AdvaMed Device and Diagnostics Compliance Group Benchmarking

November 2023

Global Third-Party Intermediary Management

Answers Collated: October 16, 2023
Total Verifiable Completions: 29

BACKGROUND

AdvaMed surveyed its members regarding their policies on third-party intermediary management. Twenty-nine companies completed the survey in September 2023. This document summarizes the survey responses, including additional commentary submitted by some (but not all) companies. The responses reflect a broad cross-section of company policies and is not intended to reflect all medical technology company policies on third-party intermediary management.

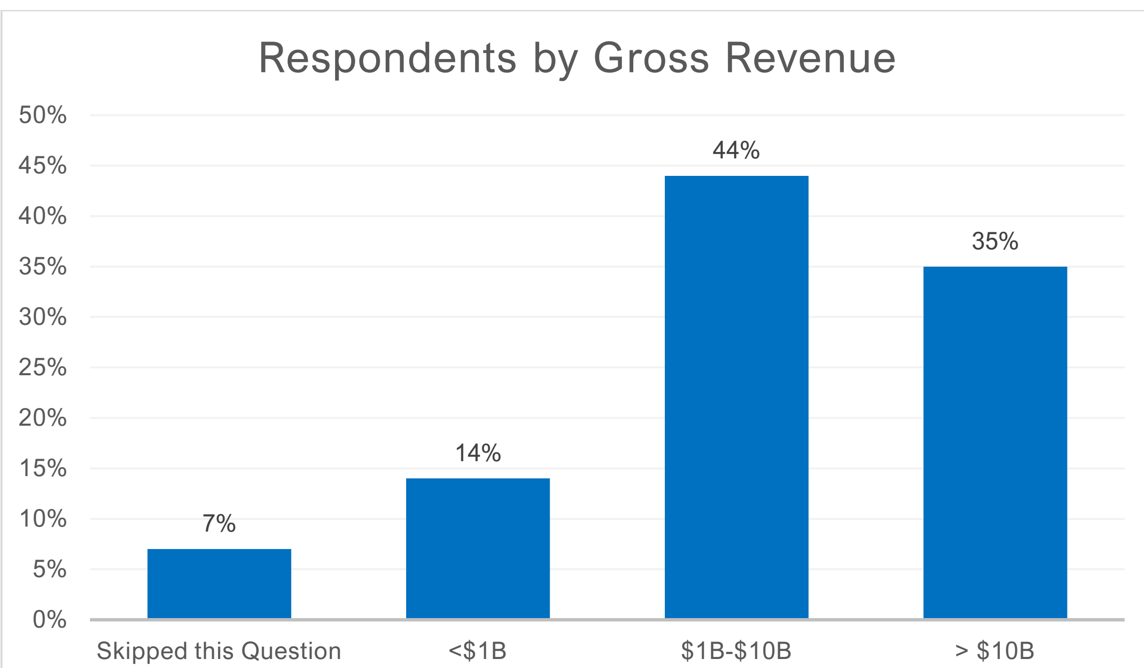
Definition of Third-Party Intermediary: *for purposes of this survey, third party intermediaries include distributors, wholesalers, distribution or sales agents, marketing agents or consultants, brokers, and commission agents.*

AdvaMed strongly encourages companies to adopt policies on third-party intermediary management, including addressing many of the aspects summarized in this benchmarking data.

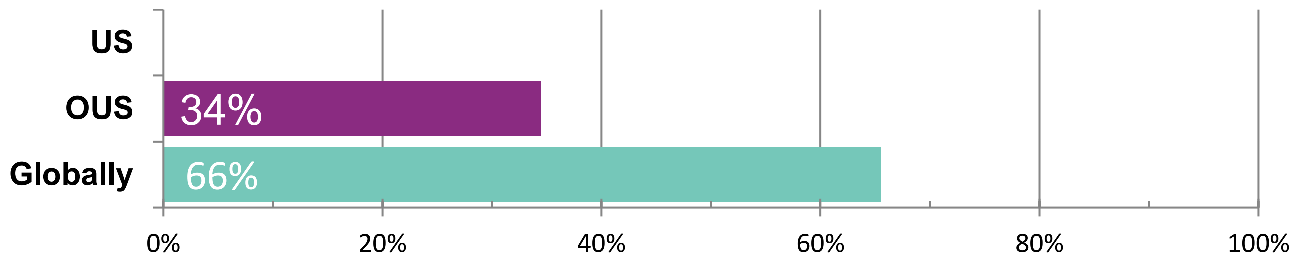
Note: AdvaMed periodically gathers and shares information from Member companies in order to assist companies in understanding industry trends and practices when the information is not competitively sensitive. In all cases, it is understood by AdvaMed and its Members that any company policy or practice that is adopted as a result of this sharing of information is done voluntarily and is a decision by the individual member. The information contained in this report is intended to provide benchmarking data on companies' existing policies only. It is not intended to endorse or mandate any one particular approach for medical technology companies' policies on third-party intermediary management.

DEMOGRAPHIC INFORMATION

Respondents reflected a broad cross-section of company sizes (by annual gross U.S. revenue from device and diagnostics technologies) and sector:



1. In which region does your company utilize third-party intermediaries?



Comments:

- A large majority of TPIs are OUS.
- We use sales agents and distributors in the US, but they are not included in our FCPA/ABAC based Third-Party Program.
- US uses the least third-party intermediaries.
- The comments on this survey will consider Americas region only.
- We do engage TPIs in the US but under a different compliance program. Responses here are therefore just for OUS.
- Our corporate parent is responsible for OUS commercialization.

2. Which department has primary responsibility for third-party intermediary management?

- **34%** Department Engaging with Third-Party Services
- **52%** Compliance
- **0%** Legal
- **0%** Human Resources
- **0%** Finance
- **0%** IT
- **0%** Medical Affairs
- **14%** Other (please specify)

Comments:

- It is a combo between the Business that manages the relationship, Compliance (Screening/Training/Monitoring) and Legal (Agreements).
- The departments engaging and managing third-party relationships are ultimately responsible, Ethics & Compliance team supports and advises them on the risks (specifically regional E&C Officers and a dedicated Business Partner Risk Management Team responsible for vetting the intermediaries).
- Global Compliance has oversight for the third-party due diligence process, but the business owner is responsible for the internal risk assessment questionnaire and having the third party complete the external risk assessment (if they are flagged as being higher risk). Then local compliance officers must

review and approve the engagement (in addition to business approvers, and the CCO for the Americas reviews ALL (worldwide) medium-high- and high-risk engagements because they have the most expertise in FCPA.

- Reports into regional GM but has responsibility for the entire organization.
- We have dedicated Channel Teams, region-specific. Smaller regions are supported by Sales or Compliance.
- Business is primarily responsible, but Compliance assists as needed.
- While Compliance owns policies and procedures related to third-party intermediary management, the ownership to appropriately manage third parties in compliance with policy lies with the business engaging the third party. Compliance owns certain parts of the process (such as due diligence and compliance training).
- In some areas of the world, we have Channel Management organizations, and they are responsible to manage third parties. In the areas where we don´t have Channel Management, the sales teams are responsible.
- Compliance has primary responsibility for TPI COMPLIANCE RISK management. Commercial & business teams have ultimate responsibility for TPI business ownership and TPI relationship management.
- This is cross-functional. Sales is responsible for management and each function plays its role -- Compliance does due diligence and compliance training, Legal does the contract, Quality does quality agreements, Regulatory manages registrations, etc.
- The department engaging with third-party services is responsible for managing the third-party intermediary and Compliance is responsible for conducting the due diligence on the third-party intermediary.
- Multiple departments manage third-party intermediaries.
- Compliance manages from a monitoring perspective.

3. Which department has secondary responsibility for third-party intermediary management?

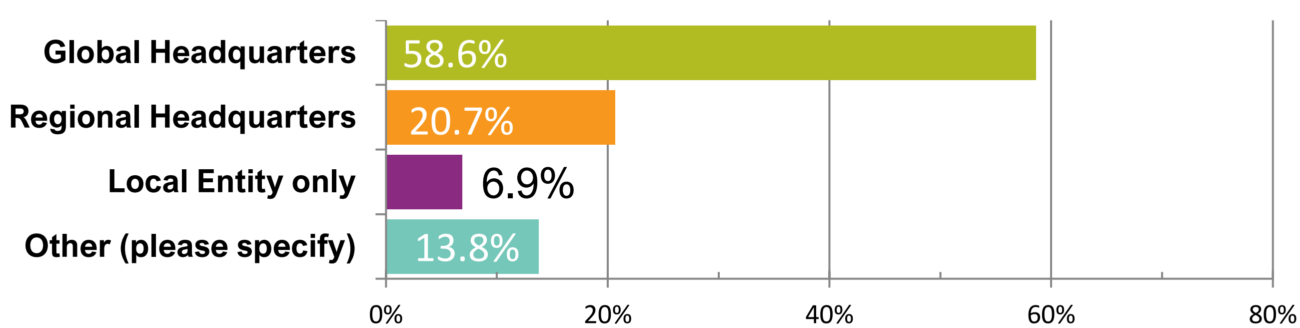
- **24%** Department Engaging with Third-Party Services
- **28%** Compliance
- **21%** Legal
- **0%** Human Resources
- **3%** Finance
- **0%** IT
- **3%** Medical Affairs
- **21%** Other (please specify)

<u>Comments:</u>

- We have a global risk assessment process that all third parties (buy side as well as sell side) must go through prior to contract or at time of contract renewal that covers 10 different risk areas from ABAC, fair labor, trade compliance, information security, etc. The process is facilitated by a tool at the front end of our SAP system and engages each respective risk owning function to review and inform the engagement owner.

- A different third-party screening scope is housed under our Legal department, generally.
- Compliance is responsible for reviewing forms and reports and determining mitigation on identified Compliance risks for third parties that are required to complete the due diligence process. The department engaging with the third party for services is the point of contact for obtaining that information and for communications with the third party.
- The Business Partner Risk Management team is responsible for performing due diligence on third parties, whereas the Ethics & Compliance team provides recommendations/guidance regarding new and existing third-party relationships. Additionally, the legal team is involved in contractual matters.
- While Compliance owns policies and procedures related to third-party intermediary management, the ownership to appropriately manage third parties in compliance with policy lies with the business engaging the third party. Compliance owns certain parts of the process (such as due diligence and compliance training).
- Again, referring to compliance risk management here.
- This is cross-functional. Sales is responsible for management and each function plays its role -- compliance does due diligence and compliance training, legal does the contract, Quality does quality agreements, regulatory manages registrations, etc.
- The Department who engages is the ultimate entity responsible while Compliance manages all the TPI Compliance program.
- The Department engaging with third-party services is responsible for managing the third-party intermediary and Compliance is responsible for conducting the due diligence on the third party.
- Finance, Compliance, Legal share this responsibility.
- The Commercial Selling team.
- Compliance oversees the third-party compliance process, but the internal business relationship owners are responsible for completing the process.
- Commercial is responsible for identifying distributors and front-end due diligence. Legal is responsible for contracts.

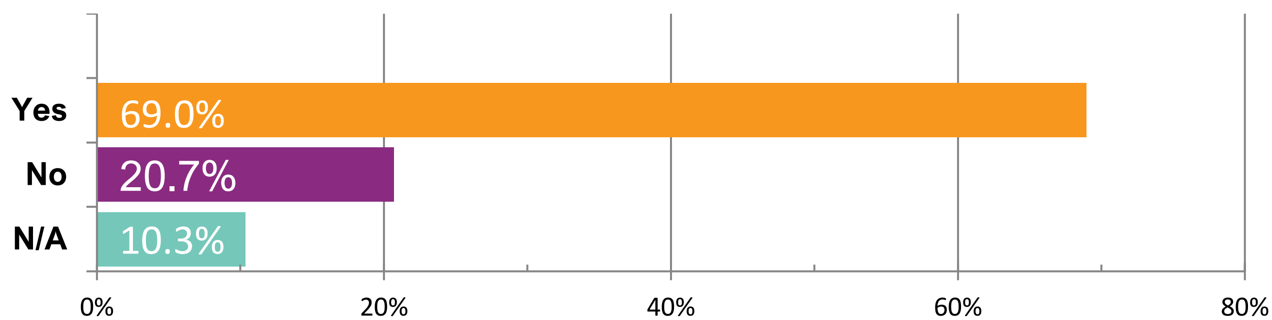
4. Where does the department with primary responsibility for third-party intermediary management report to?



Comments:

- We do not have a singular third-party management function.
- Legal/Compliance.
- Managed and operated by our U.S. Compliance team.
- Those with primary responsibility for managing third parties may report to any of the Company's locations globally.
- We maintain a Global team, but it is collaborative versus being in the required reporting structure.
- Referring to compliance risk management here.
- This is cross-functional. Sales is responsible for management and each function plays its role -- compliance does due diligence and compliance training, legal does the contract, Quality does quality agreements, regulatory manages registrations, etc.
- Depending on the individual, the reporting line could be local entity, regional headquarters, or global.
- Regional Compliance performs distributor due diligence and is required to comply with global policies. Regional Compliance reports into the Global Chief Compliance Officer.

5. If Compliance has the primary or secondary responsibility for managing third-party intermediaries, are there resources available from departments other than legal or compliance to support third-party intermediary management?



Comments:

- Business leads for indirect market management.
- No, although the business sponsors do perform initial vetting of potential third-party partners.
- The business is the primary owner and devotes resources. Internal audit also devotes resources.
- Again, referring to compliance risk management here.
- Yes, business leaders partner with Compliance to create awareness about third-party compliance and follow-up on any compliance-related actions.
- The global Compliance team supports Regional Compliance. The business/commercial teams also support the distributor program. Finance owns the calculations and approval of commission payments.

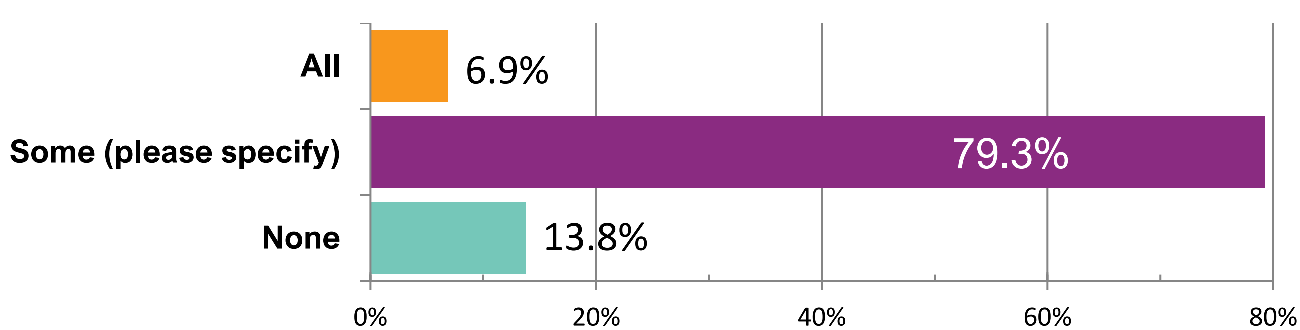
6. If you responded "Yes" to the previous question, which department's resources are available (other than legal or compliance) to support third-party intermediary management?

- **44%** Department Engaging with Third-Party Services
- **0%** Human Resources
- **13%** Finance
- **0%** IT
- **3%** Medical Affairs
- **40%** Other (please specify)

Comments:

- Compliance supplies and manages all such resources.
- Other compliance areas outside ABAC are covered by Quality, Marketing, Regulatory, Sales, etc. Hopefully, I understood the question.
- In addition to the business, internal audit also supports third-party management. HR supports the learning management system and finance reviews and approves credit lines. Regulatory and quality support quality management activity. Service department supports creation of service centers for distributors.
- I believe that not only does Channel Management have resources to manage third parties, but Finance does as well. Quality also has resources and material.
- Multiple - IT (for technical/systems build), commercial (for providing some funding/resources), finance (for reviewing FMV & margins), procurement (aligning with third-party risk management programs of other functions).
- We connect with our SAP system and legal contract management.
- Finance department is involved and needed to review and approve any new Third-Party Intermediary.
- Depending on the third-party support could be needed and available from all the departments listed above.
- The global Compliance team supports Regional Compliance. The business/commercial teams also support the distributor program. Finance owns the calculations and approval of commission payments.
-

7. Do you use external consultants for all or some of the processes related to management of third-party intermediaries?



Comments:

- **16** comments provided that they use external consultants for at least some aspect of due diligence; some comments provided that they use consultants for background checks/reports, auditing, monitoring, and language needs. Additional details are below:
    - Yes, we use Diligent for the initial due diligence, rescreening and ongoing monitoring.
    - We utilize a vendor for our due diligence software application and for background reports.
    - We engage outside consultants and/or outside consultants to assist with enhanced due diligence and/or audit distributors in certain regions.
    - Global due diligence.
    - For due diligence reports and third-party management software; in support of audits for language needs.
    - Currently use for due diligence, but we are exploring a platform for general management.
    - In some regions, the administration of TPI DD is outsourced (but following the same global process). In addition, background checks are performed by external vendors.
    - Vendors are used for the monitoring activities and for the Due Diligence process.
    - We use a third-party platform to process our due diligence and run global database checks and conduct enhanced due diligence reports, if needed.
    - We use third-party due diligence and system vendors.
    - Due Diligence and background checks.
    - Third-party due diligence reports and daily monitoring.
    - We use an external company system for ABAC due diligence and monitoring.
    - Due Diligence Service Providers, external counsel.
    - Periodic Due diligence done by third-party companies.
    - We have a third-party vendor management tool.
    - Depending on the needs, external consultants can be engaged.
    - Refinitiv.
    - OUS - China uses for some processes.
    - I believe channel management organizations gets occasional external support for specific needs.
    - Third-party-auditing and monitoring.

8. Which department(s) bear(s) the costs for external consultants?

- **28%** Department Engaging with Third-Party Services
- **52%** Compliance
- **3%** Legal
- **0%** Human Resources
- **0%** Finance
- **0%** IT
- **0%** Medical Affairs
- **17%** Other (please specify)

Comments:

- The department engaging the third-party is responsible for the cost of the background report, while Compliance bears the cost of the software used to manage the due diligence process.
- Legal covers the costs as well.
- Most costs are handled by Channel team except for audits which is handled by Compliance.
- Compliance bears the cost of the due diligence platform, but the business pays for the enhanced due diligence reports when necessary.
- The business units that make the decision to outsource the administration of the DD pay for that. Re: background checks, costs of the external vendors are covered by the compliance dept (except for high risk TPIs where it is covered by business).
- Compliance pays for the TPI tool and the monitoring while Commercial pays for the Due Diligence screening.
- Compliance covers the cost of the third-party compliance management system.
- Compliance covers costs of systems. The departments engaging third-parties bear costs of screening reports.

9. Which department(s) are involved in the third-party selection process? [select all that apply]

- **90%** Department Engaging with Third-Party Services
- **90%** Compliance
- **66%** Legal
- **66%** Finance
- **69%** Sales
- **21%** Medical Affairs
- **28%** Other (please specify)

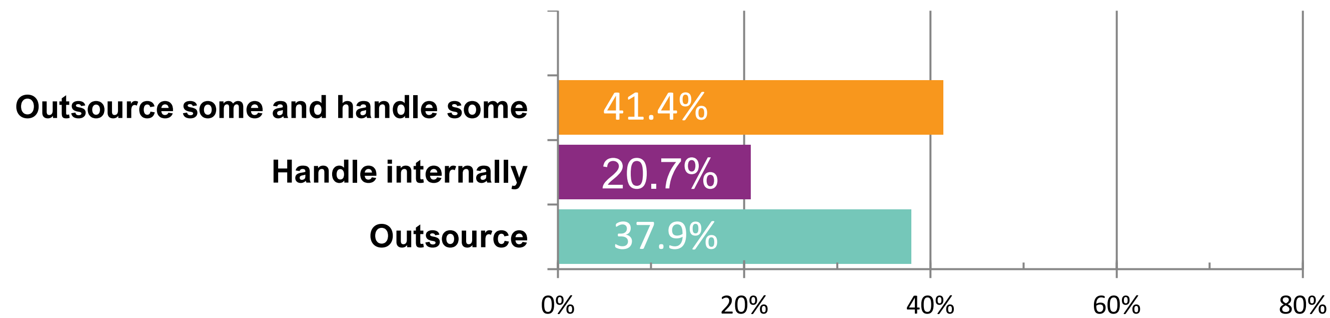
Comments:

- Any/all may be a part depending on the services being provided.
- It depends on the nature of the work and the risk. The business is responsible for selecting their vendors, but if there is a cost issue, or risk issue, the corporate functions such as Finance, Legal and Compliance may push back.
- Regulatory and Market Access.
- It varies from regions and the type of service that will be provided. Other: Procurement is also involved if the TPI is a "vendor", such as consulting, broker, etc.
- Compliance currently only ensures the prospective intermediary does not have any compliance concerns. All other reviews and decisions completed by the regional Channel and Sales teams.
- The Service department is also involved to ensure service capabilities. Legal is involved in the contracting, but not in the selection process unless there is a particular matter for their analysis.
- In some parts of the world, all of these departments are involved in the onboarding of a distributor (they all conduct their own due diligence and provide approval or not). There are regional committees that meet every month to review together new onboardings. In the rest of the world, the sales team and

Compliance will always take part in final decision to onboard a new third-party.

- Other: Also Quality and Regulatory.
- Regulatory.
- Procurement & Supply Chain.
- It depends on the services provided by the third-party, among other factors, but sometimes Compliance, Legal and Finance are involved.
- Business/Commercial teams.

10. Do you outsource due diligence with respect to the third-party intermediary or do you handle internally?

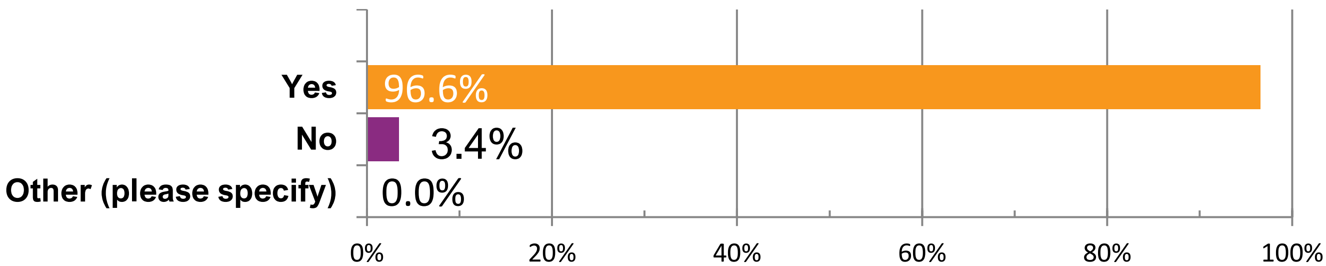


Comments:

- We use a third-party to provide company research and due diligence reports, but the remainder of the activities are handled internally.
- Diligent – Outsource.
- Our current provider is Diligent.
- We handle internally through management of our third-party platform.
- The Internal Business Partner Risk Management Team handles the due diligence process on third-parties.
- Where certain enhanced due diligence may be required, we engage FTI and outside counsel to assist. We have also hired auditors to assist with that activity to audit our distributors.
- Due diligence questionnaires are provided by Refinitiv (vendor), and the same applies to risk-assessment criteria and due diligence reports.
- We leverage a third-party vendor for our due diligence questionnaire and enhanced due diligence background screenings reports.
- The business units that make the decision to outsource the administration of the DD pay for that. Re: background checks, costs of the external vendors are covered by the compliance department.
- We internally review global database check results as well as information and assessment forms and responses to due diligence questionnaires. If enhanced due diligence is required, we leverage a third-party.
- We outsource the publicly available information to be aggregated in one report + ongoing monitoring of that information.

- Our internal teams use an external vendor to run due diligence reports and daily monitoring.
- Compliance owns and manages the due diligence process, but the actual due diligence reports are generated by an external party.

11. Do you have a due diligence questionnaire for third-party intermediaries?



Comments:

- We use internal and external questionnaires during the due diligence process.
- All distributors are subject to a due diligence interview and are also required to complete an application form.

12. Who is responsible for processing the information received in a due diligence questionnaire?

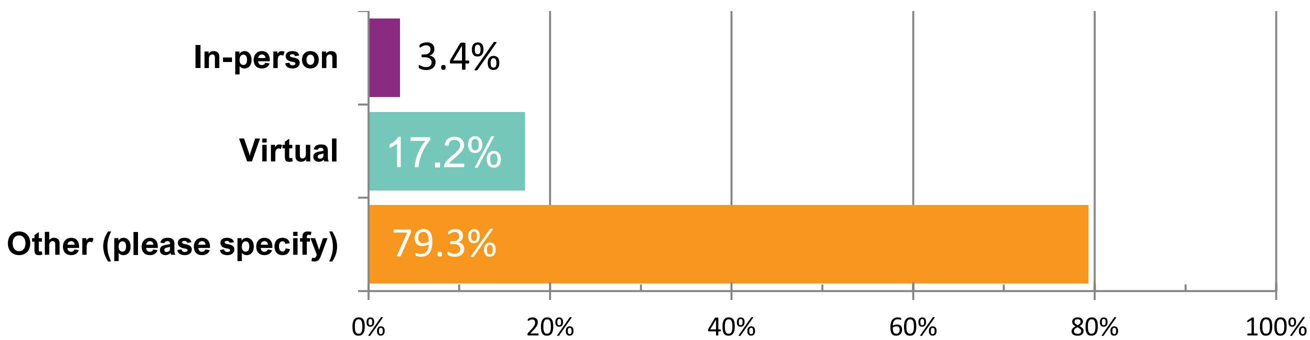
- **10%** Department Engaging with Third-Party Services
- **76%** Compliance
- **0%** Legal
- **0%** Human Resources
- **0%** Finance
- **0%** IT
- **0%** Medical Affairs
- **14%** Other (please specify)

Comments:

- We have due diligence coordinators who process the information and then engage with relevant stake holders to review and address any flags/decisions that need to be made.
- Compliance, although issues may get escalated to legal or business for follow up depending on the nature.
- The Business Partner Risk Management Team and Regional Ethics & Compliance Officers have access to the questionnaires.
- As well as the business.
- In some cases, we have Distributor Management reviewing questionnaires.
- Along with Compliance and Finance.
- If no flags are identified, the Channel team can proceed without additional review.

- Our Channel Compliance teams in the regions are responsible for this.
- Plus, the TPI business relationship owner.
- Cross-functional -- legal, compliance, business, quality, finance.
- We do not use a questionnaire as all our third-party OUS activity is handled by parent company.
- And Global Security.
- Commercial teams gather the information and enter it into the system. It is then reviewed by Compliance as part of the due diligence process.

13. Do you conduct in-person or virtual interviews for the purpose of due diligence of third-party intermediaries?

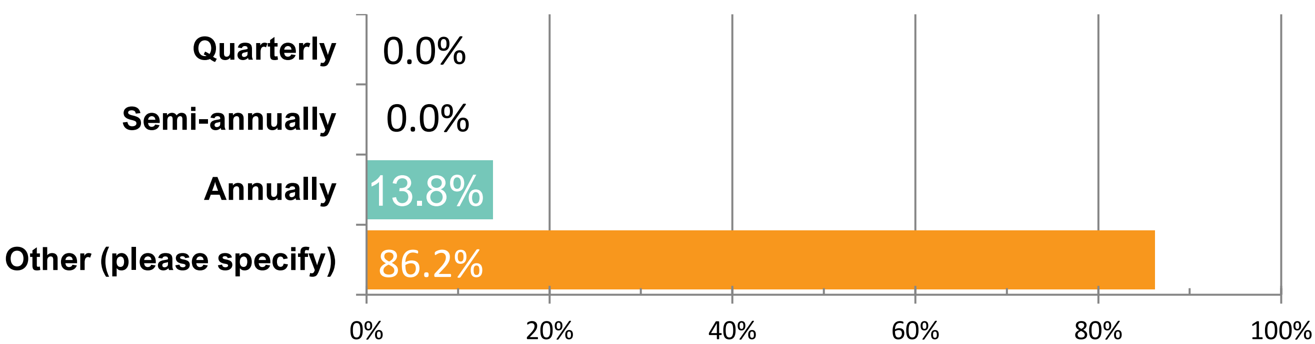


Comments:

- **10** comments provide that interviews are conducted in certain circumstances/at times. Additional details are below:
  - At times.
  - Not a mandatory step in the process but done when deemed necessary.
  - Only if additional information is needed. Would be virtual most likely.
  - When interviews are necessary, they are typically conducted via phone or other remote technology.
  - Interviews would only be conducted if there are risks that need addressing at the due diligence stage. These would normally be virtual.
  - Interviews are conducted if Due diligence have any findings.
  - It depends on the location of the third-party and level of risk.
  - It depends on the circumstances.
  - Interviews are conducted on an as-needed basis. In certain regions, a virtual conversation between compliance and the third-party is done in advance of contracting to ensure understanding of compliance requirements (this is in addition to compliance training).
  - It's a mix. Generally, not for lower risk TPIs. For higher risk TPIs, in-person or virtual interviews may be performed.
- **8** comments provide that they conduct some form of interviews. Additional details are below:

    - Business does conduct interviews prior to proposing and sponsoring the partner.
    - Both in person and virtual.
    - Both - completed by the Channel team.
    - We do both.
    - The business interviews TPIs unless there is a concern.
    - Please note that our provider will conduct either in-person and/or virtual interviews, depending on the circumstances.
    - The business interviews TPIs unless there is a concern.
    - Interviews can be in person or virtual.
- **4** comments provide that they do not conduct interviews. Additional details are below:
    - We do not conduct interviews.
    - We do not conduct any direct interviews with our prospective or current third-parties.
    - Interviews are not part of our due diligence process, however, it may happen that the Regional Ethics & Compliance Officer would contact the third-party to clarify some issues revealed during due diligence process.
    - Only online questionnaires and red flags information for clearance.
- **1** comment provides that Commercial is the point of contact of the TPI.

14. How often do you conduct due diligence of third-party intermediaries?

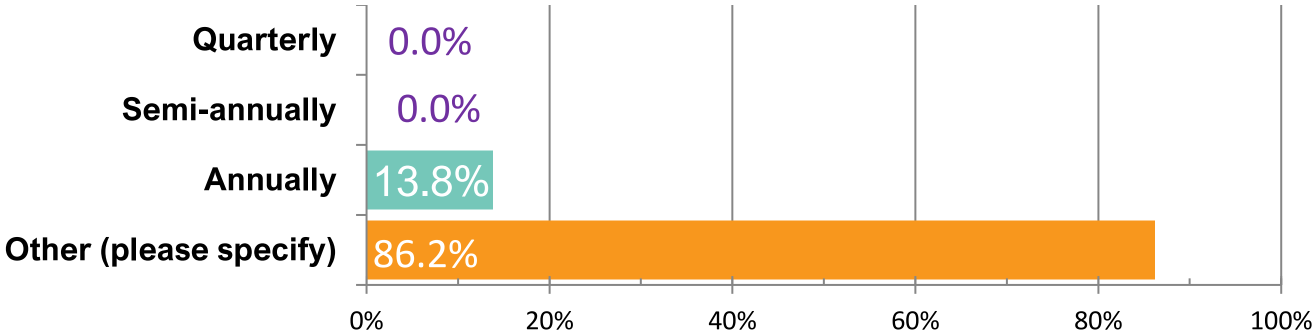


Comments:

- **9** comments provide that they conduct due diligence every 3 years. Some additional details are below:
    - We are constantly running global database checks, but all third parties are required to go through the full due diligence process every 3 years.
    - A full due diligence refresh is required every 3 years, or if a triggering event has occurred. Daily watchlist monitoring is also performed.
    - Upfront and then every 3 years. If circumstances regarding the Distributor change e.g., change in top management, change of scope, etc. then that would prompt ad-hoc due diligence.
    - Continuous; renewal due diligence every 3 years.

- **8** comments provide that they take a risk-based approach and conduct due diligence every 18 mos. - 5 years, depending on risk. Additional details are below:
  - Every 18 months to 2 years, depending on the risk.
  - Every 2 or more years on a risk-based approach.
  - We perform full due diligence on all in-scope third parties every 2-3 years (depending on the type) or at contract renewal, if shorter. We also perform on-going adverse media/event screening on a continuous basis.
  - After initial engagement, third parties that are required to complete our due diligence process must go through a renewal process every 2 - 4 years. On an annual basis, those who are responsible for engaging the third-party must complete a form about the third-party in which updates about the third-party are provided.
  - Before on-boarding: for potential third parties. On regular basis for existing relationships: every year for high risk third parties, every 3 years for medium risk third parties, and every 5 years for low risk third parties. In addition, in case there is any trigger, e.g. new contract, new capacity, substantial changes to third-party structure, e.g. change in ownership.
  - We have risk-based approach to TPI DDP. It is completed before the on-boarding. A risk profile is assigned upon completion and DDP renewal occurs at 2/3/4 years.
  - Based on risk level, we conduct due diligence every 1-4 years.
  - It's a mix. It is always conducted at new/onboarding stage. Then DD is renewed at different periods depending on risk segment/category of TPI (4 years for lowest risk category, 2 years for highest).
- We rely on our parent company to conduct diligence of third parties.
- At onboarding and renewal (two-year terms) with adverse meeting monitoring continuously.
- Initial diligence prior to onboarding, triannual rescreening, and ongoing monitoring (quarterly reports).
- Daily as part of our regular operations.
- Ongoing daily screen is done through the due diligence platform, and enhanced reports are requested every three years or at contract renewal (whichever is earlier).
- Before initial engagement and every 36 months, unless there is a significant change (e.g., ownership of the third-party, additional services to be provided, etc.).
- Always for new Third-Party intermediaries at onboarding, semiannually monitoring report, and then biannually due diligence refreshment.
- Due Diligence conducted when third-parties are engaged. Continuous media monitoring of all third parties after engagement. Annual questionnaires and training required for some (higher risk) third parties.

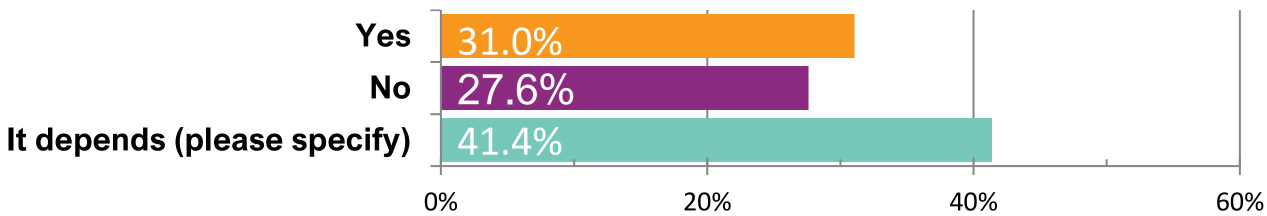
15. How often do you require a new due diligence questionnaire from third-party intermediaries?



<u>Comments:</u>

- **10** comments provide that they required a new due diligence questionnaire from third-party intermediaries every 3 years. Additional details are below:
  - Every three years or at contract renewal (whichever is earlier).
  - An annual certification is required attesting to no changes from data provided on a questionnaire. A new questionnaire is required every 3 years.
  - Due diligence questionnaires are issued based on the level of risk and are required once every three years.
  - There are annual questionnaires for higher risk third parties. Due diligence must be refreshed every three years.
  - Every three years and also have continuous monitoring.
  - Every 3 years for all third-parties.
- **3** comments provide that they take a risk-based approach and require a new due diligence questionnaire every 18 mos. - 3 years, depending on risk. Additional details are below:
  - Planning to every 18 months to 2 years, depending on risk.
  - Every 2 or more years on a risk-based approach.
  - Annual cadence of 1-3 years depending on current risk rating that is calculated by our third-party tool.
- At onboarding and renewal (two-year terms).
- At time of due diligence renewal.
- As part of tri-annual re-screening or if issues arise during monitoring that requires action.
- Our standard DDP always includes a questionnaire, renewal frequency of 2/3/4 years.
- At the point of DD renewal, or if there is a substantive change at the TPI in the interim.
- Before initial engagement and every 36 months unless there is a significant change (e.g., ownership of the third party, additional services to be provided, etc.).
- Biannually.
- At contract renewal.
- We do not use questionnaires.

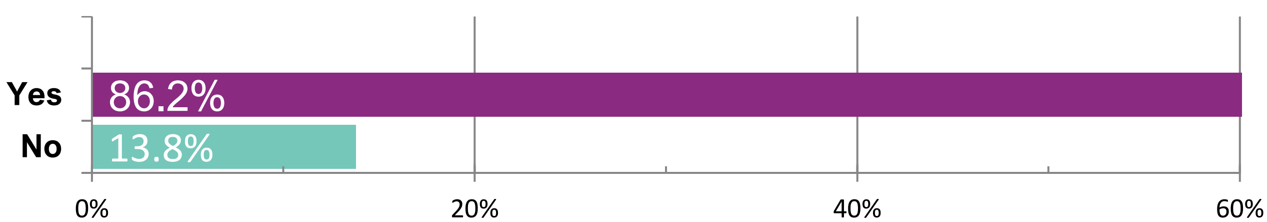
16. Do you require third-party medical device manufacturers to submit due diligence questionnaires?



Comments:

- If they are acting as a reseller, distributor, or kit packer then yes. Otherwise, they are considered an "end-user" and would not fall in the scope of our normal third-party due diligence review.
- Whether the manufacturer would need to complete the due diligence process depends on whether it would otherwise meet the criteria that require a third-party to go through due diligence.
- It depends if their activities or services are in-scope of our TPI policy.
- If such third parties have signed OEM agreements with Company, most likely they will not go through the due diligence process. If they are not an OEM partner, then yes.
- If they fall under our definition of in-scope TPI (TPI interacting with OUS HCPs or GOs as part of Company's business whom we are (to a degree) directing or controlling activity of), then we would require DD. However, most TP medical device manufacturers do not meet this definition.
- If they are acting as a distributor, then yes.
- Depending on the services that are provided to our company.
- It depends on the nature of the services provided.
- If servicing as sellers, yes we do, if serving as providers of goods we don't.
- All third parties are required to complete the questionnaire.
- Yes, if they are going to interact with non-US government officials.

17. Do you have different due diligence levels depending on your company's risk modeling assessment? If yes, please explain in the comments.



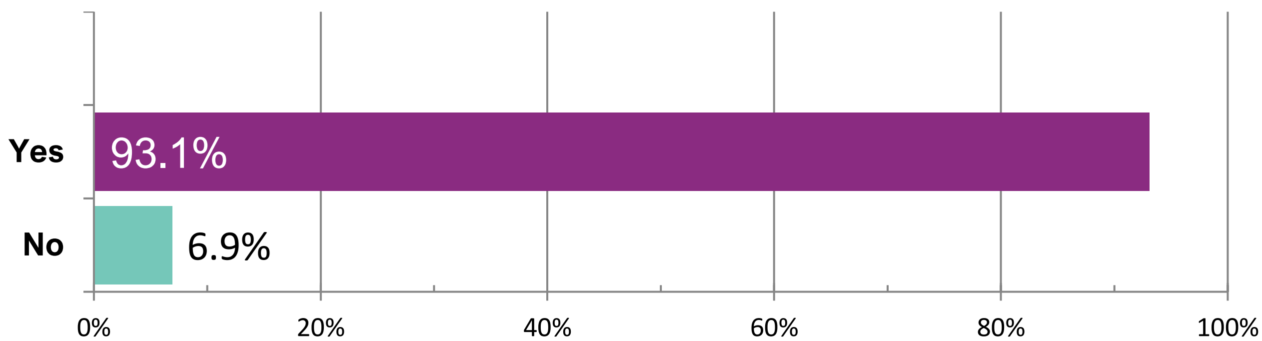
Comments:

- We rank high, medium, and low. Factors include: geography (composite matrix score using Trace and CPI Indices), DDQ responses, type and volume of activity, previous red flags, and various E&C factors.
- A risk scoring model based on multiple factors including country where service is being performed, contract size, nature of the company, etc.

- Open source and enhanced due diligence.
- More in-depth due diligence will be conducted based on risk factors.
- We have certain criteria in which we screen. There are certain values associated with each question in our third-party questionnaire which determines the risk rating of a particular third-party (i.e. frequency of interactions with government officials, operations in a sanctioned or embargoed territory).
- The level of background report that we obtain depends on the outcome of the risk matrix, which includes a number of factors, such as geography, services provided, value of services to be provided, etc.
- Yes, it depends on the initial risk assessment of the third-party. We have simplified due diligence process for third-parties assessed as low risk during initial analysis, and enhanced process for medium and high risk third-parties.
- Yes, we utilize a questionnaire risk score to determine due diligence background screening. We have 5 background screening levels available.
- Screener questions dictate level of due diligence.
- Currently, we do not change the due diligence report type based on risk, but we are working toward that.
- Depending on the risk rating from the questionnaire (based on CPI and business model risk) or other alerts that may require a higher rating.
- For higher risk regions (such as Latin America), an enhanced due diligence is conducted that includes in country public records review, including ownership (in addition to electronic records review and media review). The same enhanced due diligence would apply if an enhanced risk is identified in low-risk regions.
- Our provider offers two types of reviews: an Open Source Investigation, which is aimed to be conducted upon low-risk profiles, and an Enhanced Due Diligence, which is aimed to be conducted upon medium and high risk profiles.
- We have a risk segmentation model (with four risk categories of low, middle-low, middle-high & high). Those TPIs that are deemed low-risk have an expedited process with certain steps removed. Those that are deemed high-risk have to go through additional checks, including investigational due diligence.
- Different levels of diligence reports.
- Every 2 or more years on a risk-based approach (e.g. Corruption Perception Index of the Country, annual revenue and other factors).
- We rank our third parties as low, medium, medium plus, and high-risk based on a number of factors, including responses to our information and assessment form that is completed by the business sponsor and the responses to our due diligence questionnaire that the third-party completes.
- Different due diligence reports based on country risk.
- Risk-based model that determines the level of diligence required.
- There are several factors that determine the level of due diligence including the services provided, location of the third-party, etc.
- A basic background check (open-source investigation) or enhanced due diligence when needed.
- Yes. We have a risk model that measures country risk and additional factors. The extent of due diligence and required approvals vary based on the level of risk.

- All parties risk ranked based on responses to DD questionnaire, the types of services they will perform for our company, and the CPIs of the countries in which they operate. Level of DD screening varies based on risk level.
- We have 3 tiers based on country, CPI, and type of service. The highest tier (highest risk) has the most extensive due diligence including live interviews.
- Depending on the CPI Score.

18. Does your company permit third-party intermediaries to hire sub-distributors?



Comments:

- **5** comments provide that hiring sub-distributors is permitted but only with prior approval and/or written consent.
- We allow that if this is needed, and we perform database screening of the sub-distributors.
- Yes, but they must notify us so we can perform due diligence.
- With some territorial exceptions where it is not permitted.
- It is not prohibited. But our Distribution Agreements does contain a very robust clause on the use of sub-distributors, with responsibilities and recommendations.
- It depends, sub-distributors may also need to go through our third-party compliance process depending on the nature of the services they will provide.
- Currently evaluating. Historically we have not but have allowed some on an exception basis in connection with acquired entities.

19. If you answered "Yes" to the previous question, (i.e. your company permits third-party intermediaries to hire sub-distributors), what processes (if any) do you have to keep track of sub-distributors?

Comments:

- We have a registry and contractual requirements to notify of sub-distributors. We also conduct DD on some high-risk, high-volume sub-distributors.
- We require notification. They must perform due diligence (or we will) and they are subject to being audited.
- Sub-distributors above a certain revenue % are treated the same as distributor partners and tracked

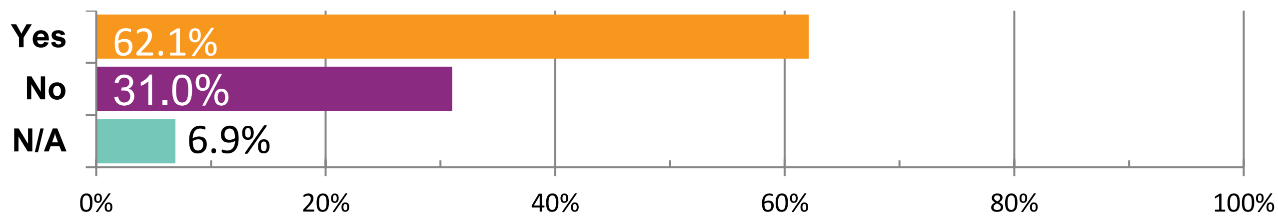
accordingly.

- Information is collected in the third-party questionnaire.
- If known to us, we will screen the sub-distributors via the same third-party screening process. We ask in advance if there is any other entity being used to carrying out services to Company.
- The third parties are required to disclose and obtain approval from the Company before they are allowed to engage the sub-distributor, and that is tracked in the system that is used to complete the due diligence process.
- Sub-distributors are revealed during initial or repeated due diligence process. We also have a clause in the contracts requiring the third parties to notify us about any new sub-contractors to be engaged by them.
- We ask the Third party to track.
- We are in the process of building out our sub-distributors guidance. Currently we ask for some information in our questionnaire.
- Questionnaires and due diligence.
- Within annual DDQs, intermediaries are required to provide us the names and addresses of their sub-distributors so we can automatically screen those names. Outside of the DDQ cycle, contractually we require our intermediaries to submit the sub-distributors information to us so we can screen and provide necessary approvals.
- Sub-distributors must go through the same due diligence process.
- Sub-distributors are not allowed as a general rule.
- Distributors must notify Company of their intent to use sub-distributors before they are engaged. They can either notify via the Distribution Agreement (which gets renewed yearly) or via the electronic means that we have available. (Smartsheet) Such sub-distributor information is also uploaded on Diligent but for tracking purposes only.
- If sub-distributors meet the in-scope definition, then they must go through DD like a primary distributor. If not, then standard contractual clauses in our agreements with primary distributor require them to manage the sub-distributor relationship to similar standards.
- Depends on region.
- We ask for them to indicate while filling the questionnaire and we review during the monitoring activity.
- It is a required question on the questionnaire as well as annual certification. Tracking is completed the same as the distributors.
- No formal process currently. We do ask third parties to disclose sub-distributors.
- Modified version of the full third-party due diligence requirements.
- Parent Company handles our diligence.
- Identification in Third-Party Questionnaire and quarterly verification.
- There are several factors that determine the level of due diligence including the services provided, location of the third party, etc. All third-parties subject to our third-party compliance process must use our third-party compliance system for tracking purposes.
- Compliance assessment for each and full due diligence depending on the risk.
- If the main distributor is considered low/standard risk, the main distributor is responsible for conducting

due diligence on the sub dealer, as well as training. We do not track low/standard risk sub dealers. If the main distributor is heightened risk, our internal teams are required to log the sub dealer in our systems as a dealer and perform due diligence and training.

- Contractual provisions require notice of use of sub-distributors.
- We have a risk-based dedicated due diligence process.
- It needs to be approved by us, the company.

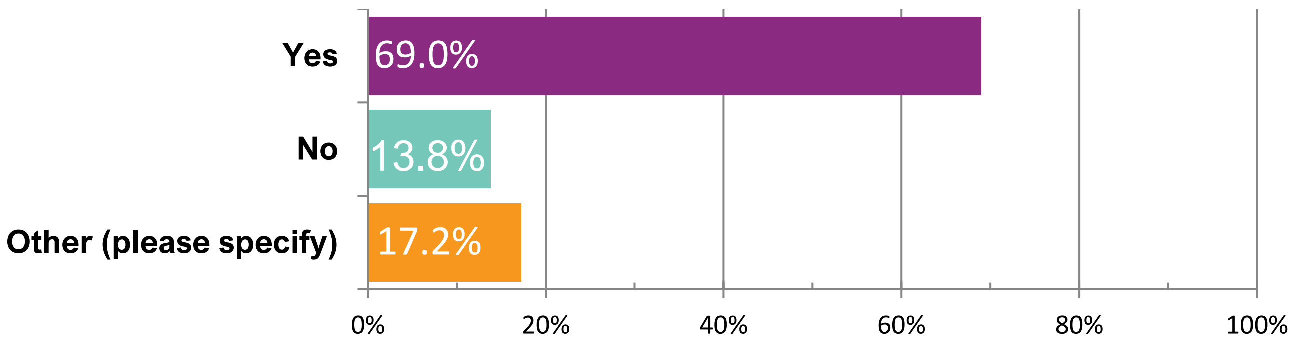
20. Do you require third-party intermediaries to perform due diligence for sub-distributors?



Comments:

- Risk based.
- We do encourage DD and our distributors are contractually responsible for the conduct of their sub-distributors.
- Yes, and above a certain revenue threshold, we conduct due diligence.
- We do advise the third parties to perform due diligence on their sub-distributors but we do not demand them to do so.
- Distribution agreements have a standard clause.
- The Distribution Agreement establishes that distributors shall conduct due diligence of sub-distributors.
- If sub-distributors meet the in-scope definition, then they must go through DD like primary distributor. If not, then standard contractual clauses in our agreements with primary distributor require them to manage the sub-distributor relationship to similar standards.
- Only if the main distributor is classified as low/standard risk. If that case, we provide the main distributor our due diligence requirements. The main distributor is responsible for due diligence and training of low/standard risk sub dealers.

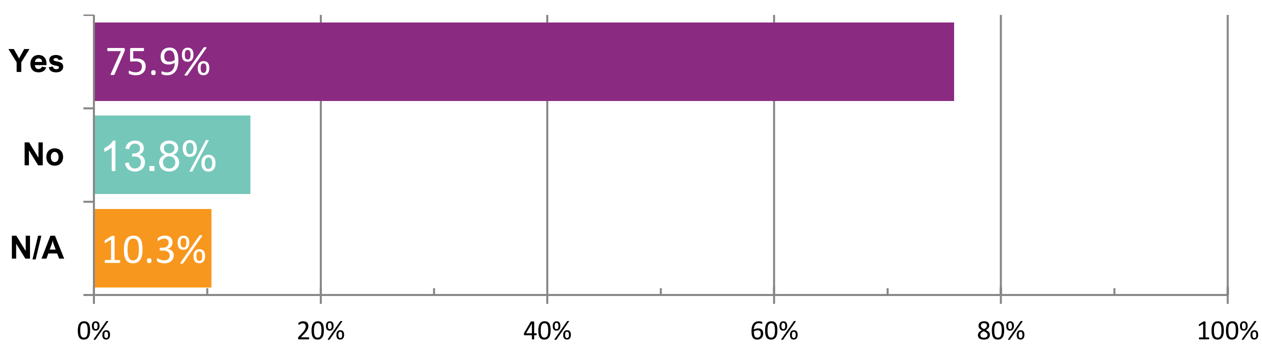
21. Do you require contracts for every third-party intermediary transaction?



Comments:

- All TPI's should have an agreement in place.
- For most direct relationships.
- Yes. There is a handful of legacy verbal agreements that we are converting to written contracts.
- We have overall contracts that cover all purchases and expectations for marketing, events, etc. We do not have any single transaction contracts.
- The Distribution Agreement establishes that distributors shall execute a sub-distribution agreement with its sub-distributors. Also, we require contracts to be executed for spot deals; with agents, travel agencies, consultants, etc.
- In most circumstances, yes. However, there are some cases where a different document (e.g., letter of engagement) may be appropriate.

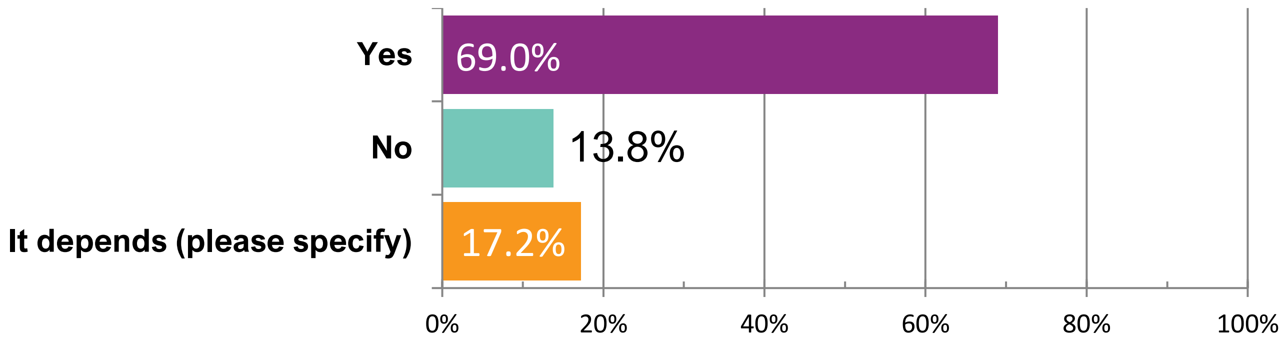
22. Do you require third-party intermediaries to have a contract for sub-distributors?



Comments:

- We do not demand it from third parties.
- The Distribution Agreement establishes that distributors shall execute a sub-distribution agreement with its sub-distributors.
- In most circumstances, yes. However, there are some cases where a different document (e.g., letter of engagement) may be appropriate.

23. Does your company perform routine audits of third-party intermediaries (i.e. “not-for-cause” audits)?



Comments:

- Supplier/distributor audits are performed routinely by the quality/regulatory department, compliance team also performs audits, but they can be performed on an ad-hoc basis rather than as part of a regular process.
- Mostly for distributors.
- It varies by region.
- Annual audits of higher risk third parties, as required.
- The program is being established.
- The program is in development.

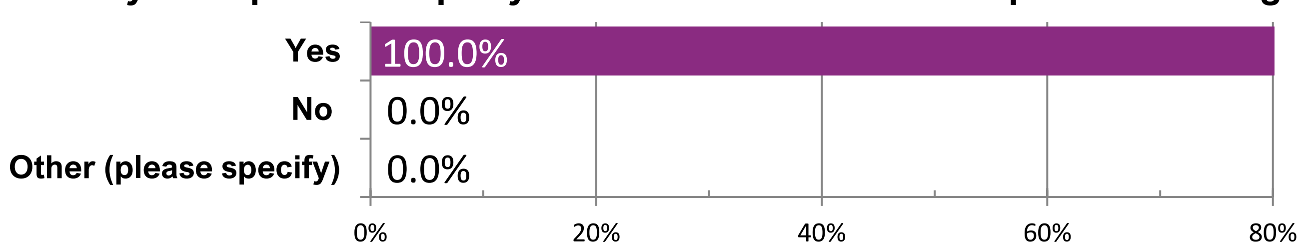
24. What processes does your company utilize to perform audits?

Comments:

- **10** comments reference a risk-based approach/assessment. Additional details are below:
  - Risk-based approach. Face-to-face with all high-risk, and a combination of desktop and virtual for others.
  - Entities are selected to be audited via a risk matrix and/or identified by Compliance or other gatekeeper functions.
  - IA selects a distributor for audit after risk assessment of distributors in country/hub which includes quantitative and qualitative analysis (also feedback from key stakeholders). Then IA engages PwC to perform the audit under the right to audit clause in distribution agreement. PwC is using the core audit program developed in conjunction with E&C, PwC and IA back in 2018.
  - Risk-based process with on-site visits, management interviews, books and records, etc.
  - Company conducts both For Cause and Not For Cause audits. In the case of FC audits, evidently these take place when a specific issue is identified. In the case of the NFC audits, we will choose candidates based on our global risk assessment and individual risk ratings.
  - Formal audits are undertaken by our Global Audit & Assurance function. Our TPI risk management team also undertakes on site visits where multiple elements of the TPIs compliance program will be reviewed and recommendations for improvements made.
  - Global audit performs distributor audits based on risk-based selection criteria.

        - Risk assessment, selection of high risk, communication with third-party, audit, reporting, feedback to the entity.
        - Depending on the situation and based on risk profile, we might perform desk-audits or in-person audits.
    - **13** comments reference an internal audit team conducts reviews with **1** comment referencing help from external resources. Additional details are below:
        - Audits are managed via Internal Audit function. We have included a minimum number of audits in each year audit plan.
        - The Compliance audit team conducts these audits with the help of external resources when necessary.
        - The Internal Audit and Monitoring division runs regular checks on the third-party population globally to ensure they have been put through our third-party due diligence process.
        - Random and targeted. Internally performed by compliance and audit.
        - An in-house audit template and process is used to identify any non-conformance to the Code of Conduct. The internal team manages and leads with external support (if needed for language purposes).
        - In person audit of books and records with compliance with contractual obligations. In addition to internal audit, third-parties are also in scope of our internal monitoring and testing program. There are also business liaisons that perform testing and training activity for certain regions.
        - We select around 5% of the total distributors based on CPI, annual revenue, and other factors.
        - It depends on what department is managing the audit (compliance, quality, regulatory, etc.). Small company typically results in very manual audits.
        - Compliance audit is managed by the audit Compliance team, and the party sellers assessments are managed by Regional Compliance Officers, both for targeted third-party sellers.
        - Rights to audit are included in the contractual language. On-site audits and/or virtual audits are performed to ensure distributor compliance with contractual terms. In addition, the internal audit/monitoring team performs reviews to ensure our internal/regional teams are following the internal policy guidance.
    - Formal request for documents and information, with follow up discussions, when necessary.
    - Hire external auditor.

25. Do you require third-party intermediaries to take compliance training?



Comments

- Via our third-party tool as a condition of approval.
- We have a business partner code of conduct, and we require third-parties to complete the training.
- Medium-high and high-risk third-parties take annual compliance training.
- Yearly.

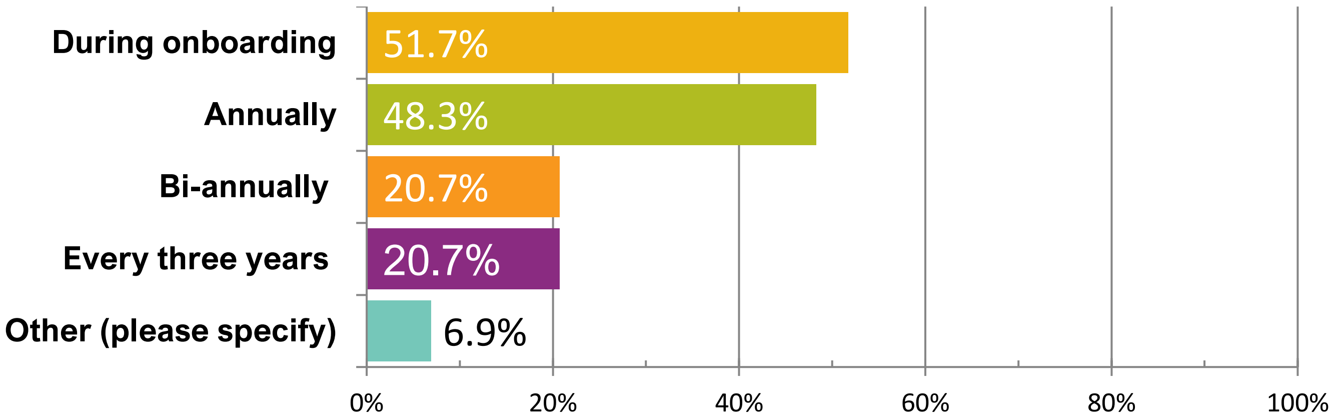
26. Who is required to take compliance training?

- **3%** All employees of the third-party intermediary
- **52%** Those employees of the third-party intermediary working directly on your account
- **7%** Those employees of the third-party intermediary at the principal level or above
- **38%** Other (please specify)

Comments:

- Principals and key employees.
- For the third-party, all key principals and those directly related to the account. Internally, all employees globally must take a company specific training on policies, procedures and key concepts related to anti-bribery and corruption.
- Usually, the training is provided to the top executives and the persons who will work with the company.
- It depends on the TPI and risks. Typically, only one or two employees complete the training, while we ask that they certify that they have/share our code of conduct with all employes working on our account.
- In Latin America, we require all employees of the third-party intermediary to be trained in compliance. In the rest of the world (OUS), we require those employees of the third-party intermediary at the principal level or above to be trained in compliance.
- At least one representative who then provides training in the distributorship or anyone who represents the company.
- Key employees at the third-party that may include the employees working directly on our account and the executives of the company.
- The person at the third-party filling the Due Diligence questionnaire, which is requested to cascade info to the company employees. Also, training is provided live by the corresponding Regional Compliance Officer to targeted Third-party sellers.
- We take a “train the trainer” approach. At least one senior person working directly on our account must take compliance training. This person is then required to train others who will work directly on our account.

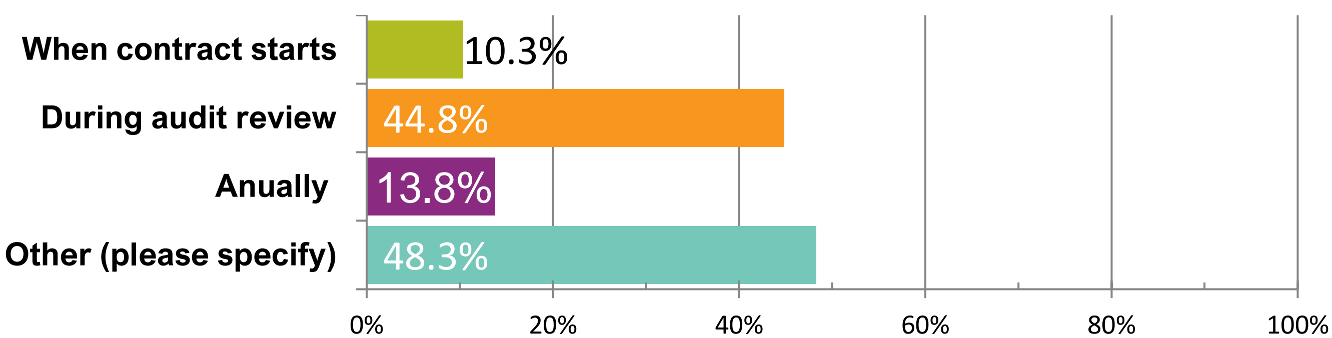
27. How often do you require third-party intermediaries to take compliance training? [select all that apply]



<u>Comments:</u>

- In-person training occurs at in-person meetings, as well for those in attendance.
- During onboarding as a part of the renewal process every 1-3 years depending on risk ranking.
- The cadence depends on risk-profile i.e., high-risk would be retrained annually.
- Every 2 or more years on a risk-based approach during the Due diligence renewal process.
- Every 2 years, or more frequently as needed.

28. How often do you request records for training? [select all that apply]

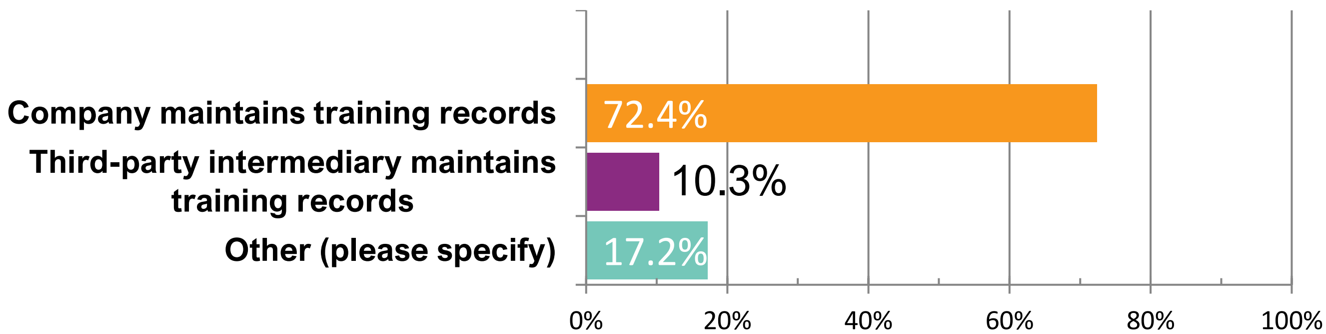


<u>Comments:</u>

- Onboarding and audit.
- We administer the training and track completions via our LMS.
- We conduct training via Diligent. We do not request records from the IDP.
- We do not request any records generally, unless there is something specific we want to add to their file (code of conduct, ABAC policy or procedures internally).
- We retain internal training records once we have completed the training.

- Training records are kept in our training platform.
- Distributors should be trained within the first six months of their business with the Company (within 6 months of execution of the Distribution Agreement) and then every two years thereafter. We request records for training every time they get trained.
- When needed/required.
- Every 2 or more years on a risk-based approach during the Due diligence renewal process.
- We train the representatives of our third-party intermediary so we have the records and do not need to request them.
- The training is completed in our third-party compliance process system before the third-party is engaged, and every 3 years when the third-party compliance process must be renewed.
- Other- we require documentation of training for certain third parties as part of enhanced controls.

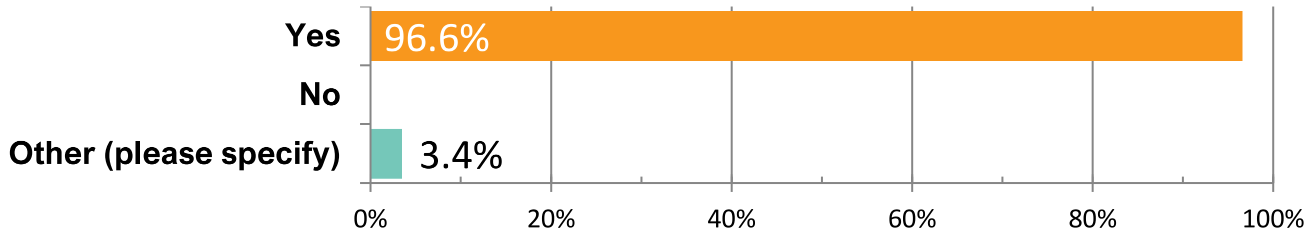
29. Does your company maintain a record of third-party intermediary training or does the third-party intermediary maintain the records?



Comments:

- Both.
- Both. We maintain records for our intermediaries we train and if any of their subs complete our training. And we expect our intermediaries to maintain their own training records to include their employees and sub-distributors.
- Both - we (company) maintain records of the training taken by the TPI authorized representative. TPI maintains training records for remainder of their Company account personnel.
- Company maintains record of training it provides; third-party maintains record of training it provides.
- For low/standard risk distributors, the main ITP is required to share the training records with HQ. For heightened risk distributors, HQ maintains the training records.

30. Do you require third-party intermediaries to adhere to your company's Code of Conduct or similar policy?



<u>Comments</u>

- We have a Channel Partner Code of Conduct to which they must certify.
- We have a third-party code of conduct that we require compliance with. For certain regions, we also have a tailored Manual of Policies and Guidelines for third-parties, which they are required to adhere to.
- We require them to provide their Code of Conduct and if it is not sufficient to ours, we provide them ours and require they read and attest to adhere to it.
- We do require adherence to our code of conduct, but we also have an exception process that requires the third-party to demonstrate their own code of conduct and that they have similar guidelines in place as our code of conduct.
- We have a set of third-party compliance guidelines that third-parties must follow.
- Distributors are required to sign off on our Code of Conduct at onboarding and renewal. They are also required to take Code of Conduct training every 2 years.

31. How is training delivered? [select all that apply]

- **62%** In-person live session
- **52%** In-person virtual session
- **79%** Learning management system
- **21%** Interactive virtual training
- **28%** Emailed training materials
- **10%** Third-party intermediaries provide training
- **3%** Other (please specify)

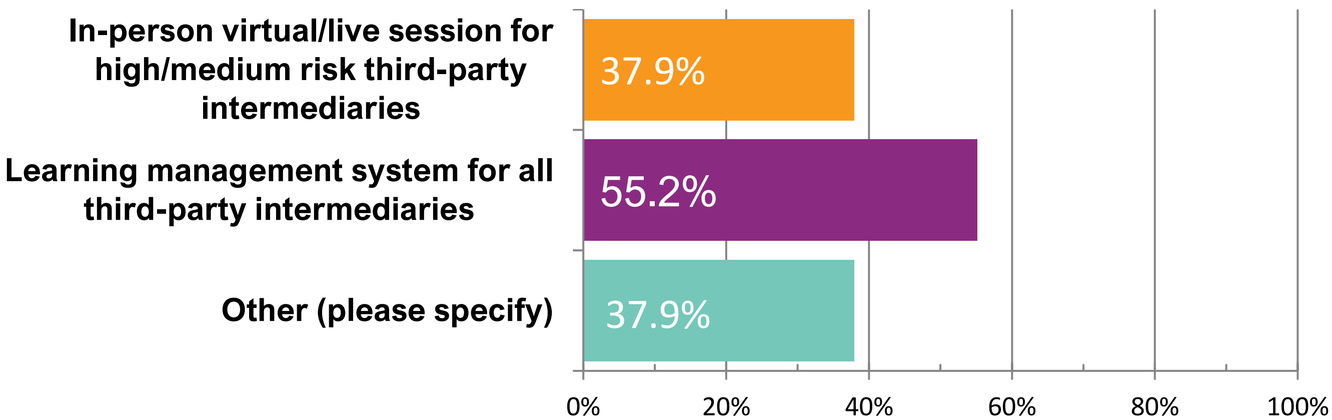
<u>Comments:</u>

- Some live training.
- Plus, our IDP portal has training materials and we have quarterly communications.
- Some regions also organize face-to-face training in addition to online training.
- Mix. Principal compliance training as part of DD is delivered through DD system. Other compliance

training may be delivered through any of the other mechanisms listed.

- As mentioned, the training is in our system, but we also conduct additional live or virtual training, as needed.

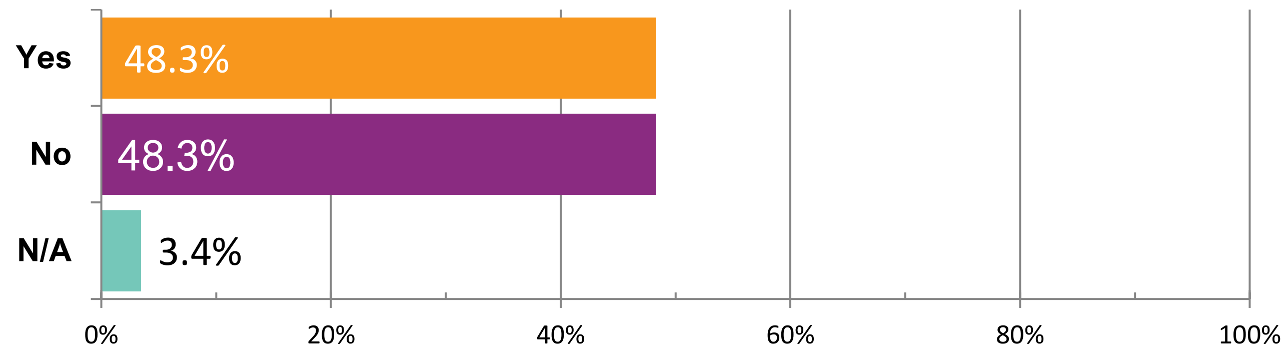
32. Is there a risk approach taken on the type of training delivered? [select all that apply]



Comments:

- In-person for some principals and teams
- In person training varies based on regional resources.
- For some ad hoc trainings, in-person sessions may be appropriate and done because of certain risk factors. But overall, the risk-based approach is not implemented for the training that all third-party intermediaries must complete.
- Training is required for those when they don't have their own compliance training and red flags are identified.
- We may provide in-person training to remediate TPI risk.
- Standard online training is required for all intermediaries. Additional training (in person/online/virtual) may be provided as needed.
- Mix. Principal compliance training as part of DD is delivered through DD system. Other compliance training may be delivered through any of the other mechanisms listed. F/up trainings for higher risk TPIs will generally be delivered in real time (in-person or virtually).
- Learning management system for all third-party intermediaries, live or virtual training may also take place for certain third-parties based on need.
- If a specific event requires additional training, we do in-person.
- Live training, online training or a combination of both are permitted.
- Not always a factor.
- No specific approach on the type of training.

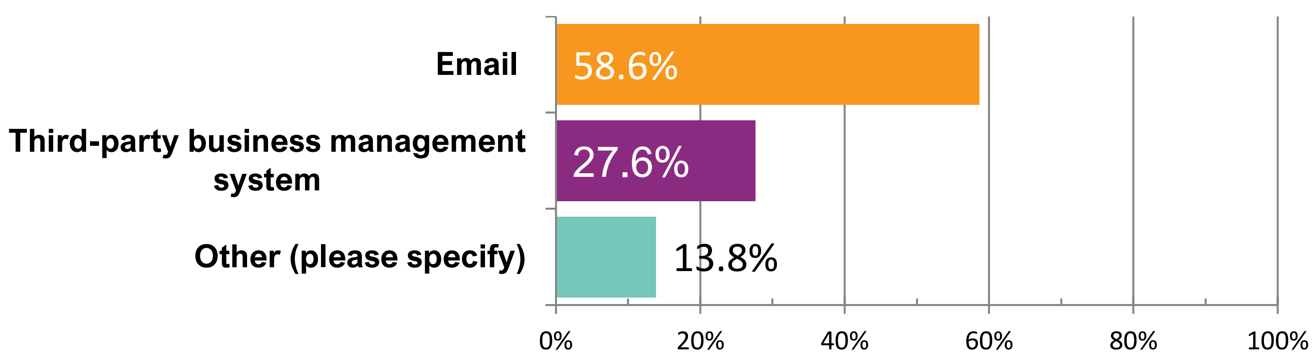
33. Do you require third-party intermediaries to perform training for sub-distributors?



Comments:

- Sub distributors above a certain threshold are trained in the same way as IDPs.
- It is a requirement included in the Distribution Agreement.
- Learning management system for all third-party intermediaries, sub-distributors that are in scope for our third-party compliance process must complete training provided by Company.
- If the main distributor is considered low/standard risk, the main distributor is responsible for conducting due diligence on the sub dealer, as well as training. If the main distributor is a heightened risk, our internal teams are required to log the sub-distributor dealer in our systems as a dealer and perform due diligence and training.

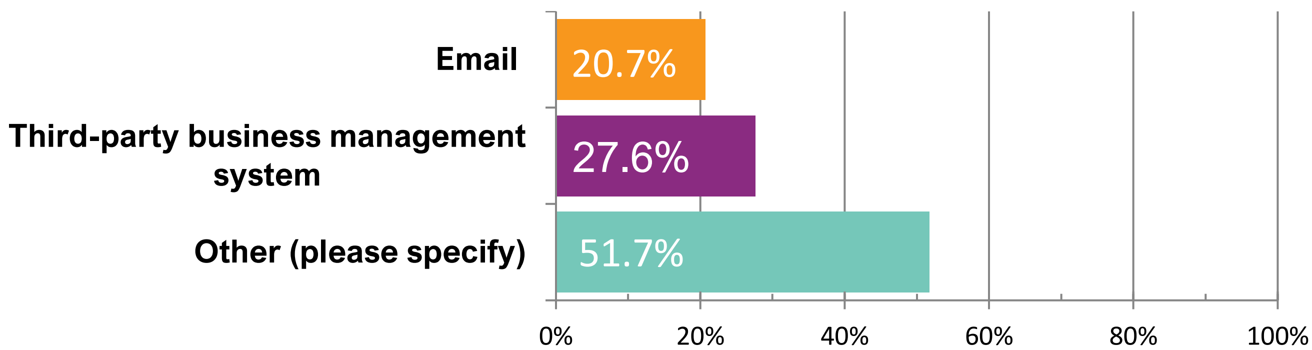
34. What method of communication do you use to communicate requests for preservation of records?



Comments:

- We have not had a need for this, but it would be email.
- Distributors are communicated to about the need to keep compliance records in the moment they receive an invitation to the training (email).
- Standard contract clauses.
- Document retention is included in contract language.

35. How do you communicate your policies regarding HCP interaction with third-party intermediaries?



Comments:

- **4** comments reference communication of the company's "Code of Conduct." Additional details are below:
  - Code of conduct is trained on, provided at onboarding and available on the IDP portal and public website); portal.
  - As part of the questionnaire, they certify to our Code of Conduct and ABAC training.
  - 1) Communicating the third-party code of conduct and Manual of Policies and Guidelines (when applicable). 2) Including requirements in contracts and training on those requirements via learning management system and live training.
- Communication is done during onboarding and contract signing, the policies and procedures are available on the company website.
- Both email and Intranet access to policies.
- Mix.
- We will remind third-parties through different means, including via emails, newsletters, and specific online training modules.
- During training sessions.
- At every training and also embedded at the agreement as an annex (Compliance Standards).
- Training.
- TPI Portal (On-line).
- Distributor Handbook.
- We direct them to a site where they have full access.