, Appendix B lists a representative set of potentially relevant security frameworks that can be used to illuminate software security.

Use of Authoritative Security Frameworks – AI-enabled Software or Services

Where AI technologies are leveraged – particularly in ways that potentially impact safety or rights of employees or consumers – retailers should evaluate how suppliers have managed AI-related risks to address impacts arising out of both cyber threats and unintended consequences of legitimate AI use. In November 2023, NRF released its Principles for the Use of Artificial Intelligence in the Retail Sector, which provide guidance on business partner accountability among other points. These guidelines build on the January 2023 NIST AI Risk Management Framework (RMF). The NIST AI Framework classifies key risks associated with the use of AI and defines structures for framing, governing, mapping, measuring and managing the use of AI inside organizations, including through test, evaluation, verification, and validation (TEVV) processes.

This NIST Framework also establishes the concept of "trustworthy AI" and defines characteristics of trustworthy AI systems, such as being valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and "fair," meaning that the potential for harmful bias is managed. The EO directs NIST to develop a companion framework addressing Generative AI-specific risks.

Attestation and Independent Validation

For critical suppliers, retailers should also consider asking to review evidence of any certification by qualified independent auditors or assessors that a service provider's security program has been effectively implemented (e.g., Payment Card Industry Data Security Standards Report on Compliance, SSAE 16 SOC 2 Type 2, International Standards Organization 27001 certification) or validation that specified security controls are in place. This provides a level of assurance that a third-party's own representations about its program have been independently verified. Several points bear particular consideration:

- Verify the ***date*** of the third-party validation to ensure it is current.
- Review the ***scope*** of the validation to ensure it covers the assets relevant to your relationship (e.g., a SSAE SOC 2 report on the vendor's corporate network is minimally relevant if the vendor is providing hosted application services run from a separate vendor network).
- Consider a two-step approach: Some retailers ask for a third-party validation report and then, if none is provided, revert to a detailed set of cybersecurity questions. Put another way, a current, properly scoped third-party validation may conserve retailer resources by limiting the scope of review, particularly for non-critical vendors.

For **software**, CISA has published an SSDF self-attestation form for federal software vendors in response to EO 14028. CISA's self-attestation form identifies minimum criteria for meeting secure software development lifecycle (SDLC) standards.

Moreover, in 2024, CISA announced a Secure By Design Pledge, whereby signatories commit to working toward seven secure software goals (enabling multi-factor authentication in products, reducing

default passwords, reducing entire classes of vulnerabilities, increasing patch installation, publishing a vulnerability disclosure policy, increasing transparency in vulnerability reporting by including Common Weakness Enumeration (CWE) in any reports, and enhancing customers' ability to gather intrusion-related evidence) within a year.

Likewise, for **Internet-of-Things technologies**, the U.S. Federal Communications Commission (FCC) has recently voted to create a voluntary cybersecurity labeling program for wireless consumer Internet of Things (IoT) products. Under the program, qualifying consumer smart products that meet robust cybersecurity standards will bear a label — including a new "U.S. Cyber Trust Mark" — intended to help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace, and create incentives for manufacturers to meet higher cybersecurity standards.

Observability

When assessing the strength of a prospective supplier's cybersecurity controls, it may also be worth considering using a real-time cybersecurity performance monitoring service (e.g., BitSight, SecurityScorecard, RiskRecon, or Black Kite, among others) to baseline and continuously monitor security performance, providing an additional lens into the effectiveness of a supplier's security program.

For **software**, EO 14028 also requires certain software vendors to eventually provide a Software Bill of Materials (SBOM), or a formal record containing details of code-level relationships and components used in building software. According to CISA, an SBOM is a nested inventory, a list of ingredients that make up software components. With sufficient instrumentation, an SBOM can provide a continuing view into the riskiness of the code in a software product.

There are different available formats for detailing software components – including CycloneDX, SPDX and SWID. Determining which format is most appropriate is based on the facts and circumstances present in each retailer's environment. Moreover, code that is theoretically vulnerable may not be deployed in a vulnerable way. An SBOM-related concept is the Vulnerability Exploitability eXchange (VEX). A VEX document is an attestation, a form of a security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities. Organizations can also use SBOMs to continuously monitor vulnerabilities across their company's third-party software.

Moreover, purchasers can also undertake certain additional technical evaluations of software even though they lack access to source code.

- **Software composition analysis** will identify risks in open-source software – for example known vulnerabilities and potential issues, typically by analyzing package managers, manifest files and related signatures. That said, these tools are generally limited to identifying risks in open-source components, not commercial or proprietary code.
- **Software build and binary analysis** will evaluate software binaries to identify embedded malware, tampering, exposed secrets and related weaknesses and vulnerabilities.
- **Integrity verification** will verify that the software has not been tampered with – e.g., through comparison of hashes, signatures, certificates, or other methods of verification.

Criticality Determination

The level of due diligence applied to a supplier, supply or service should be based on risk. See above section, **Inherent Risk Considerations – Criticality and Impact**, for considerations on determining the criticality of software or a service provider.

Automation

For organizations with multiple service and software providers, automation will increasingly be key to effectively tracking supplier security compliance. For suppliers, automation helps manage otherwise diverse and burdensome customer inquiries. Solutions (e.g., CyberGRX/ProcessUnity, Prevalent, Black Kite) are available that enable one-time completion of a supplier assessment, which can then be updated and shared with multiple customers.

Risk Management: Contract Provisions & Procurement

Devising a standard contract with cybersecurity provisions tailored to retailers' risk tolerance can contractually hold suppliers to certain standards and mitigate incident-related cybersecurity risk. A retailer should consider contractual provisions that define expectations and responsibilities of the supplier and ensure appropriate response mechanisms (and insurance coverage) in the event of an incident. This is particularly true for relationships where retailers are ceding some elements of control for the protection of its critical assets or regulated data. Any service-level agreements (SLAs) should ideally document expectations from owners and suppliers and stipulate the consequences if those requirements are not met.

Note:

- The ability to impose cybersecurity-related contractual terms and conditions will vary based on the nature of the supplier. For example, Commercial-Off-the-Shelf (COTS) and cloud software providers will often insist on using their own standardized terms and conditions.
- This guidance from the Australian Signals Directorate on choosing secure and verifiable software products, referenced above, also includes a number of contractual considerations.
- These Minimum Viable Secure Product considerations are also intended to inform desired contractual controls.

Key considerations include:

Required Security Controls

Retailers should consider developing contractual provisions that define expected security controls for suppliers to have implemented before engaging in business with your company. Cyber criminals will often target a supplier and then "island-hop," using the supplier's connection to a retailer to compromise the retailer. Retailers can mitigate this risk by requiring security standards before suppliers can do

business with the organization. The same cybersecurity frameworks utilized for due diligence (see above and Appendix B) can also be referenced for defining expected controls.

Attestations/Certifications

Retailers may also wish to condition contracts on security self-attestations or third-party certifications.

Data Protection and Privacy Considerations

If a retailer shares sensitive data with a supplier, the retailer should ensure that the supplier adheres to the retailer's data protection policies (often included as part of the retailer's notice to its customers/users to obtain their consent for data collection), or the equivalent. The transfer of the data to the supplier does not relieve the retailer of data protection-related obligations pursuant to which the data was collected. Once a retailer has collected PII or other sensitive data, it must ensure that the data is handled under the terms of the retailer's agreement with its customers, employees and partners. Additional geographic considerations may include:

- Has the geographical location of all data, including logs, been specified in the contract or configuration? If so, has this been verified?
- Are all backup copies of data, including logs, held in the region specified in the contract or configuration? If so, has this been verified?

Incident Notification and Cooperation Requirements

Retail organizations should consider requiring that suppliers commit to notifying and cooperating with the retailer in the event of a cyber breach. Where a supplier has access to a retailer's system, the supplier's logging and other relevant information may be critical to retailers' efforts to understand where and when an adversary obtained initial system access. Where a supplier holds a retailer's sensitive data within its system, incident reporting may be the retailer's only way to learn of a possible compromise. Without contractual provisions, a retailer may have little recourse to insist on supplier cooperation in the event of a breach.[1]

Business Continuity & Disaster Recovery Planning

Retailers should also consider requiring suppliers to have business continuity and disaster recovery plans in place and tested. Business continuity planning is essential to carry on operations in the event of a cybersecurity event (or a natural disaster, a terrorist attack, transportation disruptions, the loss of

[1] The U.S. Securities and Exchange Commission (SEC) updated requirements in July 2023 that impact how publicly traded companies disclose cybersecurity incidents. Under the rule, publicly traded companies are required to report cyber incidents within four days of determining the incident is material. According to the SEC, the fact that the underlying breach occurred at a third party does not exempt the company from disclosing the incident.

critical staff, or other severe disruptions to business operations). Ideally, any prospective suppliers should have already implemented business continuity and disaster recovery planning as part of a general risk management strategy.

The Right to Audit

As part of the contract, the retailer should consider ensuring that it has the right to audit implementation of contractually required controls, monitor performance, and require remediation when issues are identified. A retailer should reserve the right to conduct its own audits of the supplier's activities or to engage an independent party to perform such audits.

Insurance

Retailers may also wish to consider provisions around insurance coverage to ensure that a supplier has recourse to resources necessary to mitigate a cybersecurity incident.

Cyber insurance coverage can also indirectly mitigate cybersecurity risks when underwriters condition coverage on implementation of particularly impactful controls. Marsh, a global insurance broker and risk advisor, has identified a correlation between certain security controls and cyber incidents. Retailers and their suppliers can strengthen their organization's cyber resiliency and insurability by following Marsh's 12 recommended cybersecurity controls.

Supply Chain Risk Management

Finally, retailers may wish to consider provisions that require a supplier to have its own supply chain cybersecurity risk management program in place – that is, to manage risks associated with its own suppliers (whether of software or services).

Risk Management: Access Controls

Post contract access control considerations both to service providers and software suppliers:

Service Providers

Where third-party service providers have access to a retailer's facilities or systems, applying focused controls around third-party access is important to limit third-party risk. Many compromises today entail the misuse of legitimate credentials – a system administrator account compromised by a malicious actor or misused by a disgruntled contractor or other insider. By limiting third-party access to specified facilities or systems and ensuring effective processes for off-boarding third-party personnel no longer working on a retailer's team, retail organizations can limit the damage potentially done by a misused credential.

Retailers should consider how to leverage administrative, technical and physical controls to ensure that third-party access to the organization's facilities or systems aligns to the principle of least privilege.

- *Administrative controls* would address provisioning and deprovisioning access to systems and sensitive applications, ensuring access requests are reviewed by appropriate retailer employees and recertified at regular time intervals.
- *Physical controls* would limit physical access only to those facilities with third-party needs in order to perform contract-related responsibilities.
- *Technical controls* would include preventive, detective and responsive countermeasures regarding unauthorized activity being attempted with third-party credentials. Examples would include:
    - Provide appropriately **strong authentication** mechanisms (e.g., multi-factor authentication) for network access by a third-party.
    - Enforce **least privilege** by limiting third-party access to specified applications or subnets, and also limiting the nature of access (e.g., perhaps through a virtual desktop infrastructure connection).
    - Enable focused **monitoring** of third-party activity on the network.

Software

Access control considerations also apply to the use of purchased software. The considerations include:

- *Administrative Console Hardening*. Configure access to the management console to require multi-factor authentication and, where practicable, not be directly accessible from the internet.
- *Privileged Credential Minimization*. Where possible, minimize the level of privilege required to operate the application (e.g., avoid invoking Active Directory Domain Administrator credentials to manage the application).
- *SaaS/IaaS Provider Access*. Consider whether the provider of SaaS/IaaS solutions has access to your data.

Risk Management: Oversight and Monitoring

Ongoing oversight and monitoring for the duration of the third-party supplier relationship is important to ensure that changed circumstances or security-related decay are addressed by the retailer. The level and importance of monitoring is in direct relationship to the criticality of the supplier to the retailer's business objectives and access to the enterprise and sensitive data. An effective TPRM program leverages limited oversight resources to ensure some level of ongoing contract oversight, prioritizing resources for suppliers representing highest risk, either because of the inherent risk entailed in the relationship or residual risk based on control gaps or changed circumstances.

Compliance Testing and Audits

Auditing is the process of verifying activities to ensure compliance with requirements. An audit can apply to an entire organization or to a specific function, process or production step. Use of audits by

retailers to assess a supplier's conformity to legal or regulatory requirements, or to agreed-on security standards and best practices, can be an important component of the risk management process.

Audit Type	Description
First-party Audit	An internal audit performed within an organization to measure its strengths and weaknesses against its own procedures or methods and/or against external standards adopted by (voluntary) or imposed on (mandatory) the organization.
Third-party Audit	Performed by an independent organization, and not part of either the vendor or retailer organizations. Typically viewed as an unbiased, external party that will provide a trust view of the audit results.

Use of Independent Third-Party Performance Management Technologies

One significant challenge with the due diligence and oversight and monitoring efforts is that these measures generally offer "snapshots" in time of what the supplier has indicated its efforts are in terms of cybersecurity and risk management and often require significant personnel resources to manage. Controls and settings can change at any point, and new vulnerabilities will be discovered, but these may not be reported to the retailer.

Retailers should also consider using tools that provide continuous monitoring of supplier external systems (also described above). These tools use open-source data that can indicate potential network vulnerabilities, weak security on endpoints, or even compromise situations. In this use case, retailers would watch for significant changes in security performance – i.e., a noticeable drop in a SecurityScorecard, BitSight, RiskRecon or Black Kite score.

Ongoing Software Security Monitoring

As noted above, with sufficient instrumentation, a software bill of materials (SBOMs) can provide a continuing view into the riskiness of the code in a software product. Likewise, software composition analysis, binary analysis, integrity verification can verify the continued security and integrity of software – particularly when complemented with **runtime monitoring** and **vulnerability notification**.

Cloud Service Provider Self-Assessment Technologies for Customers

One of the biggest challenges of working with cloud service providers is ensuring that cloud technology is implemented securely by the purchaser. Security performance evaluation thus entails a "look in the mirror" effort, so to speak. Tracking asset posture can increasingly achieved through out-of-the-box tools from cloud providers, for example Microsoft's Secure Score. Some cloud systems such as Google Cloud Platform have also started to map posture to controls frameworks published by NIST and the Center for Internet Security.

Appendix A: Supply Chain Risk Types

In the MITRE System of Trust Framework, each supply chain category – suppliers, supplies and services – has its own risk types, which are summarized below:

Supplier Risk Types

Risk Type	Description
Financial Stability Risks	Risks related to characteristics of a supplier of supplies (products) or services, including their supply chain, that may potentially impact consumers of those supplies (products) or services
Organizational Security Risks	Risks related to characteristics of a supplier's personnel, facilities, transport, and cybersecurity capabilities, policies, and practices that affect the potential to resist and withstand malicious actions and the impact on customers.
Supplier Susceptibility	Risks related to characteristics of a supplier that affect the likelihood of them being targeted, compromised or otherwise adversely affected by malicious actors.
Supplier Quality Culture Risks	Risks related to characteristics of a supplier's ability to reliably deliver appropriate quality supplies (products) and/or services.
Supplier Ethical Risks	Risks related to characteristics of a supplier that could negatively impact its customers, clients, partners, or market through explicit intent, whether internally or externally driven, to violate legal/business norms or to cause harm.
Supplier External Influences	Risks related to characteristics of a supplier that make it susceptible to negative influence by external motivations or allegiances. In a nation-state context this is typically an issue of foreign influences and in the commercial context this would typically be a competitor's influence on a supplier.

Supply Risk

Risk Type	Description
Malicious Taint	Risks related to the integrity of a supply (product) introduced through explicit intent, whether internally or externally driven, to violate legal/business norms to cause harm.
Counterfeit	Risks related to the authenticity of a supply (product) introduced through explicit intent, whether internally or externally driven, to violate legal/business norms.

Hygiene Risks	Risks affecting the ability of a supply (product) to perform as expected. This involves characteristics related to establishing and maintaining the quality, security, resilience, etc., of the supply (product).

Due to suppliers having touchpoints with potentially large volumes of customers, threat actors are increasingly exploiting supplies like commercial software and related technologies as stepping stones to compromise multiple organizations, either by deliberately inserting malware ("malicious taint" in MITRE's terms) or exploiting hygiene gaps.

Risk Type	Description
Service Quality Risks	Risks related to the quality of a service delivered.
Service Resilience Risks	Risks related to the resilience of a service delivered.
Service Security Risks	Risks related to the security of a service delivered.
Service Integrity Risks	Risks related to the integrity of a service delivered.

Like supplies, services are also being exploited as stepping stones to compromise multiple organizations. Like suppliers, services are also being exploited as stepping stones to compromise multiple organizations by exploiting security and integrity gaps. Even ignoring stepping-stone risks, service interruptions due to quality, resilience, security, or integrity gaps can engender potential severe impacts on customers. Even ignoring stepping-stone risks, service interruptions due to quality, resilience, security, or integrity gaps can engender potential severe impacts on customers.

Appendix B: Supplier Cybersecurity Risk Management Resources

Below are resources that may be helpful to retailers as they evaluate supplier relationships. These resources offer additional detail companies can use when assessing security programs and establishing criteria to manage their partnerships.

1. NIST Privacy Framework and Cybersecurity Framework	
The NIST Cybersecurity Framework (CSF) offers "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks." To the extent retailers leverage this framework, we recommend that it be coupled with a controls catalogue such as NIST SP 800-53 or the Center for Internet Security's Critical Security Controls (referenced below) for traceability and auditability.	
SCRM Consideration Aligned with Resource	✓ Due Diligence, Oversight, and Monitoring ✓ Inherent Risk
2. International Organization for Standards (ISO) 27001 certification	
The **ISO/IEC 27001** is useful as an information security standard for companies that are looking to establish, maintain, and improve their information security management system. It is a helpful tool for risk management and cyber resiliency that subscribes to the three principles of information security, known as the CIA triad: 1. Confidentiality: Only authorized persons have the right to access information. 2. Information Integrity: Only authorized persons can change the information. 3. Availability of Data: The information must be accessible to authorized persons whenever it is needed.	
SCRM Consideration Aligned with Resource	✓ Due Diligence, Oversight, and Monitoring
3. Marsh Top 12 Key Controls	
Marsh's 12 key controls detail established best practices / cyber hygiene controls that have become minimum requirements with insurers. These controls will strengthen the organizations' insurability and cyber resiliency.	
SCRM Consideration Aligned with Resource	✓ Due Diligence, Oversight, and Monitoring ✓ Contract Provisions and Procurement ✓ Third-Party Access Controls
4. The Center for Internet Security (CIS) 18 Critical Security Controls	
The CIS Critical Security Controls (CIS Controls) are a prioritized set of best practices that can be used to strengthen organizations' cybersecurity posture and comply with state and federal cybersecurity regulations.	
SCRM Consideration Aligned with Resource	✓ Due Diligence, Oversight, and Monitoring ✓ Contract Provisions and Procurement ✓ Third-Party Access Controls
5. NIST SP 800-171 Protecting Controlled Unclassified Information on Non-Federal Systems	
NIST SP 800-171 provides recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CUI) when the information is resident in non-federal systems and organizations. The requirements apply to components of non-federal systems that process,	

store, or transmit CUI or that provide protection for such components. While the intended audience is federal contractors, the focus of the guidance – protection of sensitive information by vendors – is more broadly applicable across industry sectors.	
SCRM Consideration Aligned with Resource	✓ Due Diligence, Oversight, and Monitoring ✓ Contract Provisions and Procurement
6. NIST Secure Software Development Framework (SSDF)	
The NIST Secure Software Development Framework is a "set of fundamental, sound, and secure software development practices based on established secure software development practice documents from organizations such as BSA, OWASP, and SAFECode."	
SCRM Consideration Aligned with Resource	✓ Due Diligence, Oversight, and Monitoring ✓ Contract Provisions and Procurement
7. Secure Software Self-Attestation Form	
In April 2023, CISA released its Secure Software Self-Attestation Form to be used by software producers in an effort to set minimum secure software development practices. It reflects a subset of NIST SSDF practices. While this is a requirement for federal agencies, the private sector may benefit from this best practice.	
SCRM Consideration Aligned with Resource	✓ Contract Provisions and Procurement ✓ Due Diligence, Oversight, and Monitoring
8. Software Bill of Materials (SBOM)	
CISA's "software bill of materials" (SBOM) has emerged as a critical component of software security and software supply chain risk management. The SBOM acts as a nested inventory, a list of ingredients that make up software components.	
SCRM Consideration Aligned with Resource	✓ Contract Provisions and Procurement ✓ Due Diligence, Oversight, and Monitoring
9. CISA Secure By Design Framework	
CISA's Secure By Design initiative guidance provides best practices on (a) application hardening, (b) application security features and (c) secure-by-default settings. CISA's Secure By Design Pledge commits signatories to working toward seven secure software goals (enabling multi-factor authentication in products, reducing default passwords, reducing entire classes of vulnerabilities, increasing patch installation, publishing a vulnerability disclosure policy, increasing transparency in vulnerability reporting by including Common Weakness Enumeration (CWE) in any reports, and enhancing customers' ability to gather intrusion-related evidence) within a year.	
SCRM Consideration Aligned with Resource	✓ Due Diligence, Oversight and Monitoring ✓ Contract Provisions and Procurement ✓ Supplier Access Controls
10. CISA Vendor Supply Chain Risk Management (SCRM) Template	
CISA's Vendor Supply Chain Risk Management (SCRM) Template is an effort to create a standardized template of questions to communicate ICT supply chain security risk to public and private organizations. The questions outlined in the assessment aim to provide greater transparency into entity trust and assurance practices that can inform risk management practices.	
SCRM Consideration Aligned with Resource	✓ Contract Provisions and Procurement ✓ Due Diligence, Oversight, and Monitoring
11. CISA Secure By Demand Guide	
CISA's Secure By Demand guide includes questions and resources that organizations buying software can use to better understand a software manufacturer's approach to cybersecurity and ensure that the manufacturer makes secure by design a core consideration.	
SCRM Consideration Aligned with Resource	✓ Due Diligence, Oversight, and Monitoring
12. CISA Software Acquisition Guide for Government Enterprise Customers	

Customers (as often represented by their acquisition and procurement organizations) can use this guidance, developed by CISA's Information & Communications Technology Risk Management Task Force, as a basis to describe, assess, and measure suppliers' security practices relative to the software lifecycle without requiring that acquisition team members become cybersecurity experts. The guide builds on existing U.S. government cybersecurity guidance to address four phases of software ownership: software supply chains, development practices, deployment, and vulnerability management.	
SCRM Consideration Aligned with Resource	✓ Due Diligence, Oversight, and Monitoring
13. Minimum Viable Secure Product	
Minimum Viable Secure Product (MVSP) considerations are a list of essential application security controls that should ideally be implemented in enterprise products and services. MVSP is based on the experience of contributors in enterprise application security across a range of companies and driven by Dropbox's Vendor Security Model Contract and Google's Vendor Security Assessment Questionnaire. MVSP is intended for use both in procurement due diligence and to inform contractual controls.	
SCRM Consideration Aligned with Resource	✓ Contract Provisions and Procurement ✓ Due Diligence, Oversight, and Monitoring
14. Australian Signals Directorate on Secure and Verifiable Technologies	
In May 2024, the Australian Signals Directorate released guidance on choosing secure and verifiable technology products. The guidance includes externally facing and internally facing considerations throughout the technology procurement lifecycle.	
SCRM Consideration Aligned with Resource	✓ Contract Provisions and Procurement ✓ Due Diligence, Oversight, and Monitoring
15. FCC IoT Cyber Trust Mark	
In March 2024, the U.S. Federal Communications Commission voted to create a new "U.S. Cyber Trust Mark"— a voluntary cybersecurity labeling program for wireless consumer Internet of Things ("IoT") products. Under the program, qualifying consumer smart products that meet robust cybersecurity standards will bear the Trustmark label, which is intended to help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace, and create incentives for manufacturers to meet higher cybersecurity standards. Notional product criteria are listed in Appendix A of this proposed rule.	
SCRM Consideration Aligned with Resource	✓ Due Diligence, Oversight, and Monitoring
16. NRF Principles for the Use of Artificial Intelligence in the Retail Sector	
In November 2023, the National Retail Federation released Principles for the Use of Artificial Intelligence in the Retail Sector to support AI governance. Among other points, the Principles address business partner accountability for partners that are providing AI tools, data sets and services.	
SCRM Consideration Aligned with Resource	✓ Contract Provisions and Procurement ✓ Due Diligence, Oversight, and Monitoring
17. NIST AI Risk Management Framework	
In January 2023, the U.S. National Institute of Standards and Technology (NIST) released an AI Risk Management Framework, which classifies key risks associated with the use of AI and defines structures for framing, governing, mapping, measuring and managing the use of AI inside organizations, including through test, evaluation, verification, and validation (TEVV) processes. The practices described in this Framework may be instructive in evaluating and overseeing suppliers that are providing AI tools, data sets and services.	
SCRM Consideration Aligned with Resource	✓ Contract Provisions and Procurement ✓ Due Diligence, Oversight, and Monitoring
18. NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices	

In May 2022, the U.S. National Institute of Standards and Technology (NIST) released Revision 1 of Special Publication 800-161, Cybersecurity Supply Chain Risk Management Practices, which provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations. The audience is federal agencies, and the guidance is both comprehensive and voluminous. SP 800-161 includes both practices and scenarios, and these may be instructive in identifying, managing and prioritizing supply chain cybersecurity risks.	
SCRM Consideration Aligned with Resource	✓ Contract Provisions and Procurement ✓ Due Diligence, Oversight, and Monitoring ✓ Third-Party Access Controls
19. Software Supply Chain Security	
Software Supply Chain Security is a book that offers a comprehensive look at security risks and identifies the practical controls that can be incorporated into an organization's end-to-end software supply chain. It is authored by Cassie Crossley, Vice President, Supply Chain Security in the global Cybersecurity & Product Security Office at Schneider Electric.	
SCRM Consideration Aligned with Resource	✓ Contract Provisions and Procurement ✓ Due Diligence, Oversight, and Monitoring

Appendix C: Sample Risk-Based Considerations

When evaluating supplier risk, it may be useful to establish criteria to determine the appropriate level of review required for a potential supplier. Many companies have hundreds or even thousands of suppliers, making it a basically impossible task to deeply assess each security program and sets of controls. Establishing criteria and "tiers" of criticality or risk can help a retailer better manage these partnerships.

Risk Level Consideration

Inherent Risk	Third-party Examples*	Due Diligence	Procurement	Third-party Access Controls	Ongoing Monitoring
High	• Payment card processing system • Ecommerce platform provider • Critical software • Make/move/ sell software • Software processing or storing sensitive corporate information • Services supporting above systems	Independent Validation	Security performance considered as source selection factor Compliance with retailer requirements reviewed before contract signing	Baseline third-party access controls in place – enhancements based on risk	Annual review, leveraging continuous diagnostics where possible
Moderate	• Software or services supporting other non-public activities • Make/move/ sell services where redundancy exists	Self-attestation to security questionnaire	Compliance with retailer requirements reviewed before contract signing	Baseline third-party access controls in place – enhancements based on risk	Periodic review conducted on risk basis

Low	• External training vendor	Subsets of questionnaire, if any, based on risk	N/A	Baseline third-party access controls in place – enhancements based on risk	Periodic review conducted on whether risk has changed

*Determination is based on the extent to which the third party has access to the retailer's network and data (e.g., scope of third party's use by business units, regions, stores, etc. across the organization).

Sample Criteria for Criticality Determination

	Inherent Risk: High	Moderate	Low
Type of Information Accessed (Confidentiality and Integrity)	• Ability to review / manipulate sensitive corporate information • High Value Asset • Access to unencrypted PCI and/or proprietary information	• Ability to review but not alter or download sensitive corporate information • Access to company PII information	• No access to sensitive corporate information or PII
Availability of Information & Critical Business Processes	• Incident at third party prevents or limits ability to maintain critical business operations • Critical Software impacted	• Redundant suppliers are in place; impact will be felt but transitory	• Incident does not impact availability of data or critical business operations
Safety-Impacting Systems	• Impairment of technology could lead to significant safety impact		
Rights-Impacting Systems	• Impairment of technology could lead to significant impact on rights of employees or consumers		
Scale	• Large volume of information (bulk data)	• Moderate volume of data	• Minor volume
Partner Reputation / History	• Potential for high reputational impact if incident occurs	• Impact to third-party reputation but little effect on retailer	• No significant reputational impact in the event of incident becoming public

Appendix D: Inherent Risk and Control Prioritization

As noted earlier, a retailer may choose to use risk categories to assist in prioritizing supplier evaluation. The above section on Inherent Risk – Criticality and Impact, as well as Appendix C, provide general categories and criteria that a retailer may leverage to establish this prioritization process. Because suppliers will have differing inherent risk determinations, information requests to the supplier on security controls can be scaled based on the risk determination and the retailer's risk tolerance.

Some sets of authoritative guidance provide graduated sets of controls. For example, the Center for Internet Security's Critical Security Controls (CSC18) includes three Implementation Groups (IGs). IG1 reflects essential cyber hygiene. IG2 and IG3 build on the foundation laid by IG1. These categories can help retailers customize requests for information on the implementation of security controls and are based on the difficulty of implementing the control across the organization.

A retailer can determine the risk level a third party represents and then, along with the security questionnaire, provide a risk-based set of security controls the supplier should address.

The reality is that most organizations are on a journey to improve cybersecurity. Accordingly, many of the controls in question are likely to be *partially* implemented. Given this reality, several approaches are possible with respect to the data:

- Determination of minimum "passing" scores within each difficulty category – the minimums might rise depending on the inherent risk of the relationship.
- A requirement that *all* controls at lower levels of difficulty be at least *partially* implemented, and perhaps that some be *fully* implemented. At higher levels of inherent risk, then consider whether all controls at moderate levels of difficulty should also be at least partially implemented.
- A requirement that a customized set of controls be implemented – either partially or fully based on facts and circumstances of each relationship.
- Consideration of whether some controls can be counted as compensating controls for gaps in other control categories.

Appendix E: Example Compliance Standards

Compliance mandates from industry standards, government regulations and internally adopted corporate policies have had a significant impact on improving data security. Compliance standards themselves are often improperly equated to security but do help specify a minimum-bar level of data security and asset protection a retailer should adopt and implement.

Below are some example security/privacy standards relevant to retailers.

PCI

The Payment Card Industry (PCI) developed several standards to enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. These standards provide a baseline of technical and operational requirements designed to protect cardholder data and apply to everyone involved in payment card processing — including retailers, processors, acquirers, issuers, and service providers.

The standards relevant to retailers are: Data Security Standard (PCI-DSS), Payment Application Data Security Standard (PA-DSS, 2010), and the PIN Transaction Security Devices (PTS, 2010). Collectively these standards comprise a minimum set of requirements for protecting cardholder data and may be enhanced by additional controls and practices to further mitigate risks. Legislation or regulatory requirements may mandate additional specific protections for personally identifiable information or other data elements (for example, cardholder name). PCI, like other industry and corporate mandates, does not supersede local or regional laws, government regulations, or other legal requirements.

As a global standard developed and enforced by a consortium of payment card brands, PCI-DSS has had a significant influence on data security. Its specificity in requirements makes it one of the clearest to understand and implement. Payment card information includes the data on the chip or magnetic stripe of a payment card, the 16-digit primary account number, the expiration date, the cardholder's name, and the three-digit security code on the back of the card. Systems that need to be secured to protect this data include card readers, store networks (both in-store and online), and related data storage systems.

Third-party service providers can help companies maintain compliance with PCI security standards, but they do not relieve companies of all responsibility. As stated earlier in this document, it is the responsibility of the retail company to ensure, through due diligence and written agreements, that third parties are compliant with PCI security standards. Third parties that may handle retailers' PCI data include data storage facilities, payment processing systems, and call centers. Retailers should satisfy themselves that third parties handling their customers' PCI have risk-appropriate controls in place.

Please refer to www.pcisecuritystandards.org (PCI) for more information. Additionally, there is an ARTS specific whitepaper available.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was signed into US law in 1996 (Public Law 104-191). Although health care-specific, HIPAA is relevant to retail pharmacies as well as potentially to retail employee data. HIPAA covers practically any customer data held by health care providers. HIPAA compliance involves taking physical, technical, and administrative security measures to protect specified personal data, as well as reporting any breaches to the Secretary of Health and Human Services.

Protected Health Information

The HIPAA Privacy Rule protects most "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, on paper, or oral. The Privacy Rule calls this information *protected health information* (PHI).

Protected health information is information, including demographic information, which relates to: an individual's past, present, or future physical or mental health or condition; the provision of health care to the individual; or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. PHI includes many common identifiers (e.g., name, address, birth date, Social Security number) that can be associated with the associated health information.

For example, a medical record, laboratory report, or hospital bill would be PHI because each document would contain a patient's name and/or other identifying information associated with the health data content.

The HIPAA Omnibus Final Rule was released January 2013, and included updates from the Health Information Technology for Economic and Clinical Health (HITECH) Act, added breach notification and penalty tiers, and extended HIPAA compliance obligations to include both covered entities and business associates of those entities. Covered entities and business associates that create, receive, transmit, or maintain protected health information (PHI) in electronic form must make a good faith effort to protect the computing environment from reasonably anticipated threats and vulnerabilities; and take reasonable and appropriate measures to protect the integrity, confidentiality, and security of such electronic data.

The HIPAA Security Rule requires covered entities and business associates to perform an analysis of the potential risks to the electronic PHI for which they are responsible; and to then develop, implement, and maintain appropriate security measures to safeguard the integrity, confidentiality, and availability of that data. The HIPAA Security Rule incorporates recognized security objectives and protections but is intentionally technology-neutral. It provides standards and, in some cases, implementation specifications with which covered entities and business associates must comply.

The scope and nature of HIPAA compliance activities for each covered entity or business associate vary according to the specific environment and associated vulnerabilities as determined through risk assessment. Although the standard is objective, a covered entity or business associate's specific security controls may vary, because the HIPAA Omnibus Final Rule permits flexibility in the approach to compliance.

Although HIPAA-protected information may not seem as profitable to malicious actors as payment-related information, the breadth of information stored makes it a highly valuable target for committing identity theft. Data stored under HIPAA protection typically includes names, birth dates, Social Security numbers, and names of relatives, providing much of the necessary information for opening fake bank accounts, credit cards, or online accounts under victims' names. This profit incentive is a major driver behind the trend of increased cyber intrusions against the healthcare industry.

HIPAA regulations stipulate that covered entities must contractually establish security and privacy standards for any third party that is also handling or accessing its PHI.

Others

There are many different standards and types of guidance that are targeted for specific industries and circumstances. Many of these countries and regions feature different and even sometimes conflicting privacy and security principles. A company doing business and forging third-party relationships across a broad geographic area should proactively study data security and privacy regulations to understand what restrictions and challenges exist in different markets *a priori*. Some of these regulations include:

- EU Data Protection Regulations, including EU General Data Protection Regulation (2016/679), its predecessor EU Data Protection Directive 95/46/EC and related EU member state requirements. The 2016 regulation includes steep new fines as well as a "right to be forgotten." Companies were once able to rely upon the U.S.-EU Safe Harbor program as a means to meet EU data protection requirements; however an October 2015 European Court of Justice decision has eliminated Safe Harbor's protections for U.S. companies, meaning that U.S. companies will need to comply with EU member state requirements through alternative means, for example through participation in the US-EU Privacy Shield Framework (see https://www.privacyshield.gov/Program-Overview for more details) and/or implementation of EU's Binding Corporate Rules Framework and Model Contract Clauses.
- Consumer protection laws in other parts of the world also impose data security and privacy requirements on retailers, and many borrow from EU data protection laws. Some common rules include notifying customers of how their data is being stored and used, giving customers the choice to have data collected and allowing customers to access and correct the data stored about them.
- Children's Online Privacy Protection Act (COPPA), which deals with how data regarding minors is handled in the United States.
- State-level requirements, such as California's Online Privacy Protection Act and "Shine the Light" legislation.