AIM-PROGRESS

CONSULTING ethic

Third party anti-bribery & corruption risk management protocol toolkit

August 2016

Introduction

This document outlines a protocol for AIM-PROGRESS members on third party risk management, with a focus on anti-bribery and corruption.

Third party risk is an area of focus for all AIM-PROGRESS members but addressing bribery and corruption risk in a pragmatic, cost-effective way that effectively manages the risk and delivers real business benefit is challenging.

In the following pages we have provided guidance on the key elements of an anti-bribery third party risk management programme, from identifying and categorising third parties through to measuring its impact and reporting.

In its preparation we have reviewed a range of different sources and best practice documentation. Those that we found most useful are listed in the 'References' section. In addition, we have drawn on the responses provided by members to the survey undertaken and experience from other industry sectors such as pharmaceuticals, energy, aerospace and construction.

We are not prescribing a single effective way of constructing and operating an anti-bribery and corruption third party risk management programme. Members will have different organisation models, be at different stages in development of their programme and ultimately have different views on the acceptable levels of risk.

However, we have sought not to add another lengthy guidance document to the set that already exist. We have therefore focused on the practical implementation of a programme.

We have provided examples of how technology tools can be used to support elements of an anti-bribery third party risk programme. We have not attempted to provide a critical evaluation of the suppliers of such tools or their products.

Definition of third party

For the purposes of this protocol we are using the term 'third party' in the broadest sense to include anyone to whom money is paid (except for employees) and from whom money is received, in exchange for providing goods or services. This includes customers, suppliers, agents, representatives, distributors, consultants, contractors etc. However, given the remit of AIM-PROGRESS we have ensured the primary focus is on suppliers.

Definition of third party risk

The protocol is focused on addressing anti-bribery and corruption risk associated with third parties. However, we recognise that this is just one type of risk apparent in third party relationships.

One of the recommendations of this protocol is that wherever practicable third party risk should be addressed holistically both to maximise efficiency and effectiveness. Failure in one area may be an indicator of failure in another and practically in terms of time and resources, it makes sense to streamline the processes associated with different risk areas. As such, much of the guidance provided in this document could equally be applied to other third party risk areas such as human rights or health and safety.

Principles

Any effective third party risk management programme has to be founded on certain key principles:

- Practical and genuinely makes a business difference
- Sensitive to the potential burden on the business
- Integrates or dovetails with existing processes
- Repeatable and sustainable
- Responsive to business imperatives
- Cost-effective when balanced against the risk addressed
- Integrated into day to day business activity

Risk appetite

The content and focus of an anti-bribery and corruption third party risk management programme for an individual member ultimately has to be driven by the level of risk which the organisation assesses as being acceptable to it.

We cannot dictate what this should be for individual member companies and the decisions around this will drive the level of investment and resource dedicated to managing third party anti-bribery risk.

However, key anti-bribery legislation and guidance from around the world includes ‘third party due diligence’ as one of the core requirements of any programme. There are well-publicised examples of companies that have received significant fines resulting from breaches of anti-bribery legislation by associated third parties.

Clearly this risk is potentially increased where the third party is directly acting on behalf of the company, for example as a manufacturer, distributor, an agent or an advisor. However, the potential reputational damage resulting from working with any third party found to be engaged in bribery or corruption should not be underestimated.

Therefore, whilst we accept that each member company will form their own view of the acceptable level of risk, this is not a risk area that can be ignored.

Third party anti-bribery risk management process

So, what's required? What is it that member companies need to do in order to satisfy themselves that their third parties are not exposing them to bribery risk?

There are a host of guidance documents in existence from organisations such as Transparency International, the World Economic Forum, the International Chamber of Commerce and a range of consultancy companies.

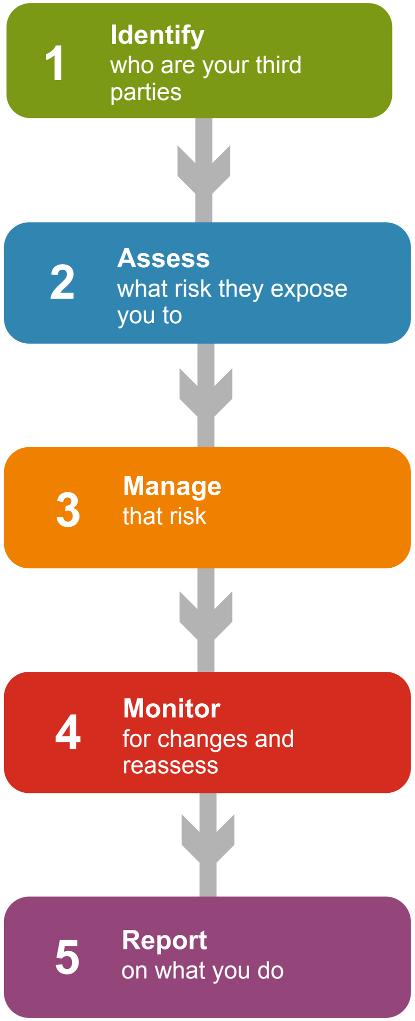
At their core they all say the same about what is involved in managing third party bribery risk:

- Know who your third parties are
- Assess what risk they might expose you to
- Decide how to deal with that risk
- Make sure you reassess them periodically

In this protocol we do not intend to propose a radically new approach - it's tried and tested and feels appropriate. What we have done is provide practical guidance on what should be included in each step, how to go about it, who should do it and what further guidance is out there to help.

Undoubtedly some of you will disagree with our recommendations but without proposing how practically to implement a programme, the protocol becomes yet another theoretical document.

So please, take it as guidance, modify it as you feel appropriate for your organisation and let us know where it works and where it doesn't.



1 **Identify** who are your third parties

2 **Assess** what risk they expose you to

3 **Manage** that risk

4 **Monitor** for changes and reassess

5 **Report** on what you do

Roles & responsibilities

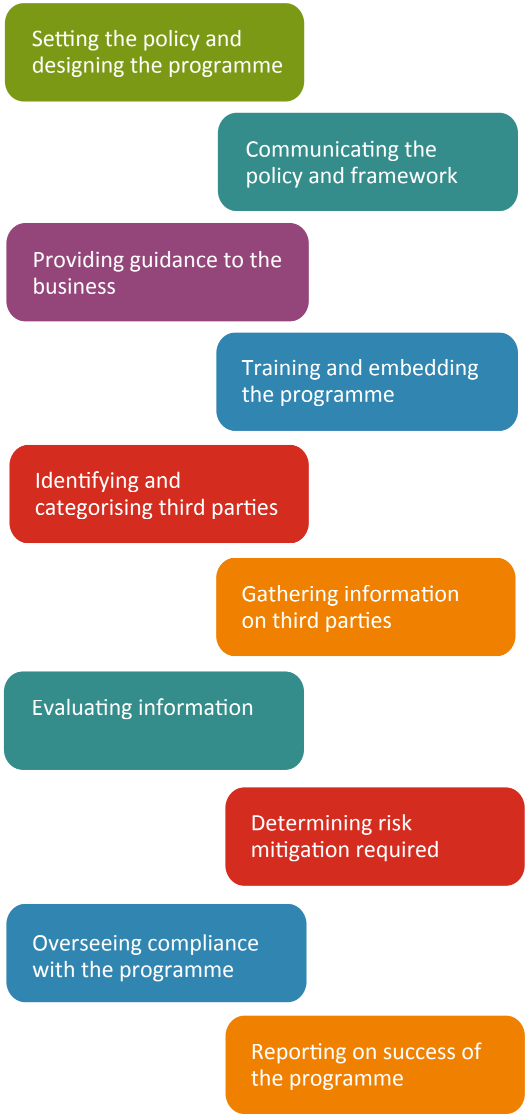
We have made suggestions as to which teams or departments are best placed to perform the activities related to different elements of the third party anti-bribery programme. However, each member company will be organised differently and whilst the key organisation roles will be fulfilled, the exact structure will vary.

What is important is that the activities detailed have clear ownership, that there is a defined process workflow and that those performing these activities have the resources and capabilities to do so effectively.

There is much debate about the extent to which third party risk management activity, specifically when it applies to anti-bribery, should be undertaken centrally or de-centrally. We propose that there must be a combination of the two and see distinct roles and responsibilities of the functions of the corporate centre, the business/ markets and local functional support:

- There should be strong centralised responsibility for setting the policy, designing and communicating the programme, and oversight of it, driven by a Compliance, Legal or Risk function
- Relationship owners, be they within procurement, sales or elsewhere in the business are best placed to provide information on the third parties with which they work
- Local functional experts, Legal, Compliance or Finance provide the subject matter expertise to evaluate the information provided and define the right response to mitigate the risk
- Internal Audit have a role to provide assurance on the extent of compliance with the programme

In summary, best practice suggests that a third-party anti-bribery programme follows a 'three lines of defence' model with the business, specialist functions and audit all having a role to play in the effective management of the risk. The model is expanded upon in the 'Tools' section.



Setting the policy and designing the programme

Communicating the policy and framework

Providing guidance to the business

Training and embedding the programme

Identifying and categorising third parties

Gathering information on third parties

Evaluating information

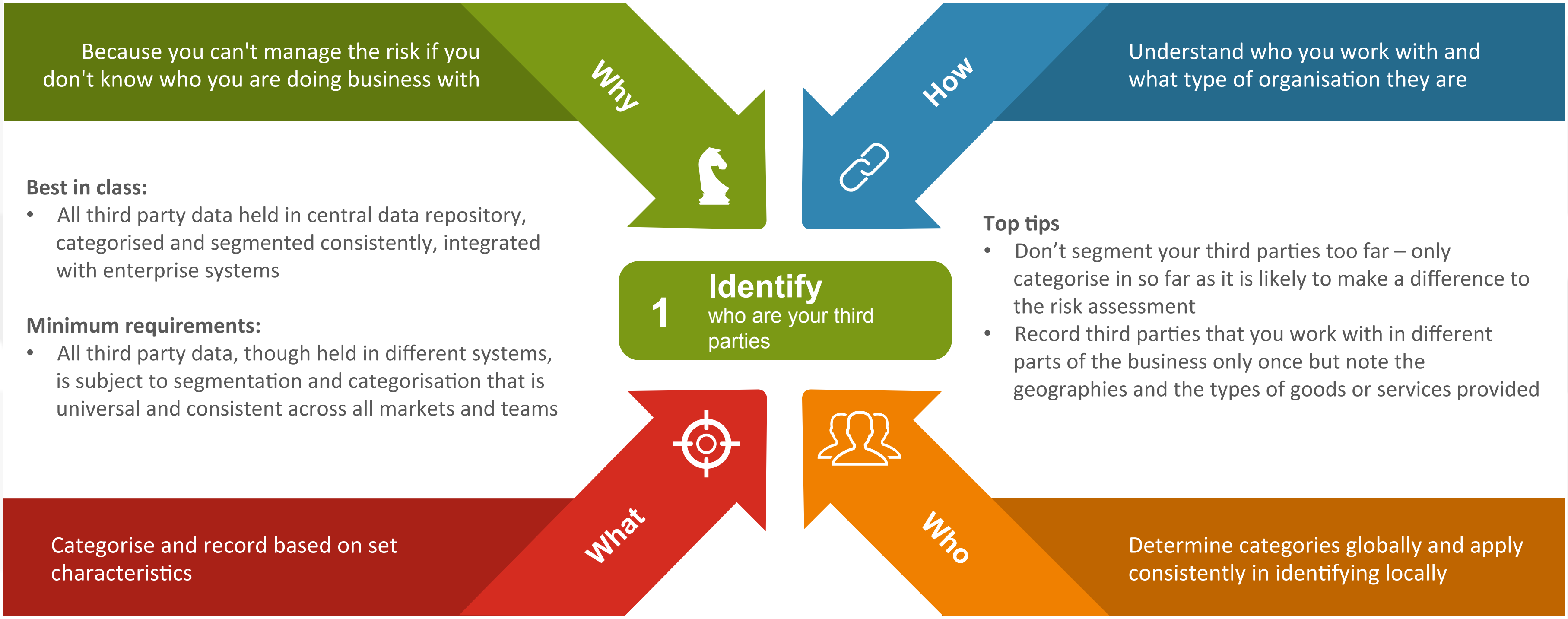
Determining risk mitigation required

Overseeing compliance with the programme

Reporting on success of the programme

- All third parties should be identified to understand the volume, nature and location of the relationships which are in existence
- Some third party relationships may be managed at a global level but the majority of the information will exist within the local business

- Employ categories already in use by the business e.g. in procurement or finance systems
- Use third party information already held in systems either globally or locally
- Create a single global data repository of third parties



Because you can't manage the risk if you don't know who you are doing business with

Understand who you work with and what type of organisation they are

1 Identify

who are your third parties

Categorise and record based on set characteristics

Determine categories globally and apply consistently in identifying locally

Best in class:

- All third party data held in central data repository, categorised and segmented consistently, integrated with enterprise systems

Minimum requirements:

- All third party data, though held in different systems, is subject to segmentation and categorisation that is universal and consistent across all markets and teams

Top tips

- Don't segment your third parties too far – only categorise in so far as it is likely to make a difference to the risk assessment
- Record third parties that you work with in different parts of the business only once but note the geographies and the types of goods or services provided

- Categorise third parties across all of the business e.g. customer, distributor, service provider using consistent terms
- Record basic information about each third party e.g. category, location, size

	Co	Le	Pr	Fi	Sa	Au	RO	TP
Global	✓		✓	✓	✓			
Local			✓	✓	✓		✓	

Compliance, Legal, Procurement, Finance, Sales, Audit, Relationship Owner, Third Party

AIM-PROGRESS

CONSULTING ethic

2a Assess – initial
what risk they expose you to

Why
How
What
Who

- All third parties should be subject to an initial risk assessment to determine the level of bribery risk associated with dealing with them
- Undertaking and recording this initial risk assessment demonstrates a comprehensive approach but allows resources to be focused on the relationships of highest risk

Why: Because only by assessing the risk can you determine what is the right response

Best in class:

- All third parties are subject to a limited initial risk assessment which classifies them as H/M/L risk with the outcome recorded and higher risk third parties are subject to further assessment

Minimum requirements:

- All third parties in higher risk locations, industries or having interaction with government are subject to an initial risk assessment to determine appropriate further action

- Develop and complete a simple questionnaire for all third parties
- Devise a scoring system to generate a simple risk rating e.g. High/Medium/Low, using
- Use existing sources for scoring e.g. TI Corruption Perceptions Index (CPI) for the location of delivery

How: Devise a simple questionnaire, scoring and risk rating, complete and record for each third party

Top tips

- Don't perform the same level of risk assessment on every third party, its not best use of resources
- Don't have different parts of the business undertaking risk assessments on the same third party unless the services provided or the location of delivery differ
- Apply a consistent assessment across all categories of third party at the initial stage e.g. customers, suppliers
- Recognise that initial assessment is an indicator only and further assessment may be requested even if a low risk rating is generated
- Make use of existing and shared data sources

What: Undertake an initial risk assessment based on a limited number of key factors

- Undertake two stages of risk assessment to ensure resources are focused on higher risk third parties
- Focus on limited information e.g. nature of goods and services provided, location of delivery, interaction with government
- Ensure opportunity exists to undertake further assessment even for low risk rating as required

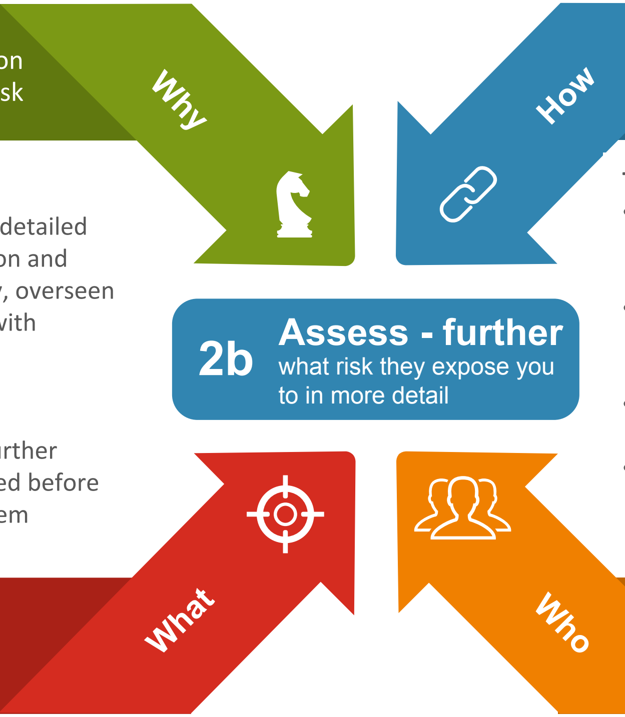
Who: The questionnaire and scoring approach should be devised globally with assessment and recording done locally

	Co	Le	Pr	Fi	Sa	Au	RO	TP
Global	✓	✓						
Local	✓		✓		✓		✓	

Compliance, Legal, Procurement, Finance, Sales, Audit, Relationship Owner, Third Party

2b Assess - further

what risk they expose you to in more detail



- The information collected at the previous stage is not sufficient to adequately assess the risk for those third parties assessed as higher risk
- Further information enables a more detailed evaluation of higher risk third parties to allow an informed decision to be taken as to whether to work with them and if so, with what conditions

Why

Because you want to focus your resources on the relationships that pose the greatest risk

Best in class:

- All higher risk third parties are subject to a detailed risk assessment which requires the collection and analysis of information from the third party, overseen by a risk function and supported by a tool with assessment and recording functionality

Minimum requirements:

- All higher risk third parties are subject to further assessment to determine if action is required before commencing or continuing to work with them

What

Based on the outcome of the initial risk assessment, determine what next

- For those third parties assessed as low risk (likely to be the majority), no immediate further action is required but a review date should be set
- For medium and high risk third parties, further information should be collected in order to enable a fuller risk assessment e.g. ownership, management, government links, business integrity measures

- Devise and complete a more detailed questionnaire for all high and medium risk third parties, with information obtained directly from them
- Use a tool to enable both recording and analysis of the third party information
- Evaluate the information provided to identify any specific risks associated with the third party

How

Devise a questionnaire to collect further information for higher risk third parties using internal sources, information from the third party and supporting tools

Top tips

- Engage with the third party and seek their declaration of the completeness and accuracy of the information provided, in a local language as required
- Record and retain all information in accordance with the organisation's records retention policy but verify all applicable data privacy requirements are met
- Ensure that more detailed (and resource-intensive) evaluations are confined to higher risk third parties
- Involve people with the right subject matter expertise to undertake the evaluation of the risk posed and do not assume this can be 'automated'

Who

Information required should be advised globally and evaluation undertaken locally – it requires judgement and cannot be fully automated

	Co	Le	Pr	Fi	Sa	Au	RO	TP
Global	✓	✓						
Local	✓	✓	✓	✓	✓		✓	✓

Compliance, Legal, Procurement, Finance, Sales, Audit, Relationship Owner, Third Party

AIM-PROGRESS

CONSULTING ethic

Why
How
What
Who

3 Manage
that risk

- There may be cases where the risks identified during the assessment lead to a decision not to work with the third party
- The aim though is to build a network of trusted third parties and therefore in the majority of cases to implement the necessary safeguards to mitigate the identified risk

Because having identified where there is risk you need to address it, otherwise assessing it was a waste of resources

Best in class:

- All third party contracts contain risk-mitigation elements, including ethics requirements. Audits are conducted on higher risk third parties. Use is made of shared information resources. All outputs are documented.

Minimum requirements:

- All highest risk third party contracts contain risk mitigation elements which are exercised regularly and the results documented.

At the extreme ends, do nothing, or don't work with the third party; In between, a range of things - contract clauses, training etc.

- Take action based on where the risk has been identified e.g. in the government links of the business or the lack of anti-bribery policies in place
- Action may be needed before or commencing working with a third party or as part of the ongoing relationships e.g. obtaining information on their anti-bribery programme or undertaking regular audits

- Define a set of potential actions to manage the identified risk
- Select the ones that are most appropriate
- Modify or add to the actions based on the specific risk assessment
- Create an action plan with clear responsibilities and deadlines for implementation

Write conditions into the contracts, deliver training, support the third party to meet the required standard

Top tips

- Critically assess what is going to make the difference in managing the risk associated with that specific third party rather than selecting generic activity from a list
- To ensure the third party completes or is committed to certain actions they include them in your contract
- For inherently higher risk categories of third parties e.g. political consultants or lobbyists, set global mandatory minimum actions

Actions defined by Compliance/Legal, particularly minimum requirements and Implemented by a combined team

	Co	Le	Pr	Fi	Sa	Au	RO	TP
Global	✓	✓	✓				✓	
Local	✓	✓	✓				✓	✓

Compliance, Legal, Procurement, Finance, Sales, Audit, Relationship Owner, Third Party

AIM-PROGRESS

CONSULTING ethic

4 Monitor

for changes and reassess

Why

Because things can change quickly, new information comes to light, and you can't rely on the fact that the risk remains constant

- Third party information will change from time to time and risk assessments are not one-off exercises
- It is necessary therefore to periodically refresh and review the information collected
- Information should be updated from that already held although the highest risk third parties may require a full re-assessment

Best in class:

- All third party information is reviewed, updated and reassessed at minimum globally applied review frequencies (annually for high risk) and a process exists to ensure new information on a third party which emerges between reviews is captured and evaluated

Minimum requirements:

- All third parties are reviewed regularly for changes in information relevant to the risk assessment

How

Have an ongoing dialogue with the third party and use a tool to check for adverse media reports

- Use a tool to set review dates and generate alerts
- Update information already available rather than starting again but ensure it is fully reviewed
- Use both internal sources and information provided by the third party
- Implement controls to prevent non-approved third parties being included in financial systems

Top tips

- Set minimum review frequencies for all third parties even those classified as low risk
- Be consistent across third party groups e.g. customers and suppliers
- Be realistic about the business burden in setting review frequencies and focus on the highest risk
- Have a mechanism in place for capturing and using information which comes to light in between reviews
- Don’t rely on individual relationship owners to trigger a review as they may well have moved on before the time comes

What

Be alert for new information and set the frequency with which you will undertake a full review of the third party

- Attach a review date to each third party when the information will be fully reviewed and assessed, with frequency determined by the level of risk
- Undertake ongoing monitoring to ensure new information which may affect the level of risk associated with the third party is known about as early as possible

Who

Compliance/Legal set the minimum review frequencies and relationship owners have an ongoing dialogue

	Co	Le	Pr	Fi	Sa	Au	RO	TP
Global	✓					✓		
Local	✓		✓				✓	

Compliance, Legal, Procurement, Finance, Sales, Audit, Relationship Owner, Third Party

AIM-PROGRESS

CONSULTING ethic

5 Report
on what you do

Why
How
What
Who

- Reporting on the programme can take a number of forms – to senior management, to committees, externally but in all cases it should be used to evaluate the success of the programme and opportunities sought to modify and enhance it where possible

Because its an important element of any anti-bribery programme and it demonstrates 'adequate procedures'

Best in class:

- Reporting on the progress, results and status of the risk management programme is provided at Board level, to appropriate risk committees, senior management and externally

Minimum requirements:

- Senior management are informed on the status of the third party risk management programme and actively support it's application in the business

- If you are using a tool, use the reporting functionality available to provide data on your third party programme e.g. numbers of third parties reviewed, numbers categorised as high risk, number of audits undertaken etc.
- If not, establish a simple reporting template to be completed at a market or function level

Use tool reporting functionality or consolidate information to report internally and externally

Top tips

- Structure your reporting in such a way to enable analysis by geography, market or function
- Focus on consolidated data rather than individual records to ensure that data privacy requirements are met in regards to who has access to individual third party records
- Include a section on your approach to managing third party bribery risk in your annual report and corporate citizenship or sustainability report

On numbers of third parties assessed, risk categories, type of risk management activities undertaken, terminations

- Provide regular reporting to senior leadership, audit and risk committees on activity being undertaken
- A global function e.g. Legal, Compliance, Risk should perform an oversight role to ensure adherence to the programme and to check for consistency
- Internal audits should incorporate the operation of the third party risk management programme

A global function should have an oversight role and report on the success of the programme

	Co	Le	Pr	Fi	Sa	Au	RO	TP
Global	✓					✓		
Local	✓		✓	✓			✓	

Compliance, Legal, Procurement, Finance, Sales, Audit, Relationship Owner, Third Party

Further detail

... to support each element of the programme

1 Identify
who are your third parties

Example categories of third parties - nature of business relationship

Category	Type	Definition
Supplier/vendor - goods	Raw materials	Supplies materials used in the production of the organisation’s products
	Finished products	Supplies materials already in a finished state e.g. printers
Supplier/vendor - services	Professional services	Provides finance, legal, accountancy, communications, consultancy services
	Contractor	Contracts with the organisation to provide a service or undertake a project
	Advisor	Provides advice in their specialist field
	Agent	Authorised to act on behalf of or represent the organisation
	Lobbyist or political consultant	Authorised to represent the organisation’s interests with government or political parties
Customer	Direct	Buys the organisation’s products for direct consumption
	Distributor	Buys the organisation’s products to sell-on
Commercial partner	Consortium partner	Collaborates in an enterprise but is a separate legal entity
	Joint venture partner	Operates a business entity in partnership with the organisation
	Industry association	Represents an industry or a group of companies working together

2a Assess
what risk they expose you to

For the initial risk assessment, information should be drawn from readily available sources, rather than by requesting information from the third party or undertaking due diligence. If a tool is used to support the risk assessment, checks may be run automatically on the third party name against adverse media databases or sanctions lists. However, in general we recommend such checks are undertaken at the next level of assessment.

Example content for initial risk assessment

Risk indicator	Questions	Assessment
Name	• What is the name of the third party?	Both the trading name and registered name (if different) can be included or this can be added if the third party is categorised as higher risk
Nature of goods or services	• What goods or services will be provided?	Certain goods or services providers are generally regarded as low risk e.g. supplies of finished consumables such as printer cartridges, whilst others will be high risk e.g. lobbyist services
Geographic location	• Where is the third party located? • Where will the goods or services be delivered?	Both where the third party is located and where the goods or services will be delivered should be assessed. Use the Transparency International Corruption Perceptions Index (CPI) to group countries into High/ Medium/Low risk
Government links	• Are any of the owners or directors, or close family members of them known to be government officials or entities? • Is the third party wholly or partially-owned by a state entity?	Close connections to government is generally regarded as a risk factor given the positions of influence that this may reflect and the focus of anti-bribery legislation
Background	• Has the third party or its owners or directors been the subject of any investigations or convictions for commercial crime?	If a tool is used to support the risk assessment process automatic checks may be run on the
Other factors	• Are there any other factors that would suggest that this third party should be subject to more detailed risk assessment?	Whilst a third party may be low risk according to the categories above there should be the opportunity at this stage to identify any factors which suggest further assessment is required

2b **Assess** what risk they expose you to

For the more detailed risk assessment applied to higher risk third parties, an evaluation must be made of what level of information to collect. Each inclusion should be critically assessed to determine if it will materially inform the risk assessment or the decision as to the mitigating action to be taken. It is tempting to collect as much information as possible but a trade-off has to be made with the collection burden.

As with the initial risk assessment, if a tool is used to record the third party risk assessment checks against key pieces of information can be undertaken.

Example content for detailed risk assessment

Risk indicator	Questions	Assessment
Name	• Has the third party operated under any other registered or trading name in the last 5 years?	This could be included at the initial assessment stage but is unlikely to be known without undertaking checks or consulting the third party
Ownership	• What is the type of business entity e.g. corporate, partnership, sole trader? • Who are the owners or shareholders that own a business interest greater than 5%? • Are there any beneficial owners of the third party? • Does any government have any direct or indirect ownership or other financial interest in the third party?	Where possible documentary evidence of ownership should obtained, certainly for high risk third parties, either from official sources or if necessary directly from the third party Ownership details can also be used for the performance of the required anti-money laundering procedures and sanctions list checks
Management	• Who are the main directors of the third party?	Collect basic information such as their name, position and nationality. Focus on the main directors of the third party and any key contacts
Government links	• Are any owners, officers, directors, principal contacts or immediate family members of the aforementioned who are, or have been in the last 3 years, government officials or Politically Exposed Persons? • Will the third party be interacting with government entities (e.g. state-owned or controlled companies), government/public officials, or other individuals with potential influence over government decisions on behalf of the organisation? • Will the third party be acting as a lobbyist or political consultant?	Anti-corruption laws have a particular focus on the bribery of government officials. The existence of interaction with government by the third party is likely to suggest that action may be required to put in place safeguards and mitigate the risk

Example content for detailed risk assessment (continued)

Risk indicator	Questions	Assessment
Business integrity standards	• Does the third party and/or its owners appear on any international or national embargoes, sanctions or blocked persons lists? • Has the third party, any affiliated companies, owners, directors or principal contacts been the subject of any convictions, charges or investigations related to bribery, corruption or other commercial crime? • What is the third party's approach to preventing bribery and corruption and promoting ethical business?	Checks should be performed against the main international and national sanctions and blocked persons lists. The performance of such checks is greatly facilitated by the use of a commercially provided tool. However, care must be taken to ensure that the search parameters employed are appropriate for the business i.e. do not return large numbers of 'false positive' hits as this can be a distraction from identifying the real risks. Focus should be on commercial crimes not personal prosecutions for breaches of laws such as those related to driving or minor violations. Evidence should be obtained of the third party's approach to managing bribery risk e.g. a copy of a Code of Conduct and/or anti-bribery policies, training provided to employees, reporting/ whistleblowing mechanisms.
Contract & transactions	• What are the bank details of the third party? • What is the anticipated annual transaction value with the third party? • Have any unusual remuneration or payment arrangements been requested – success fees, up front payments, payments in cash, payments to an account in a name other than that of the third party? • Is it anticipated that the third party will sub-contract the provision of more than 10% of the contracted goods or services?	The name of the bank, the account number and the account name should be collected. The anticipated annual transaction value may be an indicator of the significance of relationship to both parties and thereby potentially the associated risk. Sub-contracting arrangements can result in less transparency of activity.

Example outcomes from third party anti-bribery risk assessment

Third party status	Description
Approved	The third party has been approved for the organisation to do business with
Deferred approval	The third party is approved subject to certain conditions being met or actions implemented prior to commencing doing business with them e.g. signed confirmation of agreement to supplier code of conduct
Approved with conditions	The third party is approved subject to certain ongoing assurance activities during doing business with them e.g. annual audits, regular reporting
Rejected	The third party is not approved to do do business with (and controls should be established to prevent doing so)

3 Manage that risk

Dependent on the level of risk assessed to be associated with the third party, action may be required prior to engaging the them or as an ongoing requirement for working with them. An action plan with clear owners and timelines must be formulated, recorded and implemented.

Where the third party is high risk, any conditions should be formally included in contracts.

Example actions to manage identified risk

Action	Description
Enhanced due diligence	This may include further research, interviews with the third party, or commissioning a report by an external firm, before a decision is taken whether to engage with them – this should only be applied to the highest risk third parties e.g. those engaged in activities with a high bribery risk such as lobbying, or operating in high risk geographies
Anti-bribery commitments	Requiring the third party to contractually commit to abiding by the anti-bribery policies of the organisation, Code of Conduct or Supplier Code of Conduct and applicable laws and regulations
Anti-bribery programme	Requiring anti-bribery policies, training or monitoring to be put in place in the third party and an annual certification of compliance to be conducted and reported
Training	Requiring the third party to provide anti-bribery training to employees working with or on behalf of the organisation or providing the training directly to them
Accurate books and records	Obligating the third party to maintain accurate books and recorded and have in place appropriate controls
Limitations	Prohibiting the third party from undertaking certain high risk activities on behalf of the organisation e.g. interacting with government bodies
On-site audits	Including a contractual provision for a right to audit and undertaking periodic audits
Termination	Specifying the right to terminate the contract with no penalty in the event that anti-bribery standards are breached
Invoicing & payments	Undertaking periodic reviews of the invoicing being provided by the third party and an analysis of payments
Ongoing monitoring	Using a tool to undertake ongoing monitoring against databases such as sanctions and adverse media

4 Monitor for changes and reassess

The frequency with which third party information should be refreshed and re-evaluated will depend on the risk associated with them. High risk third parties should ideally be re-evaluated annually. If the risk assessment process is effective in only categorising a limited number of third parties as high risk, the time and resources required to do this will be manageable.

It is likely that where a global risk assessment is applied in geographies with a high CPI rating, a larger proportion of all third parties will be subject to more frequent reviews.

Example review frequencies

Third party risk	Frequency (recommended)	Frequency (minimum)
Low	3 years	5 years
Medium	2 years	3 years
High	1 year	2 years

Example ongoing screening information (if using a tool)

Category	Third party data	Comments
Basic information	Third party name	Could include trading name and registered name if different
Ownership & management	Names of owners	Where not publicly listed on a recognised exchange
	Names of directors	Particularly any with an ownership interest
Transaction details	Name of bank	Can be checked against sanctions lists and other databases

5 Report
on what you do

An effective risk management process needs the engagement and support of senior management, especially those involved in any audit or risk committee, and the objectives of the third party anti-bribery risk management process should be aligned with the broad risk priorities and strategic objectives of the organisation.

Example third party anti-bribery risk management programme measures

Measure
Number of third parties assessed
Number of third parties assessed as being higher risk
Number of third party audits conducted
Result of any relevant internal audits
Description of any more significant risks or issues related to third party corruption
Any issues (such as reported incidents)

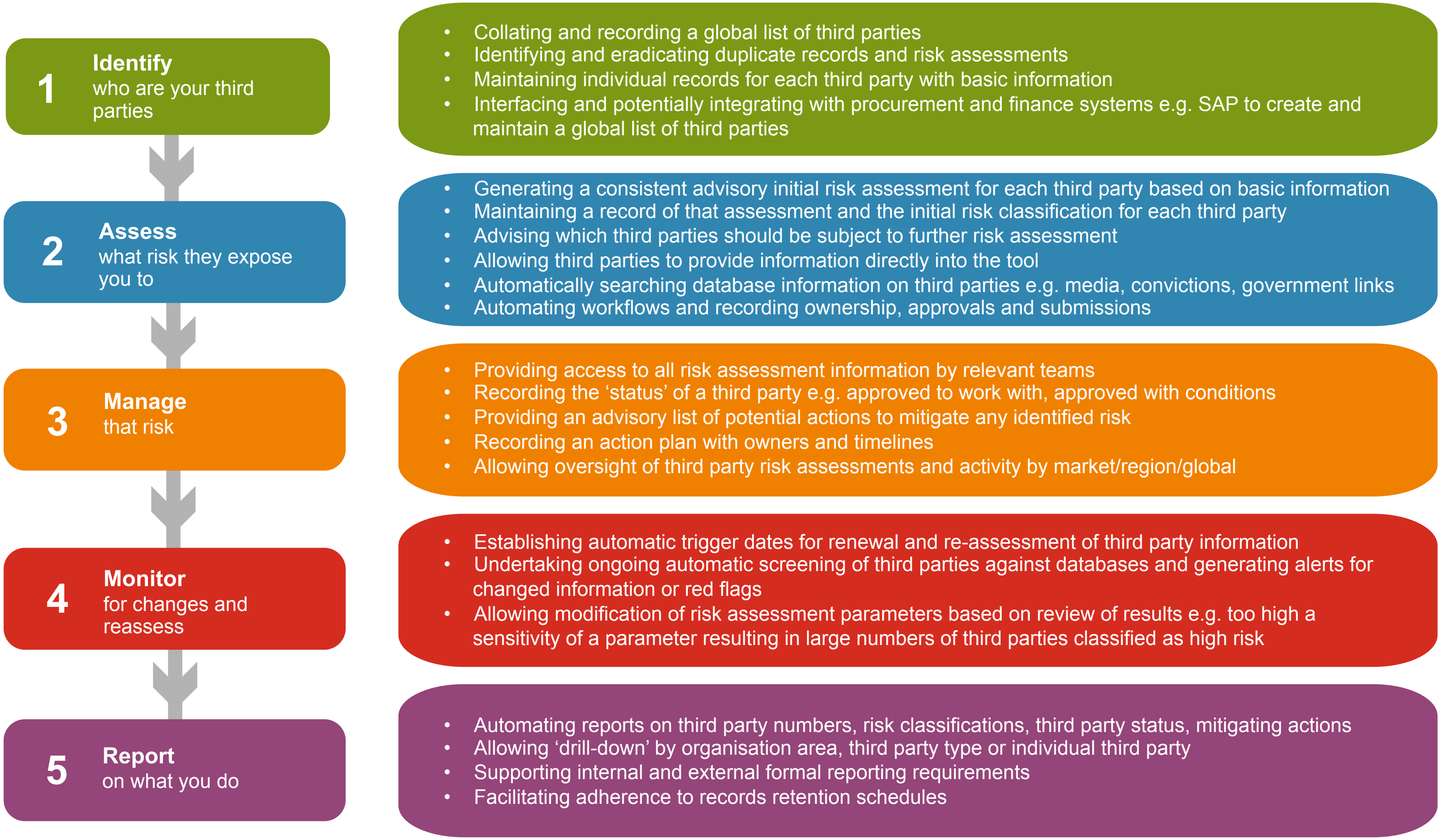
Tools

… to support your programme

Technology tools

Elements of a third party anti-bribery risk management programme can be supported through the use of technology tools or software. We have not provided an analysis of the many vendors of such tools, the features of their products, their pricing models or a view on their effectiveness. Instead, we have highlighted activities which we believe can be facilitated with such tools. In using any tool, the up-front work to design and configure it to meet the specific needs of the organisation's third party risk management programme is key to deriving real benefit from it.

Critically though, such tools should not be viewed as a means to 'automate' third party anti-bribery risk management. The effective management of such risk will always require the expertise of individuals in the business making informed decisions about the risk that exists in the relationship and the best way to manage it.



1 Identify who are your third parties

- Collating and recording a global list of third parties
- Identifying and eradicating duplicate records and risk assessments
- Maintaining individual records for each third party with basic information
- Interfacing and potentially integrating with procurement and finance systems e.g. SAP to create and maintain a global list of third parties

2 Assess what risk they expose you to

- Generating a consistent advisory initial risk assessment for each third party based on basic information
- Maintaining a record of that assessment and the initial risk classification for each third party
- Advising which third parties should be subject to further risk assessment
- Allowing third parties to provide information directly into the tool
- Automatically searching database information on third parties e.g. media, convictions, government links
- Automating workflows and recording ownership, approvals and submissions

3 Manage that risk

- Providing access to all risk assessment information by relevant teams
- Recording the 'status' of a third party e.g. approved to work with, approved with conditions
- Providing an advisory list of potential actions to mitigate any identified risk
- Recording an action plan with owners and timelines
- Allowing oversight of third party risk assessments and activity by market/region/global

4 Monitor for changes and reassess

- Establishing automatic trigger dates for renewal and re-assessment of third party information
- Undertaking ongoing automatic screening of third parties against databases and generating alerts for changed information or red flags
- Allowing modification of risk assessment parameters based on review of results e.g. too high a sensitivity of a parameter resulting in large numbers of third parties classified as high risk

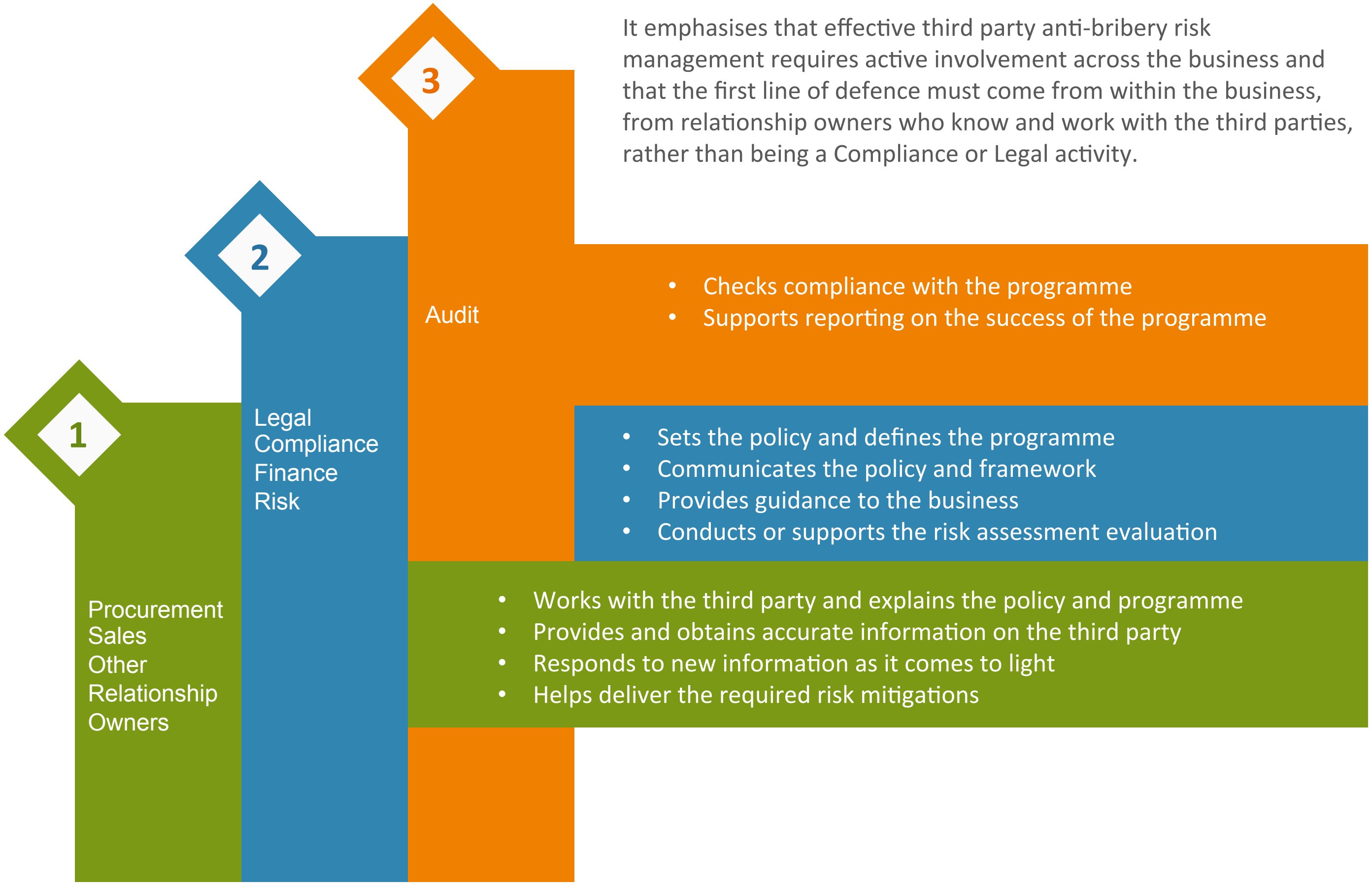
5 Report on what you do

- Automating reports on third party numbers, risk classifications, third party status, mitigating actions
- Allowing 'drill-down' by organisation area, third party type or individual third party
- Supporting internal and external formal reporting requirements
- Facilitating adherence to records retention schedules

Roles & responsibilities – three lines of defence model

The 'three lines of defence' model has been used extensively in the risk management arena and is a helpful model when applied to third party anti-bribery and corruption risk management and in determining where responsibilities should lie.

It emphasises that effective third party anti-bribery risk management requires active involvement across the business and that the first line of defence must come from within the business, from relationship owners who know and work with the third parties, rather than being a Compliance or Legal activity.



3

Audit

- Checks compliance with the programme
- Supports reporting on the success of the programme

2

Legal
Compliance
Finance
Risk

- Sets the policy and defines the programme
- Communicates the policy and framework
- Provides guidance to the business
- Conducts or supports the risk assessment evaluation

1

Procurement
Sales
Other
Relationship
Owners

- Works with the third party and explains the policy and programme
- Provides and obtains accurate information on the third party
- Responds to new information as it comes to light
- Helps deliver the required risk mitigations

Third party anti-bribery programme health-check

We have identified a number of characteristics which a successful third party anti-bribery risk management programme should display.

Members may wish to use the list below as a simple 'health-check' in order to identify potential areas for enhancement of their programme which will then allow focused action to be taken.

Programme characteristics

❑ Leadership support for the programme
❑ Business understanding of the need for and objectives of the programme
❑ Engagement with third parties on the programme
❑ Clear accountabilities for all programme elements and process steps
❑ Defined anti-bribery policy
❑ Clearly mapped process steps
❑ Universal application across the business
❑ Consistency in risk assessment evaluation
❑ Subject matter experts providing guidance to the business
❑ Training and communications for those involved
❑ Practical tools
❑ Consolidated data on the programme
❑ Regular reporting to the Board
❑ Reporting externally

In addition, below are some recommendations on implementing the programme:

Implementation characteristics

❑ A preferred global process and mandatory minimum requirements
❑ Flexibility in implementation model in market/function but with clear governance for exceptions
❑ Strong global oversight and assurance in place
❑ Periodic evaluation of the programme to ensure it meets the requirements and brings business benefit
❑ Integration with other third party risk related activity e.g. money laundering, sanctions, human rights, health & safety

References

… helpful documents reviewed and sources of further information

Selected references

A large number of guidance documents on third party risk management and anti-bribery programmes were reviewed during the development of the protocol. Listed below are those which we found most helpful.

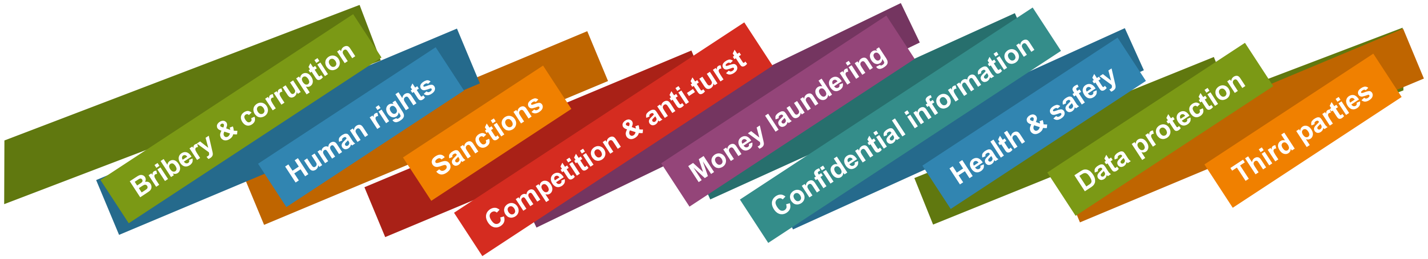
Name	Organisation
Anti-Bribery and Corruption Guidance	British Banking Association
Third Party Governance & Risk Management - Turning risk into opportunity	Deloitte
Implementing effective third-party frameworks in the life sciences industry — leading practices and challenges	EY
Anti-corruption Third Party Due Diligence: A Guide for Small and Medium Size Enterprises	International Chamber of Commerce
Integrated 3rd Party Management	OCEG
2016 Anti-Bribery and Corruption Benchmarking Report	Kroll/Ethisphere
Implementing a consistent and efficient third party due diligence process	Lexis Nexis
Managing Third Party Risk in a Changing Regulatory Environment	McKinsey & Company
2015 Ethics & Compliance Third Party Risk Management Benchmark Report	Navex Global
Third Party Anti-Corruption Management	OCEG
A Strong Compliance Culture Starts with Managing Third Party Corruption	Protiviti
Managing Third Party Risk: Only as strong as your weakest link	Transparency International/PwC
Third-Party Anti-Bribery Framework - Checklists	Transparency International
Third Party Anti-Bribery Framework – Charts	Transparency International
A Guide for Anti-Corruption Risk Assessment	United Nations Global Compact
Good Practice Guidelines on Conducting Third-Party Due Diligence	World Economic Forum

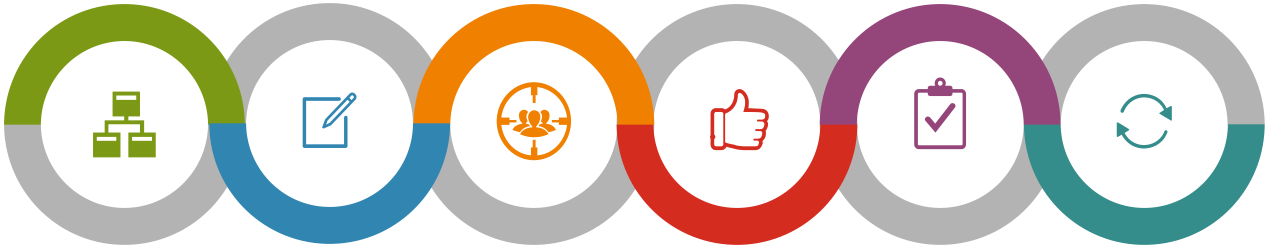
Consulting Ethic

... what we do and how we can support you

What we do

From reviewing and assessing what your organisation needs or evaluating what currently exists, through designing and building the required elements, to operating and ensuring the sustainability of the compliance programme, our goal is to reduce compliance and ethical risk. We may look at a programme in its entirety, or focus on a single element such as third party risk management or a specific event, such as a merger or acquisition. In all cases our approach is one of practicality and proportionality.





Lead & organise

Work with leadership to set objectives, create the required organisation, and develop capability in specialist functions and the business

Define & document

Create clear, accessible codes and policies, and implement supporting processes, systems, and associated governance

Engage & embed

Develop and deliver engaging, targeted training and communciations for Board level, employees and third parties, and generate a compliance culture

Motivate & censure

Design and implement incentives and enforcement approaches to generate compliant and ethical behaviours and create consistency across operations

Monitor & report

Create reporting mechanisms, undertake risk assessments, monitor compliance and report to internal and external stakeholders

Respond & improve

Establish procedures to manage responses to breaches, undertake reviews and investigations, implement continuous improvement initiatives

Disclaimer

The information in this protocol is intended for general guidance only. Recommendations and best practice guidance reflect Consulting Ethic's opinion. It does not consider the specific requirements of any individual AIM-PROGRESS member company and should not be used as a substitute for consultation with professional advisors.

Consulting Ethic LLP shall not be responsible for any loss sustained by any person acting or refraining from action as a result of any material in this publication.