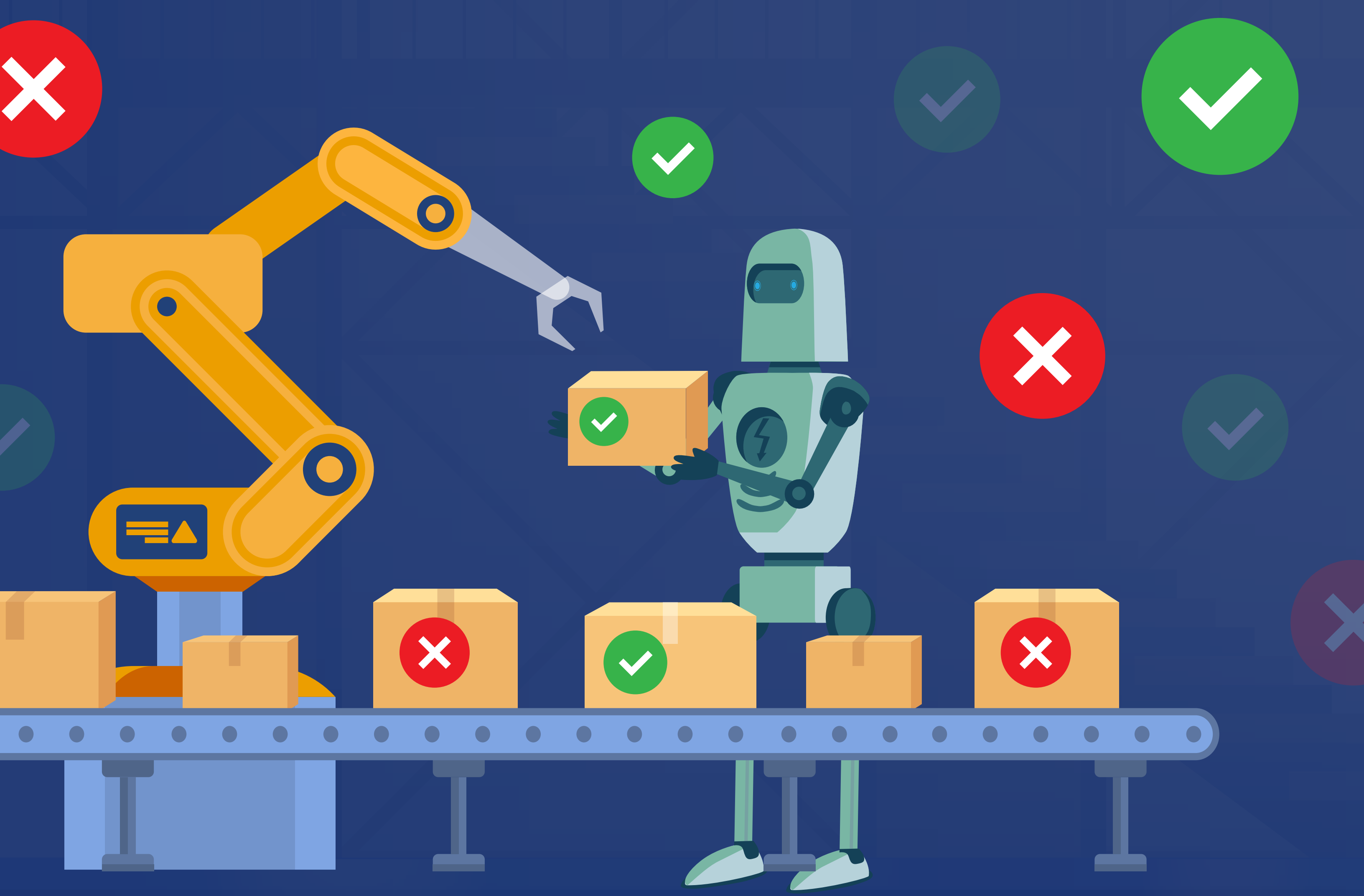
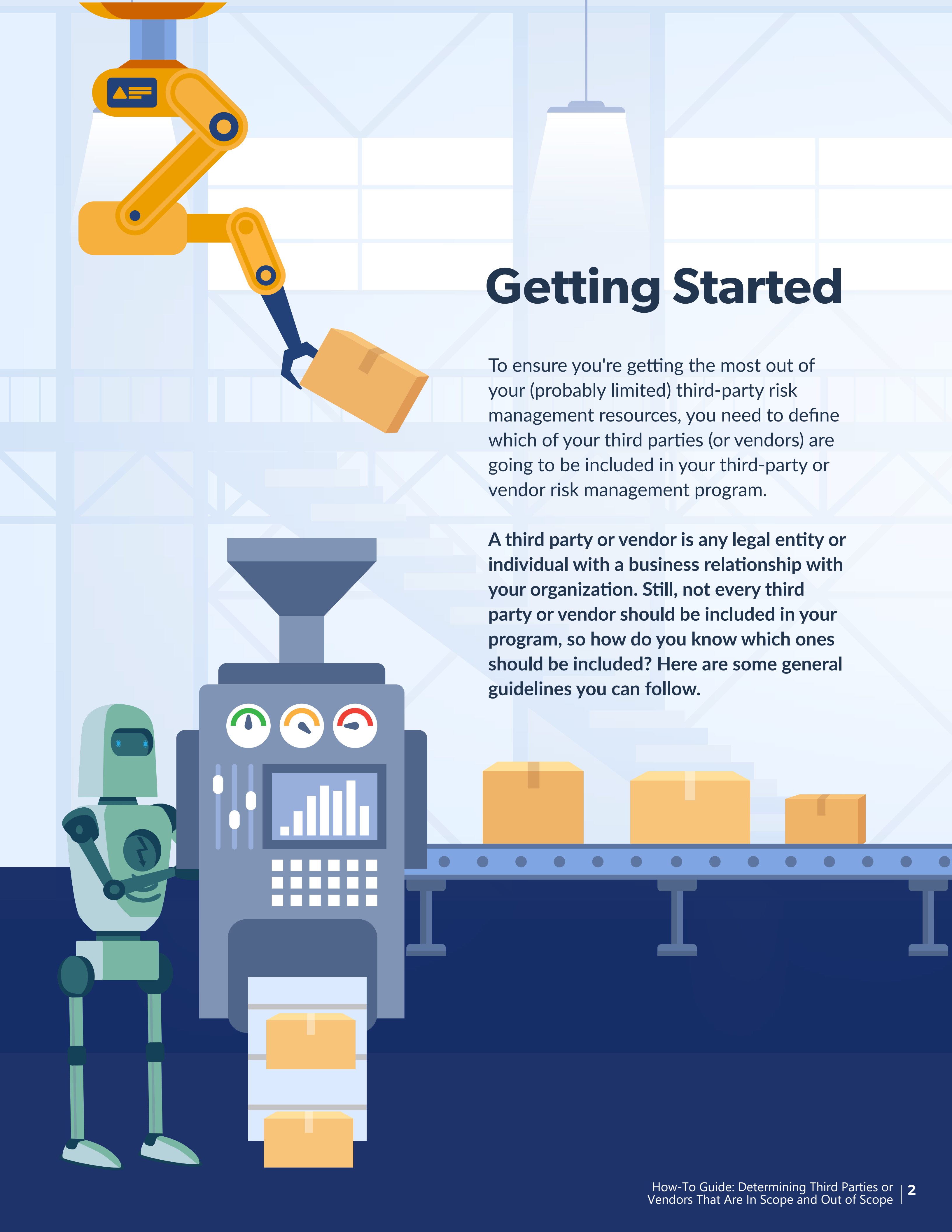
HOW-TO GUIDE:

Determining Third Parties or Vendors That Are In Scope and Out of Scope



venminder



Getting Started

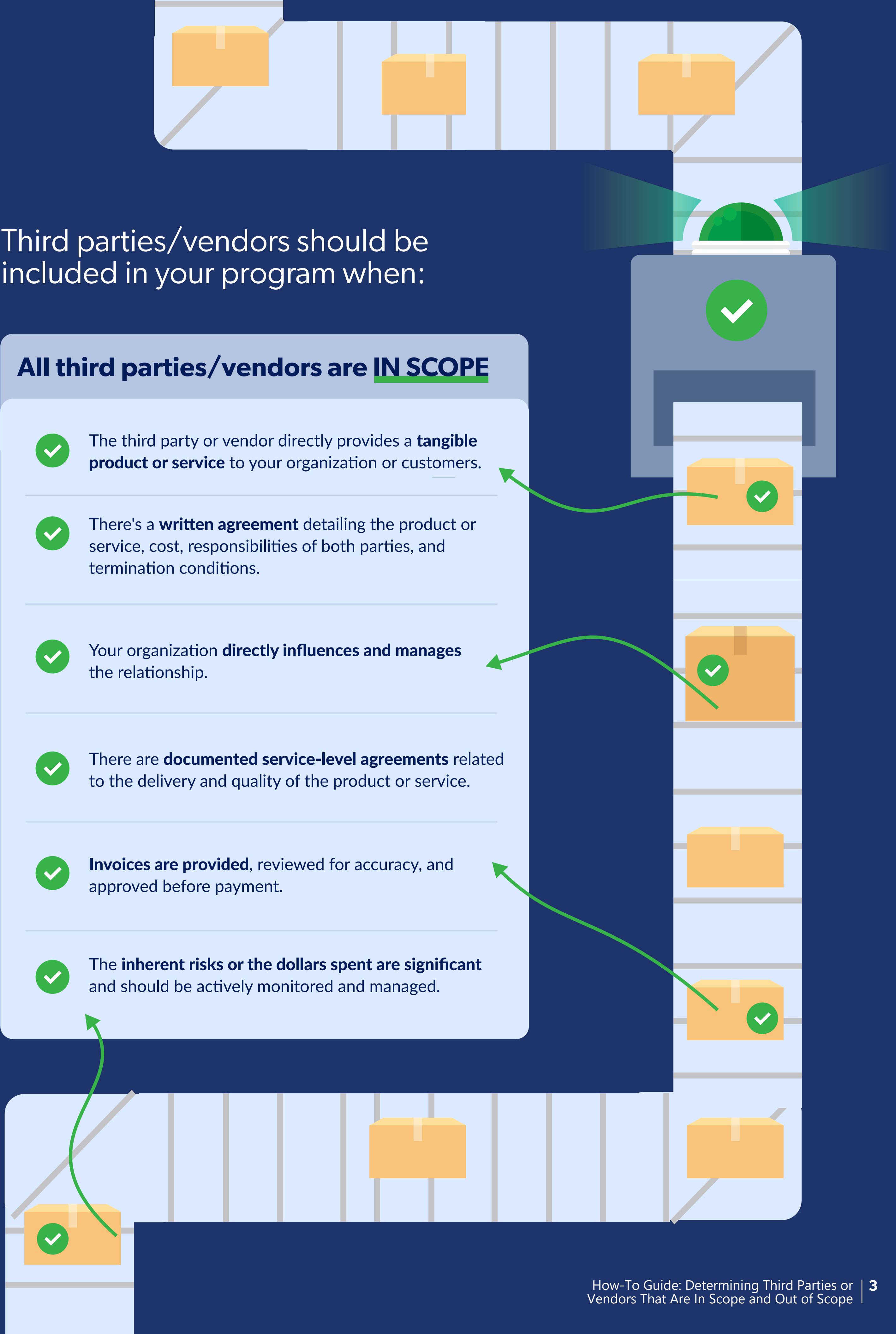
To ensure you're getting the most out of your (probably limited) third-party risk management resources, you need to define which of your third parties (or vendors) are going to be included in your third-party or vendor risk management program.

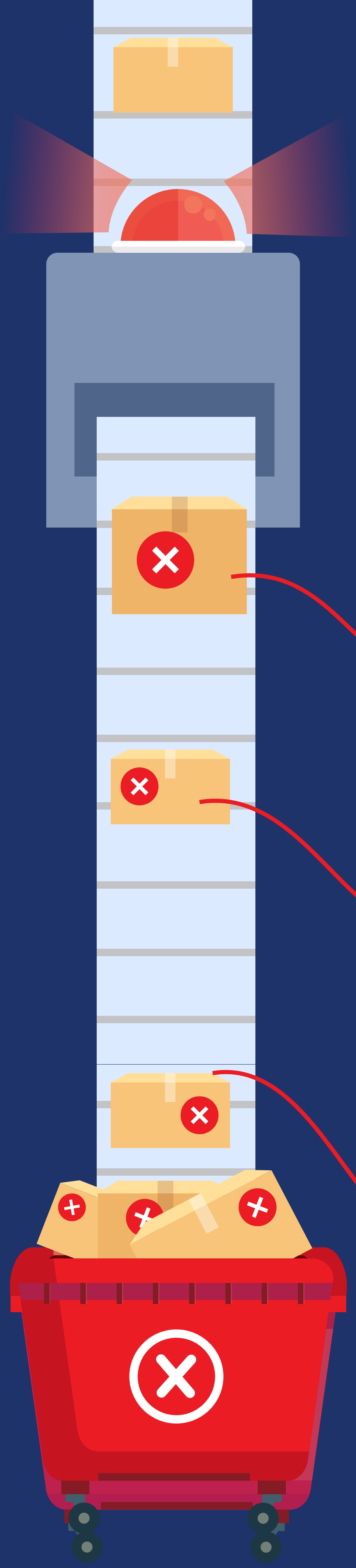
A third party or vendor is any legal entity or individual with a business relationship with your organization. Still, not every third party or vendor should be included in your program, so how do you know which ones should be included? Here are some general guidelines you can follow.

Third parties/vendors should be included in your program when:

All third parties/vendors are IN SCOPE

- ✓ The third party or vendor directly provides a **tangible product or service** to your organization or customers.
- ✓ There's a **written agreement** detailing the product or service, cost, responsibilities of both parties, and termination conditions.
- ✓ Your organization **directly influences and manages** the relationship.
- ✓ There are **documented service-level agreements** related to the delivery and quality of the product or service.
- ✓ **Invoices are provided**, reviewed for accuracy, and approved before payment.
- ✓ The **inherent risks or the dollars spent are significant** and should be actively monitored and managed.





These third parties/vendors are typically OUT OF SCOPE for most TPRM programs

Government entities: These include all state, municipal and federal governments and all boards, commissions, courts, tribunals, agencies, and other organizations exercising executive, legislative, judicial, administrative, or regulatory functions.

Payee relationships: This is considered as payment for non-product or service expenses. Examples include payments for a legal settlement or payments to board members or investors. These types of third parties/vendors are out of scope.

Travel and entertainment: Is this a covered travel or entertainment expense? You can exclude hotels, airlines, restaurants, transportation, etc. However, you should pay attention when a payment to an organization is classified as travel and entertainment (T&E) to ensure the type of product, service, or relationship falls within T&E norms.

Sponsorships and donations: Examples include sponsoring the company team at a charity walk, assisting a non-profit with an event, or placing an advertisement in a program for the local high school musical. Other types of donations, such as political donations, should be managed through other internal governance mechanisms and policies.

Public utilities: Public utilities such as your local power, water, trash collection services, and the like are out of scope. Remember that the key word here is public, as the service is available to everyone. Services specific to your organization, such as backup power generation, are in scope.

Industry group memberships: Annual dues for professional memberships and conferences should be excluded from your third-party or vendor risk management program.

Third parties or vendors that require complete independence and objectivity to perform their functions appropriately. Also known as "arm's length" third parties or vendors, examples include rating agencies, external auditors, or certifying bodies such as NIST, ISO, PCI, etc.

Some Third-Party/Vendor Categories May Be Both In Scope and Out of Scope

Some third parties or vendors may or may not be in scope depending on the service's scale and dollars spent, complexity, and significance to your organization. You'll need to investigate the details before determining if you'll include them as a third party or vendor.

Subscriptions are an excellent example of when not to use an either-or approach within a specific category.

Subscriptions Generally IN SCOPE

- ✓ **Data service subscriptions that provide non-public data**
- ✓ **Subscriptions to access monitoring information sites and SMS alerts**, including data or cybersecurity events, natural disaster alerts, or other real-time event data used by your organization to make urgent business decisions
- ✓ **Subscription resellers** that offer volume discounts when you purchase for the entire organization

Subscriptions Generally OUT OF SCOPE

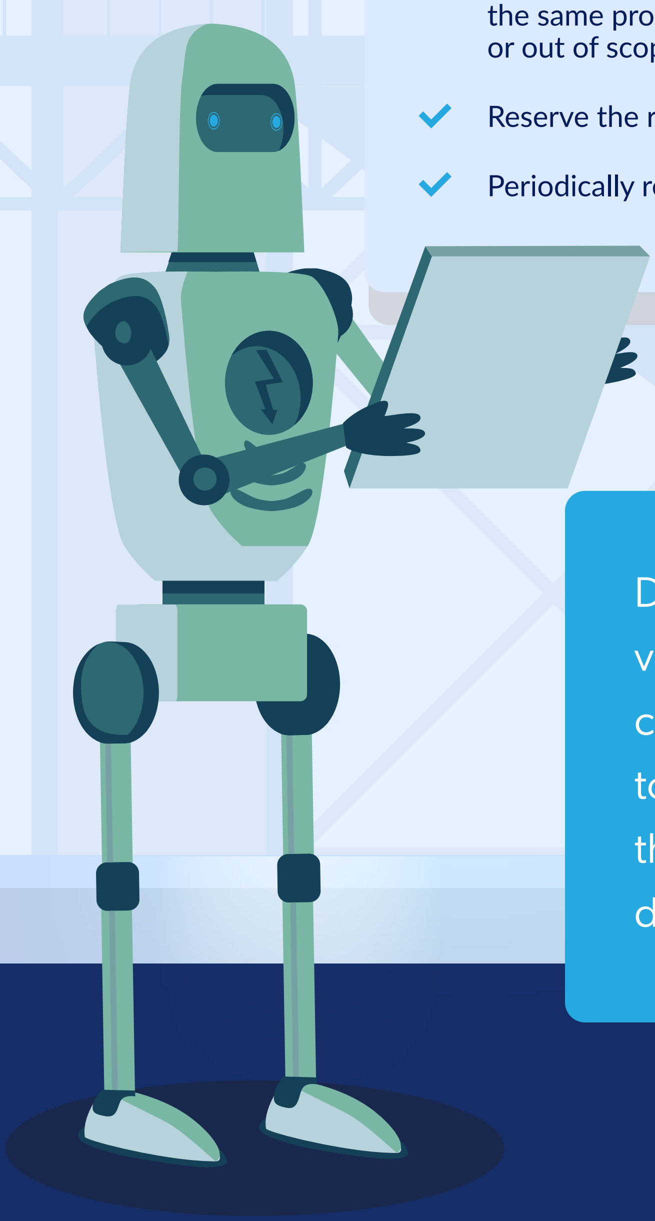
- ✗ Many types of subscriptions will be out of scope for your third-party or vendor risk management program, including **one-off subscriptions for magazines, books, newspapers, digital content (stock photography, music, etc.), industry news, or social media** websites

It's okay if your organization decides to exclude other third parties or vendors. However, always ensure that you can articulate and document your rationale for any out-of-scope decision.

Quality Control Checklist

Once you have determined who is in and out of scope:

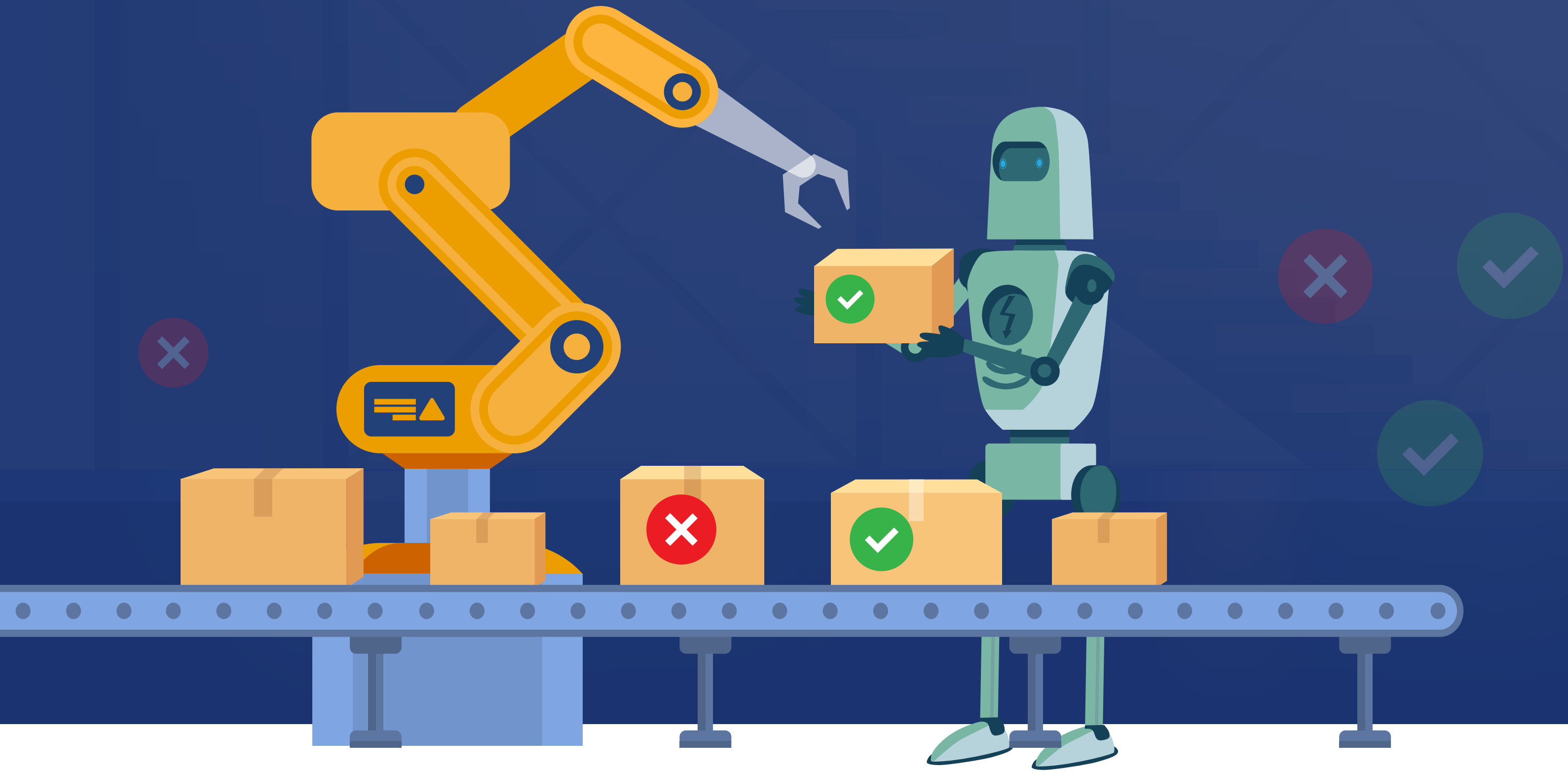
- ✓ Document your program scope and its exclusions.
- ✓ Define the program scope in your policy.
- ✓ Evaluate each third-party or vendor engagement carefully to determine if it's in scope.
- ✓ Ensure you examine any nuanced differences between vendors in the same product or service category before determining in scope or out of scope.
- ✓ Reserve the right to make a judgment call, if necessary.
- ✓ Periodically review the entire list of your third parties or vendors.



Defining the scope of your third-party or vendor risk management program is crucial to its success and will allow you to direct your efforts toward third-party/vendor relationships that deserve your focus and resources.

Download free samples of control assessments and see how Venminder can help reduce your third-party risk management workload.

DOWNLOAD NOW



venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

+1 (888) 836-6463 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise, and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting, and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals, and more, are readily available in an online exchange library. The assessments enable customers to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance, and more.