

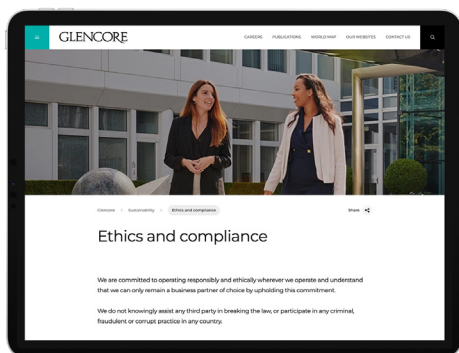


Energising today
Advancing tomorrow

Energising today Advancing tomorrow

Contents

Introduction	
Our business at a glance	3
Chairman and Chief Executive Officer's introduction	5
General Counsel and Head of Compliance annual overview	6
Ethics and compliance at a glance	8
Governance and structure	
Tone at the top: our leadership	10
Governance	11
Our Compliance team	12
Support from Group corporate functions	14
Group Internal Audit and Assurance	15
Our Programme	
The Glencore Ethics and Compliance Programme	18
Risk assessments	19
Policies, standards, procedures and guidelines	20
Training and awareness	23
Advice	25
Monitoring	26
Speaking openly and raising concerns	27
Discipline and incentives	30
Key risks	
Introduction	32
Anti-corruption and bribery	33
Conflicts of interest	35
Fraud	36
Sanctions and trade controls	37
Anti-money laundering	39
Competition law	39
Market conduct	40
Data protection	41
Our business partners	
Business partner management framework	43
Know your counterparty	45
Third party due diligence and management	47
Community investment due diligence and management	51
Joint ventures, mergers and acquisitions, and disposals	52
Additional information	
Important notice	55
Further information	56



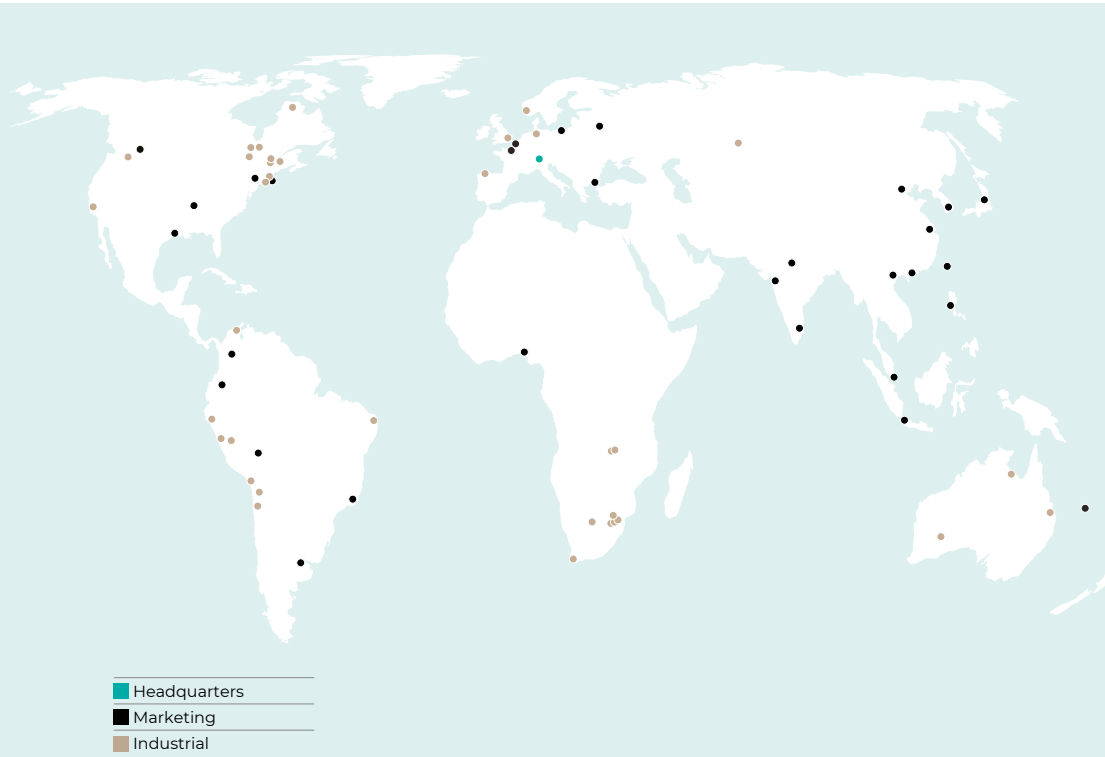
Quick links: Ethics and compliance page on our website at: <https://www.glencore.com/sustainability/ethics-and-compliance>

Explore our annual reporting suite online at: [glencore.com/publications](https://www.glencore.com/publications)

Throughout this report, references to our Programme refer to our Ethics and Compliance Programme and references to our Code refer to our Code of Conduct. This report focuses on our work undertaken in 2025, as well as continued progress to date in 2026.

Our business at a glance

Our global operations



One of the world's largest natural resource companies

6 continents
>30 countries
>140k employees and contractors

For further information, see [glencore.com/en/who-we-are/purpose-and-values/](https://www.glencore.com/en/who-we-are/purpose-and-values/)

...delivered through two business segments



Industrial activities

Our industrial business spans the metals and energy markets, producing multiple commodities from around 40 industrial assets



Marketing activities

We source, market and distribute over 60 commodities that advance everyday life

...supported by our Values



Safety

We never compromise on safety. We look out for one another and stop work if it's not safe



Integrity

We have the courage to do what's right, even when it's hard. We do what we say and treat each other fairly and with respect



Responsibility

We take responsibility for our actions. We talk and listen to others to understand what they expect from us. We work to improve our commercial, social and environmental performance



Openness

We're honest and straightforward when we communicate. We push ourselves to improve by sharing information and encouraging dialogue and feedback



Simplicity

We work efficiently and focus on what's important. We avoid unnecessary complexity and look for simple, pragmatic solutions



Entrepreneurialism

We encourage new ideas and quickly adapt to change. We're always looking for new opportunities to create value and find better and safer ways of working

Our business at a glance *continued*

Our Purpose

Responsibly sourcing the commodities that advance everyday life

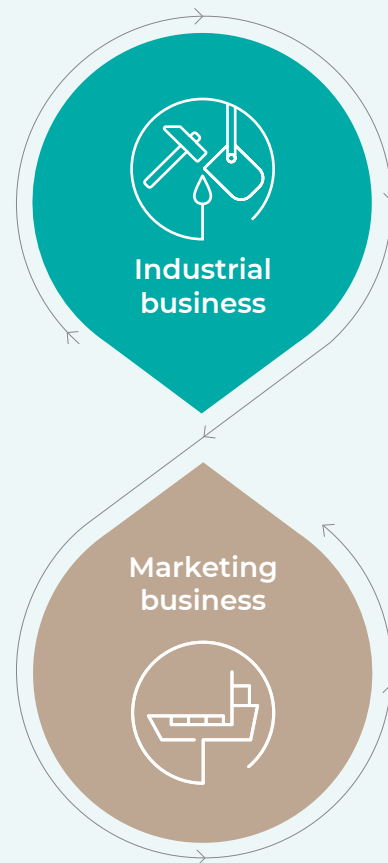
...influences our strategic priorities

Responsible and ethical business practices

Effective capital management

Strong operational and commercial performance

...which we deliver through our business model



...while engaging with our stakeholders and creating value



Chairman and Chief Executive Officer's introduction



Kalidas Madhavpeddi
Chairman

Gary Nagle
Chief Executive Officer

Dear stakeholders,

We are pleased to present to you our 2025 Ethics and Compliance Report. We recognise that ethical conduct is crucial to our operations. It protects the integrity of our business, safeguards the interests of our employees and partners, and underpins the value we deliver to our customers, shareholders and the communities where we operate.

Our Ethics and Compliance Programme is designed to deliver this Group-wide commitment and supports responsible and ethical decision-making at every level of the business.

Last year, we announced that the US Department of Justice (DOJ) ended our two monitorships approximately one year early, following an assessment of the facts and circumstances of our case. This was an important milestone for the Group and is the culmination of extensive efforts over the last number of years to develop and implement the Programme and make cultural, governance and control enhancements.

During the monitorships, we undertook significant work to constructively engage with the monitors and to further enhance our Programme.

In May 2025, following her dedicated efforts as Head of the Monitorship Liaison team, Nicola Leigh took over as our Head of Compliance.

The Board and senior management are focused on ensuring we uphold responsible business practices and maintain an effective compliance programme. We remain committed to continuous improvement and ensuring that our Programme is fit for purpose, particularly given the complex geopolitical environment in which we are currently operating.

Through continued engagement, communications and targeted training, we continue to promote awareness across different levels of the organisation. We also place continued emphasis on fostering a culture where our employees feel empowered to act with integrity and to speak up when they have concerns.

We are grateful to our colleagues and stakeholders for their constructive efforts during this past year and we look forward to your continued engagement on these important topics.

Kalidas Madhavpeddi
Chairman

Gary Nagle
Chief Executive Officer

General Counsel and Head of Compliance annual overview



Shaun Teichner
General Counsel

Nicola Leigh
Head of Compliance

We are committed to maintaining a robust, risk-based Programme that is tailored to our business

In 2025, we focused on ensuring that our Programme is operating efficiently and consistently and that it is appropriately tailored to our business needs. At the beginning of the year, our work was primarily focused on the monitorship process and completion of the second review period. Following the conclusion of the monitorships in March 2025, we concentrated our efforts on positioning our Programme for continued maturity and long-term sustainability. We have engaged actively with the Board and senior leadership throughout the organisation regarding our vision for the Programme and post monitorship priorities.

At the same time, while we believe we now have a mature programme, we recognise that it will not remain effective if it is static and that continuous improvement is required to support ongoing risk mitigation. The compliance landscape is also very dynamic, particularly in the current complex geopolitical environment, and an effective compliance programme needs to evolve in response to ongoing developments.

We have therefore used the monitors' observations, and our own continued analysis, to identify areas of improvement and assess ongoing effectiveness. There are many aspects of the Programme that have been in place for a number of years and we have been able to analyse and assess how the Programme is operating in practice. Through these continuing efforts, we have identified several opportunities to enhance our existing processes and have continued to implement targeted improvements and refinements.

Organisational structure

In 2025, we reviewed the operating model and team structure across our corporate compliance and regional compliance teams and strategically realigned certain areas to enhance oversight and increase consistency in approach. We believe that these changes make our teams more efficient and focused and will allow us to better support our business with tailored advice.

Leveraging technology

In both our marketing and industrial businesses we are making significant additional investments in systems that are aimed at improving consistency and efficiency, enhancing data quality, oversight and improving our overall control environment.

We have substantially completed the implementation of our trade and e-comms surveillance systems in our marketing departments which are designed to detect and alert us of potential market manipulation. We have also automated our vessel-related compliance processes by implementing a business-accessible list of approved vessels across the Group and automating ongoing sanctions screening.

Our teams continue to explore further ways to leverage technology, automation and build out systems controls where appropriate. This includes ongoing work enhancing existing platforms and migrating to new platforms for certain of our processes and controls, for example in relation to know your counterparty (KYC) and third party due diligence and management (TPDDM).

Risk assessments

Our risk assessments are designed to identify, record and evaluate compliance risks faced by our marketing and industrial businesses. In 2025, we initiated a comprehensive redesign of our compliance risk assessment

General Counsel and Head of Compliance annual overview *continued*

process at both Group and local levels to help ensure that our Programme is appropriately designed and tailored to respond to the compliance risks across our operations. As part of the redesign, we refined our risk categorisation to better reflect the nature of our compliance risks and support a more consistent and comparable approach to risk assessments across the Group. We also enhanced our processes to guide regional teams through structured and consistent assessments to determine the underlying activities that drive compliance risks, likelihood of occurrence and the potential consequences of these risks. Regional teams must then evaluate the effectiveness of the controls in place to mitigate the risks identified and implement appropriate corrective action if any critical controls are determined to not be operating effectively. This approach is designed to enhance consistency, transparency and responsiveness and ultimately helps us to proactively assess the effectiveness of our controls on a continuous basis.

Compliance policy architecture

The development, implementation and review of our Group policies, standards, procedures and guidelines remains an important element of our Programme. Last year, we initiated a comprehensive review of our Compliance documents to identify opportunities for improvement. Key updates were made to a number of documents and processes. These updates reflect our efforts to clarify requirements for a more efficient and consistent application across the business. For example, we implemented certain updates to our Travel, Gifts and Entertainment Standard to provide clearer guidance on home-country restrictions and simplify processes related to employee expenses and pre-approvals. We also reviewed our third party payment processes in marketing and industrial assets.

As part of this work, we conducted a risk assessment to evaluate the requirements in both documents, established more centralised approval processes and simplified onboarding documentation. These changes seek to refine processes while maintaining a focus on mitigating the underlying risks.

During 2025, we also advanced our KYC and TPDDM processes, which are critical controls in our Programme. This review confirmed that our requirements remain largely fit for purpose, reflecting the maturity of our Programme, but also identified areas that could benefit from further refinement. For example, we introduced a new Community Investment Due Diligence and Management Procedure (CIDDM Procedure). This had previously been captured as part of our Third Party Due Diligence Management Procedure, however we separated this into a standalone document to cater for the nuances around community investments and enable us to adopt a more risk-based, proportionate approach to the compliance due diligence of community investments.

Monitoring

We also began a redesign of our monitoring activities, transitioning to a more proactive, continuous compliance monitoring model, intended to enhance early issue identification, improve real-time support and use data more comprehensively. Key features of this model include a refocused monitoring team, the reallocation of traditional audit testing to our Group Internal Audit and Assurance function (GIAA), enhanced collaboration with regional compliance to support more timely and informed follow-up, and redesigned, streamlined processes to provide clearer task allocation.

As part of this transition, we are piloting the redesigned model within selected SAP environments from Q2 2026, under which the Risk Assessment and Monitoring team

develops risk indicators and dashboards, Regional Compliance performs risk-based follow-ups, and outcomes are centrally recorded, providing a scalable framework to progressively expand monitoring across systems and business areas.

In addition to this monitoring work, GIAA has continued to conduct reviews of elements of the Programme, with two such reviews occurring in 2025. One review focused on the local implementation of our Programme, with a detailed assessment at five different locations. The other review focused on the Group Market Conduct Surveillance Programme, with a detailed assessment conducted at nine different offices in scope of our trade and communications surveillance requirements.

Speaking openly and raising concerns

We continue to focus on speaking openly and raising concerns as a key element to support an open culture where employees feel comfortable raising concerns. This is integral to the successful implementation of our Programme. We have continued to promote the Raising Concerns Programme (RCP) and the various reporting channels we offer through a number of different means, including a refresh of RCP materials and posters, as well as the launch of a new Speaking Openly Hub on our intranet, which provides more details and guidance on what concerns to raise and how they should be raised. These materials are designed to encourage engagement and include real life examples and insights into how investigations are conducted.

We have also continued to invest in systems to support the RCP such as upgrading our Group reporting platform, leading to a more seamless experience for reporters, and improving the quality of information we receive to ensure appropriate action can be taken. Furthermore, we have advanced our capabilities in terms of analysing RCP data

to help us identify trends and highlight potential risks by leveraging Power BI and making relevant dashboards available to key stakeholders.

Further, we have increased Group oversight for concerns raised locally by implementing quarterly sample testing of concerns raised and increasing engagement with the departments and other local stakeholders.

These enhancements enable us to determine where additional focus or better controls may be required within our Programme.

Looking forward

Overall, we are proud of the progress that we have made this year and remain firmly committed to maintaining our Programme and ensuring that our people, systems and processes operate effectively. The progress outlined in this report reflects the continued effort across our organisation to embed responsible practices and to learn from our experiences and challenges we have faced.

We are confident that the actions we are taking position us to effectively manage our risks and build long-term trust with our stakeholders. We thank our teams for their ongoing dedication as we continue to advance our Programme.

Shaun Teichner
General Counsel

Nicola Leigh
Head of Compliance

Ethics and compliance at a glance

Under the process set out in our Joint Ventures, Mergers and Acquisitions, and Disposals Procedure we reviewed and approved¹

17
new joint ventures

2
M&A transactions

9
disposals

Approved and active third parties that we continue to monitor in our third-party due diligence programme

438
in our marketing business

1,611
in our industrial business

Rejected third parties²

0
in our marketing business

2
in our industrial business

New conflicts of interest declarations received

1,690
for 1,540 of these, a management action plan was created or they were in the process of being reviewed and signed off.

Know your counterparty approved for

4,776
marketing counterparties

12,096
industrial asset counterparties

Know your counterparty rejected for²

15
marketing counterparties

21
industrial asset counterparties

Raising Concerns Programme

697
reports were recorded through the Raising Concerns Programme, the majority of which were HR-related concerns.

798
reports were closed, 311 of which were protected concerns within the scope of the Programme and capable of investigation.

Of the 311 protected concerns investigated, 45% were either substantiated or partially substantiated, and 97% of protected concerns substantiated or partially substantiated resulted in at least one recommendation for remedial action.³

Of the substantiated concerns related to business integrity, the majority related to conflicts of interest. Refer to page 29 for further detail.

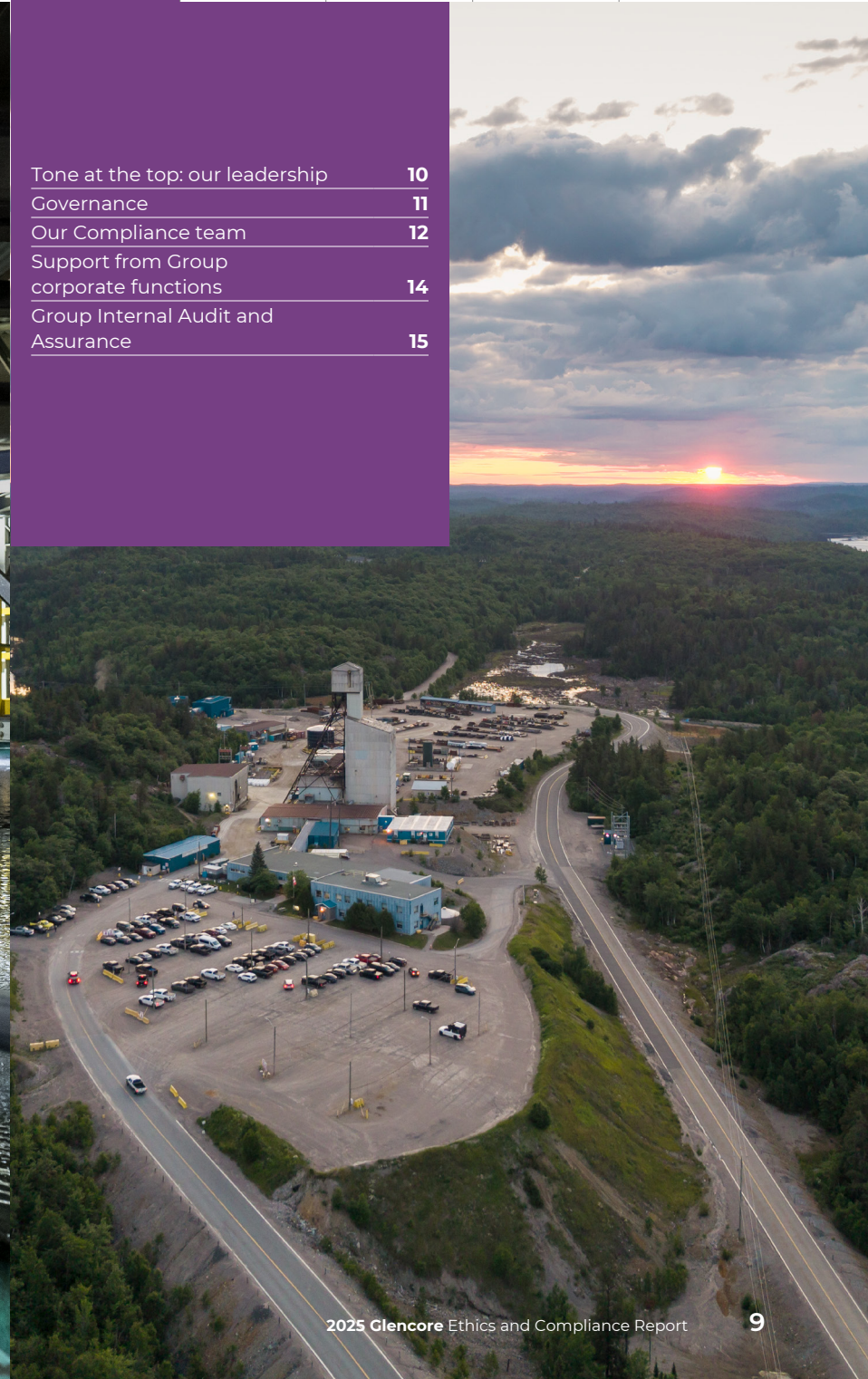
Number of Code of Conduct e-learnings completed

40,000+

1. Further internal approvals may be required following approval by Compliance, figures therefore may not correspond to the number of transactions implemented.
 2. This reflects rejections for compliance reasons following completion of the onboarding process. It does not reflect rejections where, following engagement between Compliance and the business, the onboarding process was not completed.
 3. Examples of remedial actions include improvements to policies and procedures, safety measures, implementation of IT systems and controls, vendor blocklisting, dismissals and warnings. Remedial actions may be recommended even in cases where the protected concern is not substantiated or partially substantiated.

Governance and structure

Tone at the top: our leadership	10
Governance	11
Our Compliance team	12
Support from Group corporate functions	14
Group Internal Audit and Assurance	15



Tone at the top: our leadership

Our commitment to ethics and compliance starts at the top with our Board of Directors and senior management.

Board engagement

Our Board bears ultimate responsibility for the implementation of a compliance programme that reflects our Values and strategic direction, is proportionate to our risk profile, appropriately resourced and effective in practice.

Our Board also plays a critical role in overseeing and assessing our culture of ethics and compliance and ensuring policies, practices and behaviours are consistent with our Values.

All new Non-Executive Directors receive an onboarding with the Head of Compliance, covering our Programme, compliance risks and the Board's oversight role for ethics, compliance and culture.

Key activities and responsibilities of the Board include:

- receiving quarterly updates on whistleblowing and investigation processes as well as material investigations;
- participating in annual training, which covers topics such as the Board's role, our key compliance risks and developments in ethics and compliance requirements and expectations; and
- promoting and enhancing our culture of ethics and compliance.

The Board's Ethics, Compliance and Culture (ECC) Committee comprises four independent Non-Executive Directors and is chaired by Cynthia Carroll. The ECC Committee receives quarterly updates on the Programme, including with regard to risk assessments and compliance resources.

The Board has designated workforce engagement directors who conduct engagement around key ethics and compliance topics and collect feedback on our Programme. Non-Executive Directors also play an important role in promoting a culture of integrity and have an opportunity to collect feedback during their site visits.

A typical visit to an industrial asset includes a tour of the facility and discussions with local management as to challenges and opportunities. It also includes a session with a cross-section of workers without management present to encourage the workers and Non-Executive Directors to freely and openly ask questions of each

other. In addition to meeting with the local CEO, the Board members have private meetings with other members of the local management team and other key stakeholders such as the local CFO, external audit partner, a team member from internal audit and assurance and the health, safety, environment, social performance and human rights (HSEC&HR), human resources and legal and compliance leads.

In 2025, the Board undertook site visits to EVR in Canada, as well as to our oil, ferroalloys and coal assets in South Africa.

Senior management

Our senior management team also plays a key role in outlining our expectations with regard to ethics and integrity across the Group. Individual members of senior management work to embed ethical considerations into decision-making processes and day-to-day activities. Together with the Board, they are collectively responsible for ensuring that the initiatives of our Programme are effectively cascaded across all levels of the organisation.

Senior leaders promote ongoing changes to our Programme by actively supporting their implementation led by different teams and overseeing initiatives within their respective areas of responsibility.



“Workforce engagement is key to achieving our overall strategy and maintaining a strong culture.”

Cynthia Carroll
Chair of the ECC Committee

Governance

Leadership commitment to ethics and compliance is critical and we seek to embed it and reinforce it at all levels of management.

Compliance governance by the Board and management

Board

Board oversight is provided through the Board directly, in respect of whistleblowing and investigation processes, and through the ECC Committee and Audit Committee.

ECC Committee

Responsible for overseeing the Programme and approving key ethics, compliance and culture-related matters within the Group. Comprises at least two members, all of whom must be Non-Executive Directors appointed by the Board. The committee currently comprises Cynthia Carroll (Chair), Gill Marcus, Liz Hewitt and María Margarita Zuleta.

The Head of Compliance has a dotted reporting line to the ECC Committee, meets regularly with the Chair of the ECC Committee and is afforded the opportunity to meet with the ECC Committee without the rest of the management team being present.

Audit Committee

Reviews Glencore's financial and risk management systems. Comprises at least three Non-Executive Directors, all of whom shall be independent and at least one of whom shall have the appropriate professional qualifications and recent and relevant financial experience. The Committee currently comprises Liz Hewitt (Chair), Martin Gilbert and Gill Marcus.

Management

Our Programme governance is supported by three management-level committees, namely the Environmental, Social and Governance Committee (ESG) Committee, the Business Approval Committee (BAC), which is a sub-committee of the ESG Committee, and the Raising Concerns and Investigations Committee (RCIC).

ESG Committee

Reviews and considers various ESG matters, programmes and projects implemented across the Group. It also reviews and approves Group policies and key standards and procedures.

Comprises Glencore's CEO, CFO, COO, General Counsel, Head of Compliance, Head of Corporate Affairs, Head of Human Resources, Head of HSEC&HR and Head of Sustainability. It also includes other senior members of department management representing marketing and industrial assets across different commodities.

BAC

Determines and sets guidance and criteria and reviews business relationships, transactions and counterparties that may give rise to ethical or reputational concerns.

Comprises Glencore's CEO, CFO, General Counsel, Head of Corporate Affairs, Head of Sustainability, Head of Compliance and, where applicable, heads of departments and corporate functions involved in the matter being considered by the BAC.

RCIC

Oversees the operation of our Raising Concerns Programme and the conduct of investigations, and is tasked with ensuring recommendations and sanctions are applied consistently across the Group.

Comprises Glencore's CEO, CFO, General Counsel, COO, Head of Human Resources and Head of Compliance.



Refer to our *Corporate governance* section in the 2025 Annual Report beginning on page 85 for further information.

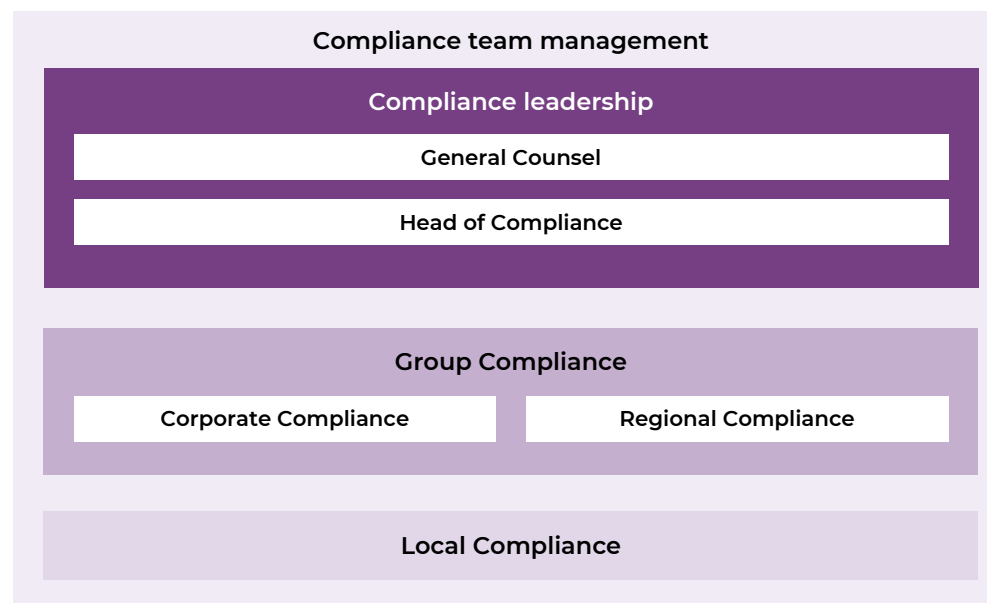
Our Compliance team

Our Compliance team designs, develops and monitors the effectiveness of our Programme.

The team is made up of full-time corporate, regional and local teams.

Regional and local team members are assigned to cover different assets and offices across our global network. Some team members cover assets and offices across multiple departments, while others may cover a single complex industrial asset, which may itself comprise multiple industrial sites.

We also have a network of local compliance contacts that support the Compliance function with compliance messaging. Local compliance contacts are appointed in lower risk jurisdictions or smaller offices or assets, where a full-time local or regional compliance person on the ground is not required. A list of compliance contacts is published on the office or industrial asset's local intranet site, or communicated via other means, such as email announcements. Compliance contacts receive tailored training regarding their role.



Compliance leadership

General Counsel

- Reports to the CEO
- Attends Board meetings and its Audit, ECC and HSEC Committee meetings
- Chairs the ESG Committee and the RCIC and is a member of the BAC
- Oversees the Raising Concerns Programme and associated investigations and updates the Board on these matters, together with the Head of Human Resources and the Head of Compliance

Head of Compliance

- Reports to the General Counsel
- Has a dotted reporting line to the ECC Committee and attends meetings of the ECC and Audit Committee, as well as the updates to the Board on the Raising Concerns Programme and associated investigations
- Member of the ESG Committee, the RCIC and the BAC
- Oversees Group Compliance and manages our Programme
- Informs the Board and senior management on our Programme's progress and obtains their support for key Compliance policies, standards and procedures

Corporate Compliance

- Responsible for designing, monitoring and continuously improving our Programme
- Based at our headquarters in Baar, Switzerland, in our principal marketing offices in London, New York, Beijing and Singapore, as well as certain other offices in our global network
- Includes subject matter experts (SMEs) for each of our key compliance risks and teams covering the Programme's different elements
- Provides guidance and advice to regional and local compliance teams and the business on implementing our Programme consistently across the business

Regional Compliance

- Responsible for the effective implementation and management of the Programme at offices and industrial assets directly or indirectly controlled or operated by Glencore across all regions in which we operate
- Provides guidance and advice to local compliance teams and the business in the regions, with support and guidance from the Corporate Compliance team

Local Compliance

- Consists of local compliance officers, full-time employees who drive the on-the-ground implementation of our Programme
- Local compliance contacts further act as an on-the-ground point of contact across our global network

Our Compliance team *continued*

Our Compliance team spans our global footprint

The geographic coverage of our Compliance function has been determined based on:

1. the risks presented by various businesses and geographies around the world; and
2. the level and nature of business activity in a particular country of operation.

As part of our commitment to embedding and evolving our Programme, we continuously assess corporate, regional and local resourcing and make adjustments as necessary, particularly in response to changes in our risk footprint and the growth of our business. In 2025, we concluded a number of key projects and strategically realigned the Compliance team in certain areas to optimise resource deployment. We believe that this will help us maintain a robust, centralised and consistent approach to compliance while allowing our regional and local teams to deliver targeted, on-the-ground support.



Support from Group corporate functions

Compliance must operate with sufficient resources and independence to credibly implement the Programme across the Group. Compliance cannot, however, operate in a vacuum.

Compliance collaborates closely with other Group corporate functions, including Corporate Affairs, Human Resources, Legal, HSEC&HR, Sustainability, Finance, Information Technology (IT) and Group Internal Audit and Assurance (GIAA).

Each corporate function, as a compliance stakeholder, plays a key role in the Programme's success. The heads of these corporate functions are responsible for supporting the implementation of the Programme and the compliance activities within their respective areas. This collaborative approach fosters a shared sense of ownership and accountability, helping to embed compliance throughout the organisation.

Corporate Affairs

- Promotes the Programme through external and employee communications across the Group, including in the form of employee-focused campaigns related to policies, speaking openly and other compliance initiatives

Sustainability

- Collaborates with Compliance on responsible sourcing initiatives by jointly sharing platforms and using screening tools, sharing data on counterparties and helping to align KYC and supply chain due diligence processes across the Group

Finance

- Shares responsibility with Compliance for developing, implementing and overseeing certain important Group standards that mitigate both financial and compliance risks

Legal

- Advises Compliance on legal issues relevant to different aspects of the Programme
- Works in close collaboration with Compliance on a variety of initiatives and implementation processes
- Includes the Raising Concerns and Investigations team, which manages our whistleblowing and investigations processes, including the Raising Concerns Programme

IT

- Provides access to a wide range of IT tools and systems and helps to identify potential risks and ensure Group-wide systems and controls are in place

HSEC&HR

- Collaborates with Compliance on human rights risks as well as security issues at our industrial assets
- Engages with Compliance on due diligence processes for our direct social contribution partners and any further necessary checks or processes for the implementation of social contribution projects, in accordance with our internal procedures

Human Resources

- Inputs into various incentive and discipline approaches which emphasise the importance of a commitment to our Values, Code and our Programme
- Promotes a strong culture of accountability by working to attract, motivate and retain a dedicated workforce
- Oversees consistent reference and background-checking requirements, with screening levels aligned to the seniority and inherent risk of the role

Group Internal Audit and Assurance

GIAA's mandate is to provide the Board and senior management with independent and objective assurance over the effectiveness of governance, risk management and control processes. This includes assessing the implementation and embeddedness of relevant aspects of the Programme across the Group.

GIAA audits specific elements of the Programme and undertakes broader assessments of compliance risks across the organisation. Some audit scopes include a range of compliance controls and processes at a particular office or industrial asset while others may focus on a particular control or process across the Group. GIAA does not rely on, but coordinates with, Group Compliance in its audit and assurance activities.

Each year, the GIAA audit plan is developed through top-down discussions with senior management and Group Compliance to obtain their input on high-risk areas, including compliance risks, together with bottom-up independent risk assessments of the audit and assurance universe, which is GIAA's view of Glencore's risks across the organisation. This process includes an assessment of ethics and compliance risks and informs the inclusion of relevant Programme elements in the audit plan. The audit plan is presented to and approved by the Board.

Following each engagement, GIAA prepares a written report containing the audit results and findings. The GIAA reports related to the Programme are reported to the Head of Compliance, as well as to senior management. GIAA also presents a summary of its audit engagement results at the quarterly Audit Committee meetings. Relevant topics regarding the Programme are also presented to the ECC Committee.

In 2025, audits related to compliance included an assessment of:

- the Group Market Conduct Surveillance Programme; and
- the local implementation of the Programme.

The audit of the Group Market Conduct Surveillance Programme assessed the effectiveness of surveillance system rule sets designed to identify potential market abuse. The review covered 12 trade surveillance rule sets applied across 169 order books, together with 23 electronic communications surveillance rule sets used across the marketing offices in scope. The audit also examined 60 trade alerts and 45 communications alerts generated during the audit period to assess how alerts were reviewed, escalated and resolved.

The audit of the local implementation of the Programme covered 118 relevant controls, together with a review of 70 newly onboarded counterparties and 185 transactions across the locations in scope of this audit.

GIAA also performed three targeted reviews to verify closure of previously identified compliance findings. In addition to these specific compliance audits, GIAA may also review compliance controls in other audits, which may lead to additional observations, opportunities for improvements and findings.

During 2025, GIAA performed 20 audit engagements that included coverage of compliance-related risks. These comprised:

2

audits focused on specific elements of the Programme, covering multiple sites

3

targeted reviews to verify the remediation of previously identified compliance-related findings

15

audit assessments of compliance-related risks within business activities

Group Internal Audit and Assurance *continued*

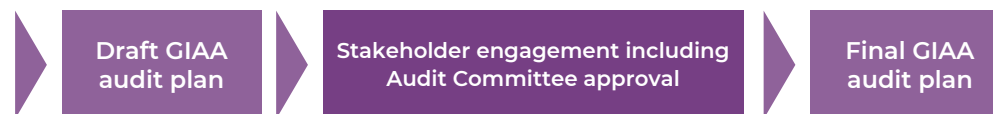
GIAA planning process overview:



Why is the top-down process important?

The top-down planning process enables GIAA to:

- link the audit plan to the strategic direction and priorities of Glencore;
- obtain input from key stakeholders to inform the audit plan; and
- consider how external factors may impact the audit plan including market hot topics, industry events and emerging risks.



Why is the bottom-up process important?

The bottom-up planning process enables GIAA to:

- link the audit plan with the outcomes of our assurance universe, independent risk assessment and coverage cycles; and
- identify assurance coverage required by industry standards, regulations, legislation and/or policies.

Our Programme



The Glencore Ethics and Compliance Programme	18
Risk assessments	19
Policies, standards, procedures and guidelines	20
Training and awareness	23
Advice	25
Monitoring	26
Speaking openly and raising concerns	27
Discipline and incentives	30



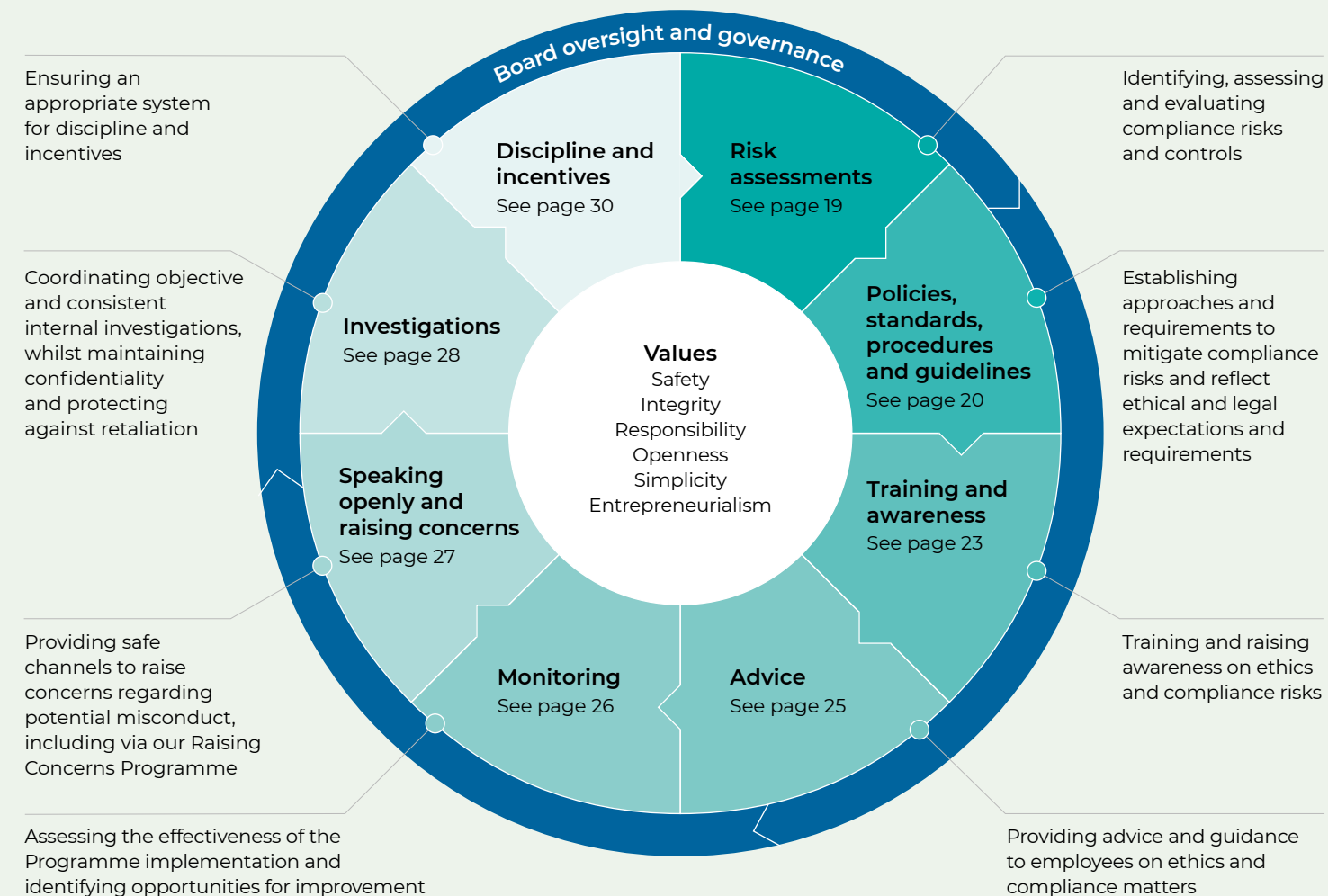
The Glencore Ethics and Compliance Programme

Our Programme includes various elements related to risk assessments, policies, standards, procedures and guidelines, training and awareness, advice, monitoring, speaking openly and raising concerns, investigations, and discipline and incentives.

Dedicated compliance IT systems and data analytics as well as various controls embedded in business systems support our Programme. The key elements of our Programme establish a risk-based approach to ethics and compliance to address the challenges presented by our diverse business operations. Together, the elements create a feedback loop, designed to ensure that compliance risks are identified and addressed across our business on an ongoing basis.

Our Programme has been designed with the support of external counsel and other advisors, having regard to the guidance from relevant authorities such as the US Department of Justice, the UK Ministry of Justice and the State Secretariat for Economic Affairs of Switzerland.

Key elements of our Programme



Risk assessments

As part of our efforts to ensure our Programme is appropriately designed and tailored to our business, and that resources are adequately allocated, we identify, record and evaluate compliance risks faced by our marketing and industrial businesses.

The Corporate Compliance Risk Assessment and Monitoring team conducts an annual Group compliance risk assessment which reviews current compliance risks in a number of different areas taking into account the nature of our business and the geographies in which we operate. We document these risks in the Group Compliance Risk Register to ensure they are up to date and relevant, and we assess whether new risks need to be added. The Group compliance risk assessment process also identifies whether existing policies, standards, procedures, guidelines and training, as well as compliance resources and skillsets, effectively address current or any newly identified risk(s).

The Group Compliance Risk Register is reviewed and updated on an annual basis to determine whether the risks remain appropriate and whether there have been any changes in the activities of the Group or the industry that might impact our view of the risks and how they may arise.

In addition to the Group compliance risk assessment, we assess our identified compliance risks in each of our offices and industrial assets across the Group. Regional compliance officers (RCOs), with the assistance and support of local compliance, conduct these local risk assessments using the Compliance Risk Register as a basis to evaluate the inherent risks that exist, assess the overall effectiveness of the controls in place to mitigate those risks, evaluate residual risks, and implement planned controls in the event that existing controls require improvement. In 2025, we completed 78 local risk assessments.

Update to the Group's compliance risk assessment process

In 2025, we initiated a comprehensive redesign of our compliance risk assessment process at both Group and local levels to help ensure that our Programme is appropriately designed and tailored to respond to the compliance risks across our business.

Historically, our Compliance Risk Register comprised numerous different areas of compliance risks as well as business activities that could present a risk to our business. We have now refined our risk categorisation to focus on the risks themselves rather than the business activities that can contribute to these risks.

Our updated Compliance Risk Register includes a comprehensive set of 15 compliance risks, each supported by a precise risk statement to better reflect the nature of our compliance risks and support a more consistent and comparable approach to risk assessments across the Group. The business activities, which include matters such as entering into a joint venture, lobbying and procurement, inform our updated approach to assessing these risks and are captured through responses to our newly introduced smart questionnaires. The update to our Compliance Risk Register allows us to capture a consistent and dynamic inventory of risk-driving activities that can be updated at any time. If a new activity emerges in our business, regional and local teams can promptly assess its potential relevance and impact.

The smart questionnaires are supported by algorithmic models to guide regional teams through a structured and consistent assessment which helps to determine:

- whether a risk applies to a particular office or industrial asset based on its activities;
- the likelihood of occurrence, considering external benchmarks (e.g., the Corruption Perception Index), relevant business activities and past occurrences; and
- the potential consequences of the risk.

Once inherent risk assessments are completed, regional teams are required to evaluate the effectiveness of the controls that are designed to mitigate the risks identified. Critical controls, such as those outlined in the Third Party Due Diligence and Management Procedure and KYC requirements, are essential to managing compliance risk. If the regional team

determines that a critical control is not operating effectively, the team is required to design and implement an appropriate corrective action.

The new categorisation approach and smart questionnaires were successfully integrated into our compliance management system, with the redesigned Local Compliance Risk Assessment process commencing in April 2026. This enables regional compliance teams to apply these enhanced tools to conduct their local risk assessments going forward.

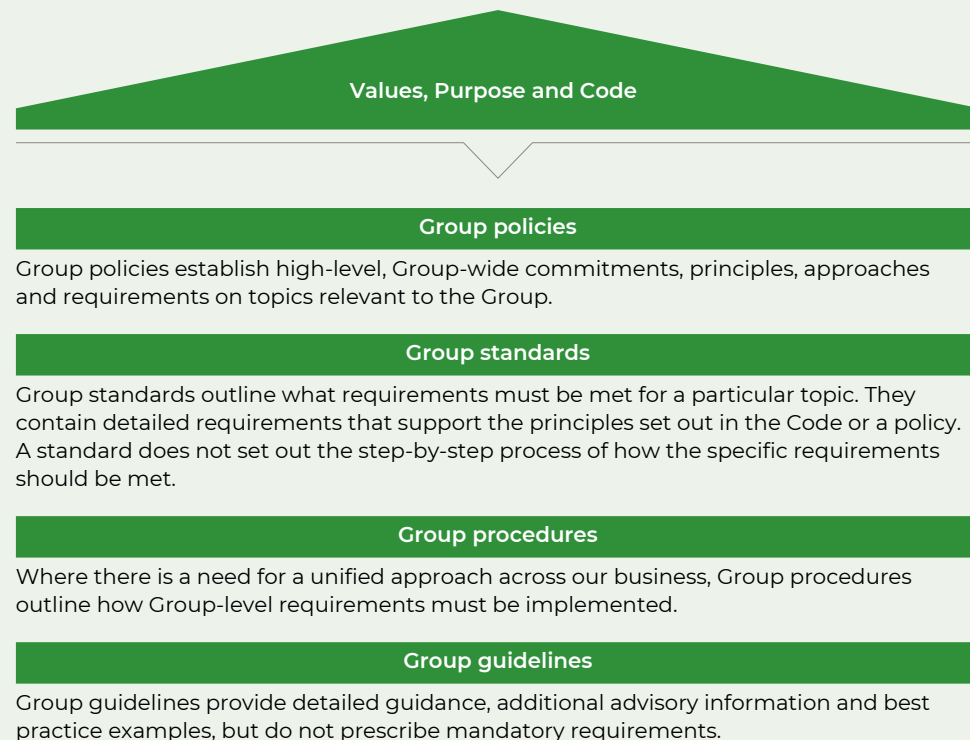
In 2026, as part of the risk assessment redesign, we will also launch a centralised management action plan (MAP) module to help centralise tracking of remediation actions and consolidate actions arising from Glencore's combined assurance activities and risk assessments into a central repository. This will support RCOs by replacing regional action plans and other tools, and is designed to reduce administrative burden, increase efficiency and strengthen follow up processes.

This strengthened risk assessment framework helps ensure that our Programme remains robust, forward-looking and fit for the complexities of our business and the use of an algorithmic model allows for new activities within our business to have their compliance risk assessed promptly. It is designed to enhance consistency, transparency and responsiveness and ultimately helps us to proactively manage our compliance risks on a continuous basis.

Policies, standards, procedures and guidelines

Our Group policy architecture encompasses our Purpose, Values, Code and a suite of policies, standards, procedures and guidelines on various key matters and risks. These are issued in accordance with the Group policy framework.

Group policy architecture



Our Purpose is to responsibly source the commodities that advance everyday life. This is reflected in our Values – Safety, Integrity, Responsibility, Openness, Simplicity and Entrepreneurialism.

Our Code seeks to ensure that our Values are reflected in Glencore's daily activities and culture. In our Code, we lay out our commitments and expectations on a range of topics, including how we treat our people, operate safely and responsibly, act with integrity, and protect our assets and information. Our Group policies support the delivery of our Values and Code, which together detail the behaviour and performance expectations for all employees working at our offices and industrial assets where we have operational control. Through our Group standards, procedures and guidelines, we seek to establish and implement consistent standards and processes across our business to support responsible and ethical business practices.

Our employees, directors and officers, as well as contractors under Glencore's direct supervision, working for a Glencore office or industrial asset directly or indirectly controlled or operated by Glencore worldwide, must comply with requirements outlined in our policy architecture, as well as applicable laws and regulations.

New Glencore employees who have access to a work computer must confirm they have read, understood and will abide by our Code and key Group Compliance policies, standards, procedures and guidelines relevant to their role.

Policies, standards, procedures and guidelines *continued*

Additionally, all Glencore employees are required to annually confirm they have read, understood and will comply with Glencore's Values, our Code and key Group policies.

Corporate Compliance is responsible for developing, reviewing and rolling out documents within the Group compliance suite in accordance with the requirements of our Group policy architecture.

Given the different structure and organisation between our marketing and industrial activities, Corporate Compliance issues different types of documents for the different parts of the business. In doing so, the different levels of risk, which are generally higher for marketing activities, are also taken into account.

For activities which are run in a more centralised manner using similar systems and processes, or in circumstances where there is a major compliance risk that requires a consistent Group-wide approach across all of our activities, Corporate Compliance generally issues Group Compliance procedures that set out a more detailed process and specific steps that need to be taken. Corporate Compliance may also issue Group Compliance standards which set out minimum requirements but provide some flexibility to develop and implement tailored local procedures.

Our offices and industrial assets are responsible for implementing Group Compliance policies, standards, procedures and guidelines. When required, they are also responsible for developing and implementing local procedures to address local risks and requirements. Due to the diverse nature of our business, we have a number of local procedures that outline how our different offices and assets implement these requirements to meet Group policies and standards.

Some offices or industrial assets may determine that a local variation of a Group Compliance document is required to include stricter requirements or additional obligations.

For any requested deviations from a Group Compliance policy, standard, procedure or other minimum requirement, an office or industrial asset must document the deviation request and obtain approval from the Head of Compliance.

Documents outlining our internal compliance processes and the operations of the Compliance team are accessible on our Compliance intranet page and ensure that both new and current Compliance employees have a road map for the implementation of various aspects of our Programme.

Developing and reviewing our policies, standards, procedures and guidelines

The annual Group Compliance risk assessment process analyses whether the risks identified and listed in the Group Compliance Risk Register are appropriately addressed by our Group Compliance policies, standards, procedures or guidelines, and whether there is a need to introduce new documents or amend existing ones.

In addition, existing Group Compliance documents are subject to periodic reviews in line with our policy governance three-year review cycle. Certain documents may be subject to more frequent reviews if deemed appropriate.

Any new Group Compliance document or a material amendment to existing Group Compliance documents, must be approved by the Head of Compliance before being submitted for approval to the ESG Committee, where required. The Board approves all of our Group policies.

Group Compliance standards, procedures and guidelines are generally translated as needed, depending on the scope, the nature of the document and the language capabilities of the intended audience.



Our policies are publicly available on our website: [glencore.com/who-we-are/policies](https://www.glencore.com/who-we-are/policies)

Policies, standards, procedures and guidelines *continued*

The Group policy governance suite supporting the Programme includes the following policies, standards, procedures and guidelines.

	Policies	Anti-Corruption and Bribery	Anti-Money Laundering	Competition Law Policy	Conflict of Interest	Fraud	
		Information Governance	Market Conduct	Raising Concerns and Whistleblowing Policy	Sanctions		
	Standards	Communications and Device	Data Protection	Know Your Counterparty – Industrial Assets	Protected Concerns Management and Investigation Standard	Travel, Gifts and Entertainment	
	Procedures	Anti-Boycott (US/Non-US Entities)	Benchmarks and Price Reporting Agencies	Benchmark Trading Rationales	Community Investment Due Diligence and Management Procedure	Conflict of Interest Management	Corporate Protected Concerns Management and Investigation Procedure
		Joint Ventures, Mergers and Acquisitions and Disposals	Know Your Counterparty – Marketing	Mandatory Compliance Training Escalation and Discipline	Ongoing Screening	Personal Account Dealing	Position Limits
		Russia Transactions	Sanctions Insulation	Third Party Due Diligence and Management	Third Party Payment – Industrial Assets	Third Party Payment – Marketing	Uncleared Derivatives and Investment Advice
	Guidelines	Benchmarks and Price Reporting Agencies	Commodity Department Protected Concern Management Guideline	Competition Law: Dealing with Competition Law in Merger and Acquisition Transactions	Competition Law Guideline: Dealing with Competitors		
		Competition Law Guideline: Dealing with Suppliers, Customers and Agents	Competition Law Guideline: Human Resources and Employment Considerations	Data Protection	Fronting/Sleeving		
		Inside Information	LME Lending Rules	Market Manipulation	Payments and In-Kind Assistance to Public Officials, Government Institutions and State-Owned Entities	Sanctions	

Training and awareness

Training and awareness provides a practical understanding of how compliance risks materialise across the organisation and encourages active engagement on compliance topics.

Training

We have a comprehensive approach to training which focuses on effective planning and delivery of materials to the right audience. We track training completions, escalate non-completions and assess the overall effectiveness of different training initiatives.

In addition to the training available to our broader workforce, we provide further training and development opportunities for members of the Compliance team to increase their understanding of key compliance risks and important trends and developments. We encourage and fund participation in relevant conferences, lectures and webinars, where appropriate, and members of Group Compliance receive ad-hoc, targeted training in their areas of expertise and on relevant areas of the business. We also leverage external law firms and other professional advisers to provide ongoing knowledge sharing.

Each year, we develop a Compliance training and awareness planner (T&A planner). The T&A planner sets training and awareness priorities based on output from a range of sources, including the annual Group risk assessment and local risk assessments, advice which the business has sought from Compliance during the year, the results of post-training knowledge checks and training feedback surveys, internal audit findings, Raising Concerns reports and other lessons learned and relevant best practices. It also includes training and/or awareness materials on any new or materially updated policies, standards, procedures or guidelines. The T&A planner includes annual mandatory training for our high risk employees on certain topics.

Each office and industrial asset is required to develop its own local training plan, based on the T&A planner, reflecting that office or industrial asset's local risk assessment, lessons learned, local legal or regulatory changes or any other local circumstances. Training materials are made available to regional and local teams, with the expectation that the materials will be customised at a local level to include specific examples relevant to the local audience.

We recognise that each training session must be tailored to its specific audience to be effective. We have a process for assigning training to employees, based on their compliance risk rating which will depend on their function or role. We regularly seek to measure the effectiveness of our compliance training and awareness activities for example by asking employees to complete short post-training or awareness feedback surveys.

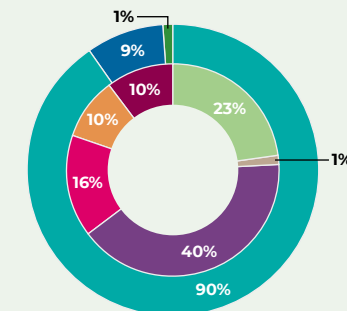
All networked employees have access to e-learning materials which cover the Code and conflicts of interest. We also develop materials to be used to train front-line employees on how to declare a conflict of interest. We raise awareness among our employees on fraud in various trainings, including our annual Code of Conduct e-learning and in-person trainings.

We actively monitor mandatory compliance training non-completions and take them seriously. Compliance escalates non-completions of trainings. Employees who repeatedly, without an extenuating circumstance, fail to attend training may be subject to disciplinary action. Compliance training non-completions are also taken into consideration when assessing an employee's end-of-year performance.

Code of Conduct training

40,000+

99% completion rate



Covers: Glencore's expectations on how to do business safely, responsibly, ethically and legally.

Breakdown by organisation type

- Industrial asset
- Marketing office
- Corporate office

Breakdown by region

- Africa
- Asia
- Australia
- Europe and FSU
- Latin America
- North America

Note: audience includes employees and contractors who either a) have regular access to a work computer or b) are given access to a work computer for purposes of training completion.

Training and awareness *continued*

Awareness

We supplement our compliance training with awareness initiatives and communications throughout the year. This allows us to communicate compliance updates in an accessible manner and equip our employees with useful tools to remain abreast of relevant guidance and the latest developments in the Programme.

While tone from the top is key, we understand that most employees interact with middle management. The compliance teams work with middle management to help them deliver appropriate messaging on ethics and compliance risks applicable to their businesses. This can include compliance messaging during townhalls and other employee engagement activities and introducing or co-presenting compliance trainings.

2025 highlights

Deal lifecycle training

In 2025, we delivered an integrated, scenario-based training to around 500 of our high-risk employees in key marketing offices, highlighting red flags across the different stages of the deal lifecycle and how to mitigate and escalate them. This training covered various compliance risks including bribery and corruption, conflict of interest and sanctions and was designed to reflect the reality of how compliance risks arise and evolve in the commodity trading business. We delivered a similar training highlighting red flags across different compliance risks applicable to different industrial assets to around 1,500 of our high-risk employees in multiple jurisdictions.

In addition, our high-risk marketing employees also received training covering our market conduct framework, including recent enforcement trends and lessons learned. This training was tailored to address both paper and physical trading, using real-life scenarios to explain different types of market manipulation.



Advice

Advice is a key element of our Programme, as the Compliance team provides the business with valuable guidance to navigate complex compliance matters and to act in accordance with our Code and policies.

Our compliance officers are professionals with compliance, legal and audit backgrounds, who have expertise in areas relating to our key compliance risks. Due to the fast-paced nature of our business, they are required to respond quickly and effectively. They guide the business on changes in laws and regulations and advise on conducting business in compliance with these evolving requirements as well as our policies, standards, procedures and guidelines.

Members of the business and other colleagues can contact regional or local compliance as well as the Corporate Compliance team with their queries. These teams have a broad range of expertise and knowledge of our business, which enables them to provide comprehensive advice on key compliance risks within our business. This strengthens the synergy and cooperation between the Compliance function and the business, enabling a collaborative partnership to help ensure we act with integrity and in accordance with our policies, standards, procedures and the law.



Monitoring

We continuously monitor the implementation of our Programme to assess its effectiveness and ensure it remains effectively implemented across our business. Monitoring helps us to identify opportunities for improvement and to adapt to changes in our operations, the environments in which we operate, and applicable laws and regulations.

Evolving our approach to compliance monitoring

Historically, the Risk Assessment and Monitoring team was established to assess the implementation of our Programme, measure its effectiveness and identify opportunities for improvement. Monitoring was performed through a combination of site reviews and desktop reviews.

Site reviews involved visits to our offices and industrial assets to assess the effective implementation of our Programme.

Desktop reviews included Corporate Compliance thematic reviews and data analytics projects. Corporate Compliance reviews assessed the design and operating effectiveness of centralised Compliance processes, systems and controls. Data analytics projects included analysis of Group systems and platforms accessible centrally by the Risk Assessment and Monitoring team, focusing on business transactions, parties and processes with an elevated compliance risk. The purpose of this monitoring was to identify activities that may violate Group requirements and assess the effectiveness of, and adherence to, existing or new compliance processes and controls.

These projects involved the development and use of risk indicators aimed at monitoring compliance risks. Risk indicators were modelled through interactions with commodity departments and other relevant corporate functions. These indicators enabled the Risk Assessment and Monitoring team to identify and sample transactions flagged as high-risk from a compliance perspective. These transactions were then subject to targeted review of underlying documentation, with testing results and observations

summarised in compliance monitoring reports and used to inform the discussion on opportunities for improvement.

The two complementary types of indicators used are key risk indicators (KRIs) and trigger alerts (TAs). KRIs highlight transactions that may present elevated compliance risk and help detect outliers, trends and emerging risks. Examples of KRIs include:

- unusual commercial margins;
- payments involving non-contractual third parties;
- transactions containing sensitive keywords; and
- travel or entertainment expenses involving public officials.

TAs are more targeted indicators that flag specific transactions that may require clarification or additional context. A TA does not imply wrongdoing, rather, it signals that a transaction may require further review. Examples of TAs include:

- cash on hand payments above defined thresholds;
- payments made before due diligence is completed;
- vendors or customers onboarded after invoices are issued; and
- donations or sponsorships above country-specific limits.

In 2025, we initiated a redesign of our monitoring activities to better reflect the maturity of the Programme. This includes transitioning to a continuous compliance monitoring model to enhance early issue identification, improve real-time support and undertake a more comprehensive use of data.

Key features of the evolving model include:

- a refocused monitoring team combining compliance expertise, data analytics and risk assessment capabilities;
- a reallocation of traditional audit testing, including the Corporate Compliance thematic reviews from the Risk Assessment and Monitoring team to Group Internal Audit and Assurance (GIAA);
- enhanced collaboration with regional compliance, supporting a more timely and informed follow-up; and
- redesigned and streamlined processes enabling clearer task allocation.

In connection with the update of our model, we have also enhanced our use of risk indicators across the Group's financial and trading systems and platforms.

The updated continuous monitoring model will be piloted within selected SAP environments. Under the new model the Risk Assessment and Monitoring team will continue to develop and maintain the trigger alerts and dashboards. The Regional Compliance teams will review the output applying their knowledge of the local businesses to prioritise areas of follow up focusing on unusual, high risk or unexpected transactions. Any outcome will be recorded centrally to support consistency, tracking and follow up actions.

When identified, follow-up areas include potential control gaps, additional controls may be designed and implemented to strengthen our Programme. The model is designed to be scalable and will be progressively expanded across systems and business areas.

Speaking openly and raising concerns

A critical element of an effective compliance programme is having a culture in which our people feel comfortable raising concerns, knowing they will be properly addressed or investigated, and that appropriate action will be taken.

We expect our employees and contractors to speak openly and require them to report any concerns regarding breaches of our Code, our policies, or the law, whether those relate to themselves or others. We also expect them to report any breaches of requirements in procedures. We encourage our employees and contractors to first raise concerns with their managers or supervisors as they are usually best equipped to resolve concerns quickly and effectively.

However, we recognise that for some concerns they may not always feel comfortable speaking with a manager or supervisor. Therefore, we offer a number of formal channels for whistleblowers to raise concerns. Whistleblowers have the option of reaching out to whistleblowing contacts, who are nominated by Glencore offices and industrial assets. Whistleblowing contacts are regularly trained on the requirements of their role, and must affirmatively confirm they understand their role and responsibilities.

Group Raising Concerns Programme channels

If a concern remains unresolved or a whistleblower is uncomfortable using local channels, concerns can also be reported via the Group Raising Concerns Programme (RCP) channels, our corporate whistleblowing programme managed from our headquarters in Baar, Switzerland, by the Raising Concerns and Investigations (RCI) team.

These channels allow whistleblowers to raise concerns anonymously in a variety of languages, by internet, voicemail or phone (for most of the countries where we operate). Contact details are available on the platform's website and on posters at our offices and industrial assets.

Raising Concerns and Whistleblowing Framework

We have a comprehensive suite of documents which establish a framework for managing concerns raised, including our Raising Concerns and Whistleblowing Policy. This policy explains the process for reporting, escalating, investigating and remedying concerns, and makes clear that retaliation is absolutely prohibited, regardless of whether the reported concern is ultimately substantiated.

All concerns are taken seriously and handled promptly, using an objective, fact-based rationale.

Protected Concerns Management and Investigation Standard and Procedures

Our Protected Concerns Management and Investigation Standard sets out the minimum requirements applicable to the classification, tracking and reporting of concerns received through local reporting channels or the Group RCP channels in a manner consistent with our Raising Concerns and Whistleblowing Policy. This intake process is critical and we have sought to ensure that we have a nuanced, sophisticated and consistent process, which is run by experienced professionals with senior oversight.

Classification takes into account factors such as:

- the seniority of those involved in the alleged breach;
- the potential consequences of the breach; and
- whether the conduct is ongoing, systemic or deliberate.

In certain cases, a single factor may be sufficient to support the classification of a concern, but in other instances a combination of factors may be relevant.

The classification of the concern determines how it will be managed and investigated. Concerns classified as low and medium are generally investigated by the relevant commodity department with oversight by the RCI team, whilst concerns classified as high are handled directly by the RCI team.

The minimum requirements of the Protected Concerns Management and Investigation Standard are implemented through procedures both at the corporate

Do what's right Tell us what's wrong

You are required to report any concerns regarding breaches of our Code of Conduct, policies or the law, whether these relate to yourself or others.

You will not face retaliation, and you can report anonymously.



Here's what you can do:

- 1) Speak openly with your manager or supervisor.
- 2) Reach out to a local Whistleblowing Contact.
- 3) If unresolved or you feel uncomfortable using local channels, visit <https://glencore.raisingconcerns.org> or scan the QR code to the right.



RAISING CONCERNS

GLENCORE

In 2025, we continued to focus on speaking openly and raising concerns as a key element to support an open culture where employees feel comfortable raising concerns.

level, for the intake process of reports raised via the Group RCP channels and investigations by corporate teams, and at the local level, for the intake process of reports raised via local reporting channels and investigations conducted locally. If a concern is received at the local level and classified as high, it is required to be reported to the corporate RCI team as soon as possible (ideally within 24 hours). Local concerns administrators who run the assessment process for locally raised concerns are trained by the RCI team.

Speaking openly and raising concerns *continued*

Corporate oversight and pattern analysis

The RCI team, through a case management system, carefully tracks concerns raised through the Group RCP channels, or otherwise escalated to them, to confirm whether they have been investigated and closed out within the RCP case management system, including any related remediation. The RCI team also conducts sample-based review and assurance activities on concerns raised through local whistleblowing channels which are also tracked through a centralised case management system.

We seek to analyse the data arising from the RCP in order to identify any potential trends and areas where specific focus will be required. We look at the number, nature and severity of the concerns raised, as well as the department and geography. We carefully monitor the time taken to review and classify reports received, close investigations, as well as substantiation rates. We further periodically assess the robustness of our whistleblowing programme using external benchmarks and third party data.

We provide quarterly updates on the RCP to management through the ESG Committee and the RCIC. The Board also receives quarterly updates.

In 2025, we continued to invest in systems to support the RCP, such as upgrading our Group reporting platform, leading to a more seamless experience for reporters and improving the quality of information we receive to ensure appropriate action can be taken. Furthermore, we have advanced our capabilities in terms of analysing data to help us identify trends and highlight potential risks by leveraging Power BI and making relevant dashboards available to key stakeholders. We have also increased Group oversight for concerns raised locally by implementing quarterly sample testing and increasing engagement with the departments and other local stakeholders.

Promoting a culture of speaking openly

We continue to actively promote our various reporting channels, including the Group RCP channels. Our ongoing global focus on 'speaking openly' reinforces our commitment to an open culture where employees feel comfortable raising concerns – something that is integral to the successful implementation of our Code.

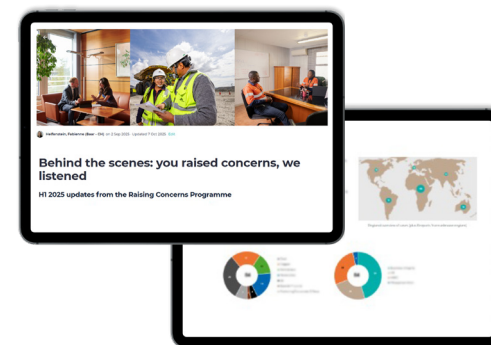
We use a wide range of materials to promote awareness, including posters, videos and talking points for managers. All of these materials have been refreshed in 2025

and we have published a new Speaking Openly Hub on our intranet providing more guidance on what to raise where and more information on the investigation process and our commitment to non-retaliation. We also share data on the concerns received and anonymised case studies to illustrate how our RCP works in practice.

Investigations

Our Protected Concerns Management and Investigation Standard seeks to ensure that investigations are performed consistently and effectively. It also sets out the importance of protecting the confidentiality of information relating to an investigation. The standard is implemented through procedures, both at the corporate level for investigations conducted by corporate teams (including the RCI, Human Resources and GIAA teams) and the local level for investigations conducted locally. The standard includes a template investigation procedure for locally led investigations. The standard permits modification of the template to account for local nuances, as long as these revisions remain consistent with the requirements of our Raising Concerns and Whistleblowing Policy.

The RCI team provides training to case owners and lead investigators on how to



conduct investigations into concerns in a manner that is consistent with our standard and procedures. It is essential that investigators are trained on the requirements and investigation skills before embarking on any investigation, and that they follow the necessary steps during their investigations. Throughout 2025, the RCI team continued to run a combination of scheduled trainings, as well as ad-hoc trainings for newly appointed investigators.

High-severity concerns

The following are illustrative examples of compliance-related allegations or concerns that would typically be classified as high severity and investigated by, or under the oversight of, the RCI team.

Bribing a public official, whether through cash payments or other means, such as gifts or entertainment, contributions to political parties or charitable donations

Trades, orders or behaviour that may constitute insider trading, market abuse or market manipulation, including attempts, whether successful or not

Violating competition laws

Violating sanctions laws

Participating in money laundering

Using inside information to deal in Glencore/other publicly traded securities

Participating in a billing or payroll scheme or skimming or stealing Glencore cash or property, particularly where the amount is significant, or the scheme involves senior employees

Manipulating company accounts so that assets or liabilities appear overstated or understated

Committing sexual assault, regardless of seniority

Engaging in unlawful discrimination, workplace harassment, or bullying by senior employees

Speaking openly and raising concerns *continued*

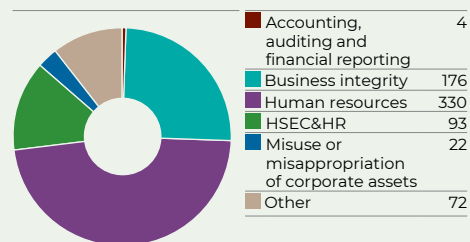
Raising Concerns Programme data

In 2025, the Raising Concerns Programme recorded

697

reports (excluding SPAM)
(2024: 735)

Type of report

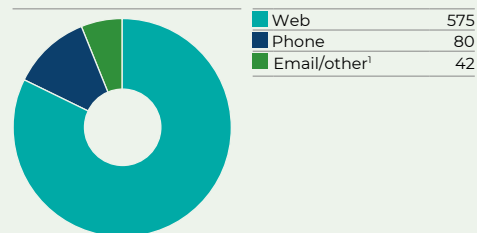


Raised anonymously

71%

(2024: 73%)

Raised via



1. Other includes direct contact with senior management, Legal or Compliance or locally raised concerns escalated to the Group

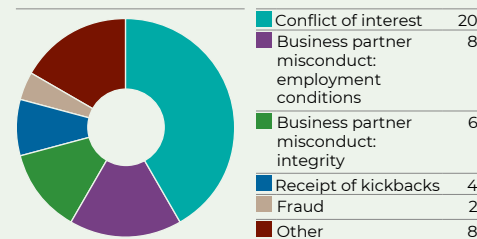
Reports closed during 2025

798

with 311 reports that were assessed as falling within the scope of the RCP, i.e., constituting protected concerns, and closed following an investigation as either substantiated, partially substantiated or not substantiated (2024: 353). These 311 reports related to 248 distinct protected concerns as the same protected concern may be raised in multiple reports. The remainder of the 487 reports were closed as outside the scope of the RCP, an issue for management action, a work-related grievance, or as not capable of investigation based on the available information.

45% of the 248 protected concerns were either substantiated or partially substantiated (2024: 48%). Of these reports, 48 related to business integrity concerns and were split across the following categories:

Type of report (business integrity)



77% of the 798 reports closed were received in 2025, with these reports taking an average of

28

days to close.

In 2025, 97% of protected concerns substantiated or partially substantiated resulted in at least one recommendation for remedial action. Examples of remedial actions include improvements to policies and procedures, safety measures, implementation or enhancements of controls, additional training, action with regard to contractors or disciplinary action in relation to employees (e.g., termination or warning). At least one disciplinary outcome was present in 44% of protected concerns investigated and closed as substantiated or partially substantiated. Disciplinary action is not taken in all cases where concerns are substantiated as the concerns may not relate to employee misconduct or the relevant employee(s) may have already left the company.

Locally raised concerns data

For 2025,

183

reports raised through local whistleblowing channels were assessed as protected concerns and recorded in our central database, and

274

such protected concerns were closed following investigation.



Follow the link to our Raising Concerns and Whistleblowing Policy.

Note: Reports closed during the year may include concerns raised in prior periods.

Discipline and incentives

We expect all employees to uphold our Values, adhere to our Code of Conduct and comply with the requirements set out in our policies and procedures, regardless of their role or location. Non-compliance with these expectations may lead to disciplinary action, including dismissal.

Measuring and incentivising the behaviour of our most senior leaders

Our senior leaders play a critical role in shaping the cultural tone of the organisation, with their behaviour serving as a key driver of our compliance culture. The performance of the senior leaders in our corporate functions, marketing departments and industrial assets is assessed through a comprehensive annual review process. The review specifically considers their behaviour, including their contribution to our commitment to acting responsibly and with integrity, and is taken into account in determining compensation outcomes.

Their compensation may be higher or lower based on an assessment of their behaviour, with strong leadership in support of our Programme being grounds for higher compensation.

The partnership between Human Resources and Compliance is a key feature of our Programme and we regularly collaborate to produce policies, procedures and other materials for the business. For example, the Mandatory Compliance Training Escalation and Discipline Procedure is a joint procedure, created and managed by both departments. This procedure sets out a mandatory compliance training roll-out, reminder, escalation and disciplinary process designed to ensure employees are abiding by their training requirements.

Creating clarity and consistency of disciplinary outcomes across the organisation

Disciplinary expectations are governed through our Group standards and outline our approach to managing conduct across the organisation. While we seek to establish a consistent global approach to discipline, these standards reinforce departmental ownership and accountability while supporting alignment with local legislative requirements.

We continue to clarify expectations across the organisation and take appropriate action where concerns are substantiated. Our approach is intended to ensure issues are resolved at the appropriate level while serious matters, including sexual harassment, serious misconduct or business integrity breaches, are escalated to senior management. This approach underpins our strong focus on compliance and associated behaviours.



Key risks

Introduction	32
Anti-corruption and bribery	33
Conflicts of interest	35
Fraud	36
Sanctions and trade controls	37
Anti-money laundering	39
Competition law	39
Market conduct	40
Data protection	41



Introduction

Our Programme addresses the following key topics:

- Anti-corruption and bribery
- Conflicts of interest
- Fraud
- Sanctions and trade controls
- Anti-money laundering
- Competition law
- Market conduct
- Data protection

Glencore is exposed to a wide range of compliance risks across its operations, including in relation to corruption and bribery, conflicts of interest, fraud, sanctions and trade controls, money laundering, competition law, market conduct and data protection. To address these risks, the Programme includes a set of policies, standards, procedures and guidelines, as well as internal Compliance manuals.

Several other policies, standards and procedures which support our Programme are issued by corporate functions other than Group Compliance.



Our policies are publicly available on our website: <https://www.glencore.com/who-we-are/policies>.



Anti-corruption and bribery

Our Anti-Corruption and Bribery Policy is clear: the offering, providing, authorising, requesting or accepting of bribes is unacceptable, and we do not engage in corruption or bribery, including making facilitation payments. We assess corruption risk within our businesses and work to address these risks through policies, standards, procedures and guidelines on various topics.

Political contributions

We do not contribute any of our funds or resources to any political campaign, political party, political candidate or any politically affiliated organisation.

Political engagement

Although we do not directly participate in party politics, we do engage in policy debate on subjects of legitimate concern to our business, employees, customers, end users and the communities in which we operate. All officers, employees and persons who lobby on our behalf must comply with all relevant Glencore policy and procedural requirements and all applicable legislation (including, but not limited to, the laws and regulations relating to registration and reporting).

Political Engagement Policy

This policy, issued by Group Corporate Affairs, sets out our approach and general requirements in connection with our engagement in the political process, and our commitment to operate transparently and in line with our Values and our Code.

Political Engagement Procedure

This procedure, issued by Group Corporate Affairs, sets out the specific steps we take to ensure we comply with the requirements in our Political Engagement Policy.

Sponsorships and charitable contributions

We never make a sponsorship or charitable contribution in order to disguise a bribe, or to gain an improper business advantage.

We take measures to ensure that when we make sponsorships or charitable contributions we conduct risk-based due diligence and, when required, monitor the use of our funds or resources to ensure that is appropriate.

Community investments

We apply a risk-based approach to performing compliance due diligence on community investments. In 2025, we transitioned the coverage of community investments from the Third Party Due Diligence and Management Procedure into a dedicated standalone procedure to better align with the complexity of such investments and to cater for varying risk profiles. The new procedure sets out proportionate compliance due diligence and management requirements for community investments that enable us to identify and effectively mitigate the specific risks identified with individual community investments.

Travel, gifts and entertainment

We only provide and accept occasional, reasonable, appropriate and lawful travel, gifts and entertainment that satisfy the general principles of our Anti-Corruption and Bribery Policy and are not given or received with the intent or prospect of influencing the recipient's decision-making or other conduct.

We have requirements for the pre-approval of travel, gifts and entertainment based on localised thresholds, and additional requirements regarding public officials. Specifically, when providing travel, gifts and entertainment to public officials, employees are not permitted to exceed locally-defined thresholds and employees must obtain pre-approval for anything in excess of such thresholds from the relevant line manager or supervisor and Compliance.

Travel, Gifts and Entertainment Standard

In 2025, we updated our Travel, Gifts and Entertainment Standard to clarify requirements and streamline certain processes. Our Travel, Gifts and Entertainment

Standard requires offices and industrial assets to establish a local travel, gifts and entertainment procedure. The purpose of the standard is to:

- set out the requirements for providing and accepting travel, gifts and entertainment to include in the local procedures; and
- provide guidance on the application and interpretation of these requirements.

We use an AI-driven expense audit tool which is integrated with our expense management system to analyse expense report data and flag high-risk events for review and approval. For example, the tool analyses attendees listed as receiving travel, gifts or entertainment against publicly available sources and watchlists, as well as internal data, to determine whether an attendee is a public official. Any positive matches require compliance review and approval, to ensure the spend is within the applicable threshold.

We monitor the frequency of travel, gifts and entertainment given to public officials through a purpose-built Power BI dashboard, which retrieves data directly from our expense management system. The dashboard is dynamic, allowing Compliance to generate insights into employee expense activity over selected time periods. It also enables tracking of how frequently specific public officials are entertained, regardless of which employee is providing the entertainment. In addition, the dashboard flags inconsistencies where an individual is classified as a public official in one expense report but not in another.

Anti-corruption and bribery *continued*

Interactions with public officials

Dealings with public officials bring a higher risk of bribery and corruption, particularly in high-risk jurisdictions, so we are especially careful in our interactions with them.

Employees must report requests for inappropriate or illegal payments, favours, or unusual or suspicious requests by a public official to Compliance immediately.

Payments and In-Kind Assistance to Public Officials, Government Institutions and State-Owned Entities Guideline

In certain jurisdictions in which we operate, we are requested by public officials, government institutions or state-owned entities, to make payments and provide in-kind assistance, in particular with respect to ongoing arrangements. For example, in certain countries we are required to make payments to public security forces who are dedicated to securing our operations. This guideline helps us navigate our response to these types of requests and sets out the steps that Compliance employees should follow to ensure that we manage the corruption risks associated with these payments and assistance.

External engagements

Anti-corruption organisations

We are a member of the Partnering Against Corruption Initiative (PACI) whose members collaborate on collective action and share leading practice in organisational compliance. PACI has a commitment of zero tolerance to bribery and requires its members to implement practical and effective anti-corruption programmes.

Local communities

We recognise that as a large multinational company we have a significant influence in the regions where we operate, both through the employees and contractors that we employ, and through our substantial procurement spend and support for local communities. We therefore believe it is important that we support local anti-corruption and bribery efforts, by clearly communicating our commitment to responsible and ethical business practices and articulating the standards that we expect from our suppliers.

Transparency

We recognise the importance of having high standards of corporate governance and transparency and we seek to maintain long-term, open, transparent and constructive relationships and dialogue with our key stakeholders.



Follow the link to our Anti-Corruption and Bribery Policy.



Conflicts of interest

Our Conflict of Interest Policy requires that we always act in Glencore's best interests and that we try to avoid actual, potential or perceived conflicts of interest. We take steps to manage conflicts and reduce the risk they present.



Conflict of Interest Management Procedure

Our Conflict of Interest Management Procedure sets out the required steps to ensure that conflicts of interest are recorded and appropriately managed in a timely manner.

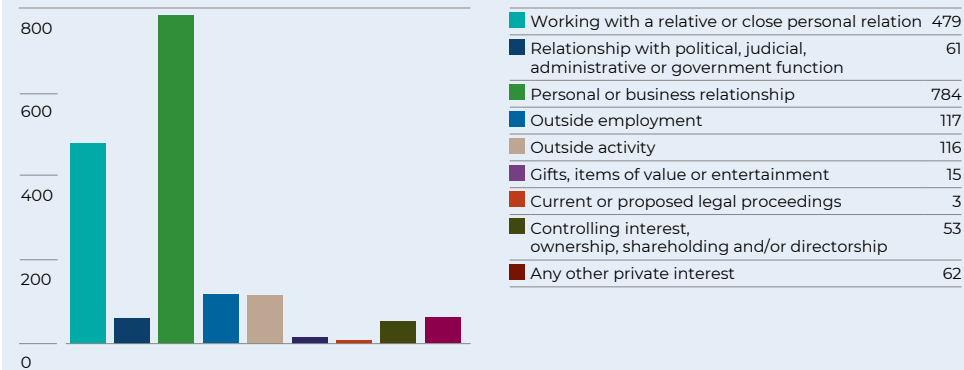
Compliance reviews the declaration to confirm whether a conflict exists and, if so, its type. If needed, Compliance requests additional information and assigns the declaration to the declarer's supervisor or manager.

Together with Compliance, the supervisor or manager develops a management action plan (MAP) to manage and mitigate the conflict. Compliance approves the MAP if it is sufficiently robust, or recommends changes where necessary. Once approved, the declarer and their supervisor or line manager are responsible for adhering to the MAP.

Employee onboarding

Human resources requires all candidates, at the outset of the recruitment process, to declare any actual or potential conflicts. Declarations are flagged to Compliance for review and further instructions. Additionally, the recruitment or secondment of current or former public officials is subject to Compliance's prior review and approval.

Conflict of interest declarations by type in 2025



In 2025 we had

1,690

(2024: 2,392)

new conflict of interest declarations, of which 150 were classified as not posing an actual, potential or perceived conflict.

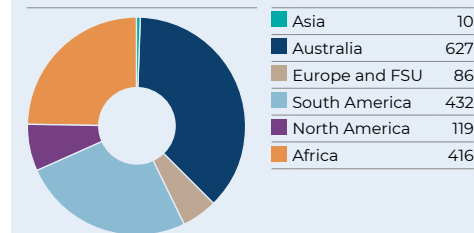
For the remaining

1,540

(2024: 2,216)

appropriate MAPs were created or were in the process of being reviewed and signed off.

Conflict of interest declarations by region in 2025



Follow the link to our Conflict of Interest Policy.

Fraud

Our Fraud Policy sets out our approach to prohibiting and preventing fraud, informs employees of the types of activities that are considered fraudulent, and sets out employees' obligations to prevent and report fraud.

We are committed to not engaging in fraudulent behaviour or knowingly assisting or facilitating any third party to commit fraud.

Due to the broad nature of the activities that can constitute fraud, the risk is managed by various corporate functions across the Group, including Legal and Finance, which implement relevant controls in their areas in order to mitigate the risk of fraud.

During 2025, we validated that our fraud risk management framework included reasonable procedures to prevent fraud in compliance with the Economic Crime and Corporate Transparency Act 2023.

Risk of fraud in fronting and sleeving arrangements

'Fronting and sleeving' refers to arrangements whereby a party is inserted as an intermediate trading counterparty in a trading chain or structure. This could involve inserting a third party into a transaction in which Glencore is the ultimate supplier or customer. Alternatively, it could be an arrangement where Glencore acts in such a capacity, sitting between two trading counterparties.

As per our Fraud Policy and Fronting and Sleeving Guideline, we have a general prohibition against dishonest and deceptive fronting or sleeving arrangements that are designed, intended to conceal, or have the effect of concealing Glencore's (or any other party's) involvement in a transaction or trading structure, even if such arrangement is legal, as it is contrary to our Code and Fraud Policy.

Our Fronting and Sleeving Guideline is particularly relevant to Glencore personnel in our offices who are engaged in market facing activities. It highlights the compliance risks associated with these types of arrangements and provides guidance on how to assess potential fronting or sleeving transactions and when employees must seek Compliance approval to ensure compliance with our Code and Fraud Policy.



Follow the link to our Fraud Policy.

Sanctions and trade controls

Our Sanctions Policy sets out our commitment to complying with all applicable sanctions and restrictive measures and we generally adhere to United States, European Union, United Nations and Swiss sanctions throughout our business, whether or not we are legally required to do so.

We do not participate in transactions designed or intended to evade or facilitate a breach of applicable sanctions or restrictive measures, and we do not:

- conduct business in, or involving any, embargoed territory or sanctions targets;
- conduct business that would violate any applicable anti-boycott laws, export controls, trade embargoes or any other sanctions or restrictive measures;
- conduct business with sectorally sanctioned entities, which is prohibited by or inconsistent with sanctions; or
- engage in any sanctionable activity that could result in the designation of Glencore as a sanctions target.

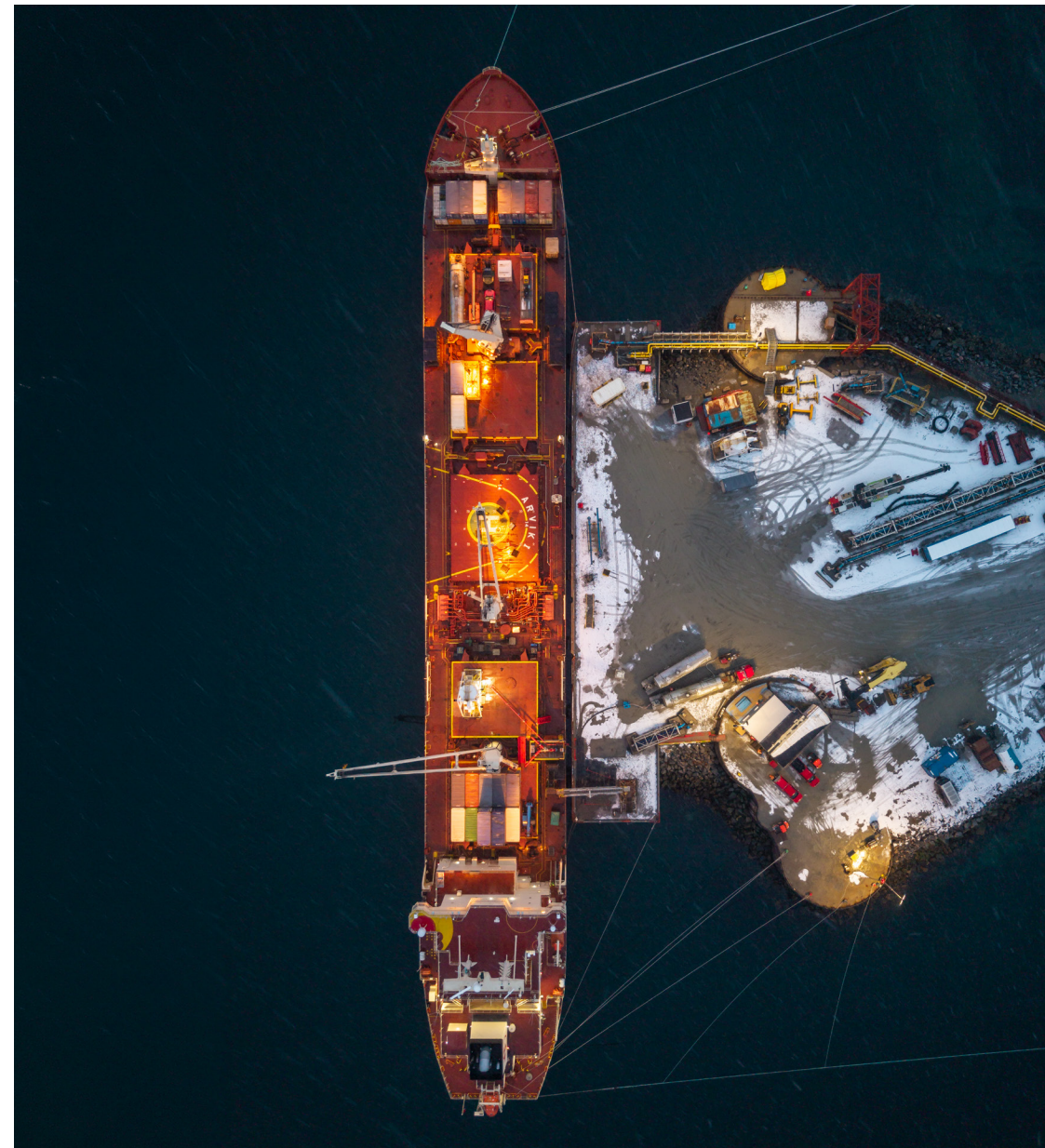
We only allow deviations from these requirements in exceptional circumstances with prior approval from Compliance and Group management and, under all circumstances, these deviations must be compliant with applicable laws.

To manage our sanctions risk exposure in our day-to-day activities and help ensure compliance, we implement a variety of controls and processes. Our sanctions risk mitigation framework covers a variety of topics and outlines the key steps and controls required to manage sanctions risks in our day-to-day activities.

Sanctions risk requirements are built into the lifecycle of our business interactions. The extent of our controls is designed to be proportionate to the level of risk incurred in connection with different types of transactions and counterparties.

We conduct screening before onboarding and during the continued relationship with a counterparty. Screening is performed on a continuous basis rather than being treated as a one-time requirement, so that we can respond quickly if a counterparty's status or risk profile changes. We assess transactions up front, and conduct appropriate due diligence on our counterparties and vessels, using a risk-based approach, to determine whether they are a sanctions target, subject to sectoral sanctions, or otherwise attract sanctions risk, and continue to review them as the business activity progresses.

We also regularly monitor updates from relevant sanctions authorities and use internal escalation requirements to ensure sanctions risks are handled in a timely manner. In parallel, we promptly review any ongoing transactions and relationships recorded in our internal reference data or watchlists that may be impacted by relevant



Sanctions and trade controls *continued*

sanctions updates. Operational controls are embedded in our trading systems and workflows so that higher-risk activities, whether relating to certain counterparties, sensitive locations or restricted products, are automatically flagged or blocked and, where appropriate, routed for additional review.

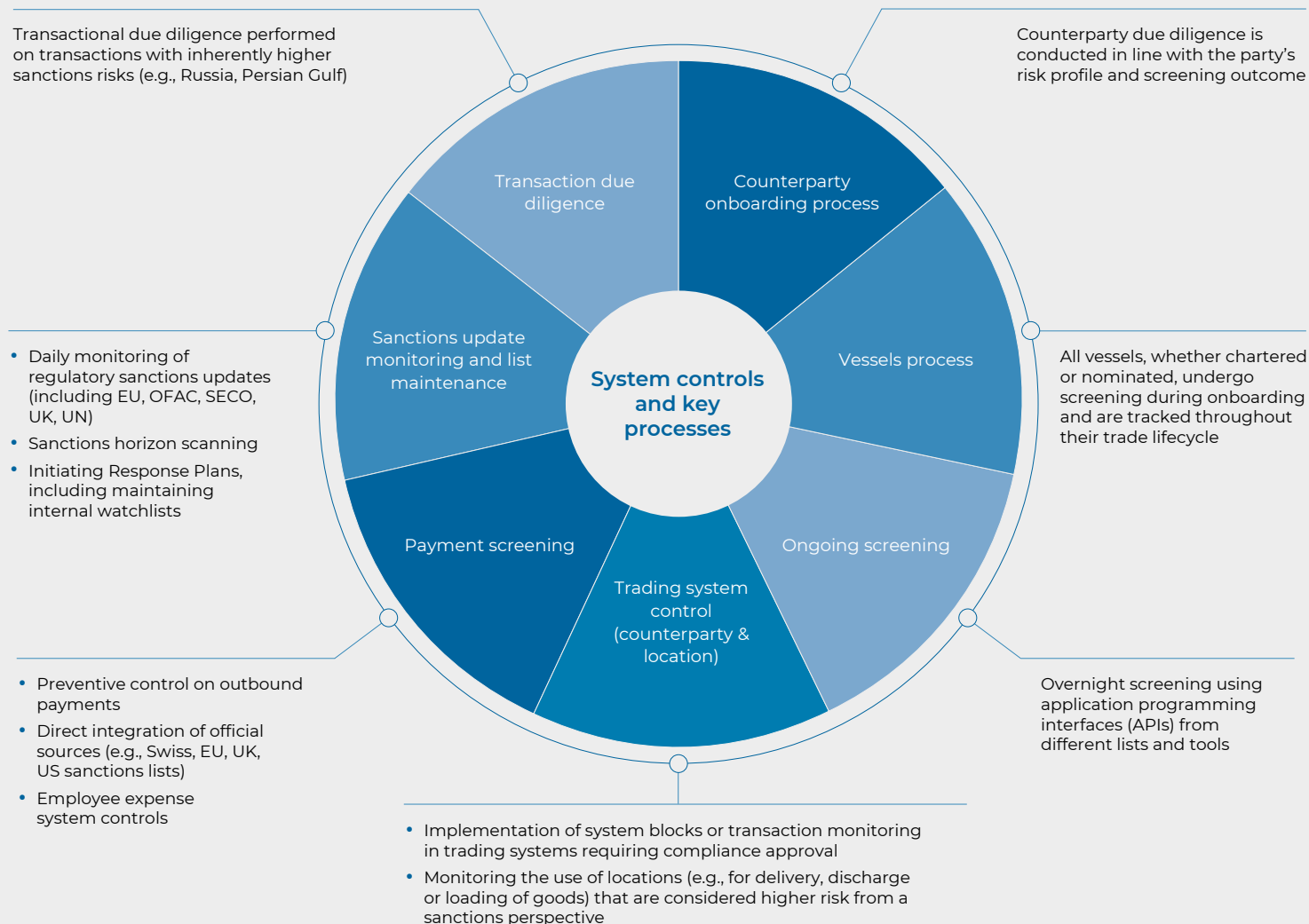
Additionally, higher scrutiny is conducted on transactions entailing a heightened sanctions risk, and payments are screened against internal and external watchlists and checked by Compliance before approval to mitigate the likelihood of unnecessary blocks at the processing level. Overall, these measures combine preventative controls with detective controls, supporting us to identify and halt prohibited activity before it takes place.

We continually assess ways to improve and streamline these processes. For example, in 2025 we automated our vessel-related compliance processes by implementing a business-accessible list of approved vessels across the Group. If a vessel is not on the list, approval can be requested via a ticketing system that automatically screens the vessel and escalates to Compliance and/or Responsible Sourcing if any red flags are identified. Where no red flags are identified, the vessel is automatically approved. Following approval, the vessel is subject to ongoing screening, a profile is created in our master database to enable use in trading systems, and the vessel is added to the approved list. Rejected vessels are automatically removed from ongoing screening, the master database and the approved list.



Follow the link to our Sanctions Policy.

Sanctions continuous monitoring controls and processes



Anti-money laundering

Our Anti-Money Laundering Policy sets out our approach to ensuring that we comply with all applicable laws and regulations to prevent money laundering and the facilitation of tax evasion, and appropriately manage the related risks.

Particularly:

- we are aware of the risk of third parties exploiting us to engage in money laundering;
- we do not knowingly assist, support, participate in or permit money laundering or terrorist financing;
- we do not accept money or other assets if we know or suspect that they derive from any kind of criminal activity;
- we do not knowingly deal with criminals, suspected criminals or the proceeds of crime;
- we do not facilitate the acquisition, ownership or control of criminal proceeds or other assets deriving from criminal activity, nor do we assist others in concealing criminal proceeds or assets; and



Follow the link to our Anti-Money Laundering Policy.

- we do not tolerate tax evasion of any kind and we do not knowingly or wilfully facilitate tax evasion.

Furthermore, our Tax Policy sets out our approach to taxation and to the management and control of our tax affairs. It also sets out the general framework within which Glencore operates when considering tax-related issues.

To manage our money laundering risk exposure and ensure compliance, we implement a number of controls and processes including, but not restricted to, payments to and from third parties.

Third party payment procedures – marketing and industrial assets

In 2025, we reviewed and updated our Third Party Payment Procedure – Marketing and converted the Third Party Payment Standard – Industrial Assets into a procedure. These two procedures are tailored to the risk profiles of the respective business segments and set out the steps on how to:

- perform due diligence on non-contractual parties who want to make or receive payments instead of our contractual counterparty;
- identify red flags in third party payment structures; and
- document acceptable payments to non-contractual counterparties, and under the marketing procedure, acceptable payments from non-contractual parties.

Competition law

Our Competition Law Policy sets out our approach to competing vigorously, but fairly and legally.

We do not engage in collusion and we don't agree with our competitors, formally or informally, to:

- fix prices;
- limit production or supply;
- allocate customers or markets;
- rig bids; and
- collectively boycott customers or suppliers.

To help employees apply our Competition Law Policy in practice, we also provide guidelines to address common competition law risks and outline practical guidance:

- Dealing with Competitors Guideline: this guideline provides detailed guidance on the key competition law risks employees need to be aware of when dealing with our competitors;

- Dealing with Suppliers, Customers and Agents Guideline: this guideline provides detailed guidance on the key competition law risks we need to be aware of when dealing with suppliers, customers and agents;
- Dealing with Competition Law in Merger and Acquisition Transactions Guideline: this guideline provides detailed guidance on the key competition law risks we need to be aware of when involved in merger and acquisition (M&A) transactions; and
- Human Resources and Employment Considerations Guideline: this guideline provides detailed guidance on key competition law risks in the human resources environment, in particular with respect to agreements between companies that compete for talent.

Risks related to competition law are overseen by the Group Legal team, with support from Compliance.



Follow the link to our Competition Law Policy.

Market conduct

Our market conduct compliance framework is centred on our Market Conduct Policy, which articulates our expectations of our employees with respect to market conduct issues.

Glencore operates in different jurisdictions and trades on both regulated markets and over the counter, in both commodity derivatives and physical commodities. We are committed to complying with all applicable laws, regulations and rules related to Glencore's activities and behaviour in the physical and commodity derivative or related financial markets.

Trading in specific markets, regardless of where we are located, means we are subject to the rules of that market and the regulatory authorities who oversee it. We adhere to global market conduct regulations such as the Market Abuse Regulation, the Markets in Financial Instruments Directive 2014 (MIFID II), the Commodity Exchange Act, and the Financial Market Infrastructure Act.

In addition, different trading venues (such as the London Metal Exchange, Chicago Mercantile Exchange, ICE Futures Europe and US) have their own rules with which we must also comply (e.g., position limits and prohibitions on wash trades).

In addition to our Market Conduct Policy, we have multiple procedures which are particularly relevant to employees in our offices who are engaged in market-facing activities. These procedures include:

- our Personal Account Dealing Procedure, which sets out the requirements applicable to personal trading in physical commodities or derivatives;
- our Benchmark Trading Rationale Procedure, which sets out the rules relating to documenting the rationale related to trading decisions when active in benchmark windows;

- position limit procedures for specific oil derivatives and related contracts that establish a framework to ensure we consistently adhere to the rules and regulations set forth by trading venues and relevant authorities, including exchange-imposed position limits; and
- benchmark and price reporting desk procedures, which set out the list of trained individuals approved to communicate with price reporting agencies and define the restrictions on such communications.

We additionally have three main underlying guidelines, which are also particularly relevant to employees in our offices who are engaged in market-facing activities:

- our Market Manipulation Guideline, which provides guidance and examples regarding different types of market manipulation as outlined in the Market Conduct Policy;
- our Inside Information Guideline, which provides detailed guidance on how to comply with prohibitions on engaging in insider dealing in commodities; and
- our Benchmarks and Price Reporting Agencies Guideline, which sets out the steps we take regarding our interactions with price reporting agencies in order to manage the risk of benchmark manipulation.

Market Conduct Surveillance Programme

Our Market Conduct Surveillance Programme aims to detect potential areas of market abuse and includes both trade and e-communications surveillance which leverage advanced data analytics and AI to monitor marketing activity in near real time. In 2025, we continued to significantly invest in and develop our Market Conduct Surveillance Programme. Significant progress was made in addressing identified areas of improvement in trade surveillance and we expanded coverage to include additional exchanges related to Glencore's natural gas and power businesses. The communications surveillance programme was also enhanced and expanded, now covering 15 languages across all of Glencore's principal marketing offices globally. Further enhancements were made to our governance framework, calibration approach, surveillance metrics and quality assurance processes. We also focused on building a data governance framework to improve the completeness and accuracy of Glencore's surveillance programme.



Follow the link to our Market Conduct Policy.

Data protection

Our Information Governance Policy forms the foundation of our Information Governance and Data Protection Framework. It defines our approach to managing personal data and other types of information responsibly.

Our Data Protection Standard and local procedures set out requirements to protect personal data processed within Glencore, including employee and business partner data. Whilst the standard stipulates minimum requirements for the entire Group, local procedures allow our offices and industrial assets to define additional obligations to comply with local laws and regulations. These documents, together with our Data Protection Guideline, provide our employees with a comprehensive overview of their legal obligations and key data protection topics, including:

- domestic and cross-border data transfers;
- data transfers to third parties (e.g., Glencore's vendors);
- data breach handling process; and
- handling of data subject requests.

The Information Governance and Data Protection (IGDP) team monitors regulatory developments, including enforcement actions, to advise the business and corporate functions and facilitate compliance with all applicable laws.

In 2025, the IGDP team put considerable effort into training local data protection contacts and functions that face high data protection risks. The team also advised on strategic, global initiatives and supported the company in centralising processes and tools.

Use of communication channels and devices

In 2025, IGDP team continued to support the implementation of local communications and device procedures in Glencore's principal marketing offices. The procedures regulate the use of communication channels and devices for business communications, as well as the retention of such communications. These documents outline the approved methods of communication for Glencore employees, tailored to their risk exposure, and help ensure that business communications are retained and accessible where necessary.



Follow the link to our Information Governance Policy.

Our business partners



Business partner management framework	43
Know your counterparty	45
Third party due diligence and management	47
Community investment due diligence and management	51
Joint ventures, mergers and acquisitions, and disposals	52

Business partner management framework

We work with a range of business partners and expect them to share our commitment to ethical business practices and conduct. Business partners include our suppliers, customers, joint ventures (JVs), JV partners, service providers and other counterparties.

We have a comprehensive framework for managing the key risks associated with our business partners, from onboarding and ongoing monitoring through to offboarding. Through this framework, we seek to comply with applicable laws (including on corruption and bribery, sanctions, money laundering and tax evasion) and manage the reputational risks that can arise from engaging with certain types of business partners.

We assert our influence over JVs we don't control to encourage them to act in a manner consistent with our Values and Code.

Business partner management framework

Our business partner management framework seeks to ensure that all business partners are assessed using a risk-based approach, which directs them to the most appropriate due diligence and management process. These processes include KYC, community investment due diligence and management, third party due diligence and management, or joint ventures, mergers and acquisitions, and disposals.

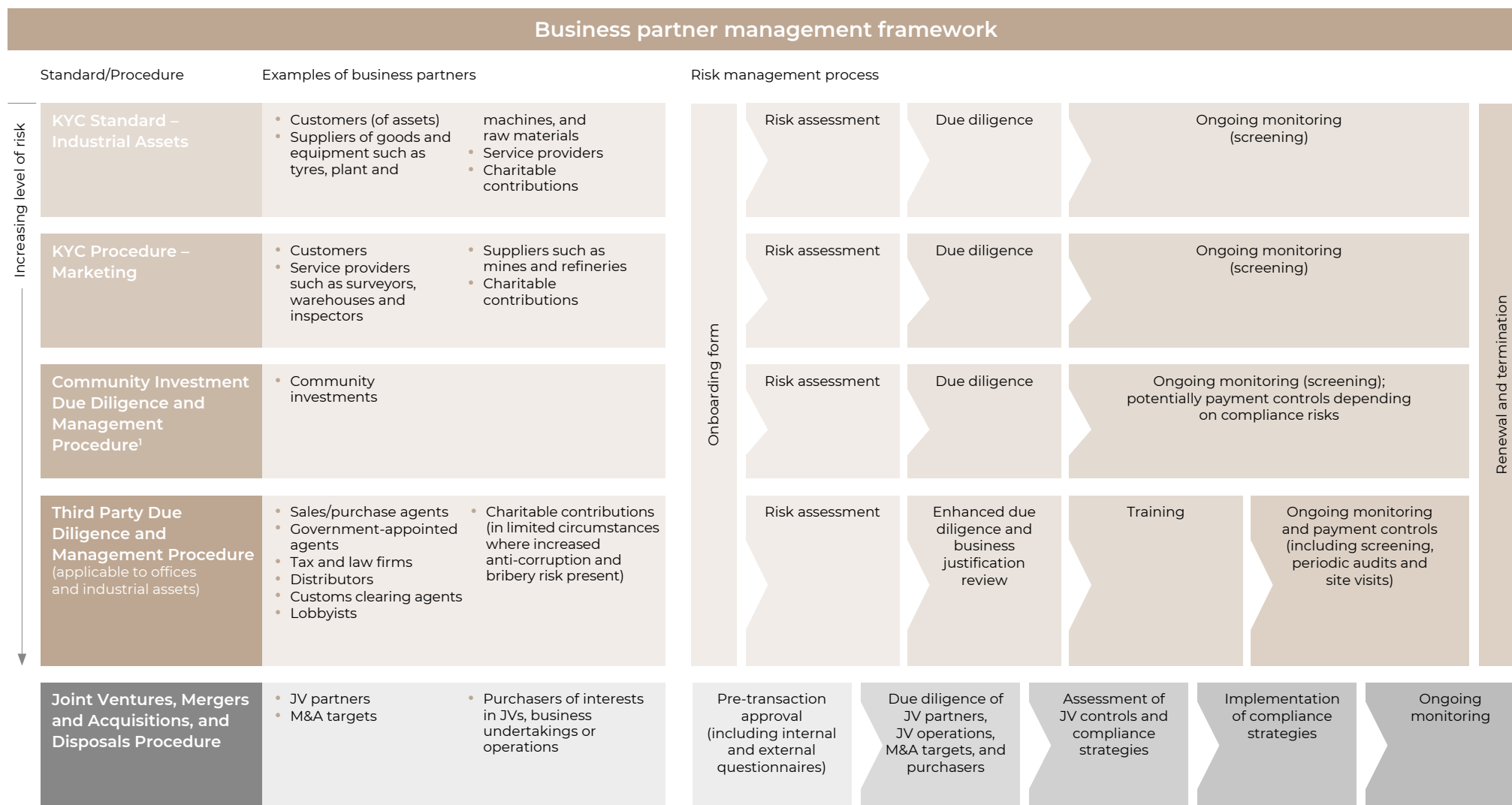
In 2025, we advanced our review of several key due diligence processes (including KYC (marketing and industrial) and third party due diligence and management) to ensure our processes are streamlined, effective, adopt a risk-based and proportionate approach and leverage systems and automation where possible. This review comprises multiple, interdependent

workstreams, including updates to processes and procedures, enhanced guidance and training for Compliance, the business and other corporate teams, and the configuration and roll out of new systems. The work also involves enhancing existing platforms and reporting by leveraging automation and simplification and incorporating system controls where possible. We have separately been working on implementing a new system for our onboarding process in marketing. The approach leverages integrations with relevant systems and removes the need for email exchanges. It further includes optimised workflows, reduces manual intervention and improves speed and consistency. The new process will also leverage internal and external sources to collect required information and data, thereby increasing quality of data while avoiding unnecessary outreach to counterparties.

On the industrial assets side, the Procurement team has been rolling out a Global Procurement System which will be implemented at the vast majority of the assets in our portfolio. The system includes integrated risk modules which implement onboarding and purchase order level compliance controls. The Compliance team has been working closely with the Procurement team over the past year to improve existing compliance controls to enhance efficiency and to ensure a risk-based approach is applied.



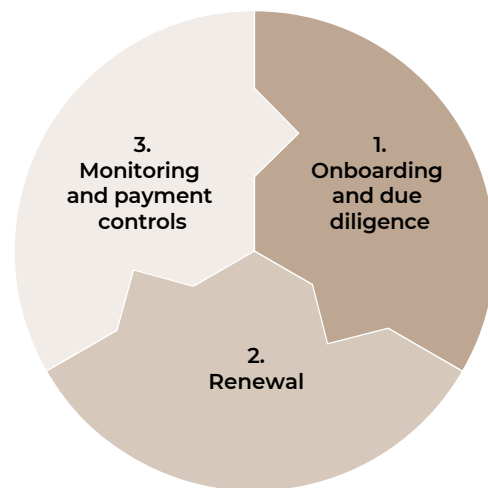
Business partner management framework *continued*



1. Introduced in 2026 as a standalone procedure.

Know your counterparty

Counterparty lifecycle



Know your counterparty processes

Our KYC processes differ for our marketing and industrial business counterparties. While we have a Group-wide approach to managing counterparties in our marketing business through the KYC Procedure – Marketing, counterparties engaged by our industrial assets are managed through local procedures which meet the minimum requirements of the KYC Standard – Industrial Assets to accommodate different local onboarding processes.

Each process applies a risk-based approach for suppliers, customers, service providers and trading counterparties (together referred to as counterparties).

The counterparty onboarding phase includes a preliminary step to determine the applicable process: KYC (marketing or industrial assets); third party due diligence and management; or joint ventures, mergers and acquisitions, and disposals. We then assign a risk rating (where applicable) and determine the type of due diligence required.

KYC Procedure – Marketing

The KYC Procedure – Marketing sets out the steps we take for marketing counterparties, including onboarding and due diligence of new counterparties, renewals of existing counterparties and, where required, mitigating measures and controls.

Our marketing counterparties include customers, suppliers, service providers and trading counterparties that are not classified as high-risk business partners under the Third Party Due Diligence and Management Procedure.

The KYC process is currently conducted through Diligent Third Party Manager (Diligent 3PM), a Group-wide system for implementation of the KYC Procedure – Marketing.

1. Onboarding and due diligence

Where the KYC Procedure – Marketing applies, different levels of due diligence are applied depending on the risk rating of the counterparty.

Depending on the counterparty's assigned risk rating as well as any red flags identified in the course of due diligence, requirements may include:

- screening the counterparty, its ultimate beneficial owners and directors in WorldCheck One, our sanctions and regulatory list screening tool;
- screening the counterparty, its ultimate beneficial owners and directors, using our adverse media screening tools;
- receipt of duly completed questionnaires (depending on the information to be requested from the business or counterparty);
- collection and verification of company, ownership and directorship information from relevant sources, such as trade registers or other approved sources;
- receipt of other supporting documentation (e.g., representation letters);
- identification of the ultimate beneficial owners of the entity; and
- receipt of a valid passport copy for ultimate beneficial owners.

Once due diligence is complete, the KYC team prepares a risk report which summarises:

- relevant counterparty information;
- the business justification;
- any concerns or red flags; and
- controls and mitigating actions to reduce identified risks.

This report is written by a KYC team member and then approved or rejected by a member of the Compliance team with the relevant seniority according to the risk rating of the counterparty. If the relevant Compliance team proposes to reject the counterparty, the rejection is discussed with, and ultimately agreed with, the Head of Compliance. If the business challenges Compliance's decision to decline a counterparty, the engagement may ultimately be escalated to the BAC. Following approval, Compliance is responsible for ensuring that any specific risk mitigating measures required prior to the engagement are implemented.

2. Renewal

Diligent 3PM notifies Compliance shortly before a counterparty's KYC is due for renewal. The renewal process is effectively a repetition of the onboarding process. The frequency of the KYC renewal depends on a counterparty's risk rating.

Know your counterparty *continued*

3. Monitoring and payment controls

Compliance documents any red flags and mitigating measures in Diligent 3PM. The business is expected to monitor these red flags and comply with identified mitigating measures.

In addition, Compliance monitors trades with certain counterparties identified as higher risk. If new trades are entered into the system with such counterparties, Compliance is notified and takes appropriate action. Compliance may also impose controls on payments to such counterparties by requiring outgoing payments to be approved by Compliance in the relevant payment system in order to be released.

Compliance also documents all counterparties under the KYC Procedure – Marketing and KYC Standard – Industrial Assets that have been rejected or are associated with material red flags in the Declined Party & Red Flag List.

Finally, counterparties are automatically screened by WorldCheck One overnight to identify any new red flags. Compliance reviews all hits and takes appropriate follow-up actions.

KYC Standard – Industrial Assets

Lower-risk counterparties engaged by the industrial assets are managed through local procedures which meet the minimum requirements of the KYC Standard – Industrial Assets. The standard sets out the due diligence requirements for engaging counterparties such as suppliers and service providers. The standard is risk-based and the requirements for counterparties are determined based on the category of goods or services provided, annual spend and supplier country. Under the standard:

- the lowest risk counterparties are subject to overnight screening only;

- most counterparties are also screened prior to onboarding; and
- for certain types of counterparties, further information is gathered via a questionnaire, including on the identity of ultimate beneficial owners (UBOs) and directors. UBOs and directors are also subject to screening.

The standard establishes decision making, approval and escalation processes and sets out requirements for renewal and termination. It also requires procedures to be in place to block or deactivate counterparties where there are compliance concerns. These counterparties may not be reactivated without Compliance approval.

In 2025, KYC approved for

4,776

marketing counterparties

12,096

industrial asset counterparties

In 2025, KYC rejected for¹

15

marketing counterparties

21

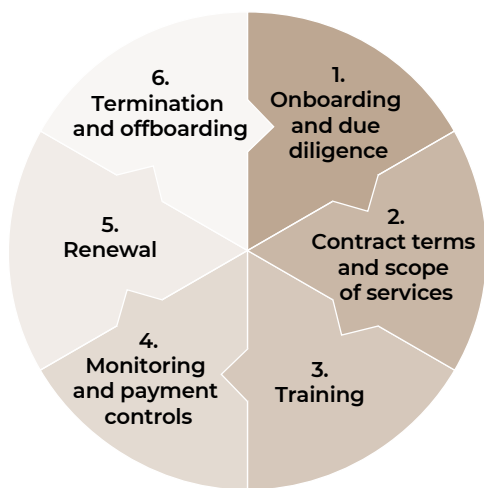
industrial asset counterparties



1. This reflects rejections for compliance reasons following completion of the onboarding process. It does not reflect rejections where, following engagement between Compliance and the business, the onboarding process was not completed.

Third party due diligence and management

Third party lifecycle



Third Party Due Diligence and Management Procedure

Our Third Party Due Diligence and Management (TPDDM) Procedure applies across our offices and industrial assets. It sets out a detailed, risk-based assessment process whereby we identify, manage, mitigate and monitor the corruption risk exposure of those third party engagements presenting the highest risk to our business.

Business partners determined to be higher-risk third parties include:

- business-generating intermediaries (such as marketing sales and purchase agents, distributors, certain physical brokers, profit share partners and back-to-back purchasers); and
- government-facing intermediaries (such as customs clearing agents/brokers, lobbyists, law and tax firms, port agents/agencies, freight forwarders and work permit/visa processors).

These third parties are higher risk because they often act on our behalf, interact with public officials on our behalf or engage in activities that have been identified as posing a heightened risk from a corruption perspective.

The TPDDM Procedure sets out the steps we take in respect of the management of third parties, including onboarding and due diligence, contract terms/scope of services, training, monitoring and payment reviews/controls, renewal, and termination and offboarding.

1. The Natural Resource Governance Institute is an independent non-profit organisation dedicated to improving countries' governance over their national resources

Disclosure of marketing sales and purchase agents

Given the inherent risks associated with marketing sales and purchase agents, we only engage marketing sales and purchase agents who provide a clear, tangible service that would otherwise need to be provided by our employees, and where we have no office or on-the-ground presence.

In line with our approach to transparency and the Natural Resource Governance Institute's recommendations, we publish and keep updated a list with the names and ultimate beneficial owners of all marketing sales and purchase agents. These agents perform substantive tasks for or on behalf of Glencore, such as engaging on business matters with existing and potential customers. Their contracts are renewed annually following fully refreshed due diligence and audit by an independent auditor.

In 2025, Glencore's Oil Marketing business had

0

marketing sales and purchase agents

Glencore's Metals, Minerals and Coal Marketing business engaged only

2

marketing sales and purchase agents, all of whom are subject to stringent due diligence and monitoring



Find out more about our sales and purchase agents.

Third party due diligence and management *continued*

1. Onboarding and due diligence

The onboarding phase includes a number of steps, such as a risk assessment and due diligence.

After the third party has been classified in Diligent 3PM:

- the proposing employee automatically receives an invitation to complete the relevant internal questionnaire and must provide a business justification for the engagement or transaction; and
- the third party automatically receives an invitation to complete the relevant external questionnaire and must provide the required due diligence documentation.

With this information, the proposed engagement is assigned a risk score by Diligent 3PM, which is calculated based on the following criteria:

- **third party risk:** considers the type of third party and its ownership;
- **country risk:** the risks associated with the country in which the services are to be provided, taking into account a Glencore bespoke risk matrix (Anti-Corruption and Bribery Country Risk), which reflects leading anti-corruption indices such as Transparency International's latest Corruption Perceptions Index (CPI) Score and TRACE International's Bribery Risk Matrix; and
- **remuneration risk:** considers the overall value of the engagement and proposed type of payment structure.

Third parties receive a risk rating of severe, high, medium or low based on their risk score. All third parties (including ultimate beneficial owners, directors, shareholders and employees working on the engagement) must at this stage be checked using relevant

sanctions and adverse media screening tools. This screening includes checks against Compliance's Declined Party & Red Flag List, which includes entities which have previously been rejected, terminated or that are currently monitored for compliance reasons and with whom we prohibit or restrict business interactions. If a proposed third party appears on this list as a declined party, onboarding will not proceed unless an exception is approved by the Head of Compliance.

Compliance next performs due diligence on the third party. Depending on the third party's assigned risk rating, due diligence requirements may include:

- completion of an enhanced due diligence report by an external service provider;
- review of the third party's compliance policies and procedures (to the extent a third party has them);
- conducting an interview with the proposing employee and separately with the third party;
- conducting a reference check;
- verification of the third party's standing against public online registers;
- confirmation that the third party is the account holder of the bank account used for the engagement and that it is in the same country where the third party is incorporated or where services are being provided;
- review of proposed compensation to ensure it is market-standard in the country in which the services are provided;
- review of financial statements; and
- identification of other red flags.

Once due diligence is complete, Compliance drafts a report which summarises the proposed engagement, including:

- relevant third party-related information;
- the business justification;
- any concerns or red flags identified during the due diligence process;
- any mitigating measures required to address identified red flags;
- a recommendation from Compliance on whether the third party should be engaged; and
- any applicable monitoring requirements.

By way of example, Compliance's red flag assessment includes whether:

- the third party, its beneficial owners or shareholders have a track record of adverse media coverage or are listed on a sanctions watchlist;
- the third party's employees, shareholders or beneficial owners are past or present public officials or politically exposed persons, or whose close relatives are/were;
- the third party's employees, shareholders or beneficial owners have a close personal relationship with any public official or representative of a commercial counterparty;
- the third party and/or its employees, shareholders or beneficial owners is/are associated with public entities;
- the third party has been recently incorporated or has an unusual corporate structure (including complex or offshore ownership or banking structures);
- the identification information cannot be readily verified or is inconsistent with the information in the external questionnaire;
- the third party failed to provide complete responses to the due diligence;
- the third party was unwilling to disclose its beneficial owners;
- the third party uses subcontractors to deliver part of the services under the engagement;

- the proposed payment terms contain upfront amounts, commissions, bonuses or elements dependent on success factors or they appear to be above market rate;
- the third party offers gifts and entertainment to public officials;
- there is a conflict of interest between the third party and a Glencore employee; and
- the third party's policies and procedures (where provided) materially conflict in any way with Glencore's.

This report is reviewed, and the engagement is approved or rejected, by:

- Compliance per defined approval levels;
- for offices, the head of department or corporate function or the line manager of the employee proposing the third party engagement depending on the type of engagement; and
- for industrial assets, the CEO, General Manager, CFO, or, in their absence, a senior member of management of that industrial asset or the line manager of the employee proposing the third party engagement, depending on the type of engagement.

If Compliance and the business cannot reach an agreement on whether to engage a third party, they may escalate the matter to the Head of Compliance. If an agreement cannot be reached, the Head of Compliance may refer the matter to the BAC.

Following approval, Compliance, in coordination with the employee responsible for the third party relationship, is responsible for ensuring that any mitigating measures included in the report are recorded on the third party's due diligence file and that any specific measures required prior to engagement are implemented.



Third party due diligence and management *continued*

2. Contract terms and scope of services

The TPDDM Procedure does not permit us to start an engagement with any third party without having a written agreement in place. Compliance works with the proposing employee and Legal to include compliance clauses in the written agreement. Compliance ensures that documentation for the engagement is complete and that relevant documentation is uploaded onto Diligent 3PM.

We also have in place specific template service agreements with tailored compliance clauses that we use for our severe and high risk intermediaries and a template agreement we encourage to be used for any charitable contributions or sponsorships we provide.

Third parties ranked as severe or high risk also receive an onboarding pack which the third party must acknowledge receipt of and which includes:

- a summary of our compliance requirements and what we expect from our business partners;
- a copy of our Code;
- a copy of our Supplier Code of Conduct;
- a copy of our Anti-Corruption and Bribery Policy;
- a copy of our Responsible Sourcing Policy;
- a description of our Raising Concerns Programme; and
- for road transporters, a copy of our 'Say no to Facilitation Payments' leaflet.

They must also acknowledge that they have read, understood and will comply with our policies.

3. Training

Compliance ensures that third parties onboarded under TPDDM Procedure receive relevant training in accordance with the Third Party Training and Monitoring (TPTM) Plan. Training requirements for third parties, including the frequency of training, vary according to the third party's risk rating and include digital training as well as in-person anti-corruption and bribery training. Where relevant to their engagement, third parties are also enrolled in market conduct digital training.

4. Monitoring and payment controls

After third parties are engaged, in addition to training, Compliance actively monitors the engagement to ensure that third parties are providing the services they have been contracted to provide.

Compliance and the business work together to manage and monitor third parties in accordance with the TPTM Plan, which outlines requirements for third parties based on their risk rating and the nature of their engagement. GIAA also monitors the application of aspects of the TPDDM Procedure generally and the TPTM Plan on an ongoing basis.

For severe and high-risk third parties, the employee within the business who is assigned to work with that third party on a regular basis, must monitor the third party. They maintain records of communications and services provided by the third party, inform Compliance of any material changes to the way the third party provides its services, request and review the third party's activity reports and liaise with

the Corporate Compliance Anti-Corruption and Bribery team prior to making any amendments to the third party's terms, commission levels or payment structures.

Group Compliance is required to review and approve in advance the invoices of and payments to all severe and high-risk business-generating intermediaries, to confirm that payments match the agreed contract rates, and that invoices include necessary details and are itemised to clearly indicate the services provided. Payments to third parties for any work carried out without a written agreement or acknowledgement in place are prohibited without approval from the Anti-Corruption and Bribery team. On a weekly basis, Corporate Compliance receives reports outlining:

- invoices relating to customs clearance;
- any new business partners that have been booked in the relevant payment system as providing customs clearance; and
- any new law firms engaged to interact with public officials on Glencore's behalf.

These enable Compliance to mitigate the risks that business partners are not taken through the appropriate due diligence (TPDDM Procedure) when interacting with public officials (e.g., by conducting customs clearance or representing Glencore in legal proceedings) in high-risk jurisdictions.

Auditing and site visit requirements for third parties are two fundamental elements of the TPTM Plan. Depending on the third party's risk rating, these requirements may consist of a full financial audit performed by an external auditor and/or a site visit by Group Compliance. In addition to audits and site visits, Compliance, in consultation with the

business, reviews activity reports containing detailed information on the nature of services that the third party performs.

For third parties rated severe and high risk, Compliance additionally corroborates the information received through the activity reports via interviews conducted periodically.

In total, depending on the third party's risk level, a third party's training and monitoring activities within a period of one year may include:

- a full financial audit by external auditors;
- twice-yearly reviews of activity reports and interviews;
- digital learning and in-person anti-corruption training and, where appropriate, market conduct training;
- onboarding and due diligence renewal;
- daily adverse media and sanctions screenings;
- compliance certifications; and
- review and pre-approval by Compliance of any payment.

Third party due diligence and management *continued*

5. Renewal

Compliance coordinates the process of renewing third party relationships with the proposing employee or the Glencore Business Third Party Manager, in accordance with the TPDDM Procedure.

Depending on the third party's assigned risk rating, the renewal process may include:

- obtaining an updated internal questionnaire, or confirmation of no changes to the previous questionnaire;
- obtaining an updated external questionnaire (or confirmation of no changes to the previous questionnaire) and relevant due diligence documents;
- re-screening or requesting an updated enhanced due diligence report on the third party and its shareholders, beneficial owners and directors; and
- preparation of a renewal compliance report reflecting any identified changes, including to beneficial ownership and scope of services and an assessment of whether there have been any issues identified by the business during the course of dealing with the third party, including lack of competence, difficulties raised over compensation, general ethical concerns, unusual requests and implementation of any mitigating measures.

6. Termination and offboarding

If a severe or high-risk third party engagement expires without being renewed, or if the engagement is terminated, Compliance will coordinate with the business employee responsible for the relationship and Legal to send the third party an end-of-service termination letter. This letter will confirm that the engagement has expired/been terminated and that the third party must cease performing services for Glencore and will not be paid for any future services performed. The relevant business employee must ensure the third party is deactivated in the relevant accounting or finance systems at the office or industrial asset.

If a third party engagement is terminated due to compliance concerns (regardless of risk level), Compliance must add the third party to the Declined Party & Red Flag List, change the third party's status to inactive in Diligent 3PM, and liaise with the business to deactivate the third party from the relevant accounting or finance systems at the office or industrial asset. Any reactivation of declined third parties must be approved by the Head of Compliance.

If a third party engagement is not renewed and there are no compliance concerns, the third party is placed in inactive status in Diligent 3PM and the relevant accounting or finance systems and cannot be re-engaged without going through the onboarding process again.

In 2025, we had

438

approved and active third parties that we continue to monitor in our marketing business (of these 106 were newly approved in 2025) and

1,611

approved and active third parties that we continue to monitor across our industrial assets (of these 444 were newly approved in 2025).

In 2025, we rejected¹

0

third parties in our marketing business and

2

third parties in our industrial business.

In 2025, we commissioned

6

annual audits by an external auditor, all of which were on government-facing intermediaries, 4 in our marketing business and 2 in our industrial business.



1. This reflects rejections for compliance reasons following completion of the onboarding process. It does not reflect rejections where, following engagement between Compliance and the business, the onboarding process was not completed.

Community investment due diligence and management

We make discretionary and non-discretionary community investments that are intended to create a lasting social and economic benefit for the communities where we operate. The structures in place that facilitate these investments (e.g., a foundation or community investment agreement (CIA)) can be Glencore controlled or third-party controlled and often involve working with local stakeholders such as members of local communities, civil society organisations, local municipalities or other government institutions.

In some cases, we have limited or no control over the governance of third-party controlled structures, the selection of projects or the suppliers engaged in connection with the community investment. It is therefore not always possible to apply full KYC or TPDDM to the community investment, as we do when it is Glencore controlled.

To cater for the nuances around community investments and enable us to adopt a more risk-based, proportionate approach to the compliance due diligence of community investments, we separated the compliance assessment of community investments from the TPDDM Procedure and introduced a new, standalone Community Investment Due Diligence and Management Procedure (CIDDM Procedure).

The purpose of the CIDDM Procedure is to set out:

- the level of due diligence to apply when we seek to enter into a new community investment (i.e., we become a party to a foundation or other type of arrangement);
- the level of due diligence to apply when we make a community investment directly or pursuant to an existing foundation or other type of arrangement; and
- mitigating controls that we should seek to implement to manage the compliance risks associated with community investments.

Entering into new foundations or CIAs

While we may not always be able to negotiate the terms of our entry into new foundations or CIAs, for example, because they are non-discretionary, in principle we seek to avoid agreeing to enter into new third-party controlled foundations or CIAs where we are unable to implement

appropriate mitigating controls, except in exceptional circumstances. Examples of mitigating controls include:

- including Compliance-related representations and warranties in relevant agreements;
- agreeing veto or voting rights over a project, supplier engagement and any other proposal in connection with a community investment;
- monitoring and/or reviewing the foundation or CIA's compliance with, for example, the terms of the CIA, the provision of a community investment and the use of funds in connection with community investments;
- including Glencore representation on relevant committees;
- conducting due diligence on the suppliers and/or beneficiaries (as relevant);
- conducting ongoing screening of suppliers and/or beneficiaries (as relevant) in our sanctions screening tool;
- monitoring the use of funds where we have identified a specific compliance risk that we are seeking to manage;
- reviewing annual reports, to the extent that a foundation or CIA publishes annual reports, financials and/or provides written updates to stakeholders; and
- where appropriate, leveraging existing supplier networks to provide in-kind support to a project or procure the community investment ourselves.

To assess the mitigating controls that we should seek to apply, we conduct a compliance risk assessment. This assessment also determines whether we should, in principle, provide the community investment. Risk factors include:

- whether it is made through a Glencore controlled or a third-party controlled vehicle (e.g., a fund or foundation);
- whether it is discretionary or non-discretionary (e.g., pursuant to a court order or because it is required by law);
- the country in which the community investment will take place;
- whether any suppliers will be involved in the project selection, execution and/or management of the community investment;
- any government institution, public official or politically exposed person (PEP) involvement;
- whether the initiative might, directly or indirectly, personally benefit or otherwise provide anything of value to a public official;
- the overall value and length of the project; and
- the nature of the contribution (i.e., financial contributions, in-kind provision of goods/services and/or in-kind personnel time).

Where the community investment is made directly or via a Glencore controlled foundation, the risk assessment informs the decision on whether to apply KYC or TPDDM to the investment.

Where the community investment is made pursuant to an existing third-party controlled fund, foundation or other arrangement, the risk assessment also takes into consideration existing controls and determines any additional controls we should seek to implement in addition to the applicable due diligence we should apply to any suppliers engaged to manage or execute the community investment.

Joint ventures, mergers and acquisitions, and disposals

Our Joint Ventures, Mergers and Acquisitions, and Disposals Procedure (JVMAD Procedure) requires that our Programme is implemented at all JVs that we control or operate.

For those JVs we do not control or operate, we seek to influence our JV partners to adopt our commitment to responsible business practices and implement appropriate compliance programmes accounting for the nature and risks associated with the JV and JV partners, and which meet the minimum requirements as determined by Glencore.

In respect of M&A activity, we conduct thorough pre-transaction due diligence. Our JVMAD Procedure requires us to rank the risk of each M&A and JV transaction on the basis of the information typically available in the early stages of the transaction, including considering the relevant jurisdictions, the future JV partners and/or target entity, and the level of control or ownership that we intend to acquire. The risk category assigned determines the compliance due diligence steps that we take in connection with the transaction which may only be varied with the approval of the Head of Compliance.

The pre-transactional due diligence process includes:

- initial approval by the relevant head of marketing department or industrial lead;
- due diligence of JV partner/purchaser and/or JV operation/M&A target;
- assessment of due diligence findings;
- determination of JV level of control;
- determination of compliance provisions and Programme requirements in the relevant agreement; and
- preparation of a compliance report.

Transactions rated as “high risk” also require us to obtain a transaction-specific enhanced due diligence report from a third party on the relevant counterparties (i.e., target entity, JV partner/seller), and interview the representatives from the compliance function at JV partners/sellers and/or operating company.

To commence the process, the relevant commodity department seeking to enter into a JV/M&A transaction or dispose of an undertaking nominates an employee to serve as the transaction responsible person (TRP), who must manage the JV/M&A transaction or disposal with Compliance. Before starting due diligence, the TRP is required to obtain approval for the transaction/disposal in principle from the Head of Department and notify Compliance.

All JV partners and the target JV operation itself, regardless of our anticipated ownership or operational control of the proposed JV, are subject to due diligence. The TRP responds to an internal questionnaire and informs Compliance of any red flags that they are aware of or unusual payment requests made by any party. The TRP works with the Legal

and Compliance functions to gather the documentation and information required from the JV partner/target entity to perform thorough due diligence, which includes responses to an external questionnaire and additional documents requested.

A post-transaction risk assessment and review for all target entities in which we acquire majority ownership or control is also required. This review consists of three primary components: (1) an initial risk assessment, to understand the risks particular to the newly acquired entity and its operation; (2) transaction testing, to assess the control environment and risk prevention mechanisms, as well as to identify any potential misconduct that may need to be reported; and (3) a compliance programme gap analysis to assist in implementing the Programme. Upon completion of these activities, Compliance develops a compliance programme implementation plan to implement our Programme at the entity.

When we dispose of our interest in JVs, business undertakings or operations, we conduct due diligence on the purchaser, which focuses on source of funds, reputational issues and money laundering risks.

Compliance assesses the compliance risks of the transaction by considering the risks associated with the proposed JV partners, the existing business or operations in which we will acquire an interest, the risks associated with the proposed business undertaking/operation of the JV/M&A activity going forward, and/or the risks associated with the purchaser in a disposal transaction (including the source of funds).

Compliance issues recommendations on mitigating any identified compliance risks, including working with Legal to set out the proposed mitigating actions and remedies in the JV, M&A or disposal agreements.

Compliance management in JVs

After the completion of due diligence and assessment of the compliance risks associated with a JV partner and its JV operation, Compliance, Legal and the relevant commodity department determine the level of control we should seek to exert over the JV in light of the risks identified, our commercial objectives, and our negotiating leverage with the JV partner(s). The extent of our control will generally be linked to the percentage of ownership we will have in the JV. However, if the compliance risks associated with the JV are assessed to be high, Compliance and the business may determine that in order to mitigate those risks we need to obtain control that is disproportionate to our level of ownership. The JV’s compliance programme requirements will vary based on our level of ownership and control.

For non-controlled JVs where we hold 20% or more of the voting rights, and for independently managed JVs, we require that JVs implement a compliance programme that is appropriate for the JV, having regard to the nature and risks associated with the JV, and that meets certain minimum requirements. To ensure these requirements are met, relevant compliance provisions are included in the applicable agreements. For non-controlled JVs where we hold less than 20%, we make reasonable efforts prior to entering into the JV to influence the JV to adopt an appropriate compliance programme.

Joint ventures, mergers and acquisitions, and disposals *continued*

In respect of all non-controlled JVs, we seek to influence the JV's approach to compliance through the activities and advocacy of any board members that we appoint. Such board members undergo compliance training, which allows them to be aware of compliance risks, raise compliance issues during board meetings, regularly request and review audit reports, and ensure that dissatisfaction with board decisions we are unable to block is duly recorded. In addition to the JV board member training, we publish a brochure on our Programme's core elements which provides additional key guidance for board members we appoint. Compliance also seeks to regularly liaise with a compliance contact at relevant JVs.

Existing non-controlled JVs

For non-controlled JVs already in existence when the JVMAD Procedure was initially rolled out in 2020, Compliance conducts risk assessments on a periodic basis, which include a review of the JV's compliance programme measured against the core elements of an effective compliance programme. Broadly speaking, this includes assessing:

- compliance resources at the JV;
- whether the JV has a code of conduct and compliance policies and procedures governing topics such as anti-corruption and bribery, gifts and entertainment, conflicts of interest, charitable contributions and sponsorships, whistleblowing, interactions with public officials, sanctions, anti-money laundering and data privacy;
- how the JV manages third party relationships;

- whether there is a confidential reporting structure and investigations process in place;
- compliance incentives and disciplinary processes; and
- monitoring, testing and review of the compliance programme in place.

Depending on the outcome of the risk assessment and any follow-up engagement with the JV partner, we may recommend additional compliance measures.

In 2025, under the process set out in our JVMAD Procedure we reviewed and approved¹:

17

new JVs

2

new M&A transactions

9

disposals

Types of JVs in our framework

Glencore-controlled JVs

A JV that is Glencore-controlled or-operated is an entity where we are responsible for controlling or operating the JV and implementing relevant policies, systems and controls. This model of control must be applied in any JV where we hold more than 50% of the voting rights. For controlled/operated JVs, we require that the JVs implement our Programme, including all policies, standards and procedures. We monitor and implement controls where our Programme applies, as we would with any other Glencore entity.

Non-controlled JVs

We differentiate between two types of non-controlled JVs: partner-controlled JVs and independently managed JVs.

Partner-controlled JVs

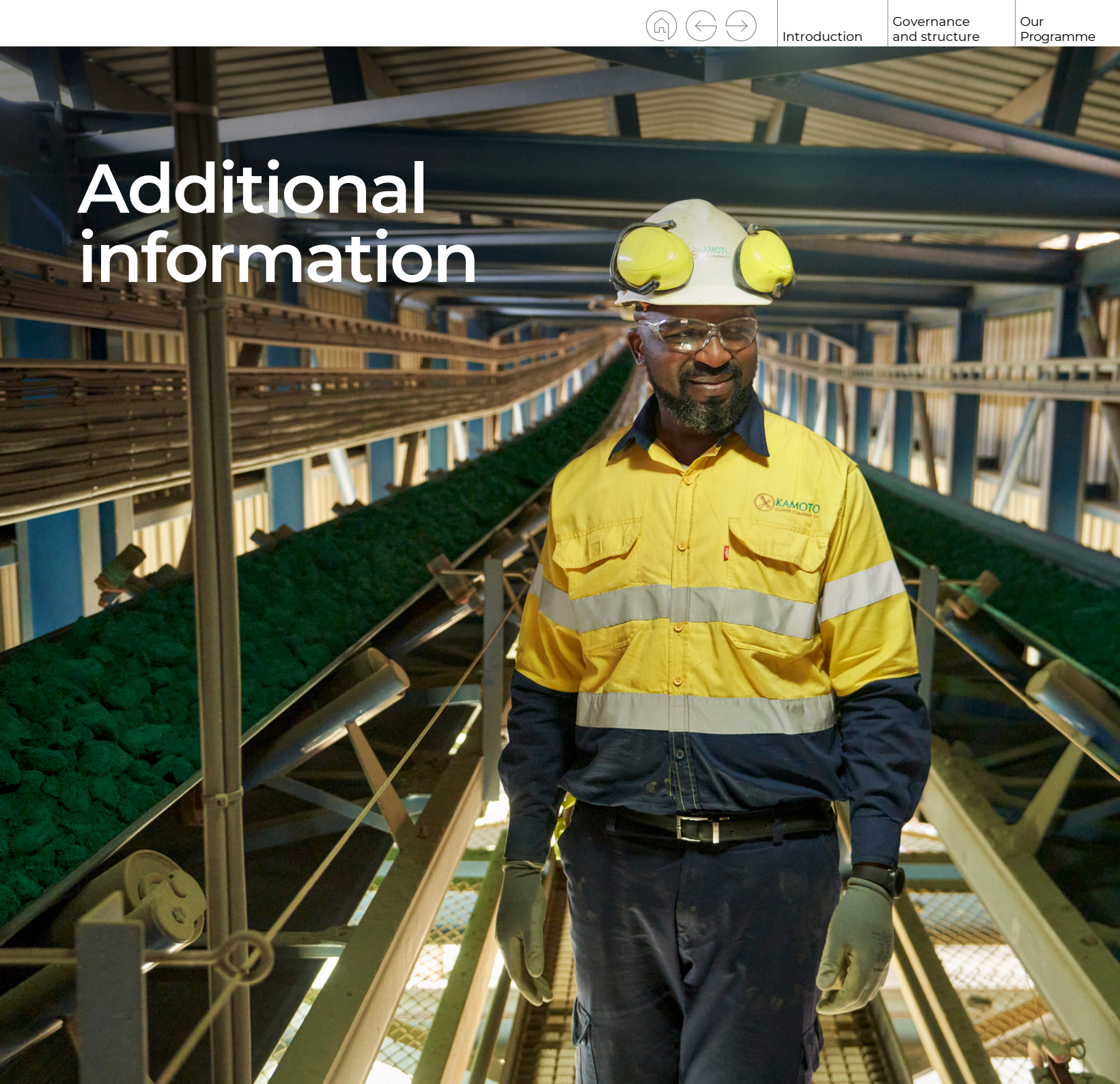
A JV in which the JV partner controls or operates the JV and implements compliance policies, systems and controls. This level of control creates more risk for us since it relies on the JV partner to control and operate the JV and implement appropriate systems and controls. It is therefore only acceptable if we hold less than 50% of the voting rights and if we are satisfied that the JV partner has (or makes commitments that it will have) the resources and ability to implement an appropriate compliance programme.

Independently managed JVs

JVs which operate independently from the shareholders, meaning that an independent board of directors, management and corporate functions, including finance, legal and internal audit, will be established for the purpose of operating the JV. The shareholders' involvement in the JV is typically limited to participation in the board and shareholder governance bodies. This level of control can be acceptable for all levels of Glencore ownership, although it is typically not implemented where we hold more than 50% of the voting rights. For independently managed JVs, we are required to ensure the JV has the resources (or makes commitments to expand its resources) to implement an appropriate compliance programme without the support of its shareholders.

1. Further internal approvals may be required following approval by Compliance, figures therefore may not correspond to the number of transactions implemented.

Additional information



Important notice	55
Further information	56





Important notice

This document does not constitute or form part of any offer or invitation to sell or issue, or any solicitation of any offer to purchase or subscribe for any securities. This document does not purport to contain all of the information you may wish to consider.

Cautionary statement regarding forward-looking information

Certain descriptions in this document are oriented towards future events and therefore contain statements that are, or may be deemed to be, "forward-looking statements" which are prospective in nature. Such statements may include, without limitation, statements in respect of trends in commodity prices and currency exchange rates; demand for commodities; reserves and resources and production forecasts; expectations, plans, strategies and objectives of management; expectations regarding financial performance, results of operations and cash flows; climate scenarios; sustainability (including, without limitation, environmental, social and governance) performance-related goals, ambitions, targets, intentions and aspirations; approval of certain projects and consummation and impacts of certain transactions (including, without limitation, acquisitions, disposals or other corporate transactions); closures or divestments of certain assets, operations or facilities (including, without limitation, associated costs); capital costs and scheduling; operating costs and supply of materials and skilled employees; financings; permitting, anticipated project timelines, productive lives of mines and facilities; provisions and contingent liabilities; and tax, legal and regulatory developments.

These forward-looking statements may be identified by the use of forward-looking terminology, or the negative thereof including, without limitation,

"outlook", "guidance", "trend", "plans", "expects", "continues", "assumes", "is subject to", "budget", "scheduled", "estimates", "aims", "forecasts", "risks", "intends", "positioned", "predicts", "projects", "anticipates", "believes", or variations of such words or comparable terminology and phrases or statements that certain actions, events or results "may", "could", "should", "shall", "would", "might" or "will" be taken, occur or be achieved. The information in this document provides an insight into how we currently intend to direct the management of our businesses and assets and to deploy our capital to help us implement our strategy. The matters disclosed in this document are a 'point in time' disclosure only. Forward-looking statements are not based on historical facts, but rather on current predictions, expectations, beliefs, opinions, plans, objectives, goals, intentions and projections about future events, results of operations, prospects, financial conditions and discussions of strategy, and reflect judgments, assumptions, estimates and other information available as at the date of this document or the date of the corresponding planning or scenario analysis process.

By their nature, forward-looking statements involve known and unknown risks, uncertainties and other factors which may cause actual results, performance or achievements to differ materially from any future events, results, performance, achievements or other outcomes expressed or implied by such forward-looking statements. Important factors that could impact these uncertainties include, without limitation, those disclosed in the risk management section of our latest Annual Report and/or Half-Year Report, which can each be found on our website. These risks and uncertainties may materially affect the timing and feasibility of particular developments. Other factors which may impact risks and uncertainties include, without limitation: the ability to produce and transport products profitably; demand for our products and commodity prices; development, efficacy and adoption of new or competing technologies; changing or divergent preferences and expectations of our stakeholders; events giving rise to adverse reputational impacts; changes to the assumptions regarding the recoverable value of our tangible and intangible assets; inadequate estimates of resources and reserves; changes in environmental scenarios and related regulations, including, without limitation, transition risks and the evolution and development of the global transition to a low carbon economy; recovery rates and other operational capabilities; timing, quantum and nature of certain acquisitions and divestments; delays, overruns or other unexpected developments in connection with significant projects; the ability to successfully manage the planning and execution of closure, reclamation

and rehabilitation of industrial sites; health, safety, environmental or social performance incidents; labour shortages or workforce disruptions; natural catastrophes or adverse geological conditions, including, without limitation, the physical risks associated with climate change; effects of global pandemics and outbreaks of infectious disease; the outcome of litigation or enforcement or regulatory proceedings; the effect of foreign currency exchange rates on market prices and operating costs; actions by governmental authorities, such as changes in taxation or laws or regulations or changes in the decarbonisation policies and plans of other countries; breaches of Glencore's policy architecture and other internal requirements, applicable laws or regulations; the availability of sufficient credit and management of liquidity and counterparty risks; changes in economic and financial market conditions generally or in various countries or regions; political or geopolitical uncertainty; and wars, political or civil unrest, acts of terrorism, cyber attacks or sabotage. Readers, including, without limitation, investors and prospective investors, should review and consider these risks and uncertainties (as well as the other risks identified in this document) when considering the information contained in this document. Readers should also note that the high degree of uncertainty around the nature, timing and magnitude of climate-related risks, and the uncertainty as to how the energy transition will evolve, makes it particularly difficult to determine all potential risks and opportunities and disclose these and any potential impacts with precision. Neither Glencore nor any of its affiliates, associates, employees, directors, officers or advisers, provides any representation, warranty, assurance or guarantee as to the accuracy, completeness or correctness, likelihood of achievement or reasonableness of any forward-looking information contained in this document or that the events, results, performance, achievements or other outcomes expressed or implied in any forward-looking statements in this document will actually occur. Glencore cautions readers against reliance on any forward-looking statements contained in this document, particularly in light of the long-term time horizon which this document discusses in certain instances and the inherent uncertainty in possible policy, market and technological developments in the future. No statement in this document is intended as any kind of forecast (including, without limitation, a profit forecast or a profit estimate), guarantee or prediction of future events or performance and past performance cannot be relied on as a guide to future performance.

Except as required by applicable rules or laws or regulations, Glencore is not under any obligation, and Glencore and its affiliates expressly disclaim any intention, obligation or undertaking, to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise. This document shall not, under any circumstances, create any implication that there has been no change in the business or affairs of Glencore since the date of this document or that the information contained herein is correct as at any time subsequent to its date.

Sources

Certain statistical and other information included in this document is sourced from publicly available third-party sources. This information has not been independently verified and presents the view of those third parties, and may not necessarily correspond to the views held by Glencore and Glencore expressly disclaims any responsibility for, or liability in respect of, and makes no representation or guarantee in relation to, such information (including, without limitation, as to its accuracy, completeness or whether it is current). Glencore cautions readers against reliance on any of the industry, market or other third-party data or information contained in this document.

Information preparation

In preparing this document, Glencore has made certain estimates and assumptions that may affect the information presented. Certain information is derived from management accounts, is unaudited and based on information Glencore has available to it at the time. Figures throughout this document are subject to rounding adjustments. The information presented is subject to change at any time without notice and we do not intend to update this information except as required.

Subject to any terms implied by law which cannot be excluded, Glencore accepts no responsibility for any loss, damage, cost or expense (whether direct or indirect) incurred by any person as a result of any error, omission or misrepresentation in information in this document.

Other information

The companies in which Glencore plc directly and indirectly has an interest are separate and distinct legal entities. In this document, "Glencore", "Glencore group" and "Group" are used for convenience only where references are made to Glencore plc and its subsidiaries in general. These collective expressions are used for ease of reference only and do not imply any other relationship between the companies. Likewise, the words "we", "us" and "our" are also used to refer collectively to members of the Group or to those who work for them. These expressions are also used where no useful purpose is served by identifying the particular company or companies.

Further information

Glencore is one of the world's largest global diversified natural resource companies and a major producer and marketer of more than 60 commodities. Through a network of assets, customers and suppliers that spans the globe, we produce, process, recycle, source, market and distribute the commodities that advance everyday life.

With over 140,000 employees and contractors and a strong footprint in over 30 countries in both established and emerging regions for natural resources, our marketing and industrial activities are supported by a global network of offices.

Glencore's customers are principally industrial consumers, such as those in the automotive, steel, power generation, battery manufacturing and oil sectors. We also provide financing, logistics and other services to producers and consumers of commodities.

In addition to our Ethics and Compliance Report, our annual corporate reporting suite reflects our commitment to transparent disclosure across a broad range of topics and includes our:

- Annual Report
- Sustainability Report
- Payments to Governments Report
- Modern Slavery Statement

Glencore plc
Baarer mattstrasse 3
6340 Baar
Switzerland

Tel: +41 41 709 2000

Fax: +41 41 709 3000

E-mail: info@glencore.com

glencore.com/contact-us

Our Purpose

Responsibly sourcing the commodities that advance everyday life

Our Values



Safety

We never compromise on safety. We look out for one another and stop work if it's not safe



Integrity

We have the courage to do what's right, even when it's hard. We do what we say and treat each other fairly and with respect



Responsibility

We take responsibility for our actions. We talk and listen to others to understand what they expect from us. We work to improve our commercial, social and environmental performance



Openness

We're honest and straightforward when we communicate. We push ourselves to improve by sharing information and encouraging dialogue and feedback



Simplicity

We work efficiently and focus on what's important. We avoid unnecessary complexity and look for simple, pragmatic solutions



Entrepreneurialism

We encourage new ideas and quickly adapt to change. We're always looking for new opportunities to create value and find better and safer ways of working