

Antitrust Compliance Toolkit

Second edition

ICC (2024) Antitrust Compliance Toolkit | Second edition

Copyright © 2024 International Chamber of Commerce

© 2024, International Chamber of Commerce (ICC)

The text below is a collective work, initiated and drafted under the authority and control of ICC, and to which ICC holds all rights.

Participation in the development of this text will not give rise to any rights for contributors in this collective work, of which ICC is sole copyright holder.

This shall not affect pre-existing rights in extracts from third party texts included in this Toolkit which shall remain vested in the copyright holder of those texts.

Express written permission must be obtained for any modification, adaptation or translation, for any commercial use, and for use in any manner that implies that another organisation or person is the source of, or is associated with, the work.

The work may not be reproduced or made available on websites except through a link to the relevant ICC web page (not to the document itself).

Permission can be requested from ICC through ipmanagement@iccwbo.org

ICC Publication No. 450/1081-12E
ISBN: 978-92-842-0698-8

2go.iccwbo.org

In memoriam

The International Chamber of Commerce (ICC) dedicates the second edition of its Antitrust Compliance Toolkit (Toolkit) to Anne Riley in tribute to her exceptional leadership in the field of antitrust compliance and advocacy.

A trusted colleague and friend to many of the contributors to this publication, Anne played a pivotal role in the elaboration of the first edition of the Toolkit in 2013 and its SME version in 2015.

Her insights and deep expertise are reflected throughout this updated Toolkit—reflecting the unique vision and passion she brought to this field. She was so passionate that she did not hesitate to challenge herself the approach taken in the 2013 version of the Toolkit, with a view to adapt the new edition to the evolution of antitrust compliance in the last decade.

Anne will be deeply missed throughout the antitrust community, but her legacy as a thought leader and innovator will most certainly endure.

Foreword

by Olivier Guersent, Director General for Competition of the European Commission

In today's world, businesses operate in a complex and rapidly changing landscape where there is an increased need to be aware of the dividing line between legitimate commercial behaviour and illegal anti-competitive practices. With authorities around the world engaging in strong enforcement against such illegal practices, compliance with competition law is now of paramount importance.

But compliance is not simply a legal requirement, rather it is a business necessity, which brings many benefits to companies. It serves to avoid the imposition of potentially large fines from public authorities and damages actions from private victims. It allows businesses to uncover illegal cartel behaviour that can be reported to authorities under leniency programmes, which give immunity from fines or a reduction in the amount of fines. It also preserves the reputation of companies, which can be severely damaged if found to have committed antitrust violations.

It is therefore important for businesses to have access to documentation that will allow them to comply with the competition rules and take advantage of the benefits that compliance can bring. In this context the International Chamber of Commerce's (ICC) revised Antitrust Compliance Toolkit is most welcomed.

The revised Toolkit builds on its predecessor and provides practical guidance on how companies can build an effective compliance programme. Although, there can be no 'one size fits all' compliance programme, the Toolkit clearly sets out the core elements of compliance on the basis of which companies can construct programmes tailored to their individual needs. Furthermore, the fact that this edition is more concise than its predecessor only serves to enhance its accessibility and user-friendliness.

I can only commend ICC for this latest compliance initiative, which follows many years of fruitful cooperation with DG Competition on compliance and other competition issues. We share the same goal of supporting compliance, which brings benefits to companies, regulators and society as a whole.

Contents

In memoriam	2
Foreword by Olivier Guersent, Director General for Competition of the European Commission	3
Introduction	6
1. Compliance embedded as company culture and policy	7
a. Recognising antitrust as a risk that your company needs to address	7
b. Obtaining management commitment	7
c. Code of Conduct and/or Statement of Business Principles	8
d. Integrate your antitrust programme into your other programmes and controls	9
e. Ongoing and sustained senior management commitment	9
2. Compliance organisation and resources	10
a. Compliance leadership and organisation	10
b. Regular reporting to the Board and other senior management	10
c. Adequate resourcing	11
3. Risk identification and assessment	12
a. Understanding the company's overall approach to risk management	12
b. Introducing or improving control points	13
c. Effectiveness of control points	14
4. Antitrust compliance know-how	15
a. Antitrust know-how: manuals, handbooks, guides	15
b. Antitrust training	15
c. Find ways to stimulate positive employee engagement	17
d. Information about antitrust investigations	18
5. Antitrust concerns-handling systems	19
a. Different kinds of internal reporting systems	19
b. Communicate, educate and create a culture of speaking up	20
c. Non-retaliation and confidentiality	20
d. The company's prompt and fair response to a concern	21
6. Handling of internal investigations	22
a. Types of internal investigations	22
b. Things to consider/practical tools and tips	23
7. Disciplinary action	27
a. General requirements for disciplinary proceedings	27
b. Possible disciplinary measures	28
c. Potential aggravating and mitigating factors	28
d. Specific considerations in antitrust cases	29

8. Antitrust due diligence	31
a. Due diligence in hiring new employees	31
b. Due diligence in assessing substantive compliance	31
c. Antitrust assessments (audits) or selective deep dives	32
d. Due diligence in relation to trade associations	32
e. Due diligence in M&A situations	33
9. Compliance incentives	35
a. Why have compliance incentives?	35
b. Types of incentives	35
10. Monitoring and continuous improvement	37
a. Monitoring and assessing processes and controls	37
b. Measuring effectiveness of processes and controls	38
c. Auditing and benchmarking	38
d. Monitoring and assessing substantive compliance	39
e. Compliance programme improvement plan	39
Acknowledgements	40



Introduction

The **ICC Antitrust¹ Compliance Toolkit** (Toolkit) was first published in 2013. The 2024 update is intended to recognise and reflect changes that have taken place over the last decade in antitrust compliance programmes, the developing views of antitrust agencies, as well as developments in areas of antitrust risk. The toolkit provides **practical tools for companies²** wishing to build a **robust antitrust compliance programme**.

There are **many possible triggers** for your decision to develop an antitrust compliance programme:

- Unexpected antitrust investigations by antitrust agencies may spur your company into rolling out a dedicated new programme as a matter of urgency;
- Your business leaders may operate successfully based on awareness that all antitrust risks must be assessed and managed effectively—and actively sponsor and support a coherent ongoing strategy to develop risk management capability;
- Your antitrust compliance focus may be driven by informed parts of the company, such as your Legal, Audit, or Finance teams, or by new recruits.

Processes and systems alone will not manage risks, **individuals** (and especially management) will. Hence the need for structured antitrust compliance processes to give your business the skills it needs to develop a **common position** and secure **consistent ongoing commitment from employees and management**.

A **comprehensive antitrust risk assessment** will help clarify what sort of **substantive know-how** needs to be disseminated internally and how best to present.

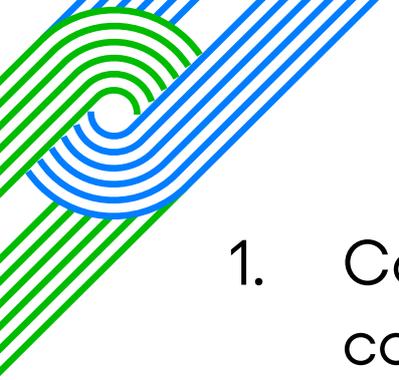
In addition, you will need an **antitrust concerns-handling systems** (*i.e.* the means to **investigate issues internally** and, where necessary, take **disciplinary action** and impose **disciplinary measures** on individuals who fail to live up to corporate expectations). This should include day-to-day **due diligence and compliance assurance**, due diligence in respect of trade associations, and due diligence in an M&A context.

The enduring nature of a compliance culture may also depend on the extent to which a company builds **screening mechanisms** and **compliance incentives** into its programme as well.

Finally, a commitment to **ongoing monitoring and continuous improvement** is an essential feature of any good antitrust compliance programme.

1 In this document, the term “antitrust” is used for the laws (in all jurisdictions) relating to the control of anti-competitive agreements and practices, whether these are known in some countries as “competition” laws or as “trade practices” law. Where relevant this term also includes the antitrust compliance elements relating to M&A transactions.

2 The term “company” is used in this document to mean any entity engaged in any commercial activity—ranging from multinational companies through to small and medium-sized enterprises (SMEs). The use of the word “company” does not suggest any particular corporate structure, and this document is intended for all types of entity, whether incorporated, unincorporated, partnership or consortium.



1. Compliance embedded as company culture and policy

The key to any successful antitrust compliance programme is to reach the stage where the behaviour required under the programme is an **indistinguishable part of your company culture**³.

However, creating a culture of compliance and integrity is not something which can be achieved through a single training session or e-mail message from your CEO.⁴ Your antitrust compliance programme must be designed to **foster a continuous ethical culture** of antitrust integrity that promotes free and fair competition and compliance with the law.

The ethical element of antitrust compliance can be understood as a “positive” business culture or philosophy that fosters **consensus on the need to “do the right thing”**, as well as stressing that knowing and adhering to antitrust laws creates important opportunities for your company.

Your company’s challenge is to ensure that applicable antitrust rules are both **understood and upheld** by management and employees, to avoid unnecessary and inappropriate risks.

The leadership of your company has an essential role to play in persuading all employees to behave pro-competitively in all their commercial and other external engagements. **Actions speak louder than words.** Where the culture and **tone at the top** are clear and successfully embedded, employees will generally comply because they believe that this is the right thing to do.

a. Recognising antitrust as a risk that your company needs to address

The **first practical step** is to ensure that your company recognises that antitrust law compliance is relevant to its operations. Most major companies have a Legal function which should identify antitrust compliance as something the company needs to address. If there is no Legal function, you should have a Finance manager or similar company officer who can raise these points.

Once the risk has been recognised, someone in your company needs to **take ownership of the compliance effort.**

In terms of dealing with antitrust risks, the difference between a corporation thriving and facing potentially significant issues hinges on a well-designed compliance programme.

b. Obtaining management commitment

Another essential practical step in building a compliance culture is to get buy-in and **commitment from your senior management** (including Board level commitment), as the culture of your company is almost inevitably driven by senior management.

3 DOJ, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, July 2019 (see: <https://www.justice.gov/atr/page/file/1182001/download>) ; DOJ, Monaco memo: “Further Revisions To Corporate Criminal Enforcement Policies”, September 2022 (see: https://www.justice.gov/d9/pages/attachments/2022/09/15/2022.09.15_ccag_memo.pdf) ; Canadian Competition Bureau, “*Build a credible and effective compliance program for your business*”, 2023 (see: <https://competition-bureau.canada.ca/how-we-foster-competition/compliance-and-enforcement/compliance-hub>).

4 The term CEO is used to mean the company’s Chief Executive Officer or similar most senior corporate officer.

Successful compliance programmes are also **critically dependent upon the engagement and support** of employees and management at all levels of your company. Simply rolling out a training programme will never lead to full or sustainable compliance. That being said, successful compliance programmes will inevitably assist the company as it will help to identify behaviours that infringe antitrust law⁵. In addition, depending on your jurisdiction, competition authorities may reward compliance programmes, for instance, through reduction of fines subject to certain conditions⁶.

The **means of drawing management’s attention to antitrust as a significant business risk** and securing their commitment to compliance will differ from company to company, but might include:

- Using examples from the press/media on damage to companies’ reputations (including—for public companies—the negative effect on share price) from non-compliance (antitrust violations or other compliance topics such as anti-bribery and corruption);
- Using statistics about antitrust violations (fines, personal penalties);
- Learning from experience of compliance issues—whether relating to antitrust or not (including the value of detecting these early);
- Setting out a realistic plan for management of the steps required to roll out a credible antitrust compliance programme, and the necessary resources⁷, including timing for the introduction of controls and the required budget⁸.

c. Code of Conduct and/or Statement of Business Principles

There has been a **dramatic increase in the ethical expectations of businesses and professions** over recent years. This has led many companies—both SMEs and larger businesses—to adopt a Code of Conduct/Statement of Core Values/Statement of Business Principles.

A Code of Conduct (or similar document) is intended to be a **central guide and reference for all individuals** in your company in support of day-to-day decision making. A Code is an open and public disclosure of the way your company intends to operate. A Code is also a tool to encourage discussions of ethics and compliance, and to improve how your company’s employees deal with ethical dilemmas and grey areas that are encountered in everyday work. A Code of Conduct or Compliance Manual is, however, insufficient on its own to demonstrate that the company has a commitment to compliance (and may even be counter-productive if

5 French Competition Authority, Framework document of 23 May 2022 on competition compliance programmes (see: https://www.autoritedelaconurrence.fr/sites/default/files/2022-06/Conformite_nouveau%20doc-cadre_VEN.pdf) Guidance on Competition Compliance Programs in Canada (see: <https://competition-bureau.canada.ca/how-we-foster-competition/compliance-and-enforcement/specific-areas-enforcement-bureau>) Department of Justice in the USA, Corporate Compliance Programme (see: <https://www.justice.gov/atr/page/file/1182001/dl>). The 10th amendment to the German Act against Restraints of Competition enables the German Federal Cartel Office to take compliance programmes into account.

6 OECD Policy Document DAF/COMP/WP3/M(2021), *Summary of the Discussion on Competition Compliance Programmes*, 2021, at page 3 (see: [https://one.oecd.org/document/DAF/COMP/WP3/M\(2021\)1/ANN1/FINAL/en/pdf](https://one.oecd.org/document/DAF/COMP/WP3/M(2021)1/ANN1/FINAL/en/pdf)) and also European Commission, DG COMP, *Compliance matters*, 2012, at page 9 and 10 (see: <https://op.europa.eu/en/publication-detail/-/publication/78f46c48-e03e-4c36-bbbe-aa08c2514d7a/language-en>)

7 Chapter 2: Compliance organisation and resources; DOJ, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, July 2019 at page 2 and 3 (see: <https://www.justice.gov/atr/page/file/1182001/download>); Canadian Competition Bureau, “[Build a credible and effective compliance program for your business](#)”, see at: “[Core principles to develop a credible and effective compliance program](#)”, 2023 (see: <https://competition-bureau.canada.ca/how-we-foster-competition/compliance-and-enforcement/compliance-hub>).

8 DOJ, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, July 2019 at page 2 and 3 (see: <https://www.justice.gov/atr/page/file/1182001/download>); Canadian Competition Bureau, “[Build a credible and effective compliance program for your business](#)”, see at: “[Core principles to develop a credible and effective compliance program](#)”, 2023 (see: <https://competition-bureau.canada.ca/how-we-foster-competition/compliance-and-enforcement/compliance-hub>).

the company does “live up” to its values)—the further steps articulated in this Toolkit should also be considered.

d. Integrate your antitrust programme into your other programmes and controls

Your antitrust compliance programme should not be developed in isolation from other compliance risks. From the start, therefore, it is important that you give some thought to how you might **link** your antitrust compliance programme to your company’s other compliance programmes (for example the anti-bribery and corruption and data privacy programmes etc.) and into your company’s risk, controls and governance systems.

A holistic approach to compliance is important and is more effective:

- All companies from SMEs to the very largest will have a Finance function/Finance manager or Financial advisor who will consider all the material risks that the company faces. If antitrust features are in your central list of corporate risks, it becomes easier for appropriate controls to be rolled out consistently across your company;
- This approach would involve the application of a consistent risk assessment methodology that recognises the negative potential impact of antitrust issues (notably the occurrence of cartels) with a view to mitigate such risks.

It is **essential that the antitrust programme and those supporting it get sufficient dedicated resources**⁹.

e. Ongoing and sustained senior management commitment

Senior management support for your antitrust programme **needs to be sustained** on an ongoing basis. “Tone from the top” should be clearly demonstrated not just by initial management commitment and by issuing a company Code of Conduct, but also by senior leaders and managers

Effective compliance starts with leadership. By actively highlighting the importance of compliance training and personally endorsing it, senior management can create a culture of awareness and empower employees to make ethical decisions. This ongoing focus ensures the organisation operates within legal boundaries and avoids unnecessary risks.

Statements **from senior managers** proactively reaffirming their own commitment to antitrust compliance can have a more profound and enduring impact than any written document. Promoting leaders who have a track record of showing a similar commitment to compliance helps to set up a strong competition culture in companies, which is positively considered by competition authorities¹⁰.

To avoid the impression that antitrust compliance is only communicated by your CEO and the Board and not seen to be embraced by your whole company, you could arrange for regular e-mail and other direct communication by other senior and lower level managers to their teams, underlining the importance of antitrust compliance, referring to the compliance policy and expectations and indicating what individuals should do if they have any compliance concerns.

⁹ DOJ, Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations, July 2019 at page 2 and 3 (see: <https://www.justice.gov/atr/page/file/1182001/download>); Canadian Competition Bureau, “Build a credible and effective compliance program for your business”, see at: “Core principles to develop a credible and effective compliance program”, 2023 (see: <https://competition-bureau.canada.ca/how-we-foster-competition/compliance-and-enforcement/compliance-hub>); French Competition Authority, Framework document of 23 May 2022 on competition compliance programmes at page 6 (see https://www.autoritedelaconurrence.fr/sites/default/files/2022-06/Conformite_nouveau%20doc-cadre_VEN.pdf)

¹⁰ Chapter 9: Compliance incentives



2. Compliance organisation and resources

While the organisation and resourcing of an antitrust compliance programme will differ from company to company, every company should have a clear internal reporting structure with regards to antitrust compliance.

The following key elements should be covered:

a. Compliance leadership and organisation

Although **senior management in the company must be accountable** for promoting a sustainable compliance culture, the day-to-day implementation of an effective and credible programme may be delegated to a **designated senior person**. Whether a **dedicated compliance team** is required will depend on the size, scale, and the nature of your business, including the risks your company faces.

Antitrust agency guidelines have made it very clear that a **senior** individual either on or **reporting to the company Board/management committee** should be responsible for your company's compliance programme (including the antitrust programme). It could be the **General Counsel/Chief Legal Officer** or even the Chief Compliance Officer/Chief Ethics and Compliance Officer (CECO).

It will be essential that this individual has **direct access** not only to the Board/Executive management committee, but also to other relevant internal committees such as the Audit Committee and Corporate/Social Responsibility (or ESG) Committee.

Large companies are likely to have one or more in-house lawyers, and it would be sensible to recruit **dedicated antitrust counsel** to contribute key substantive knowledge. In companies that have an in-house antitrust lawyer, that lawyer would normally regularly **report to board level**.

Larger companies typically need to decide whether to opt for **centralised or country/regional compliance structures**, taking into account the overall business and organisational structure of the company. The **pros and cons** of each option very much depend on the general structure of the company. Very large companies with multiple business lines may even appoint a number of Business Compliance Officers (by business line or by country/region), to track compliance metrics (training completion numbers, incident reporting, investigation management etc.) within the business line.

b. Regular reporting to the Board and other senior management

Senior management engagement depends on **management following and understanding** how a compliance programme (including antitrust) is being implemented, which in turn requires **regular reporting opportunities**. In many companies with well-developed compliance programmes, **an annual report** on all compliance programmes (including antitrust) (highlighting past deliverables, potential future issues (such as algorithmic and AI collusion) and further plans) is often presented to the Board, non-executive directors, and to the Audit committee (and/or Group Risk committee).

In addition, to ensure that your company's Board (or other responsible body) is appropriately informed of—and can react to—all relevant antitrust law risks, **regular updates** must be made to the CEO, business leadership teams and other key stakeholders at all levels of the management chain. Particularly if companies are publicly listed, this may take place on a **quarterly basis** (in accordance with other quarterly reporting requirements), but there should also be a **process that allows for urgent reporting of developments** that create additional material risk for the company, as well as regular dialogue on compliance with management teams.

c. Adequate resourcing

The resources dedicated to the antitrust compliance programme will clearly depend both on the size of your company and the risks your company faces. SMEs do not have the same resources as larger companies. **Even within very large companies, resources are constrained** with significant competing demands, both from other high-profile risk and related compliance areas such as anti-bribery and corruption and Data Protection. Where senior executives see a tangible benefit in dedicating merely “adequate” resources to a given area because having done so in other compliance areas can—in some jurisdictions—provide a **complete defence to the company**.¹¹

If your company does not have a specialist in-house antitrust lawyer, the larger and medium-sized **private practice law firms** now have specialist antitrust departments that your company could turn to for advice in establishing its compliance programme.

Funding antitrust compliance must not be viewed as a “sunk cost” as antitrust fines imposed by competition authorities can now reach millions or even billions of euros, for example in the case of repeated infringements. In addition, many antitrust proceedings are now followed by private enforcement actions seeking damages to compensate for individual harm caused by antitrust violations.

In this respect, the proper implementation of an antitrust compliance programme can even lead to lower fines and damages in the event of a violation.¹² Robust compliance measures can also prevent the damage to a company's reputation caused by antitrust enforcement, including—for listed companies—the negative impact on the share price. Finally, funding antitrust compliance **must** not be seen as a sunk cost because that more and more national regimes provide for a criminal liability of the managers and employees involved in antitrust violations.¹³

11 See the “Adequate Procedures” defence in Section 7 of the UK Bribery Act, and guidance on what constitutes “Adequate Procedures” issued by the UK Ministry of Justice *Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing* available at <https://www.gov.uk/government/publications/bribery-act-2010-guidance> and the US DOJ's Guidelines on FCPA compliance: *A Resource Guide to the U.S. Foreign Corrupt Practices Act* available at <https://www.justice.gov/criminal/criminal-fraud/file/1292051/dl?inline>. <https://www.justice.gov/criminal/criminal-fraud/fcpa-resource-guide> and <https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf>

12 As provided by the German Act against Restraints of Competition (“ARC”), see § 81d para. 1 no. 5 ARC. For example, jurisdictions that offer fine reductions as well are Czech Republic (see: “*Notice of the office for the protection of competition on compliance programmes dated 1/1/2024*”), Canada (see: “*Build a credible and effective compliance program for your business*”), Australia (see: “*Guidelines on ACCC approach to penalties in competition and consumer law matters*”), Spain (“*Antitrust Compliance Programmes Guidelines*”), United States (see: « [Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations](#) »), Italy (see: « [Guidelines on Antitrust Compliance](#) »), Brazil (see: « [Guidelines on Competition Compliance](#) »), Singapore (see: « [CCCS Guidelines on the appropriate amount of penalty in competition cases](#) »).

13 For example, jurisdictions whose laws provide for substantial fines and/or imprisonment against individuals include Australia, Brazil, Canada, Greece, Ireland, Israel, Japan, Mexico, South Africa and the United States.



3. Risk identification and assessment

The **effectiveness** of your company's antitrust compliance programme and related allocation of resources will depend on whether **resources are deployed in the right areas**. Understanding the business and **operational risks** your company faces will not only help focus on relevant activities.

To give a couple of simple examples, it may not be relevant to raise awareness of the dangers of bid-rigging within businesses that do not operate in a procurement/tender context. Similarly, it may not be an efficient use of resources to train employees about the risks of abuse of dominance/market power if the company operates in very highly fragmented markets where players all have low market shares.

Companies should therefore **define a risk assessment methodology and process**¹⁴, so they can tailor their compliance programme to their specific risk profile. According to antitrust agencies a **credible compliance programme** depends, ultimately, on being able to justify the rationale for your company's chosen approach to risk management, considering risk, likelihood and impact of behaviour infringing antitrust laws.

a. Understanding the company's overall approach to risk management

There is significant merit in aligning your company's overall approach to (and methodology for) risk management and the risk assessment approach your company decides to use as part of an antitrust compliance programme. In undertaking a risk assessment, it is useful to involve your Finance function (e.g. Group Controllers, Risk and Assurance or the Audit function) and (if at all possible) a specialist antitrust lawyer.

Finding a meaningful way of **taking account of the "human factor"** in compliance can be challenging; it may be worth considering what indicators to estimate compliance maturity such as the proportion of employees who complete training when first requested and the "employee turnover" rate within your company.

The validity of taking a risk-based approach in establishing internal compliance standards and procedures for antitrust compliance is acknowledged by a number of agencies.¹⁵ However, your company may legitimately approach antitrust compliance by managing antitrust risks as these are likely to occur in the real world.

Typical antitrust risks which are important to consider include:

- Anti-competitive agreements such as potential cartel activity between competitors, including price-fixing, market sharing, bid-rigging, collective boycotts and production limitation agreements;
- Exchanges of commercially/competitively sensitive information that could potentially result in cartel activity which may be seen as the biggest risk of illegal cartel activity, even unintentionally;
- Resale price maintenance in jurisdictions where this is prohibited;

¹⁴ See e.g. "Build a credible and effective compliance program for your business" published by Canada Competition Bureau, Section *Core principles of a credible and effective compliance program* ([canada.ca](https://www.competitionbureau.ca/en/your-business/build-a-credible-and-effective-compliance-program)).

¹⁵ See e.g., U.S. DoJ, [Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations](#), 2019; [CMA, Guidance Competition law risk: a short guide](#), 2020; EC, [Compliance matters, What companies can do better to respect EU competition rules 2012](#); Competition Bureau Canada, "Build a credible and effective compliance program for your business" 2024.

- Exclusionary conduct by companies with significant market power (e.g. abuses of a dominant position and other prohibited unilateral conduct);
- Emerging risks such as cooperation in the fields of artificial intelligence (AI) and sustainability cooperation, human resources related agreements such as discussions on wages and “no poaching” agreements with other companies. Human Resources activities are very often underestimated as an antitrust risk by business, because those activities are often not viewed as “commercial”, but they are becoming an increased focus of antitrust agencies globally.

A meaningful corporate commitment to antitrust compliance must include a clear ban on manifestly illegal conduct (such as price fixing and market sharing). The “likelihood” of enforcement action should never be viewed as a relevant factor in determining risk.

Assessing the likelihood of any of the above activities or risks can be challenging. So, it will be important for you to involve risk assessment as well as antitrust experts in the risk management process. Relevant considerations might include:

- The relevant antitrust laws wherever your company operates;
- Focus of competition agencies and regulations on certain types of conduct or industries, e.g. due to a history of collusion in the industry;
- Past antitrust compliance of the company, skill level and industry standards;
- Sensitive markets that may be higher risk due to concentration levels as opposed to fragmented markets;
- Expansion strategies of the company, such as moving into new business areas, aggressive pricing or expanding the geographic scope of the business;
- Staff turnover or recruitment from competing businesses;
- Interactions with competitors (such as at trade associations, industry events or through joint ventures);

The impact and assessment of relevant risks must include negative reputational impact, corporate fines, damages claims, resources bound due to antitrust investigations, legal fees, nullity of anti-competitive clauses or agreements, and personal sanctions for managers and employees.

b. Introducing or improving control points

Internal controls are processes designed to provide **reasonable assurance** for risk mitigation and compliance with applicable antitrust laws. They involve **ongoing tasks and activities (controls)**, implemented by a company’s employees at various levels and designed meaningfully to reduce the likelihood of problematic conduct, but are unlikely to eliminate risks completely.

In this view, employees should be exposed to a combination of compliance handbooks, training courses, awareness actions for top management and employees, business alerts, internal checks or registers and other business partnering activities of consultancy in direct contact with the business.

For example, if your company wishes to introduce **controls specifically designed** to address risks associated with **taking part in industry events** (such as trade associations, industry conferences and other events), these may involve:

- Guidance materials in the form of antitrust policies, standards, training leaflets or e-learning;
- Specific procedures and controls such as requirements to secure prior line manager approval (and perhaps even to register attendance in an internal database);
- Record-keeping duties around meetings (for example, keeping records of agendas and minutes, if relevant).

c. Effectiveness of control points

A robust antitrust compliance programme that successfully embeds a strong company culture to “do the right thing” should significantly reduce or mitigate antitrust risks through:

- Raised awareness of unlawful antitrust behaviour;
- Early detection and resolution of antitrust issues;
- Potentially lower fines and reduced adverse reputational impact (bad publicity and negative effect on share price / loss of investor confidence) in the event of non-compliance;
- Increased opportunities to benefit from antitrust (agency) leniency programmes; and
- The ability to recruit and retain talented staff that want to work for an ethical company.

To measure this and take stock of potential risk, you can consider the following:

- Does an appropriate control exist? (this could include a Code of Conduct, messages from management, a properly executed and documented training plan etc);
- How is the control articulated (is it clear and unambiguous)?
- Is control documentation readily available and regularly updated?
- How are individuals made aware of the control?
- What is the “hit rate” (for example the percentage of target audience successfully trained)? It should also track those not trained and find out why not.
- What structure exists to track awareness and compliance with control? (For example, many larger companies now run regular tests or “quizzes” for employees—these can be made “fun” by awarding minor prizes (a bar of chocolate or modest bonus) to those who demonstrate the best understanding of the programme and requirements of antitrust law)
- What sanctions exist for failure to operate the control?



4. Antitrust compliance know-how

The next step after identifying the antitrust risks and their geographic spread is to determine the required antitrust training and supporting documentation to increase employee awareness and minimise the risk of antitrust violations.

Even with excellent antitrust compliance training, some individuals may still ignore company policy. Therefore, antitrust compliance should be a proactive ongoing discussion, and legal advisers should be involved in projects and daily business decisions. In this regard, antitrust compliance should not be viewed as a standalone process or a checkbox exercise.

In larger companies, there is consideration given to training third parties¹⁶ such as joint ventures, distributors, and trade associations, in addition to the company's own employees. This should not, however, evade liability issues, and the company should not neglect to train its own employees in antitrust risk management, not least by providing them with simple guidelines for behaviour (including “Do’s and Don’ts” in industry events or when competitors raise sensitive issues).

a. Antitrust know-how: manuals, handbooks, guides

Whatever the size of your company, it is unreasonable to expect your company's employees to understand what constitutes antitrust-compliant and ethical behaviour if they have not received some guidance or simple, “jargon” free, “Do’s and Don’ts” on antitrust.

Whether through guidance documents provided by in-house lawyers or external law firms, antitrust training materials should be relevant to the company's activities, different business units and specific antitrust risks.

Some **key concepts and issues** that you may wish to consider include:

- Have clear, simple and concise rules—use plain business language, without legalistic jargon or detailed references to laws, and avoid lengthy antitrust guidance notes.
- Tailor guidelines to the needs of different business units and situations, and consider the use of short notes for specific topics or risks;
- Present the guidance in ways that makes sense from a business perspective—confirm what is possible, perhaps where necessary subject to certain limits or thresholds (reflecting “safe harbours”);
- Think about how to achieve maximum reach (method and language of delivery, etc.).

b. Antitrust training

Antitrust training remains a fundamental part of an effective antitrust compliance programme, whether organized by outside counsel or in-house departments.

You should ensure that your company's antitrust training is designed to provide practical (business-specific) examples. It should explain the aims and reasons for your company's antitrust compliance policies and procedures, and the consequences if these are not followed.

¹⁶ See the UK Ministry of Justice guidelines on the Bribery Act referred to at footnote 13 above, in particular principle 5.7 relating to the (possible) need to train “associated persons” about anti-bribery compliance.

Practical considerations you may wish to take into account when setting up antitrust training include:

- **Identifying employees to be trained.** The requirement to be trained, as well as the methods and frequency of antitrust training should be suitable for the antitrust risk profile of the business activities of those employees whose roles are deemed to be higher risk, such as sales personnel or those who attend trade or industry meetings and business networks with competitors (as opposed to those who do **not** have a sales / procurement or management role);

New employees should receive antitrust training as required by their job's risk profile during their induction/on-boarding. The same applies when employees move from a lower risk role to a higher risk role at the company or economic agent;

- Ensuring the **style and content of training** reflects your company's antitrust needs and risk profile. Considering whether your company needs online training, face-to-face (FTF) training, "virtual" training (a mixture of computer-based training and a webcast/ conference call with an antitrust trainer), or a combination:
 - Online and virtual training is useful for global reach and for employees who are remotely located. The COVID-19 pandemic made online training essential. However, online training on its own is probably not adequate for roles that are deemed to be higher risk, as employees in such roles need to be able to ask questions and receive immediate answers. In such cases, you may want to consider a "virtual" antitrust training module, as it combines the reach of online training with the ability to ask questions (such as "Zoom" or "Outlook Meetings" calls or similar platforms).
 - Many off-the-shelf online training products are available from third-party providers, but some may be too generic or legalistic, covering all antitrust issues, whether relevant to the company's business or not. Therefore, some multinational companies have developed their own specific online or virtual computer-based antitrust training.
 - Today, a useful approach to apply is "Gamification", which means using computer based game design and system processes to encourage learning in a user-friendly and pleasant way".¹⁷ This can be used to help employees understand complex antitrust concepts through challenges that simulate real-life situations, including elements like rewards, leaderboards and badges to incentivise employees to complete training and help companies create a compliance culture. It also helps companies approach compliance in a holistic way, since the "game" can include many compliance challenges, including not just antitrust but also ABC, AML (Anti-Money Laundering), Data Protection and so forth.
 - Effective online systems help employees track their performance and provide users with readily available materials that can be consulted when their schedules allow. Online training's flexibility and cost-effectiveness features help companies easily update their materials. The possibility of including a "FAQ" section or a direct communication channel to send a message to an attorney or start a chat online section with an antitrust expert (e.g. through a dedicated App or WhatsApp group) is helpful in creating a sense of familiarity between employees and the antitrust trainer, thus easily triggering recognition for potential issues.

¹⁷ Mario Silic & Paul Benjamin Lowry (2020) Using Design-Science Based Gamification to Improve Organisational Security Training and Compliance, *Journal of Management Information Systems*, 37:1, p. 131.

- **Identifying appropriate trainers** for antitrust training:
 - The trainers selected to conduct your company’s antitrust compliance training must be knowledgeable in antitrust laws. However, if resources are limited, your company may need to consider developing a “train the trainer” course. This is more suitable for larger companies with a legal department, but may not be feasible for SMEs, which may have to rely on external trainers;
 - In larger companies, it may be helpful to provide additional guidance on antitrust to in-house lawyers who are not proficient in this area, as part of an ongoing professional education programme. External counsel can offer antitrust newsletter, publications, dedicated Apps and webinars that provide high-quality updates on recent developments. Suitable conferences are also a useful way of finding out more about topical antitrust issues and trends.
- Deciding on the **size of the group to be trained**, whether FTF or online, is of critical importance. There may be short-term cost savings in “training” a large group in a lecture-style format. However, this may be less effective in getting employee engagement since large groups are less likely to be interactive and lively.
- Incorporating senior management or team leaders into antitrust training will help reinforce the importance of the company’s culture of ethics and compliance, which it expects employees to embrace and demonstrate;
- Ensuring **suitable attendance records** are made and retained of at all trainings is important when it comes to measuring the effectiveness of controls and improving the programme (see Chapter 10: Monitoring and continuous improvement).

c. Find ways to stimulate positive employee engagement

To be effective, mechanisms for raising awareness of antitrust compliance guidance should include the following clear and concise **reminders and reference materials** that communicate messages in ways that stimulate employee engagement:

- Wallet cards and /or posters;
- Newsletters and brochures;
- Compliance “games” (as discussed above);
- Intranet and Internet (such as a dedicated antitrust—or at least an ethics and compliance—internal website);
- Promotional giveaways (*i.e.* pens, memo pads, calendars, mugs);
- Frequent encouraging messages from management about the importance of antitrust compliance and the importance of seeking guidance.

To achieve positive employee engagement, an antitrust compliance programme should focus on empowering employees and providing clarity, on what they can do lawfully (the “Do’s”), what they cannot do (the “Don’ts”—and importantly—when to ask for help).

Some companies celebrate “compliance heroes” (and heroines) as a means of encouraging a positive image for compliance (see Chapter 9: Compliance incentives).

d. Information about antitrust investigations

It is obviously important for your company's employees and management to **understand what happens in an antitrust investigation**, and in particular to understand the duty of cooperation in the event of an inspection and that any form of obstruction during the investigation (whether it involves seal breaking or otherwise) will be treated seriously by the company and may result in disciplinary action. Training employees about what happens in antitrust investigations or "dawn raids" in the event that a real investigation takes place may be useful in certain cases, for example:

- **IT colleagues** are now critical in any antitrust investigation, as much—perhaps most—of the investigation and document searches are conducted digitally using forensic IT tools. It should be clear to everyone that no device, whether professional or personal, no communication platform or messaging application is exempt from the forensic IT tools used by competition authorities in their antitrust investigations.
- For **employees on reception/in security** in your company's facilities, they need to understand how to handle investigators courteously, expeditiously and appropriately, in order to minimise the risk that an antitrust agency alleges obstruction or a failure to cooperate by your company;

Some companies use "mock" dawn raids that mimic surprise inspections, although opinion is divided on the merits and the problems associated with employing "mock" raids.



5. Antitrust concerns-handling systems

When your company has “tone from the top” that **actively** encourages and stimulates employees to behave ethically, your company’s employees will (most likely) be more vigilant and willing to raise concerns when they are uncomfortable about certain forms of conduct. To facilitate this, it is important to have well-publicised mechanisms that allow employees to “speak up”, outside normal reporting lines, and be protected against possible retaliation¹⁸.

Corporate social responsibility, ESG, and business ethics have led to the development of increasingly sophisticated compliance strategies, including the adoption of **internal whistleblower procedures**, reporting channel, “help lines” or hotlines. These mechanisms allow individuals—both inside and outside the company—to report compliance concerns, enabling management and their lawyers to uncover and deal with corporate crimes, antitrust violations, corruption, and other compliance problems. These concerns-handling mechanisms may also serve as a deterrent for employees who may be tempted to circumvent controls and violate your company’s Code of Conduct.

a. Different kinds of internal reporting systems

There are **a variety of internal reporting systems** that you can choose from to enable your company’s employees to raise compliance concerns or report suspected misconduct:

- One approach to raising compliance concerns is the informal “open door” approach, which allows concerns to be raised directly with management at any time. While this approach is simple, it does not provide anonymity and relies on the existence of an environment where employees feel comfortable speaking up. This becomes problematic if the line manager is involved in the allegation the employee wishes to discuss. Even if the Line Manager is not involved, many employees feel embarrassed to be seen “complaining” about another.
- The compliance programme should encourage managers and employees to ask for help. Depending whether you work for a large company or an SME, help and advice could be obtained from in-house Legal, the Compliance Officer or another appropriate function such as Finance, Audit, or HR.
- Companies can also establish a formal whistleblower weblink or telephone line sometimes known as helpline/hotline or Code of conduct reporting line. Whether a formal helpline is necessary depends on the risks the company faces and its size, scope and geographic reach. Many companies operate some form of **internal helpline system** (often in addition to a formal “whistleblower” line) designed to answer employees’ questions about ethics, company policies and compliance matters, providing answers to everyday compliance dilemmas.

Antitrust agencies now encourage individuals to contact them directly when they become aware of problematic conduct, sometimes offering financial rewards. This creates a tension between your company’s internal efforts to prevent and detect non-compliance and the antitrust agencies’ focus on effective deterrence. For this reason also, it is in your company’s interest to foster an environment where concerns are raised internally first, to address them

¹⁸ See, for instance, CMA Guidance on Whistleblowing, 16th July, 2021; Directive (EU) 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law, OJ L 305, 26.11.2019; H.R.2988—Whistleblower Protection Improvement Act of 2021. Georgina Halford-Hall, Chief Executive WhistleblowersUK. “We must normalise speaking up and help those who feel alone and abandoned by society. Whistleblowing is vitally important to keep us all safe”. <https://www.wbuk.org>.

promptly, investigate matters and potentially prepare a corporate leniency application if appropriate.

Implementing a **confidential and anonymous reporting system** is crucial for companies committed to stronger and more effective governance practices.

Workplace whistleblower hotlines/help lines take many forms and is very much dependent on the availability of resources. Some companies run their hotline in-house while others are outsourced. Some combine in-house resourcing (for investigations purposes) and external (independent) management and recording of the complaint to ensure anonymity.

Where genuinely problematic anti-competitive conduct (such as price fixing) is uncovered, it is usually necessary to involve specialist (antitrust) external legal advisors without delay, to assist with follow-on investigations and provide advice on a **legally-privileged** basis, and to determine whether an application for **immunity or leniency** is appropriate (or even possible).

A **hotline/whistleblower line system should evolve to meet new needs** as compliance requirements and companies grow and change (for example, the recent focus on AI and Human Resources issues by agencies has changed the focus of compliance programmes). This may include adding risk categories as new areas of the business emerge, adding locations, business units as your company grows, and providing reports or capturing new data points from individuals reporting compliance concerns as compliance requirements dictate.

b. Communicate, educate and create a culture of speaking up

Whatever the size of your company, it is important to recognise that it is not enough to establish a compliance concerns-handling system and expect employees to start asking questions or making reports. To be effective, employees need to know the hotline/whistleblower line is available and why and when they should use it, and how they will be safeguarded if they use it.

Companies should promote the use of the hotline/whistleblower line through a broad communication and education programme throughout the company—and indeed, for a public company, through its various Disclosures and Reports.

Cultural sensitivities should be considered when implementing a whistleblower line system, as some employees may react negatively to the concept of whistleblowing associating it with spying on colleagues. In some countries, there may also be reticence to report issues using lines associated with head office instead of local operations. It is important to be sensitive of these considerations to avoid an ineffective structure that generates scepticism and acrimony instead of support.

Ultimately, the goal is for all your company's employees to know that they have a way of reporting compliance concerns and are encouraged to speak up in the knowledge that their report will be treated confidentially and that they will not suffer retaliation.

c. Non-retaliation and confidentiality

Maybe even more important than communicating the availability of different concerns-handling systems are measures taken within your company to create a **non-retaliatory work environment** in which employees feel comfortable and are encouraged to raise concerns. A key step in creating this environment is ensuring that your company's compliance concerns-handling system includes appropriate whistleblower protection safeguards. All employees should be in a position to report serious occurrences without fear of retaliation

or of discriminatory or disciplinary action. Therefore, the whistleblower's employment, remuneration and career opportunities should be protected by your company.

You should try to maintain, to the fullest extent possible, the confidentiality of the data revealed through whistleblowing and the identity of the whistleblower, subject to overriding legal requirements necessitating disclosure, and should protect such data with the most appropriate means.

d. The company's prompt and fair response to a concern

A slow or non-existent response to a compliance concern raised by an employee can undermine their trust in your company's compliance concerns-handling system. Therefore, it is crucial that your company provides enough and qualified resources to respond appropriately to concerns raised through the system. Regarding reports about compliance concerns, your antitrust compliance programme should make clear that:

- Managers have an obligation to take seriously any compliance concerns that are raised with them;
- The company will investigate any *bona fide* report or genuine concerns of rules being broken;
- Appropriate action will be taken to prevent similar incidents again (if the rules have been broken);
- The investigation process will be full and fair for everyone involved (see Chapter 6: Handling internal investigations);
- Action will not be taken against anyone before an accusation/concern has been appropriately investigated; and
- Non-retaliation and confidentiality will be guaranteed.

Your company's employees will be interested to know and to have confirmation that your company's compliance concerns-handling system is effective and produces fair results, so you should also consider communicating the effectiveness of your company's chosen approach.



6. Handling of internal investigations

Companies are often challenged by the need to conduct internal compliance investigations to examine allegations of wrongdoing. This applies not only to antitrust but also to other compliance areas.

In order to investigate any allegation of non-compliance (whether the allegation is made externally, internally, through the hotline/whistleblower line or internal helpline), your company's management should consider putting in place an efficient, reliable, and properly-funded process for investigating the allegation and documenting your company's response, including any disciplinary or remediation measures taken.

Your company will want to consider taking “lessons learned” from any reported compliance violations or concerns and the outcome of any resulting investigation, and updating your company's internal controls and your antitrust compliance programme (see Chapter 10: Monitoring and continuous improvement).

Incorporating lessons learned in corporate compliance programmes is a cornerstone of effective communication. By integrating these lessons into presentations, you establish credibility with your audience. This approach transcends the mere recitation of legal statutes or hypothetical case studies. Instead, you convey the tangible consequences of non-compliance through the presentation of real-world scenarios that have directly impacted similar businesses. This fosters a deeper understanding of the practical implications of compliance and its vital role in achieving success.

a. Types of internal investigations

There are many types of internal compliance investigations, some of which may be (and often are) triggered by external events such as an investigation by an external agency. Internal investigations help your company understand what happened and determine appropriate courses of action (and help you update and improve your company's antitrust compliance programme). In many jurisdictions, it is critical to retain outside counsel to assist the company in these internal investigations and to ensure that communications are protected by Legal Professional Privilege.

The **types of internal compliance investigations** that you could consider include:

- *Ad hoc* “screening” using AI (see below for more details);
- In-depth legal assessments (using a combination of internal and external legal resources);
- Internal compliance process audits and substantive forensic compliance investigations¹⁹ to address whistleblower allegations or other compliance concerns or complaints;
- Due diligence investigations to detect inappropriate conduct by officers, directors or employees;²⁰
- Special litigation and other Board committees designed to investigate and address allegations of potential wrongdoing.

¹⁹ Some companies also use “mock” dawn raids that mimic surprise inspections by antitrust agencies, although opinion is divided as to the merits of undertaking such exercises as a means to uncover substantive problems (see Chapters 5: Antitrust concerns-handling systems).

²⁰ See Chapter 8: Antitrust due diligence.

As many laws around the world emphasize, a frank assessment of the scope and nature of the conduct and evaluation of the possible advantages and disadvantages of self-disclosure to relevant Government (or supra-national) agencies of wrongdoing are essential to achieve the best outcome for the company.

b. Things to consider/practical tools and tips

Internal investigations can pose serious risks to companies and your company's employees, damaging your company's reputation, interfering with your company's business operations, and exposing your company to heightened antitrust agency and public scrutiny, as well as to potential criminal, civil and regulatory liability.

The range of considerations that you may wish to bear in mind includes:

- Formulating the best possible defence to accusations of antitrust misconduct;
- Deciding whether and how to disclose (criminal) antitrust conduct voluntarily to relevant antitrust agencies;
- Deciding whether to discipline those responsible in your company;
- Deciding whether to waive or retain any Legal Professional Privilege with respect to antitrust matters under investigation;
- Determining how to conduct interviews of your company's management and employees as well as who to interview;
- Determining how to investigate former employees (if legally and practically possible);
- Determining how to treat whistleblowers (your company should have a clear policy of non-retaliation—see Chapter 5: Antitrust concerns-handling systems) and cooperating witnesses, as well as a process for filing complaints and requesting information anonymously and confidentially;
- Determining which types of complaints and “red flags” require an internal in-depth investigation;
- Determining how to document the internal antitrust investigation;
- Establishing safeguards to ensure privacy, data and employees' rights protection during the internal investigation process;
- Assessing learnings and identifying measures to be implemented to prevent (or at least reduce the chances of) a recurrence.

Overall responsibility for the internal investigation

Generally, if your company has a Chief Ethics and Compliance Officer (CECO), operation of the internal investigation would usually be delegated to that person or to other functions working with the CECO. If your company does not have this capability in-house, you may wish to outsource all or part of the investigation.

Even if you work in a very large company with your own in-house forensic capability, you may still choose to outsource all or part of the internal antitrust investigation, either for Legal Professional Privilege reasons, or to demonstrate the impartiality of the investigatory methods.

However, regardless of the size of your company, it would be common for the CECO (or similar person with overall responsibility for the compliance programme) to retain ultimate supervision and responsibility for internal Code of Conduct/Compliance investigations.

Establishing general investigation principles

It is important—for the sake of transparency—for your company to establish and make available to your company’s employees the principles that your company (and its advisers) will observe when undertaking internal Code of Conduct/Compliance investigations (including into alleged antitrust violations). These principles would commonly include rules on confidentiality, impartiality of investigators, timelines, scope of investigation and protection from retaliation.

Specific antitrust investigation principles²¹

In addition to general investigation principles that could apply to the internal investigation of any potential Code of Conduct/Compliance violation, depending on the risks faced by your company (in particular if your company has had previous antitrust investigations), you may like to consider preparing specific antitrust investigation principles. The purpose of these is to account for the peculiarity of internal antitrust investigations, where one issue that may need to be considered is an application for immunity/leniency.

These antitrust investigation principles could cover an explanation of:

- Who will be on the investigations team (in-house Legal, external counsel, others who may need to be involved);
- The roles of other internal functions which may be involved in the investigation (i.e. internal/external forensic investigators, IT, Audit, HR, External Affairs as applicable);
- Confidentiality and the need for/importance of Legal Professional Privilege (if relevant in the jurisdiction);
- The importance of the preservation of documents and electronic records (as well as the integrity of the chain of evidence);²²
- The point in time when the individuals being investigated are informed about the investigation (a delay in informing employees might be desirable—if legally possible—to avoid the possible risk of destruction of evidence. However, it is also important to avoid employees hearing about the investigation through internal leaks or rumours—see below);
- How (in what manner) interviews will be conducted and who will be present;
- How electronic searches will be conducted, by whom and by what means, including addressing data privacy concerns;
- What is the scope of the investigation (and how it is delimited) and which communication channels will be controlled. Particular attention should be paid to new communication channels, especially through the use of personal devices, communication platforms and messaging applications, including ephemeral messaging applications. WhatsApp communications can typically be controlled whether or not messages are deleted;
- Whether and how AI will be used during the internal investigation (see below for more details);
- The individual’s right to separate counsel (in the event of a potential conflict, and in particular in jurisdictions with individual criminal liability) and your company’s policy on paying legal fees;

²¹ See also Chapter 8: Antitrust due diligence.

²² It may be useful to seek the advice of a litigation expert on the need to issue Document Preservation Notices.

- The next steps in the investigation and (insofar as it is possible to predict) the likely future timeline of the investigation.

Other items to manage during an internal antitrust investigation

- If your company is conducting an internal antitrust investigation, it would be wise to consider (with the assistance of external antitrust counsel as appropriate) your company's approach to applying for immunity/leniency (including liabilities that may arise in relation to follow-on damages claims).
- Equally important will be controlling rumours/leaks within all your company's business teams, in order to ensure that business continues during the internal antitrust investigation without tipping off third parties (the risk is that other parties may apply for immunity/leniency before your company and/or that the antitrust agencies conclude that your company is actively trying to obstruct their investigation).
- All documents obtained during the internal investigation must be appropriately itemised and controlled indicating the provenance of the document, and the identity of the person in the company (or within your external advisers) who has taken and is keeping control of the document(s). These steps are essential to preserve the chain of evidence.
- Depending upon the outcome of the internal investigation, if your company is listed on any Stock Exchange you will need to consider (with your advisers) whether a disclosure will need to be made to any relevant Stock Exchange or to any other relevant body (e.g. US Securities and Exchange Commission). If your company is regulated by any Financial Authority (such as the Financial Conduct Authority in the United Kingdom) your company may have a legal duty to report the outcome of the investigation to the regulator (if the investigation identifies wrongdoing).

Use of AI in internal compliance investigations

With the development of digital technologies and algorithms, direct evidence of practices infringing antitrust laws is increasingly complex to detect, intensifying the need for active in-house screening.

The use of AI in internal compliance investigations forms a complementary tool to support companies in their monitoring, prevention, and detection of anti-competitive practices.

Through screening programmes, AI will allow companies to proactively identify potential violations, which can be particularly interesting in the context of leniency applications.²³

More specifically, the benefits of data-driven compliance include:

- Simplified monitoring of anti-competitive behaviour, with keyword-based searches for suspicious signs in internal communications and with third parties or competitors, especially on new communication channels, platforms or messaging applications;
- Faster detection of anti-competitive behaviour and easier gathering of evidence, with the ability to report harmful acts to competition authorities at an early stage as part of a leniency procedure;
- A dissuasive effect on employees, who are aware that it is more difficult to dissimulate illegal behaviour;

²³ Early detection and facilitated access to a large data set in a very short space of time offer considerable added value in leniency proceedings. The high cost of using screens can be quickly offset by the benefits of preventing antitrust risks. On the added value of screening tools, see Rosa M. Abrantes-Metz & Albert D. Metz, "Why Screening is a "Must Have" Tool for Effective Antitrust Compliance Programs", *CPI Antitrust Chronicle*, November 2019 and "Antitrust & Regulatory Compliance in the 21st Century: New Challenges, New Opportunities and the Role of AI", *CPI Antitrust Chronicle*, September 2023.

- A better allocation of resources, as the use of empirical screens improves the identification of high-risk areas and enables audits to be targeted at these areas.

The company must also be aware of the risks associated with using AI for business purposes, especially when pricing algorithms and similar tools are used. In both compliance programmes and business processes, AI and algorithms must be employed responsibly. Use must be transparent, continually risk-assessed, and allow for full accountability.



7. Disciplinary action

It is essential for your company to develop an **internal disciplinary code** or policy addressing employees and company officers who initiate or participate in conduct that is in breach of your company's Code of Conduct (including antitrust compliance). This is important not only for deterrence purposes, but also as a reflection of your company's real commitment to embedding and fostering a compliance culture.

A credible antitrust compliance programme should make clear that disciplinary action (up to and including suspension, demotion, dismissal or even legal action against an employee or former employee—if the latter is possible under applicable local law) will be taken if anyone in your company contravenes antitrust law. It is important that the disciplinary policy is applied consistently throughout your company and, in particular, that senior employees/managers are not shielded from disciplinary action in the event that they violate the rules.

Enforcement agencies (including antitrust agencies) increasingly expect companies to show they are serious about compliance by building antitrust compliance programmes that include provisions for appropriate disciplinary action or “Consequence Management” as this is seen as fundamental to the programme's effectiveness.²⁴

a. General requirements for disciplinary proceedings

Your company will need to develop its own **disciplinary policy** in a way that is best suited to your company's needs and takes into account all applicable employment laws (*i.e.* the employment laws in every country in which your company has employees) and other fairness and human rights considerations. In this respect, it is essential that any disciplinary measures envisaged are reviewed by a local advisor specialising in labour law, to ensure their compatibility with local practices.

To ensure the credibility of your company's compliance programme, it is important that any disciplinary measures taken are fully and consistently applied. The company must not be perceived as “turning a blind eye” to Code of Conduct violations.

In addition, a clear and transparent disciplinary policy in its design and implementation strengthens the legitimacy of the compliance programme. To properly integrate risks, employers must have visibility and knowledge of existing disciplinary measures.

In preparing your company's disciplinary policy, you may wish to address various general points,²⁵ such as:

- Who in your company will make the decision about whether to impose disciplinary measures and which measures to impose? As a general recommendation, it is suggested that disciplinary measures for Code of Conduct violations should not be left to one individual. Disciplinary decisions would be better taken (for consistency reasons) by a panel of individuals, including from Compliance, Legal and HR, as well as senior management in the business line concerned.
- If a panel in your company will take the decision on disciplinary measures, how will the panel be structured?
- What notice of concerns and rights of defence/representation should affected employees be given?

²⁴ U.S. Department of Justice Criminal Division, *Evaluation of Corporate Compliance Programs*, Updated March 2023, page. 12. This guidance can be found at: <https://www.justice.gov/criminal-fraud/compliance>.

²⁵ Note that your company will need to obtain specific employment law advice in the relevant country or countries.

- What potential aggravating or mitigating circumstances should you take into account?
- What action should your company take against line managers who fail to take reasonable steps to prevent (or even worse, who encourage or tolerate) misconduct?
- How will you balance the need for confidentiality (and in some situations Legal Professional Privilege around the circumstances of the case) and the need to document disciplinary actions and procedures fully against employees who violate antitrust laws?

b. Possible disciplinary measures

To establish a consistent and fair disciplinary policy, your company can draw up a scale of possible sanctions, depending on the gravity of the employer’s misconduct. This will help determine the most appropriate and proportionate sanction in each case (subject to local employment law advice). It will also prevent similar misconduct from being treated in a disparate manner.

The scale of graduation can be defined as follows:

- Use of an internal “compliance score”/tracker as part of performance evaluations;²⁶
- Informal warning plus a required course of antitrust training and counselling;
- Formal written warning plus a required course of antitrust training and counselling;
- Demotion or non-promotion plus a required course of antitrust training and counselling;
- Forfeiture of compensation components (deferred bonus, loss of bonus, stock options or other pay elements);
- Dismissal with or without notice (as appropriate under the applicable local law);
- Other actions may be considered in appropriate cases (action for damages/ withdrawal of bonus/pension benefits) subject to local legal considerations.

Your company’s disciplinary policy for Code of Conduct violations should be clearly articulated and should be distributed to/made known to all your company’s employees and managers. However, it will be important not to suggest a pre-determined outcome to disciplinary proceedings that would interfere with a full and fair review of available facts relating to the employee’s involvement in conduct prohibited under the Code.

c. Potential aggravating and mitigating factors

First, you may wish to decide, when developing your company’s policy, whether a progressive approach to disciplinary sanctions is needed. If your company previously has had a culture of not taking appropriate disciplinary action against employees, a fair amount of warning (perhaps coupled with an opportunity for employees to come forward voluntarily)²⁷ might offer a less dramatic transition towards “zero tolerance”.

Secondly, mitigating and aggravating factors may be considered in order to properly assess the most appropriate sanction for the situation. The **mitigating factors** that may be considered by your company during disciplinary proceedings against an employee for antitrust violations include the following: (i) the employee’s full cooperation with the internal investigation; (ii) the employee’s non-managerial / non-senior level role; (iii) the employee’s

²⁶ These performance factors can be used both as disciplinary measures and as incentives for employees to meet and exceed compliance targets—See Chapter 9: Compliance incentives.

²⁷ See Chapter 8: Antitrust due diligence: Any internal (within company) “amnesty” to employees would have to be strictly internal, and could only relate to the company’s intention to discipline the individual—no guarantees can be given in relation to the actions of external agencies and/or prosecutors towards the individual.

attendance at non-mandatory antitrust training;²⁸ (iv) the employee acted in good faith (and in accordance with legal advice);²⁹ (v) the activity was permitted, knowingly overlooked, or encouraged by the employee's line manager.³⁰

Aggravating factors for your company to consider may include the following: (i) failure to cooperate during the internal investigation; (ii) employee's managerial role (see below for considerations relating to senior employees); (iii) employee's completion of antitrust training (employee was on notice about standards of conduct required); (iv) employee's failure to complete antitrust training (despite your company requiring it);³¹ (v) employee's involvement in previous infringement in the same area ("repeat offender"); (vi) the employee encouraged other employees to take part in the infringement;³² (vii) the employee ignored or failed to take legal advice before engaging in the activity that violated antitrust law.

With a **senior person** (e.g. a line manager up to and including members of your company's Board of Directors)³³ who is not clearly directly involved in the unlawful discussions, your company may wish to consider whether that line manager actively encouraged the violation, "turned a blind eye" to it—or negligently failed to ensure proper control over the business concerned. In this context, when looking at whether a line manager "knew or ought to have known" of the activity, the relevant factors you may wish to consider are:

- The line manager's role, responsibility and authority in your company;
- The line manager's relationship to those who committed the violation;
- The knowledge and understanding that a person in that position and of that job group would be expected to possess;
- The antitrust training that the leader himself/herself has had (or should have had);
- If the line manager encouraged or approved of the violation (or knowingly created a situation where an employee understood or reasonably believed that financial results and business targets were to be delivered at any cost), this would be a clear aggravating factor which would suggest that some disciplinary action in relation to that line manager is warranted.

d. Specific considerations in antitrust cases

The credibility of your antitrust compliance programme will be tested when it comes to determining how your company deals with employees involved in serious antitrust violations such as cartels or other hard core antitrust infringements.

If your company's Code of Conduct and related policies place a clear ban on participation in cartels, and your company's disciplinary policy envisages dismissal as a sanction for the most serious forms of Code of Conduct breaches, disciplinary sanctions should logically apply to clear Code of Conduct violations by the employee.

28 If employees have not been identified properly for the purpose of ensuring the right people attended antitrust training, this would be an issue with the effectiveness of the compliance programme itself, and must trigger an urgent review of training nominations (as part of the continuous monitoring and improvement—See Chapter 10: Monitoring and continuous improvement).

29 Note, incorrect legal advice is unlikely to protect the company from being fined if an antitrust violation occurs, although if an individual employee relies on credible legal advice, they may have a defence to any individual criminal liability—however this is a matter of local law applying in the relevant jurisdiction.

30 This would be an aggravating factor for your company to take into account when considering disciplinary action in relation to the line manager (see below).

31 If employees are regularly failing to take required training, this is a matter that should be addressed in a review of your antitrust programme (See Chapter 10: Monitoring and continuous improvement).

32 As noted, if the employee is himself/herself a line manager who approved of or encouraged the violation, this is a clear aggravating factor.

33 Concerning the commitment of senior and middle managers, see U.S. Department of Justice Criminal Division, *Evaluation of Corporate Compliance Programs*, Updated March 2023, pages 9 and 10.

However, if your company is considering applying for immunity/leniency, certain precautions need to be taken in implementing your disciplinary policy. Indeed, the decision to discipline (and when to discipline) an employee for a very serious antitrust infringement (such as engaging in a cartel) can be complex. In such cases, it will be important for your company to secure the ongoing cooperation of the employees involved in the violation in order to meet your company's own obligations (as part of the conditional grant of immunity or leniency) to assist and fully cooperate with relevant antitrust agencies in their investigations. This means your company will need to keep employees available for the purposes of the external antitrust investigation and any subsequent antitrust proceedings. Dismissal may therefore not be an option for the duration of the antitrust proceedings, or until such time as the antitrust agencies no longer require the employee's input.³⁴ Your company may set up a system of "deferred sanctions" and may need to retain the employee on paid leave/absence until the final resolution of the antitrust case against the company.³⁵ It may be useful for your company to consider entering into an agreement with the employee to the effect that payment for the leave of absence is dependent on the employee cooperating fully with your company and with all relevant antitrust agencies.

You may also need to reconsider your company's general position in relation to funding/refunding employees' personal legal fees and or personal fines in the event of an antitrust investigation, in particular if the employee is found personally criminally liable. It is important to seek local legal advice in each relevant country, as legal and public policy considerations often prevent the payment of individual fines and in some cases also require the recovery of legal fees associated with a criminal case.³⁶ Even if your company is not actually prohibited from making such payments, you might wish to consider the (negative) message that such payment might give to employees (and agencies) about your company's genuine commitment to ethical behaviour and compliance.

34 You should also bear in mind that the increase in civil litigation and "follow-on" damages claims may even further extend the need to ensure that "guilty" employees continue to be available to your company during any follow-on litigation.

35 You should note that a decision to defer sanctions and to send an employee on "gardening leave" will be complicated (and may indeed not be possible) if the individual is subject to personal criminal sanctions in any jurisdictions. In any event, whether or not the employee is subject to criminal sanctions, you will need to ensure that you seek employment law advice in the relevant country.

36 If the relevant employee is a director or an officer of your company, you should also check your company's insurance policy, since many directors' and officers' insurance policies will not cover criminal acts by your company's directors and officers.



8. Antitrust due diligence

Antitrust due diligence takes many forms. It encompasses day-to-day checking of substantive antitrust compliance within your company as part of the operation of your antitrust compliance programme, it includes more structured “deep dives” and audits / *ad hoc* or regular compliance “screening” on particular businesses if areas for concern have been flagged (or are suspected). It also covers more specific legal due diligence exercises, such as due diligence around trade associations and in an M&A (mergers, acquisitions, and joint ventures) context to verify the existence of antitrust related risks and contingencies.

Antitrust due diligence is not only important as part of the operation of your company’s compliance programme (to ensure that the programme is adequately monitored and that antitrust risk assessments are kept up to date),³⁷ but a number of agencies also expect companies to undertake appropriate due diligence to prevent and detect violations of antitrust law (which may also be criminal conduct depending on the jurisdiction) and to promote a corporate culture that encourages ethical conduct and a commitment to compliance.³⁸

a. Due diligence in hiring new employees

To demonstrate a commitment to compliance, your company should endeavour to **exercise due diligence in hiring new employees**. If at all possible, it is important not to recruit or allocate responsibilities to executives or employees who are known to have violated antitrust laws or who are reasonably (objectively) suspected of having done so.³⁹

Even if a background check is not possible, your company should have a clear on-boarding process where new recruits are instructed in your company’s expectations regarding compliance with your Code of Conduct and with antitrust laws.

b. Due diligence in assessing substantive compliance

Due diligence of substantive antitrust compliance (i.e. checking compliance with the law in practice) can range from light touch self-assessment through to checklists,⁴⁰ antitrust counselling and antitrust training follow up, selective “deep dives” into particular areas of the business and, at the other end of the scale, comprehensive forensic antitrust “audits”. Increasingly, it may also become necessary to consider whether the data produced by a company during its day-to-day activities can be used (also with the help of artificial intelligence)⁴¹ to proactively identify possible antitrust risks.

Some companies choose to include as part of their antitrust programme materials⁴² an “Antitrust Due Diligence” self-assessment toolkit (ADD Kit), which is essentially a list of questions/checklist to allow employees to check whether something is likely to be problematical under antitrust laws. The purpose of the ADD Kit is not to replace the need

37 See Chapter 3: Risk identification and assessment and Chapter 10: Monitoring and continuous improvement.

38 See the [US Federal Sentencing Guidelines, §8B2.1\(a\)\(1\)](#), (“an organisation shall exercise due diligence to prevent and detect criminal conduct” and “an organisation shall otherwise promote an organisational culture that encourages ethical conduct and a commitment to compliance with the law”, and the disclosure obligations under the US Sarbanes-Oxley Act (available [at http://www.law.cornell.edu/uscode/text/15/chapter-98](http://www.law.cornell.edu/uscode/text/15/chapter-98)).

39 While not specifically requiring pre-employment due diligence, the US Federal Sentencing Guidelines state at [§8B2.1\(b\)3](#): “The organisation shall use reasonable efforts not to include within the substantial authority personnel of the organisation any individual whom the organisation knew, or should have known through the exercise of due diligence, has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program”.

40 See, e.g. the Competition Bureau of Canada’s [materials](#) in this regard.

41 Likewise the use of AI for purposes of internal compliance investigations (See Chapter 6: Handling of internal investigations), the use of AI may also be consider to complement due diligence process.

42 See Chapter 4: Antitrust compliance know-how.

for specialist antitrust advice or other legal advice, but rather to provide practical tools to allow your employees to identify “red flags” or antitrust danger areas.

c. Antitrust assessments (audits) or selective deep dives

This section considers **antitrust assessments** (or selective “deep dives”) involving a legal review of business activities and practices to detect whether actual or potential violations of antitrust laws have occurred or may be likely to occur. It will be important that any antitrust legal assessments or deep dives are conducted consistently with the company’s Investigation Principles.⁴³

It is important to distinguish a **substantive legal assessment** of antitrust compliance from a compliance programme process or controls audit. A process/controls audit examines whether your company has in place and has implemented best practices, controls, and procedures, in order to monitor, escalate, and take action on actual or potential compliance violations. A substantive antitrust assessment focuses on whether, in fact, an actual violation of substantive antitrust law has occurred or is likely to have occurred. It aims to:

- Identify actual or potential antitrust violations before a company faces an investigation or challenge by a third party or an antitrust agency;
- Determine or confirm the nature and extent of an antitrust violation where there is already a specific allegation or suspicion;
- Identify business practices which present risks of potential antitrust violations, for example, businesses involving markets with historical record of antitrust violation (even if the target company was not involved) or with high levels of market share concentration;
- Assess the effectiveness of your company’s antitrust compliance programme and antitrust training in avoiding antitrust violations.

d. Due diligence in relation to trade associations

Attendance of your company’s employees at **trade associations** (or similar events such as industry “roundtables” / social events) gives rise to specific antitrust risks. Trade associations can perform many useful and perfectly legal functions, and often perform a pro-competitive and useful role in the economy, or at least act in a way that is competitively neutral. If managed carefully and with full regard to antitrust advice, the worthy and legitimate goals of most trade associations can be accomplished without undue antitrust risk.

However, trade associations are—by their nature—a place where competitors meet to discuss matters of interest and importance to the industry. If your company’s employees who attend trade associations are not constantly on their guard to ensure that no competitively sensitive information is disclosed, there is a significant risk that discussions at the association meetings could encounter serious antitrust risk, and possibly even violate antitrust law.

If trade associations (and their members) fail to take account of antitrust concerns, they could end up engaging in anticompetitive or even illegal collusive conduct, involving liability both for the trade association members and for the trade association itself (as well as, potentially, individual personal liability for those involved).

Due diligence around trade associations typically takes a couple of forms:

- Due diligence before attending trade association meetings by ensuring that your company’s employees are fully trained and aware of the antitrust risks of inappropriate information exchange;

⁴³ See Chapter 6: Handling of internal investigations.

- Due diligence on the activities of the trade associations themselves (including ensuring that the trade association itself has an appropriate antitrust compliance policy that is followed diligently).

If your company's employees attend trade association meetings or events, it is essential to ensure they are appropriately **trained**. To ensure that the right employees get the right antitrust training, you will need to understand who in your company attends trade associations and similar events. Some larger companies with several hundred (or even several thousand) employees track trade association membership in the company using an online "platform of registration" or "registration tool", where the employee registers membership of the association, giving management an opportunity to check on the activities of the employee in the association and intervene if appropriate. Such an online tool may not be necessary for SMEs or even for larger companies where relatively few employees attend trade associations. However, it can be a useful tool where the numbers are sufficiently large, since it enables the company to target antitrust training at higher risk employees.

Because of the antitrust risks inherent in trade associations, you may choose to undertake "due diligence" (from time to time, as appropriate) on the **activities of trade associations** of which your company is a member.

e. Due diligence in M&A situations

If your company does not perform adequate antitrust "due diligence" prior to a merger, acquisition or the creation of a Joint Venture (JV), your company may face both legal and business risks. Inadequate due diligence can allow a course of anti-competitive conduct to continue undetected after the relevant transaction, in violation of your Code of Conduct, with all the attendant harms to your company's reputation, as well as potential civil and criminal liability. In contrast, if you conduct effective antitrust due diligence on an acquisition target, you will be able to evaluate more accurately the target's value and negotiate for the costs of the antitrust compliance violation to be borne by the seller. However, even a thorough due diligence exercise may not succeed in uncovering hard core cartels, as these are covert by their nature.

It has been more common, before approaching a potential target/vendor/purchaser or JV counterparty, to pay close attention to potential compliance risk (in particular relating to antitrust and bribery & corruption, but other compliance risks may be relevant too).

There are certain key issues that should be looked at in conducting due diligence in M&A situations to avoid compliance surprises and understand weaknesses that will need to be corrected in the future.

- **Is the antitrust compliance programme (and the controls in other compliance areas) state-of-the-art and up-to-date?**
- **What is the target's risk profile?** Consider: (i) the nature of the target's business and industry, (ii) the nature of the jurisdictions in which it operates, (iii) how it conducts business (e.g. does it use intermediaries, consultants, third parties, joint venture partners?) and (iv) the profile of its customers and competitors.
- **Is there a culture of compliance?**
- **Is there a strong compliance control environment?**
- **Are any (internal or external) compliance investigations currently under way?** Obtain reports on any ongoing antitrust investigations (including pending, threatened, or anticipated investigations).

- Additional antitrust compliance due diligence could enquire into;⁴⁴
- Existence of closed antitrust procedures/litigation (within a specified period) involving the target company;
- Existence of antitrust sanctions/penalties/damages awards imposed on, or antitrust remedies/commitments (structural and/or behavioural) undertaken by the target company (within a specified period) for infringement of antitrust law;
- Existence of any outstanding antitrust warranties or indemnities given by the target company;
- Details of the target’s participation in any trade or industry association, copy of the by-laws of such association, description of its goals, copy of the minutes of the last [stated number of] meetings;
- Participation in any joint production, joint logistics, joint distribution/sales arrangement or joint procurement (whether formal or informal, incorporated or unincorporated);
- Details of directorships, shareholdings or other interests held in any competing company;
- Existence of merger control clearances for all relevant M&A activity within the target (to ensure the target has obtained all relevant merger clearances and has not engaged in “gun jumping”—*i.e.* that the target has not implemented a transaction before receiving all necessary antitrust clearances).

Due diligence, however, is normally only the start of the compliance process for mergers, acquisitions and the formation of JVs. As the acquiring company, you will also need to ensure that the acquired company promptly adopts and satisfies all your own company’s internal controls, including your antitrust compliance programme.

You should consider arranging antitrust training for all new employees in a commercial role (*i.e.* those who qualifying under your antitrust training nominations criteria—see Chapter 4: Antitrust compliance know-how). Where appropriate, you should also consider conducting in depth legal antitrust assessments on new business units (see paragraph (c) of this chapter, above).

Internal “amnesty”

In order to identify antitrust compliance violations more quickly—some companies have considered offering an internal “amnesty”⁴⁵ to the employees of the target company post-acquisition if they come forward within a short period of time to confess to wrongdoing. The intention of this from an antitrust perspective is to allow you—as the acquiring company—to make an amnesty/leniency application to the relevant antitrust agencies, and to trigger contractual indemnities if relevant in a timely fashion. However, the legal difficulties of going down this route should not be underestimated, and if you are contemplating this, your company should seek legal advice, in particular in relation to employment law, directors’ duties, disclosure requirements (for quoted companies and for companies regulated for example by the Financial Conduct Authority or similar), Legal Professional Privilege, anti-money laundering, and proceeds of crime considerations to name but a few.

44 This is not intended to be a comprehensive due diligence checklist; it is merely a suggestion of some antitrust related questions that could be asked as part of a more comprehensive due diligence exercise. Nor does it attempt to suggest any due diligence questions for other compliance areas outside of antitrust.

45 As mentioned above, “internal amnesty” would clearly have to be strictly internal, and could only relate to the company’s intention to discipline the individual—no guarantees can be given in relation to the actions of external agencies and/or prosecutors towards the individual.



9. Compliance incentives

Compliance **incentives** can help to **change behaviour** positively within your company. Incentives can work as effective tools for a business that wishes to promote compliance by employing concrete actions and can play an important role in fostering a culture of compliance. Introducing compliance incentives may be more suitable if your company already has a well-developed and mature compliance programme.

Incentives are seen (particularly by agencies) as offering support to a company's culture of compliance.⁴⁶ However, unlike other mainstream antitrust compliance programme measures, such as training and in-depth antitrust legal assessments, incentives have sometimes proven to be controversial in theory, and difficult to implement in practice. Therefore, you should carefully consider what incentives your company wishes to (or legally can) provide to ensure that antitrust compliance processes are followed.

a. Why have compliance incentives?

The main reason why you might consider having incentives to bolster your company's compliance programme is because many agencies view incentives an important part of a credible programme audit result could drive.

b. Types of incentives

There is a **wide range of compliance incentives**, from “softer” incentives to more tangible ones:

- The “softer” incentives include non-tangible encouragement/recognition, such as commendations (public or not, as appropriate) from your senior business leaders for an employee's exemplary compliance-related conduct (*i.e.* as “compliance champions” or “compliance heroes”);
- These “softer” incentives can also be addressed to a group (*i.e.* publicising a country or business unit being the first within your company to have 100% employee completion of training);
- They may include tangible rewards, possibly monetary (which can be very effective, but occasionally offend those who feel that doing what is right is part of everyone's job)—they could also include (short of monetary rewards) commendation in staff appraisals, which may in turn in due course be taken into account in promotions or performance bonuses);
- You could consider using compliance criteria in personnel evaluations (employee appraisals), which—along with other criteria—can impact an employee's compensation and / or promotion prospects;
- Compliance incentives can be either general or risk-area specific—for instance, in a personnel evaluation (employee appraisal) you could test whether an employee has demonstrated an understanding of and adherence to your company's policies and procedures;
- Some companies require consideration of compliance performance as part of succession planning—which can be a powerful compliance-related motivator for leaders and future leaders in your company;

⁴⁶ See the [section on incentives in the Canadian Bureau of Competition antitrust compliance materials](#).

- You should also consider how other incentives (such as bonuses linked to stretching business targets) could deter compliance (for example, if the rewards scheme prompts employees to take undue risk, e.g. promotes “do or die” attitude).

For internal career planning, you may wish to consider whether promotions could depend also on an individual employee’s compliance track record.



10. Monitoring and continuous improvement

Your company should take reasonable steps regularly to evaluate the effectiveness of its antitrust compliance programme. **Regular evaluations are essential features** of any antitrust compliance programme given the dynamic business and regulatory context in which companies operate and how this affects both internal and external risk factors (see Chapter 3: Risk identification and assessment). Your company's compliance and ethics programme should be measured like any other critical capability.

There are two aspects of compliance monitoring and assessment that your company could use to determine whether the design of its compliance programme meaningfully assists in preventing, detecting, and responding to violations of applicable antitrust laws (also known as “assurance”):

- The first involves checking that your programme's **processes and controls** are—and continue to be—appropriate, and are being implemented and are operating effectively and efficiently;
- The second (considerably more difficult) aspect is a regular review of parts of your company's business or of certain practices to assess whether these are compliant (*i.e.* a **substantive compliance assessment**).⁴⁷

a. Monitoring and assessing processes and controls

By using accurate recent data to measure whether your company's antitrust compliance programme processes and related controls are appropriately designed and are being applied consistently and adequately throughout your company, you should evaluate the effectiveness of those controls and improve them where necessary. This assurance process may be done as part of your regular risk assessment (discussed in Chapter 3: Risk identification and assessment) or may be done as a separate exercise.

Monitoring and assessing processes and controls involves a regular review and assessment of your company's compliance programme by:

- Monitoring whether individual behaviours within your company meet the programme's process requirements (*i.e.* tracking antitrust training attendance completion rates, ensuring other antitrust controls are operating effectively and assessing whether employees are complying with other “control” measures (such as keeping a Trade Association database updated (if applicable)));
- Checking managerial tasks designed to increase the likelihood of success of the programme are followed—for example, if your company adopts a control requiring line manager approval for attendance at trade associations, ensuring that processes are in place for employees to obtain such approvals and for these approvals (or refusals) to be tracked and monitored;
- Reviewing information produced by internal and/or external auditors (*i.e.* on levels of employee awareness and understanding of relevant antitrust controls);
- Considering scope for internal and external benchmarking against commonly accepted “best practices”.

⁴⁷ See also Chapter 8: Antitrust due diligence.

Whether undertaking an internal review of the programme or whether undertaking an external benchmark, it makes sense to decide in advance what metrics to use so relevant data can be gathered and captured from the outset; *ex-post* data-gathering may be more complex.

b. Measuring effectiveness of processes and controls

There is merit in your company deciding “upfront” **how to measure related processes and controls**, focusing on three key aspects:

- Effectiveness *i.e.* the quality of a programme’s (i) design effectiveness (degree to which the programme’s processes and controls are logically designed to meet defined requirements) and (ii) operational effectiveness (degree to which the programme operates as designed);
- Efficiency *i.e.* the cost of the programme. It is very important (to ensure the integrity and effectiveness of the antitrust compliance programme) that the cost of certain systems or controls is not used as a reason to implement cheaper but less adequate/less effective controls that do not appropriately mitigate risk;
- Responsiveness *i.e.* the programme’s ability to operate quickly and flexibly in response to changing circumstances.

The selected approach should be designed to help ensure, maintain, and improve the performance of your antitrust compliance programme, based in the findings that emerge. Key metrics and indicators should be specific, simple, measurable, actionable, relevant, and timely. Your company’s performance measurement system (for assessing the effectiveness of your company’s compliance processes and controls) should be refined on an ongoing basis—but is best designed with your company’s existing financial and risk control framework in mind. By gaining experience of measuring your company’s programme performance you can fine-tune and improve the system over time.

- If the antitrust programme has been well designed, does it function correctly?
- Does it operate the way it was designed?
- If not, how must it be managed/alterd to improve its level of operation?

c. Auditing and benchmarking

Audit reports from your company’s external and/or internal auditors (*i.e.* performing confidential departmental programme audits) can be very useful sources of information about the operation of the process elements of an antitrust compliance programme. Audits with an antitrust component or “focus theme” generally consider the operation of the programme in terms of the effectiveness of its processes and controls in raising awareness and understanding of compliance considerations that are relevant to a company’s operations, but are not an audit of substantive compliance (which auditors are often not best placed to assess—see below).

Reviews of your company’s antitrust compliance programme by informed (*i.e.* specialist) antitrust counsel can also be useful to identify trends.

Ultimately, the objective is to encourage **constructive dialogue in which companies can challenge themselves** (or be challenged) on how well their approach works and what improvements can be made (and within what time frame).

d. Monitoring and assessing substantive compliance⁴⁸

Periodically assessing whether parts of your company's business or certain business practices are complying with antitrust laws in practice allows senior managers to know whether the company is moving closer to its antitrust compliance objectives. It helps ensure that there is continued, clear and unambiguous commitment to antitrust compliance from the top down, that the antitrust risks are identified, or the assessment of these risks have not changed (or if they have changed, to reassess controls) and that the risk mitigation activities/controls remain appropriate and effective. It may also enable your company to identify substantive antitrust concerns, rectify any illegal behaviour, and to assess if it is appropriate to apply to one or more antitrust agency for immunity/leniency.

An important early consideration when planning to undertake a **substantive antitrust assessment** is to ensure that appropriate resources are dedicated to it. This implies consideration of the following:

- **Who should undertake the assessment?**
It will generally be advisable for the assessment to be undertaken by people with specialist antitrust knowledge and experience. For this reason, many companies rely on specialist in-house or external antitrust counsel for such assessments rather than (for example) having such assessments conducted by financial auditors or controllers.
- **Will Legal Professional Privilege be maintained?**
This is a reason why companies often choose to use external antitrust legal counsel for compliance assessments in order to protect its results.
- **How will the review be conducted?**
It may involve electronic searches of documents and databases, the use of AI to undertake continuous searches of internal documents (to the extent this is permitted under the applicable local law), interviews of key employees etc. The company must take into account legal issues such as data privacy, employment law considerations (the need to seek staff council approval) and so on.
- **How will the results of the assessment be shared within the company?**
You will want to balance the need to share learnings with the importance of protecting Legal Professional Privilege (see above).
- **How will the review be funded (internal budget considerations)?**

e. Compliance programme improvement plan

Having assessed the effectiveness of an antitrust programme's processes and controls, (and having tested substantive antitrust compliance as appropriate), it will be important to consider whether the company should develop a compliance programme improvement plan (CPIP).

If your company adopts a CPIP, it should set out deliverable actions to address identified control gaps, to introduce new controls (as required) and should articulate timelines for delivery, including details of who is accountable in the company to ensure delivery. The plan would also usually articulate how delivery of the action points agreed will be tested and how desired improvements to the programme will be objectively monitored.

⁴⁸ See also Chapter 8: Antitrust due diligence.



Acknowledgements

ICC is grateful to the ICC Task Force on Antitrust Compliance Policy Harmonisation and other ICC members and national committees whose contributions have been essential to the development of the ICC antitrust compliance Toolkits, and especially:

ICC Global Commission on Competition

- Paola Pugliese Partner and Head of the Antitrust/Competition Practice, Lefosse—*Chair of ICC Global Commission on Competition*

ICC Task Force on Antitrust Compliance Policy Harmonisation co-editors of the Toolkit

- Charlotte Breuvert, Partner, Jones Day, Belgium
- Gordon Christian, Principal Counsel Competition, Siemens Energy, Germany
- Joyce Honda, Lawyer, Cescon, Barrieu, Flesch & Barreto Sociedade de Advogados, Brazil
- Anne Riley, former Global Group Antitrust Counsel, Shell plc, – former Chair of the ICC Task Force on Compliance and Advocacy; Co-Chair of the ICC Task Force on the ICN, United Kingdom
- Dan Roskis, Partner, Eversheds Sutherland, France
- Carolina Soto, Lawyer, Prieto, Chile
- Mickael Viglino, Lawyer, J.G. Assis de Almeida Advogados e Associados—Sociedade de Advogados, Brazil
- Johannes Wiehe, Associate, White & Case, Germany (views expressed here are strictly personal and should not be attributed to his law firm, its affiliates or clients)

ICC Global Headquarters

- Caroline Inthavisay, Global Policy Lead—Competition

ICC Task Force on Antitrust Compliance Policy Harmonisation contributors

ICC would also like to thank the contributors of the first edition without whom this new edition would not have been possible.

The contributors of the new edition are:

- Jesús Alvarado-Rivera, Global Director—Antitrust, Anheuser-Busch InBev, United States
- Sahin Ardiyok, Partner, Dentons, Türkiye
- José Gabriel Assis de Almeida, Partner, J.G. Assis de Almeida Advogados e Associados—Sociedade de Advogados, Brazil
- Oguczan Bülbül, Competition Compliance Group Manager, Anadolu Efes, Türkiye
- Daniel Castelo, Director, Bustamante & Fabara, Ecuador
- Cecil Chung, Head of International Antitrust, Yulchon LLC, Republic of Korea
- J. Brady Dugan, Partner, Squire Patton Boggs, United States
- Andreas Gayk, Director Policy Relations, Compliance Officer, Markenverband E.V., Germany
- Christoph Hirschmann, Chief Compliance Officer, ÖBB-Holding AG, Austria

- Wei Huang, Senior and Managing Partner, Tian Yan Law Firm, China
- Dina Kallay, Head of Competition Law, Ericsson INC., United States
- Kyu Hyun Kim, Partner, Yulchon LLC, Republic of Korea
- Elise Lelong, Lawyer—Competition, BNP Paribas—Paris, France
- Katerina Mandulova, Manager, PwC, Czech Republic
- Guilherme Misale, Partner, Caminati Bueno Advogados, Brazil
- Jacques Moscianese, Head of Antitrust Affairs & Strategic Support-International and Regulatory Affairs Department, Intesa Sanpaolo Spa, Italy
- Leonardo Ortiz Mendieta, Legal Director, CCB, Colombia
- Luca Pardo, Managing Partner, Ontier, Italy
- Svitlana Pereverzeva, General Secretary, ICC Ukraine
- Théodore Plat, Junior Associate, Jones Day, Belgium
- Brian Rafkin, Partner, Baker & McKenzie, United States
- Ulrike Suchsland-Maser, Legal Advisor, Bundesverband der Deutschen Industrie E.V., Germany
- Andreas Traugott, Partner, Baker & McKenzie, Austria
- André Uhlmann, Compliance Officer, Thyssenkrupp AG, Germany
- Andrea Von Chrismar, Counsel on Regulation and Competition, Prieto, Chile
- German Zakharov, Partner, Competition/Antitrust and White collar crime, Compliance and Investigations practices, Alrud Law Firm, Russia
- Lixia Zhou, Senior Conference Interpreter, University of International Business and Economics, China

About the International Chamber of Commerce

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 170 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, MSMEs, business associations and local chambers of commerce.



33-43 avenue du Président Wilson, 75116 Paris, France

T +33 (0)1 49 53 28 28 E icc@iccwbo.org

www.iccwbo.org [@iccwbo](https://twitter.com/iccwbo)

