Download Supply Chain Component Inventory

Jacob Moorman
Independent
download@zerotrack.net

Abstract

The download supply chain is a tool for delivering business-critical information to customers. When we focus solely on cybersecurity risk and think only about software engineering and delivery, we may overlook risks of great potential severity.

The existing body of supply chain knowledge is often presented in formats suited for large organizations with dedicated resources. Every download supply chain is different, and every download supplier has unique needs.

Download Supply Chain Component Inventory has been constructed to support teams of all sizes, including teams producing non-software downloads and small open source projects, to illuminate invisible download supply chain risks. Download Supply Chain Component Inventory is a lightweight approach that can be used during the design, implementation, and audit of download supply chains.

Available Support

Contact the author for paid consultative support, commercial licensing, or to support our work as a patron. Download Supply Chain Component Inventory is a publicly-released component of a more considerable family of download supply chain design and implementation resources.

The author can be reached by email at download@zerotrack.net

Disclaimers

Download Supply Chain Component Inventory does not represent the views or experiences of any current, past, or future company or any specific company, organization, or individual's supply chain, product, product experience, processes, people, technologies, supply chain design, supply chain implementation, audit findings, security, supply chain risks, or risk decisions. This research has been conducted independently. See "License Terms" for terms, including additional disclaimers.

Table of Contents

Introduction to Download Supply Chains

Millions of separate download supply chains collectively serve billions of downloaders worldwide. In modern terms, a download occurs when a file is retrieved from a server and saved to a computer. Downloaded files can contain an application, a document, an image, a video, or other data. Downloads typically occur over the internet. An estimated 67% of the world population is internet-connected[1]. Downloads can also occur over a corporate or university network. Downloads can occur to a mobile device, tablet, laptop, desktop computer, server, virtual machine, or cloud environment. There are billions of active devices globally[2].

Download activity differs from other types of internet activity in several ways. File assets are typically prepared in advance by a person or process and stored statically for exact, unaltered delivery. File assets are often opened by dedicated software on the computer or through a browser plugin. The saved copy of the data could be processed either immediately or later. File assets can range from very small to large, with transmission times varying from sub-second to hours.

Downloadable files are produced and delivered through a download supply chain. Downloaders may have varying degrees of technical knowledge and expertise and may or may not know that a download is being performed or how delivery occurs through the supply chain. Downloads can be initiated by a person, such as when a PDF document is requested, or can happen automatically, as is the case when the operating system performs automated updates to software installed on a computer. Regardless of whether the downloader knows the details, customer satisfaction, brand reputation, and business results may depend on successfully delivering downloadable files.

With millions of different sources for downloadable assets, there are millions of varying download supply chains. Some download supply chains are operated by paid employees of a company, such as one of the 55,000 companies listed on a stock market[3], and others are operated by volunteers or hobbyists. Some download supply chains serve paying customers, while others serve a broad community or ecosystem of users. The download producer entirely operates some download supply chains, while others depend on centralized infrastructure from a hosting provider.

[1] Wikipedia: List of countries by number of Internet users

[2] Wikipedia: Usage share of operating systems

[3] World Federation of Stock Exchanges (2024)

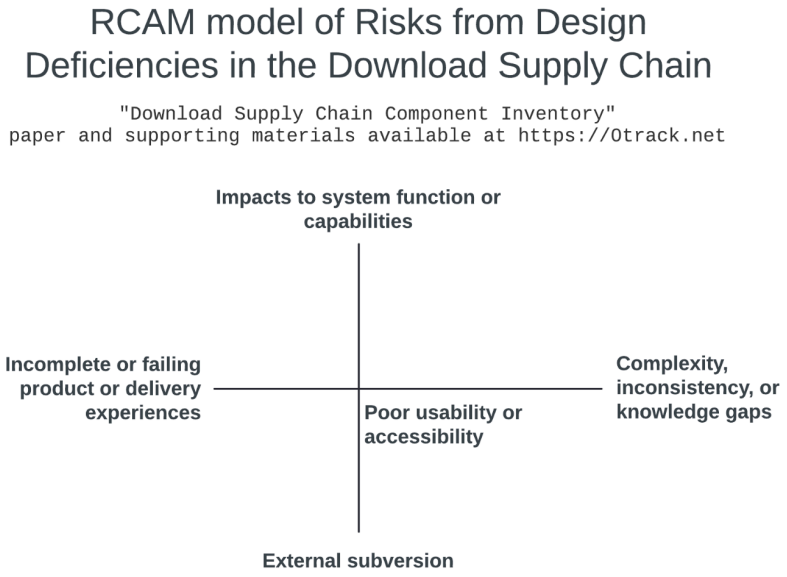
Download Supply Chain Risks

Every download supply chain is different, and every download supplier has unique needs. Business requirements and risk appetite can guide design priorities.

Download supply chain integrity is the ability of a download supply chain to correctly and accurately deliver the intended product experience. Problems with download supply chain integrity can be visible or latent. Download supply chain integrity problems may be expressed as IT (information technology) issues, UX (user experience) issues, or risks.

The risk present in every download supply chain and the severity of the potential impact will differ. A download provider may place different levels of value on customer satisfaction, protecting their brand reputation, and achieving business results that depend on successful download delivery. Perceived cost may also be critical in download supply chain design and implementation decisions.

Design Risks



RCAM (Resource Constrained Action Model) is a problem-solving technique available from `zerotrack.net` that enables problems to be visualized and attacked from multiple directions. RCAM was used to evaluate different risk impacts related to design deficiencies for the download supply chain. The following risks were identified:

Complexity, inconsistency, or knowledge gaps

- Every component of the supply chain may contribute to complexity and potential risk. Each aspect of each component present in the download supply chain can offer an opportunity to align supply chain behavior to the needs of the user and the business. Industry best practices and standards can provide helpful guidance on technology implementation.

- Components in the download supply chain are interconnected and interdependent. These relationships provide an opportunity to validate the correctness and consistency of the download supply chain design and implementation – whether the supply chain is consistent with itself.
- Knowledge gaps can mask risks. While download supply chain risks can be assessed and managed using established risk practices, these risks are likely to be overlooked, ignored, or incorrectly prioritized if the download supply chain is not part of a risk management program.
- It is important to document why decisions have been made since guidance changes over time.
- People are the least controlled element of the download supply chain. Whether we have staff under a contract, work with volunteers under an honor code, or have good relationships with our end users, people remain the greatest source of risk in the supply chain.
- Siloed and stovepiped implementations can be inconsistent. When different components of the download supply chain are not maintained consistently, the user can receive conflicting information, legitimate user needs can be impeded, and controls may not effectively prevent undesired behavior. When people, processes, and systems are handled consistently, there is potential to present a smaller attack surface.
- Download supply chain measurement is critical for business understanding and consistent production of business value but is sometimes underdeveloped. Measurement data, logs, reporting, oversight, and audit activities can be helpful in the timely detection of emerging threats and rapid diagnosis of business concerns. Governance, policies, regulations[4], and other factors may constrain how data is collected, stored, or used.

Impacts on system function or capabilities

- When installing some products, changes to the system are required to turn off network firewalls, malware detection software, or security mechanisms like SELinux. The user should be aware of these changes and their potential impact.
- The product installation, upgrade, downgrade, or uninstallation should not leave the system in a non-functional state[5].
- Finally, it is considered best practice that the product is secure by default[6]. The product installation, upgrade, downgrade, or uninstallation should not require further user action or configuration to reach a secure state.

[4] For example, GDPR (European user privacy protections), CCPA (Californian user privacy protections), and data retention policies
[5] https://en.wikipedia.org/wiki/2024_CrowdStrike-related_IT_outages
[6] https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf

Incomplete, failing, or unnecessary product or delivery experiences

- Supply chain risks are not all *security* risks. A download supply chain is successful if user needs are met, including fast and secure delivery of a product that meets the user's needs. While *some* supply chain risks are security risks, the download supply chain can also be impacted by information technology (IT) risks, such as capacity planning and availability issues, and by user experience (UX) risks, such as a failure to correctly manage end-user expectations, respond to failures, or align with end-user capabilities.

- It can be better to have only those components that serve a legitimate need rather than having more components, even when those components are implemented to best practices. The download supply chain is a way download providers address the needs of their users and businesses. Right-sizing depends on understanding both user and business needs. Only by understanding needs can the download provider plan an appropriate download supply chain.

- People seek solutions when they encounter problems. Do we want a user to respond with rash actions suggested by a third-party forum when encountering a problem? Do we want staff to subvert controls to enable an on-schedule release? When an experience breaks, who will users and staff rely on to guide them? How and when can norms be resumed?

- Problem detection should be considered, especially when trusting large-scale providers. Many download supply chains leverage cloud infrastructure, hosting providers, or centralized package repositories. These can be practical tools that provide consistency and high-quality delivery with less staff overhead. However, where a download provider cannot perform an in-depth audit or establish their controls on vendor-supplied infrastructure, additional consideration should be given to how problems with their downloads could be detected. Is the business dependent on users to find problems?

Poor usability or accessibility

- Every download supply chain is built to deliver a specific set of files, a product, to an intended set of users. The legitimate needs of the intended users are paramount, and supply chains can be designed and implemented to support user needs.

- A download supply chain may require security, information technology to support the production and delivery of assets, and consideration of user experience to understand and address user and business needs.

- The downloader considers success first based on whether the download accurately met their needs. If the product does not meet their needs, they may feel their time is wasted. Download delivery interfaces have a role in educating potential users about the product.

- The downloader expects downloads to be delivered securely and quickly, and secure and fast delivery is the primary purpose of a well-built download delivery system.

- The downloader also expects to pivot from downloading the product to using it with minimal fuss. If the product experience has been built well, this can be achieved.

- Accessible interfaces make the product available to the most significant potential audience.

External subversion

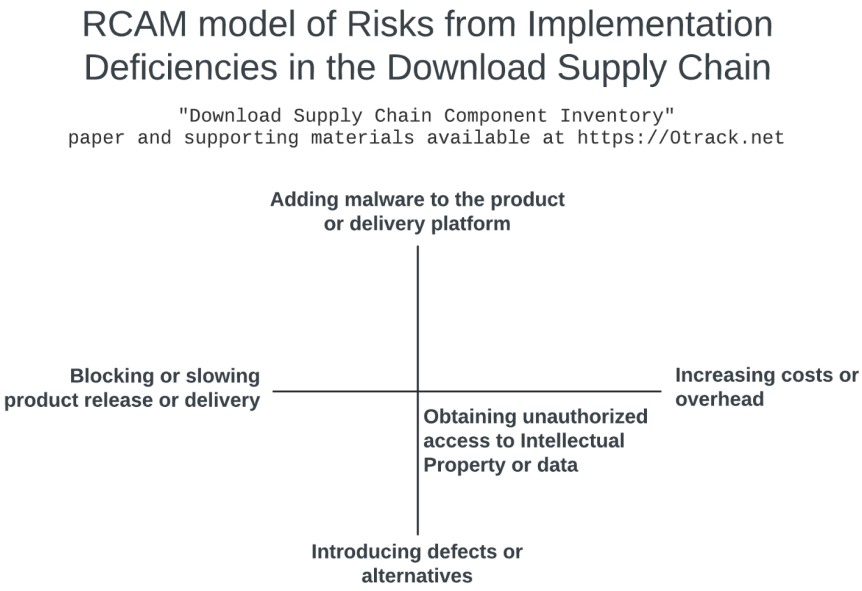
- Users may go around a protected supply chain. The ability to connect intended users to a protected supply chain may be subverted by third parties offering competing links through SEO (search engine optimization)[7], diverting user clicks through advertising content[8], instructing users to use the product differently than intended or to obtain the product or an entirely different product from a different source, resulting in one person's *potential* users becoming someone else's *actual* users. Where the user is human, we might need to consider any point where disinformation could taint the user's behavior and lead them away from our intended experience.

- Temporal (time) and longitudinal (over time) factors are often underappreciated. Rather than thinking about just the initial launch, we need to consider the full lifecycle, both internally and externally. Internal considerations include what happens if a person leaves the company and is the file owner for files related to the product? External considerations include what happens when a product is discontinued, to the domains, namespaces, and hosting infrastructure once used? Attacks on expired domains[9] are perhaps better known, but recent research[10] has identified that the users of end-of-life software may be attacked through previously legitimate distribution channels.

- We have the most significant potential to control our behavior and less potential to control the behavior of others (end users, third parties, and the greater ecosystem). Awareness of risks outside our control can enable risk responses within our controlled areas, such as informing the user of norms, monitoring download traffic for unexpected patterns, and providing channels for support issue escalation.

[7] https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/seo-poisoning/
[8] https://support.google.com/adspolicy/answer/13528034?hl=en
notes Google Ads prevents advertising free desktop software for this reason, but there are other ad platforms
[9] https://portswigger.net/daily-swig/how-expired-web-domains-help-criminal-hackers-unlock-enterprise-defenses
[10] https://jfrog.com/blog/revival-hijack-pypi-hijack-technique-exploited-22k-packages-at-risk/

Implementation Risks



RCAM (Resource Constrained Action Model) is a problem-solving technique available from `zerotrack.net` that enables problems to be visualized and attacked from multiple directions. RCAM was used to evaluate different risk impacts related to implementation deficiencies for the download supply chain. The following risks were identified:

Increasing costs or overhead

- Attackers can target supply chains at any time, using any single or multiple methods, so defenders must maintain effective supply chain defenses, even when limited resources restrict available defenses.
- Denial of service (DoS) attacks, distributed denial of service (DDoS) attacks[11], the generation of download activity or communications that do not serve a legitimate purpose, competitive behavior, and anti-competitive[12] behavior have the potential to increase cost or overhead.

Adding malware to the product or delivery platform

- Many initiatives[13], with due cause, focus on hardening software engineering practices and consider improvements to third-party software dependency management as ways to reduce the likelihood of malware being introduced to a product before product delivery.
- The delivery environment may also be targeted, either injecting malware into the product during the product delivery process or using the platform to separately distribute malware.

[11] https://www.perimeter81.com/blog/network/ddos-attack-cost
[12] https://en.wikipedia.org/wiki/Anti-competitive_practices
[13] For example, https://slsa.dev/

- Malware delivery or malware behavior may be targeted to specific downloaders.
- Many points in the download supply chain can work together to maintain integrity even if some supply chain controls fail or are bypassed. There is no one-size-fits-all approach to defense in depth for a download supply chain.
- Non-software downloads can also contain malware. While most guidance on digital supply chains is focused on software production, some downloadable assets are PDF documents, images, and video files. Since the production of these non-software assets could be corrupted to include malware, it is crucial to consider these download supply chains.

Blocking or slowing product release or delivery

- A download supply chain is successful if user needs are met, including fast delivery. The downloader can be located anywhere, on any type of internet connection. The downloader may use VPN (virtual private networking) or onion routing. The speed of the download delivery will depend on factors such as the speed of the downloader's internet connection, the speed of the internet connection for the server delivering the download, and the proximity of the downloader to that server. It may be impractical or impossible to receive large files in some locations or over some internet connections.
- Problems that impede the release or delivery of product updates can leave users on older, potentially more vulnerable product versions. The ability to mitigate user problems can depend on the timely release and uptake of new versions. Users may be more likely to upgrade if they know the risks associated with not upgrading and understand what has changed in the latest product versions. Testing and validation remain essential.
- Dependencies and dependents can both introduce unexpected outcomes. Many initiatives are working to enumerate software dependencies[14] and mitigate the risk of malicious code[15] introduction via dependencies. There has been less focus on the influence of dependents, the software that depends on the product. Dependents influence product sourcing, including the product used to satisfy a named dependency, installed product versions, and the instructions used to implement products. Dependents can block upgrades to a product.

Obtaining unauthorized access to Intellectual Property (IP) or data

- In addition to supporting the legitimate needs of intended users, the download provider may also consider rejecting unauthorized users and illegitimate needs essential. Controls can be established within the download supply chain to enforce policies and security requirements and perform other risk mitigation.
- Controls may be needed to limit who can access approved releases, prevent the unauthorized release of intellectual property (IP), or prevent unauthorized access to collected data such as log data, measurement data, or reports.

[14] https://cyclonedx.org/
[15] https://en.wikipedia.org/wiki/XZ_Utils_backdoor

Introducing defects or alternatives

- A supply chain consists of multiple components. When considering the product experience, the supply chain includes the production of a downloadable asset, delivering the downloadable asset, and the resulting product experience.
- Download supply chain integrity can be corrupted by:
    - Design limitations
    - Defective implementation
    - Accidental, incorrect, unexpected, or complicated behavior
    - Inattention, ineptitude, or responsibility failures
    - Malicious acts
- A corrupt download supply chain can impact availability, compliance, confidentiality, cost, intellectual property, opportunity costs, overhead, people, reputation, resources, satisfaction, trust, and vulnerability.
- The ecosystem may influence users through third-party websites and associated search results. The product ecosystem includes our product, products that have our product as a dependency (dependents), products our product depends on (dependencies), and the extended community, which includes our product, dependents, dependencies, peers, partners, competitors, and their users.
- Promotion of alternatives, such as competing products, third-party product variants, malware, or off-label product use, can generate unexpected user outcomes.

Download Supply Chain Component Inventory

If a download supply chain is poorly understood, whether small or complex, risks may remain invisible until impact occurs. An inventory can bring into focus the areas that require deeper technical understanding.

Download Supply Chain Component Inventory enables product level and portfolio (many products) level inventory of a download supply chain. Download Supply Chain Component Inventory can be used on small and large scales by download providers who manage a single PDF file and providers with complex software and product portfolios.

Download Supply Chain Component Inventory can be used in several ways, including:

- Document an existing download supply chain, considering the maximum relevant scope to reduce the risk of missing important details.
- Identify the minimum necessary scope needed to serve the needs of users and the business, reducing the risk of extraneous or unnecessary requirements.
- Visualize risk and maturity present in the download supply chain to support risk discussions and decisions.
- Prepare project plans using “today” and “future” views to prioritize enhancements, understand expected risk reduction, and understand change risks. Given the standardized structure, an inventory can also help track progress as part of continuous improvement efforts.

Design and implementation practices and the resulting complexity of a single supply chain substantially vary. Recognizing that every supply chain is different, Download Supply Chain Component Inventory can serve as a starting point that can be expanded, reduced, or modified to account for the desired or actual implementation of a specific download supply chain.

When auditing a download supply chain, beginning with product specifications and working backward through the inventory from the data collection experience to product supports may be appropriate.

Download Supply Chain Component Inventory can be used in tandem with and does not supersede or supplant the work of existing standards, which can be used to inform best practices for each component and the download supply chain as a whole. Existing initiatives are centered around the software engineering process, third parties, the delivery process, or a specific segment. These areas are important and are a subset of the components included in the Download Supply Chain Component Inventory. For additional information, see “Suggested Resources”.

Component Diagram

The following diagram summarizes the components included in the Download Supply Chain Component Inventory. When used as a visualization, the diagram can be colorized, or data overlays can be added.

For a listing of the components, see “Component Listing and Inventory Questions”. Download supply chains vary. The listed components are intended as a starting point, and the listing can be amended to account for the specific needs of a download supply chain.

This diagram is available in several formats from `https://zerotrack.net/`

Download Supply Chain Component Inventory

A. **Product Specifications**	A01. Product Name	A02. Product Purpose	A03. File Naming Scheme	A04. File Formats	A05. Product Branding	A06. License Terms	A07. Canonical Home	A08. OS Platforms	A09. Hardware Architectures	A10. Versioning Scheme	A11. Conformance, Compliance Requirements	A12. Dependencies
B. **Product Supports**	B01. Product Discovery	B02. Product Documentation	B03. First Party Support	B04. First Party Training	B05. User Management	B06. User Authentication	B07. Download Initiation	B08. Release Awareness	B09. Vulnerability Reporting	B10. Dependent Applications	B11. Third Parties & Community	B12. Ecosystems
C. **End-User Responsibilities**	C01. Usage Purpose	C02. Authorization	C03. Prerequisities	C04. Instructions	C05. Product Configuration	C06. Change Approval	C07. Validation	C08. Issue Escalation	C09. Product Licensing	C10. Update Management	C11. Product Training	C12. Product Operation
D. **Product Experience**	D01. Installation Action	D02. Upgrade Action	D03. Downgrade Action	D04. Uninstall Action	D05. Manual Methods	D06. Semi-Auto Methods	D07. Automated Methods	D08. Delivery to Everyone	D09. Progressive Delivery	D10. Latest Release Target	D11. Specific Release Target	D12. Specific Maturity Target
	D13. Expected Result Achieved	D14. Experience Aligns to Spec/Guidance	D15. Preservation of Existing Data/Configs	D16. Product Secure by Default	D17. Resulting System Security	D18. Usability	D19. Accessibility	D20. Error Handling	D21. License Keys	D22. License Term Enforcement	D23. Phone Home/ Telemetry	D24. EOL Product Behavior
E. **Delivery Methods**	E01. HTTPS / HTTP	E02. rsync, rsync+ssh	E03. P2P Technologies	E04. Source Reporitory	E05. Distribution Inclusion	E06. Repository Inclusion	E07. Backups and DR	E08. Download Mirrors	E09. CDN	E10. Network File Shares	E11. FTP, TFTP, exotics	E12. 2nd & 3rd Party Delivery
F. **Delivery Environment**	F01. Domains	F02. DNS	F03. Ports and Addresses	F04. Keys and Certificates	F05. Storage	F06. Servers	F07. Delivery Applications	F08. Limits and Controls	F09. Initiated Behavior	F10. Security Infrastrtucture	F11. Logging Infrastructure	F12. Measurement Infrastructure
G. **Lifecycle Management Experience**	G01. New Version Release	G02. New Product Release	G03. Maturity Levels	G04. Release Removal	G05. Product Version EOL	G06. Product EOL	G07. Product Name/Brand Change	G08. URL Management	G09. License Terms Change	G10. Timed or Embargoed Release	G11. Source Tagging	G12. Package Metadata
H. **Producer Responsibilities**	H01. Hardened Systems	H02. Secure Comms	H03. Trained	H04. Authorized	H05. Understands Requirements	H06. Maintains Change Awareness	H07. Communicates Changes	H08. Produces Changes	H09. Maintains Records	H10. Verifies Changes	H11. Obtains Approval	H12. Verifies Effects
I. **Production Experience**	I01. Change Authorization Process	I02. Change Tracking Process	I03. Build Process	I04. Dependency Management Process	I05. Test Process	I06. Packaging Process	I07. Sums and Signatures Process	I08, IP Protection Process	I09. Staging Process	I10. Push Process	I11. Rollback Process	I12. Producer Supports
J. **Production Environment**	J01. Change Authorization Tooling	J02. Change Tracking Tooling	J03. Build Tooling	J04. Dependency Management Tooling	J05. Test Tooling	J06. Packaging Tooling	J07. Sums and Signatures Tooling	J08, IP Protection Tooling	J09. Staging Tooling	J10. Push Tooling	J11. Rollback Tooling	J12. Producer Supports Infrastructure
K. **Oversight Responsibilities**	K01. Hardened Systems	K02. Secure Comms	K03. Oversight Capability	K04. Authorized	K05. Understands Requirements	K06. Approved Change Requests	K07. Maintains Records	K08. Necessary Reporting	K09. Verifies Work	K10. Approves Release	K11. Manages Escalated Issues	K12. Delivery SLA
L. **Data Collection Experience**	L01. Availability	L02. Anti-Abuse	L03. Compliance	L04. User Account Events	L05. Initiated Downloads	L06. Completed Downloads	L07. Download Timing	L08. Install Base Segments	L09. Use of Supports	L10. Unauthorized Release Detection	L11. File Change Detection	L12. Policy Alignment

Component Listing and Inventory Questions

The following download supply chain components can be evaluated when considering a download supply chain. Supply chains vary, and some listed components may not be relevant to some download supply chains. Listed components are intended as a starting point, and the listing can be amended to account for the specific needs of a download supply chain.

Each component includes a representative starter question that can aid the inventory process. In follow-up, additional questions should be asked to gain a sufficient understanding of how the supply chain design and implementation address the component.

A. Product Specifications

Product Specifications define the products to be produced, and the number of product variants delivered through a download supply chain.

ID	Description	Question
A01	Product Name	What names are used for the downloadable product?
A02	Product Purpose	What does this product do for the user?
A03	File Naming Scheme	What file naming scheme, including file extensions, is used for product downloads?
A04	File Formats	What file formats are used for product downloads?
A05	Product Branding	What branding is associated with product downloads?
A06	License Terms	Under what license terms is the product provided?
A07	Canonical Home	What is the canonical web page for this product?
A08	OS Platforms	What operating systems (OS) are supported by product downloads?
A09	Hardware Architectures	What hardware architectures are supported by product downloads?
A10	Versioning Scheme	How are versioning numbers used for the product?
A11	Conformance, Compliance Requirements	What voluntary conformance and required compliance must be met by the product and product delivery?
A12	Dependencies	What software libraries, data, or other materials does the product depend on?

B. Product Supports

Product Supports guide or influence an end user's behavior when implementing or using a product. Incorrect guidance can result in unintended outcomes.

ID	Description	Question
B01	Product Discovery	How does the user discover this product?
B02	Product Documentation	What information supports the proper use of the product?
B03	First Party Support	How does the end user obtain "official" support for the product?
B04	First Party Training	How does the end user obtain "official" training on the product?
B05	User Management	How can an end user register to gain access to product downloads?
B06	User Authentication	How can an end user log in to gain access to product downloads?
B07	Download Initiation	How does an end user initiate a product download?
B08	Release Awareness	How does an end user become aware of new product releases?
B09	Vulnerability Reporting	How does an end user report a product vulnerability, and what happens if vulnerabilities are reported through any other channel, such as a feedback reporting mechanism?
B10	Dependent Applications	What applications are dependent on our product?
B11	Third Parties & Community	What resellers, partners, marketplaces, community repositories, translations, support providers, community forums and chat systems, expert community members, power users, or competitors have posted information about our product?
B12	Ecosystems	What ecosystems, such as technology-focused communities, does our product belong within?

C. End-User Responsibilities

End Users are the reason that downloadable assets exist. By considering what a responsible end user would want to do and understanding that some end users may not align with this motivation, we can appreciate critical interactions between the end user, the product, and the infrastructure.

See “Human Factors” for a timeline view that includes these responsibilities.

ID	Description	Question
C01	Usage Purpose	What legitimate reasons would cause the end user to want to download and use the product?
C02	Authorization	How does an end user obtain authorization to download and use the product?
C03	Prerequisites	What requirements must be met before an end user can use the product?
C04	Instructions	What instructions does an end user follow to download and use the product successfully?
C05	Product Configuration	In what ways is the product configurable by an end user?
C06	Change Approval	What changes to an end user's system must they approve before installing and using the product?
C07	Validation	How can end users confirm they have downloaded, installed, and used the product correctly?
C08	Issue Escalation	How can end users contact us if they encounter issues downloading, installing, or using the product?
C09	Product Licensing	How can end users obtain a license for the product?
C10	Update Management	What actions must an end user take to manage updates to the product?
C11	Product Training	Is there an expectation that the end user will obtain training on the product?
C12	Product Operation	What are the functions typically performed by an end user using the product?

D. Product Experience

The **Product Experience** includes product capabilities, behaviors, and procedures, which are significant user behavior factors. When the product experience does not align with the end user's expectations, this can trigger the user to take actions that have unexpected outcomes.

ID	Description	Question
D01	Installation Action	How is the product installed?
D02	Upgrade Action	How is the product upgraded to a higher product version?
D03	Downgrade Action	How is the product downgraded to a lower product version?
D04	Uninstall Action	How is the product uninstalled?
D05	Manual Methods	How is the product managed by the end user using manual methods, such as interactive commands?
D06	Semi-Auto Methods	How is the product managed by the end user using semi-automated methods, such as an automated script executed manually or manually executed package manager commands?
D07	Automated Methods	How is the product managed independent of the end user using automated methods, such as scheduled cron jobs, actions taken when the product is executed, or actions performed automatically by the package manager software?
D08	Delivery to Everyone	Are new product versions rolled out to all end users concurrently?
D09	Progressive Delivery	Are new product versions rolled out to a subset of users progressively?
D10	Latest Release Target	Is it possible to request the installation of the "latest" product release?
D11	Specific Release Target	Is it possible to request the installation of a specific release version of the product?
D12	Specific Maturity Target	Is it possible to request the installation of "stable", "development", "test", "beta" or other specific maturity levels of the product?
D13	Expected Result Achieved	Do supported actions, using supported methods against supported targets, produce the expected result?
D14	Experience Aligns to Spec/Guidance	Does the product's download, installation, and usage align with released specifications and guidance?
D15	Preservation of Existing Data/Configs	Do supported actions, using supported methods against supported targets, preserve existing data and configuration information?
D16	Product Secure by Default	Do supported actions, using supported methods against supported targets, result in a secure product state without further action or configuration by the end user?

D17	Resulting System Security	When the product is implemented in alignment with released instructions and guidance, is the resulting system security impact understandable by the end user? For example, if standard security features of the operating system are turned off, is the user made aware of this?
D18	Usability	Does the product experience meet the end user's usability expectations?
D19	Accessibility	Does the product experience meet the end user's accessibility requirements?
D20	Error Handling	Does the product generate meaningful error messages and guidance?
D21	License Keys	How does the product use license keys?
D22	License Term Enforcement	How does the product enforce license terms?
D23	Phone Home/Telemetry	Does the product contact vendor servers during installation or usage?
D24	EOL Product Behavior	When a product reaches end-of-life, what happens to product licenses, downloads, downloaded files, and installations?

E. Delivery Methods

Delivery Methods include the protocols and technologies used to serve traffic to the end user. Each delivery method uses a different delivery application and configuration, has different security attributes and control capabilities, has different associated best practices, and is applicable only if end users use compatible client technology.

ID	Description	Question
E01	HTTPS / HTTP	Is the product delivered to end users using HTTPS or HTTP?
E02	rsync, rsync+ssh	Is the product delivered to end users using rsync or rsync over SSH?
E03	P2P Technologies	Is the product delivered to end users using peer-to-peer file sharing?
E04	Source Repository	Is the product delivered to end users using source repository tools like Git?
E05	Distribution Inclusion	Is the product included in operating system distributions, such as Linux OS distributions?
E06	Repository Inclusion	Is the product included in any technology-focused repositories, such as Python's PyPi, Docker's DockerHub, or TeX's CTAN?
E07	Backups and DR	Are backups and a disaster recovery environment maintained for the production environment and delivery environment?
E08	Download Mirrors	Is the product delivered to end users from download mirrors?
E09	CDN	Is the product delivered to end users from a content delivery network (CDN)?
E10	Network File Shares	Is the product delivered to end users using network file shares?
E11	FTP, TFTP, exotics	Is the product delivered to end users using unencrypted or unsecured protocols such as FTP, TFTP, or any in-house or exotic method?
E12	2nd & 3rd Party Delivery	Is the product mirrored by end users for redistribution or delivered by any third parties?

F. Delivery Environment

The **Delivery Environment** allows the end user to retrieve downloadable materials upon request. A separate delivery environment may exist for each delivery method, product experience, and product variant.

ID	Description	Question
F01	Domains	What domain names, domain name registrars, and domain name registries are involved in delivery, and what domain names are present in the product?
F02	DNS	What DNS records (including hostnames), DNS providers, and DNS configuration are involved in delivery, and what hostnames are present in the product?
F03	Ports and Addresses	What IP addresses, IP address owners, and non-IP networking are involved in delivery, and what IP addresses are present in the product?
F04	Keys and Certificates	What encryption configuration, certificates, and certificate authorities are involved in delivery, and what cryptographic materials are present in the product?
F05	Storage	What equipment, operating system (OS), networking, applications, access controls, administrative authentication, and logging are used on devices that store files before delivery, and where are storage devices located?
F06	Servers	What equipment, operating system (OS), networking, applications, access controls, administrative authentication, and logging are used on servers that deliver files, and where are servers located?
F07	Delivery Applications	What software, software configurations, protocols, headers, cookies, cookie consent management, analytics, government licenses or permits, privacy policy statements, and terms of service are involved with download delivery?
F08	Limits and Controls	What anti-DDoS, robots.txt, rate limiting, blocklists, user authentication, IP controls and geolocation, path restrictions, time-based URLs, timeouts, queue sizes, and file limits are used to restrict or control download delivery?
F09	Initiated Behavior	When a download is initiated, what file delivery, failure handling, redirects, MIME type handling, automated script execution, and command-line download utility behavior are expected?
F10	Security Infrastructure	What security infrastructure, including physical-, network-, and system-level infrastructure, supports the policies, governance, regulatory, and other requirements that apply to the security of the delivery environment?
F11	Logging Infrastructure	What logging infrastructure supports the policies, governance, regulatory, and other requirements that apply to the delivery environment?
F12	Measurement Infrastructure	What measurement infrastructure supports the policies, governance, regulatory, and other requirements that apply to the delivery environment?

G. Lifecycle Management Experience

The **Lifecycle Management Experience** defines various capabilities related to managing the product life cycle, such as launching a new product version or declaring a product's end-of-life. These capabilities may offer problem-solving options when new business needs arise.

ID	Description	Question
G01	New Version Release	What process releases a new version of the product?
G02	New Product Release	What process releases a new product?
G03	Maturity Levels	What maturity levels (e.g., stable, development, test, beta) or maturity programs (e.g., customer beta, public beta) are used for the product?
G04	Release Removal	What process removes a previously released version of the product? (e.g., for severe defects such as catastrophic data loss or due to a legal requirement)
G05	Product Version EOL	What process is used when a product version reaches end-of-life?
G06	Product EOL	What process is used when a product reaches end-of-life?
G07	Product Name/Brand Change	What process carries out a product name change or branding change?
G08	URL Management	How are URL paths or namespaces managed on delivery servers?
G09	License Terms Change	What process is used if license terms need to change?
G10	Timed or Embargoed Release	What process is used if a release must occur on a timed basis, such as after an embargo deadline?
G11	Source Tagging	What process tags source materials with version information that matches the associated product downloads?
G12	Package Metadata	What process manages package metadata, including dependency information?

H. Producer Responsibilities

Producers are people who take the actions needed to generate downloadable assets and contribute to product success. These responsibilities can be segmented or duplicated among multiple people.

ID	Description	Question
H01	Hardened Systems	Do producers work from hardened systems and devices?
H02	Secure Comms	Are secure communication systems used among producers and when communicating with overseers?
H03	Trained	Have producers been trained to securely use the production environment, including technologies, programming languages, and software?
H04	Authorized	Are producers authorized to produce change by working in the production environment?
H05	Understands Requirements	Do producers have access to and fully understand the requirements for changes they produce?
H06	Maintains Change Awareness	Do producers maintain awareness of changes they are executing, changes made by others, the production environment and the delivery environment, and changes in upstream software dependencies?
H07	Communicates Changes	Do producers maintain an accurate record of changes, including any variances between the produced change and the requirement?
H08	Produces Changes	Do producers execute only approved changes and execute only using the production environment?
H09	Maintains Records	Do producers safeguard records, such as logs, produced by the supply chain?
H10	Verifies Changes	Do producers verify that their changes align with requirements and are functional?
H11	Obtains Approval	Do producers obtain approval to release change only after verification?
H12	Verifies Effects	Do producers monitor and verify the actual effect of changes after release?

I. Production Experience

Production Experience considers the processes used when generating downloadable assets.

ID	Description	Question
I01	Change Authorization Process	What process authorizes changes to the product, production environment, or delivery environment?
I02	Change Tracking Process	What process tracks changes (such as edits to source code, configuration files, and installed software) for the product, production environment, or delivery environment?
I03	Build Process	What process produces product downloads from source materials, and to what extent is that process repeatable and automated?
I04	Dependency Management Process	What process manages the software dependencies (e.g., build tools, compilers, interpreters, software libraries, document editors) used to build the product?
I05	Test Process	What process tests the product, including quality assurance, continuous integration, and automated testing?
I06	Packaging Process	What process packages the product for release, including file archive management and package repository management?
I07	Sums and Signatures Process	What process generates cryptographic sums and signatures for the product or downloadable files?
I08	IP Protection Process	What process confirms that files prepared for release contain the correct intellectual property, meet licensing requirements, and do not contain material unintended for release?
I09	Staging Process	What process stages change for release?
I10	Push Process	What process pushes materials out at the time of release?
I11	Rollback Process	What process rolls back a release, e.g., if the release fails or the released product must be withdrawn shortly after release?
I12	Producer Supports	What information, tools, and other resources are consulted by producers during production?

J. Production Environment

The **Production Environment** includes the systems, tools, and infrastructure to generate downloadable assets.

ID	Description	Question
J01	Change Authorization Tooling	What systems, tools, and infrastructure are used for change authorization?
J02	Change Tracking Tooling	What systems, tools, and infrastructure are used for change tracking and change review?
J03	Build Tooling	What systems, tools, and infrastructure are used to build the product, automate the build process, or store build results?
J04	Dependency Management Tooling	What systems, tools, and infrastructure are used to retrieve, build, test, integrate dependencies, or store test results?
J05	Test Tooling	What systems, tools, and infrastructure are used to perform testing, CI/CD, test automation, or store test results?
J06	Packaging Tooling	What systems, tools, and infrastructure are used for packaging or store packaging results?
J07	Sums and Signatures Tooling	What systems, tools, and infrastructure are used to produce cryptographic hashes, signatures, keys, tokens, certificates, or store cryptographic materials?
J08	IP Protection Tooling	What systems, tools, and infrastructure are used to confirm that IP protection mechanisms (e.g., DRM) are appropriately included and that there is no unintended IP release?
J09	Staging Tooling	What systems, tools, and infrastructure are used for a staging environment or to produce a staging environment that matches end user-facing environments?
J10	Push Tooling	What systems, tools, and infrastructure are used to push a release or to prevent unintended release?
J11	Rollback Tooling	What systems, tools, and infrastructure are used to roll back a release or prevent unintended rollback?
J12	Producer Supports Infrastructure	What systems, tools, and infrastructure are used to deliver producer supports, authenticate to producer supports, or authenticate to the production environment?

K. Oversight Responsibilities

Oversight of people, processes, and systems helps ensure supply chain operations occur as intended. These responsibilities may be segmented or duplicated among multiple overseers.

ID	Description	Question
K01	Hardened Systems	Do overseers work from hardened systems and devices?
K02	Secure Comms	Are secure communication systems used among overseers and when communicating with producers?
K03	Oversight Capability	Do overseers have the capability (e.g., skills, training, time) to provide effective oversight?
K04	Authorized	Have overseers been authorized to perform all oversight functions?
K05	Understands Requirements	Are overseers aware of control requirements, implemented controls, product requirements, and the intended product experience, lifecycle management experience, production experience, data collection experience, the delivery environment, and the production environment?
K06	Approved Change Requests	Do overseers prepare, review, and approve or reject all proposed change requests before implementation?
K07	Maintains Records	Do overseers safeguard records, such as logs, produced by the supply chain?
K08	Necessary Reporting	Do overseers produce and deliver all necessary reporting as directed by policies, governance, regulatory, or other relevant requirements?
K09	Verifies Work	Do overseers confirm that produced changes align with policies, other requirements, and requested changes except for approved variances?
K10	Approves Release	Do overseers approve the release of product changes, the delivery environment, the delivery experience, the production environment, and the production experience?
K11	Manages Escalated Issues	Do overseers receive and manage all escalated issues and vulnerability reports?
K12	Delivery SLA	Do overseers maintain, measure, and monitor the delivery alignment to service level agreements (SLA)?

L. Data Collection Experience

The **Data Collection Experience** defines various types of information commonly used to confirm the proper functioning of the download supply chain. This list includes typical download supply chain KPIs (Key Performance Indicators). Data can offer insights when business questions arise, but collection must be planned since retroactively obtaining data may not be possible. Policy, governance, and regulatory requirements may guide how information is collected, stored, and used.

ID	Description	Question
L01	Availability	What information is collected regarding the availability of the delivery environment and production environment?
L02	Anti-Abuse	What information is collected to support anti-abuse controls?
L03	Compliance	What information is collected to verify the effectiveness of required controls?
L04	User Account Events	What information is collected about user account creation, authentication, and changes?
L05	Initiated Downloads	How and where are initiated downloads measured, and what information is collected about initiated downloads?
L06	Completed Downloads	How and where are completed downloads measured (e.g., each 51% delivery per file/IP address/day or 100%), and what information is collected about completed downloads?
L07	Download Timing	What information about DNS resolution times, first byte delivery times, download completion times, or other delivery timing is collected?
L08	Install Base Segments	What information is collected about installed versions, upgrade events, operating systems, hardware architectures, user locations, or other segmentation of the product install base?
L09	Use of Supports	What information is collected about end user use of product supports, and is this correlated to customer support activity or product success?
L10	Unauthorized Release Detection	How are product releases monitored, and can unauthorized releases be detected?
L11	File Change Detection	How are file changes monitored, and can unauthorized file changes be detected?
L12	Policy Alignment	Based on governance, legal requirements, location-based requirements given the placement of servers, data retention policies, or other factors, what additional requirements must be met by the product, product production, product delivery, supporting environments, measurement or monitoring, or people involved with the product? For example, in the case of people, background checks, export compliance, geographic location, policy compliance, training, or honor codes.

Deep-dive Questions

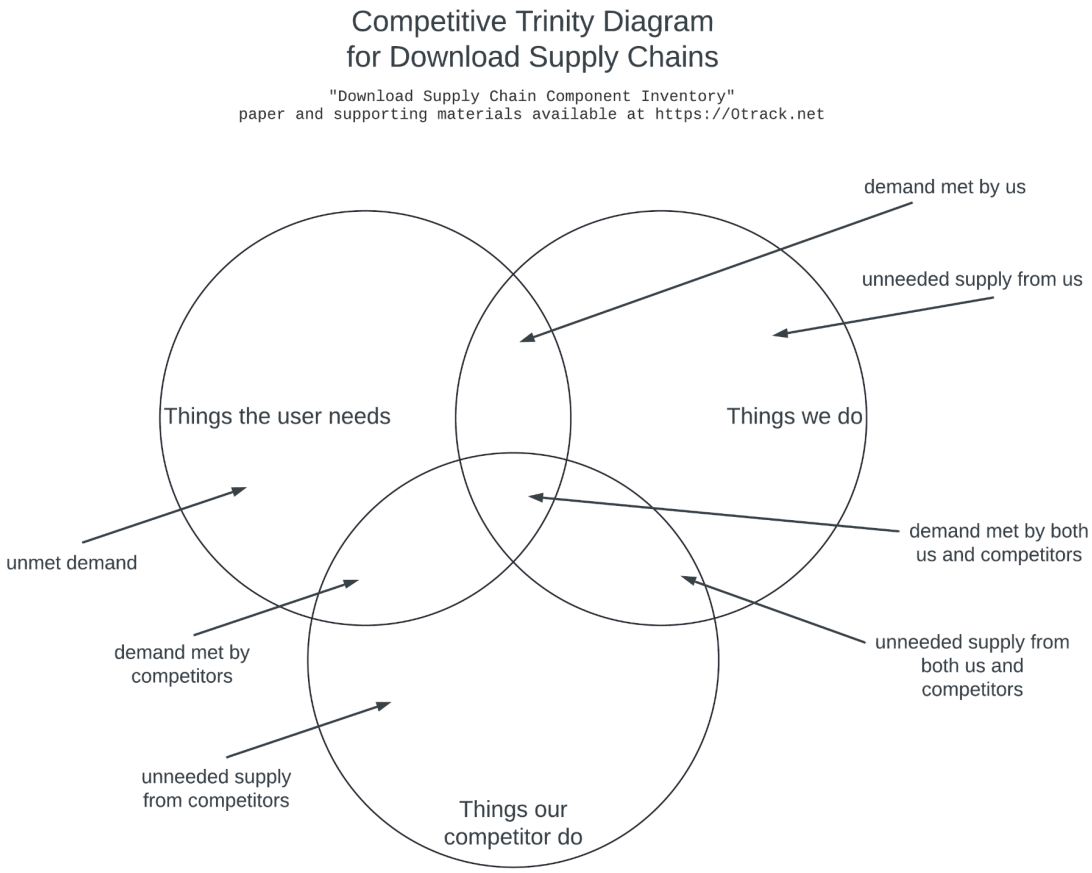
After initial inventory, the following questions can aid a deeper understanding of the maturity and invisible risk present in the download supply chain:

1. Does the download supply chain implementation align with business-desired outcomes?
2. Are there any extraneous components within the download supply chain?
3. Are aspects of the implementation consistent with each other, except for intended variants?
4. Which processes are automated, and which are manual?
5. Do sufficient controls exist across the download supply chain?
6. Is effective oversight present for all aspects of the download supply chain, including people, systems, processes, and data (e.g., files, logs, measurements)?
7. Have best practices been identified and applied in the implementation?
8. Do sufficient supports exist for the end user to be successful?
9. Does our product include other products or advertising, or is our product ever bundled with other products?
10. Are all aspects of the supply chain genuinely accounted for, or are there tools and information used that are outside our awareness?
11. Are there any known cases where normally-collected data, such as logs, were not collected, or were modified, removed prematurely, or lost?
12. Are there any known cases where a storage or server device, network infrastructure, hard drive, cryptographic key or certificate, domain, hostname, IP address, product, product version, release, or released file was decommissioned, replaced, removed, or lost; or known cases where physical security, network security, or system security were breached?
13. Are there any known cases where availability was impacted, delivery was unavailable or slower than expected, or a delivery SLA (service level agreement) was breached?
14. Are there any known cases where intellectual property was released accidentally, where a release was rolled back, where the release or rollback process failed, where malware detection triggered an alarm, or where a release occurred accidentally or without proper approval?
15. Are there any known incidents, policy violations, or honor code violations, including cases without a formal response and cases that invoked an incident response plan?

Next Steps

While Download Supply Chain Component Inventory can help identify and assess risks, further steps are needed for risk management. Risk conditions in a download supply chain are not equally important; some require a greater or faster response. Download supply chain risks cannot be eliminated but can be avoided, transferred, mitigated, exploited, or accepted. Professional guidance from IT risk management, user experience (UX), legal, and IT operations professionals may be needed. Risk response can include compliance activities, IT controls, capacity planning, availability management, Quality Assurance (QA), focus on operational excellence, continuous improvement, User Research (UR), and User Testing (UT).

Strategic Planning



The following considerations are helpful when evaluating a download supply chain strategically:

- What are the needs of the user and the business?
    - The answer is influenced by the things the user needs.
    - The answer may include things the user needs, future-looking things we believe future users will need, things needed to counter competitor offerings, or things required by governance.

- How would the business measure success, and how would a user measure success?
    - The answer is influenced by the things the user needs.
    - The answer may indicate a competitive misalignment in the approach.
    - The answer may indicate an unneeded supply.

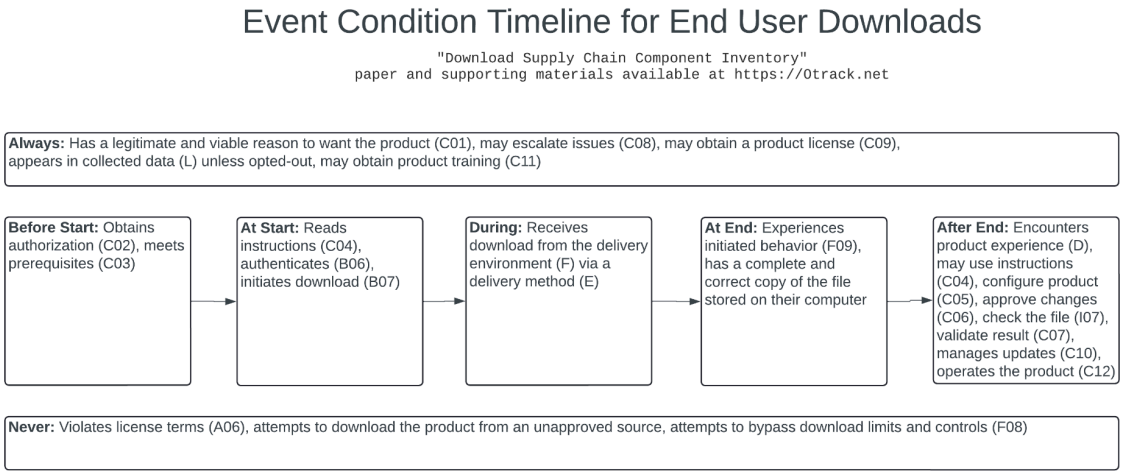
- How does the approach differ from that of competitors?
    - The answer is influenced by the things our competitors do and the things we do.
    - The answer may indicate a competitive advantage or competitive disadvantage in the approach.
    - The answer may indicate an unneeded supply.

- What norms would users expect based on the other products they use?
    - Considering any one product, most users spend more time on other varied products.
    - The answer is influenced by the things the user needs.
    - The answer may indicate a competitive disadvantage in the approach if norms are not met.

Human Factors

Consider the human factors carefully. People remain the most significant source of risk in the supply chain because their actions are most challenging to predict, complex, leverage substantial resources, and subject to outside influences. To a limited extent, a business can modify human actions through norms setting, training, honor codes, and contractual obligations. For example, a business could instruct users to scan downloads with anti-malware tools[16], verify cryptographic sums and signatures, and download the product from reputable sources. Compliance monitoring and enforcement of policies may be needed.

Event Condition Timeline is a problem-solving technique available from `zerotrack.net` for experience mapping. The following model considers the potential experience of a responsible end user through the event of downloading the product:



Several techniques can help model the user experience for download supply chains:

- User Experience Inventory is a problem-solving technique available from `zerotrack.net` for comprehensive, holistic analysis of a user's experience. User Experience inventory uncovers gaps in understanding and helps to account for the variability, constraints, and complexity in download supply chains. User Experience Inventory can consider not just users and customers but also adversaries who want to gain unauthorized access to downloads. User Experience Inventory internally detects misalignment between expectation and experience.
- KLM-GOMS[17] can be used to predict the time needed for a user to complete a series of interactions with an interface, such as a download interface and the product interfaces. KLM-GOMS can help evaluate potential interface improvements and perform competitive comparisons.
- NASA-TLX[18] can be used to measure the load placed on a user asked to perform tasks, such as performing a download and product installation.

[16] For example, https://virustotal.com/
[17] https://www.usabilitybok.org/klm-goms
[18] https://en.wikipedia.org/wiki/NASA-TLX

Suggested Resources

The author of this paper is not associated with these resources.

Background on supply chain risks:

- Supply Chain Security Gaps: A 2022 Global Research Report from ISACA, https://www.isaca.org/resources/reports/supply-chain-security-gaps-a-2022-global-research-report
- Uptime Institute annual outage analysis, https://uptimeinstitute.com/resources/research-and-reports
- Systems Thinking: A Product Is More Than the Product, Don Norman (2010), https://jnd.org/systems-thinking-a-product-is-more-than-the-product/
- Schneier on Security, tagged “supply chain”, https://www.schneier.com/tag/supply-chain/
- Deque University accessibility courses, https://dequeuniversity.com/

A starting point for identifying or implementing supply chain best practices:

- NIST Cybersecurity Framework, https://www.nist.gov/cyberframework
- NIST Cybersecurity Supply Chain Risk Management, https://csrc.nist.gov/projects/cyber-supply-chain-risk-management
- NIST SP 800-161 Rev. 1
- NIST SP 800-218
- Executive Order on Improving the Nation’s Cybersecurity (2021, United States)
- Cybersecurity and Infrastructure Security Agency (CISA) guidance
- CISA ICT Supply Chain Risk Management Task Force guidance, https://www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force
- Cloud Native Computing Foundation (CNCF) secure supply chain projects, https://www.cncf.io/
- OWASP Software Assurance Maturity Model (SAMM), https://owasp.org/www-project-samm/
- ISO/IEC 20243-1:2023 (OTTPS)
- ISO/IEC 27036 Series
- ISO 28000:2022 (Security and resilience)
- OpenChain, https://openchainproject.org/
- TUF, https://theupdateframework.io/
- Uptane, https://uptane.org/
- SLSA, https://slsa.dev/
- in-toto, https://in-toto.io/
- Software Package Data Exchange, https://spdx.dev/
- Building Security In Maturity Model (BSIMM)
- CycloneDX
- Software Identification (SWID) tagging
- Semantic Versioning (SemVer), https://semver.org/
- Reproducible Builds, https://reproducible-builds.org/
- CSA Cloud Controls Matrix, https://cloudsecurityalliance.org/research/cloud-controls-matrix
- code signing standards (e.g., RFC 3161, X.509 Certificates)
- various Secure Software Development Lifecycle (SSDLC) standards
- various package manager security enhancements (e.g., Debian, Red Hat, Docker, Python)

Available Support

Teams of any size (be it one or one thousand) who need help managing a download supply chain should seek external support. Professional guidance from IT risk management, user experience (UX), legal, and IT operations professionals may be needed.

The following topics are expansive and, as real-world needs can substantially vary, are areas where expert guidance may be needed:

- Strategic planning
- Technology implementation
- Metrics and KPIs
- Risk prioritization
- Risk mitigation approaches
- CI/CD pipelines
- Automation
- Scalability and high availability
- Governance
- Regulatory compliance, privacy laws, export restrictions, and content delivery licenses
- License compliance and standards conformance
- Open source licensing
- Best practices identification and standards implementation
- Human risk management
- Dependency management
- Proactive threat detection
- Continuous Improvement
- Audits
- Control implementation
- Vendor and third-party management
- Incident response and recovery

Download Supply Chain Component Inventory is a publicly-released component of a more considerable family of download supply chain design and implementation resources. Contact the author for paid consultative support, commercial licensing, or to support our work as a patron.

The author can be reached by email at `download@zerotrack.net`

License Terms

The canonical home for information about Download Supply Chain Component Inventory is `https://zerotrack.net/`

This document is the first release of Download Supply Chain Component Inventory, dated 2024-10-31.