Leading governance

In this section

Our values direct us to respect the environment and stakeholders. We aim to make a positive contribution to society, including by conducting our business ethically, honestly, responsibly and legally.

We expect our suppliers to live up to the standards we set for ourselves to ensure there are no adverse impacts linked to our operations from business partners.

We seek to ensure that Valterra Platinum and its people and partners are not impacted negatively by physical safety and cybersecurity issues.

We are committed to achieving these governance goals using measures that respect human rights.

Polokwane smelter

SDGs

SDG 8

SDG 16

SDG 12

SDG 17

PROMOTING BUSINESS ETHICS

Why this matters

We recognise that our reputation is a critical asset to sustain our social licence to operate, avoid sanctions and facilitate opportunities to operate in new locations.

Maintaining our reputation as a trusted company will enable us to continue building strong relationships with our stakeholders.

Failure to maintain an ethical reputation puts our business at risk in various ways, threatening our sustainability and damaging the trust of investors, employees and other stakeholders. We seek to be a trusted company and a preferred commercial partner and employer.

Our approach

We protect and bolster our reputation by choosing to do the right thing and conducting our business with integrity.

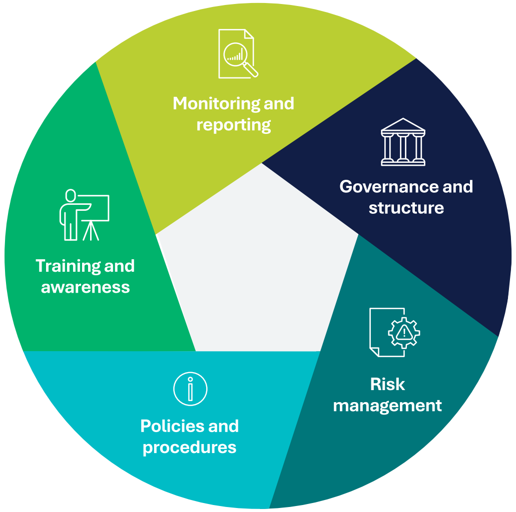
Ethical conduct is embedded in our governance structures, overseen by the board and supported by senior leadership. All employees are expected to uphold the highest standards of integrity and comply with our code of conduct.

Our compliance framework is designed to ensure we meet legal and ethical obligations through clear policies, robust risk management and continuous monitoring. We strengthen this framework through regular training, transparent reporting and independent oversight.

Our compliance framework provides the foundation for ethical business conduct. It is designed to:

- Ensure strong governance through independent oversight and leadership accountability
- Identify and manage risks proactively, prioritising areas of greatest impact
- Establish clear policies and procedures that guide responsible decision-making
- Build awareness and capability through mandatory training and targeted initiatives
- Monitor and report transparently, with regular updates to governance committees.

Key elements of the compliance framework



Material issues and related principal risks	
Material issue	**Principal risks (PR), emerging risks (ER) and opportunities (O)**
Upholding ethical business conduct and protecting against corruption.	Social licence to operate (PR).

Disclosure against standards (content index in Supplementary info)		
SASB Mining and Metals Standard 2023-12		
Business ethics and transparency		
EM-MM-510a.1		Description of management system for prevention of corruption and bribery throughout the value chain
GRI Foundation 2021		
GRI 414-2	14.17.9	New suppliers that were screened using social criteria
GRI 414-2	14.17.10	Negative social impacts in the supply chain and actions taken
GRI 408-1	14.18.2	Operations and suppliers at significant risk for incidents of child labour
GRI 409-1	14.19.2	Operations and suppliers at significant risk for incidents of forced or compulsory labour
GRI 205-1	14.22.2	Operations assessed for risks related to corruption
GRI 205-2	14.22.3	Communication and training about anticorruption policies and procedures
GRI 205-3	14.22.4	Confirmed incidents of corruption and actions taken
	14.22.5	Contract transparency
	14.22.6	Beneficial ownership
GRI 201-4	14.23.3	Financial assistance received from government
GRI 415-1	14.24.2	Political contributions

PROMOTING BUSINESS ETHICS CONTINUED

Compliance management programme

Implementation of the compliance framework is set out in our compliance management programme. The programme has seven compliance areas that are fundamental to operating in accordance with our commitments:

1	2	3	4	5	6	7
Antibribery and corruption	**Fair competition and antitrust**	**Tax integrity**	**Data privacy and information security**	**Anti-money laundering and counter-terrorism funding**	**Fraud prevention**	**Trade controls and sanctions compliance**
Preventing unethical practices and ensuring transparency in all interactions	Promoting fair markets and compliance with competition laws	Ensuring responsible tax practices and compliance with global standards	Protecting personal and business information	Safeguarding against financial crime	Detecting and preventing fraudulent activities	Adhering to international trade regulations

These areas reflect our commitment to global best practice and continuous improvement.

Performance against targets

Performance in 2025

Types of breaches of standards	Jan–May 2025*	Jun–Dec 2025**	2024
People – employment, personnel policy and other people-related matters	**16**	22	93
People – bullying, harassment, victimisation and other related matters	**32**	27	96
Bribery, corruption and fraud	**36**	9	42
Suppliers and procurement	**8**	8	35
Safety and health	**2**	4	11
Information security and data privacy	**3**	0	3
Social and environment	**1**	0	2
Other (YourVoice)	**5**	4	2

* *This reflects data as received from Anglo American for the period 1 January 2025 to 31 May 2025.*
** *This reflects data as extracted by Valterra Platinum from 1 June 2025 to 31 December 2025.*

Year in review

Valterra Platinum has introduced mandatory training for all connected employees as part of our initiatives to build a safer, more ethical and more united workplace. The training is designed to ensure all employees understand and embrace their obligations and responsibilities in these fields. Training content is tailored to risk areas and includes practical scenarios to strengthen decision-making. The 2025 training covered:

Learning course	Audience	Completion rate
SHE policy	Connected employees bands 1–10	**99%**
Bullying, harassment and victimisation	Connected employees bands 1–10	**99%**
Information management security and data privacy	Connected employees bands 1–10	**99%**
Conducting business with integrity	Connected employees bands 1–10	**99%**

Strengthening our antibribery and corruption approach

Valterra Platinum is committed to maintaining the highest standards of integrity in all jurisdictions where we operate. In line with global benchmarks such as the Transparency International Corruption Perceptions Index, we seek to strengthen our approach to managing bribery and corruption risks.

Prior to the demerger, we conducted a comprehensive antibribery and corruption risk assessment across the business, engaging key stakeholders to reinforce our commitment to proactive risk management. As a result, we enhanced our stakeholder engagement standard and introduced additional controls to ensure transparency in interacting with government officials and third parties.

Our actions include:
- Maintaining accurate registers of all interactions with government officials across our sites
- Recording all gifts, entertainment and hospitality offered or received
- Requiring appropriate levels of management approval for such engagements
- Launching a new disclosure tool in 2025 to streamline reporting and strengthen oversight of conflicts of interest and gifts, entertainment and hospitality.

Whistleblowing

YourVoice is Valterra Platinum's confidential whistleblowing channel, independently operated via a third-party service provider's platform to ensure anonymity and integrity. It is available to all employees, contractors, suppliers and stakeholders to report unethical, unlawful or unsafe conduct, including breaches of company policy, harmed dignity and financial misconduct.

PROMOTING BUSINESS ETHICS CONTINUED

Following the demerger, Valterra Platinum assumed full responsibility for the governance of YourVoice. Oversight rests with our legal and compliance teams, ensuring reports are managed fairly, confidentially and in line with our code of conduct. Investigations are conducted independently to maintain objectivity and uphold the highest standards of integrity. Each case is assessed promptly and directed to the appropriate team for resolution, reinforcing our commitment to transparency and accountability.

Stakeholder engagement

To advance its strategic objectives, Valterra Platinum works to cultivate meaningful relationships with a diverse network of stakeholders who both influence, and are influenced by, the company's operations. We recognise that our long-term success depends on the strength of these relationships and the trust we build through consistent engagement.

Government

Following the launch of Valterra Platinum as a standalone company, we introduced an integrated stakeholder engagement plan to guide strategic communications and strengthen relationships with key government departments. The primary objectives of these engagements were to formally introduce the company, articulate its brand identity and value proposition and explore opportunities for collaboration, particularly in support of government-led community development initiatives.

The CEO has led high-level engagements with key government stakeholders and ministers (finance; trade, industry and competition; energy and electricity; forestry, fisheries and the environment (DFFE)). Additional meetings with the ministers of water and sanitation (DWS), mineral and petroleum resources (DMPR) and new DFFE minister are scheduled for 2026. The CEO also met with the premier of Limpopo and an engagement with the premier of North West is planned for 2026.

These discussions have centred on aligning Valterra Platinum's operations with national priorities and fostering collaborative partnerships. The meetings were constructive, paving the way for improved regulatory alignment and operational efficiency.

On the regulatory front, the executive head: corporate affairs has led engagements with the directors-general of the DMPR, DWS and DFFE, recognising their critical role in regulatory processes. A meeting with the director-general of national treasury is scheduled for the first quarter of 2026.

Valterra Platinum was also invited by the Department of Trade, Industry and Competition to join the official business delegation at the Tokyo International Conference on African Development in Yokohama, Japan.

Industry associations

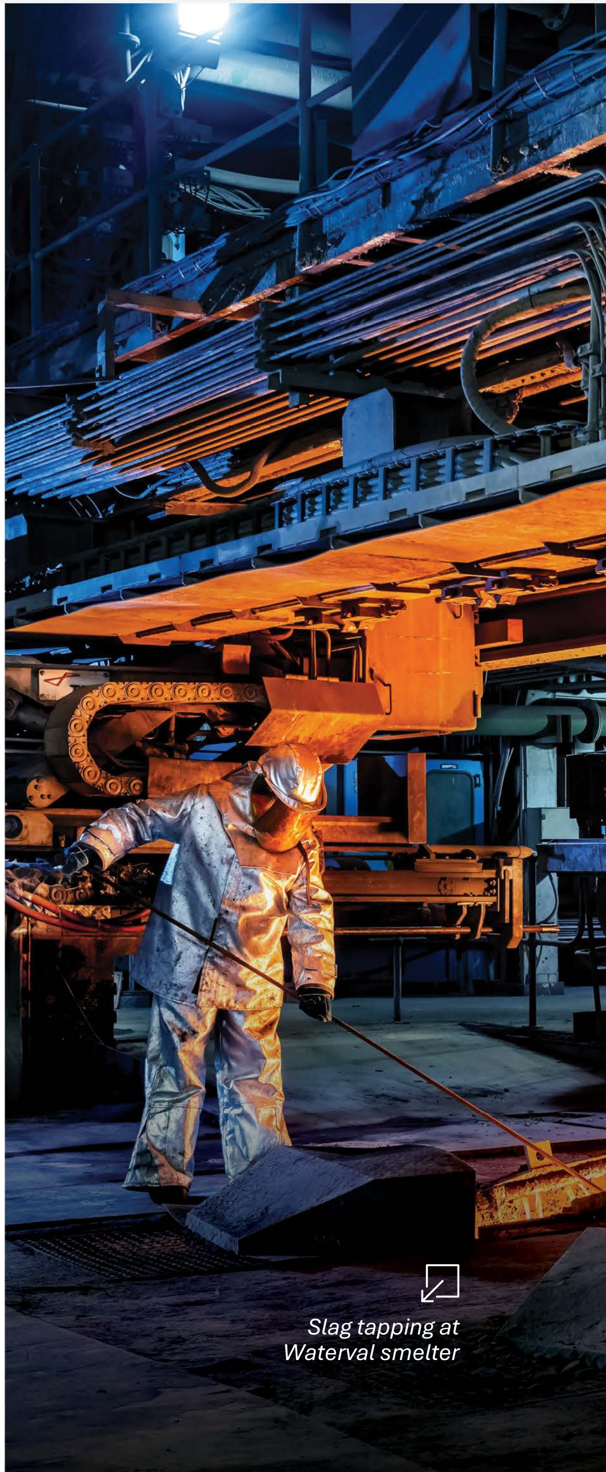
Industry associations play an important role for Valterra Platinum. Our memberships of, and partnerships with, these associations allow us to share best practice and remain informed on relevant technical, political and social developments. They open a route for Valterra Platinum's views to be heard alongside those of our peers on policy and other debates.

As a responsible global mining business, we engage with – and, where appropriate, help – industry associations that develop and implement best practices for our sector. Valterra Platinum is a member of the LBMA (London Bullion Market Association), LPPM (London Platinum and Palladium Market) and IPA (International PGM Association). The robust third-party assurance processes that come with those memberships mean we can convey to our stakeholders, including employees, regulators and customers, that we observe the highest safety standards at our sites and conduct diligent product stewardship.

We actively participate in the South African Minerals Council as well as the Zimbabwe Chamber of Mines. This year, for example, we engaged with both on proposed amendments to the minerals' regulatory regimes in those countries.

NGOs

Valterra Platinum is building strategic partnerships with credible NGOs and civil society organisations to support future training, capacity building and independent monitoring.



Slag tapping at Waterval smelter

PROMOTING BUSINESS ETHICS CONTINUED

Transparency

We are implementing measures to ensure compliance with prevailing national data protection and access to information laws. We continue to align with the principles of the Extractive Industries Transparency Initiative, although we are not, as Valterra Platinum, registered as a supporting company.

Our social and economic contribution in 2025	Total tax
Overall tax contribution This includes:	**R4.2 billion**
› **Corporate income tax** Payments to governments based on taxable profits under legislated income tax rules. This includes payments made to revenue authorities in respect of disputed claims and withholding taxes on dividends, interest and royalties	**R2.2 billion**
› **Royalties and mining taxes** Payments to governments in relation to both revenue or production generated under licence agreements and royalty-related income taxes	**R1.5 billion**
› **Other payments borne** Taxes or other payments to governments borne by the group, including payroll taxes and those taxes and payments relating to environmental policy and licensing requirements, carbon taxes, landfill taxes, aggregate taxes, permits and other entry fees and considerations.	**R0.5 billion**
Taxes collected Payments in respect of taxes by Anglo American Platinum or Valterra Platinum, which are borne by other parties (eg customers or employees), directly arising from the economic activity of the company.	**R3.7 billion**

For more detail, see the tax transparency report 2025.

Focus areas for 2026

We will enhance third-party due diligence processes.

Ethics training for contractors and suppliers will be expanded.

Our digital compliance tools for monitoring and reporting will be strengthened.

INVESTING IN THE SECURITY OF PEOPLE AND ASSETS

Why this matters

We have a duty to all stakeholders to protect our people, assets and processes from harm, including harm caused by criminal actions.

We also have a duty to ensure the security actions we take are carried out in full compliance with the law and our obligation to respect human rights. This includes adhering to the terms of the Voluntary Principles on Security and Human Rights (VPSHRs).

Our approach

In support of Valterra Platinum's strategic pillars, we aim to ensure the security of people, operations and assets through the best use of technology, resources and intelligence.

We seek to lead a comprehensive security capability, working across the business to drive excellence and inform decision-making. In the department, we are working towards increased standardisation, coordination and continuous development of an effective security organisation and capability.

Our security team has four workstreams:
- Governance, risk and compliance
- Threat intelligence
- Protective security
- Investigations.

We seek to drive compliance with evolving site security standards and continuously enhance operational capabilities to optimise loss prevention. We generally pursue excellence in digitisation and technologies. We ensure losses are prevented through last-line-of-defence measures, including:
- Disruptive operations
- Waste-area recoveries
- Sting operations
- Copper-cable recovery
- PGM recovery.

In addition to VPSHR adherence, our policies and management systems align with the South African constitution, UN Global Compact, UN guiding principles on business and human rights and IFC performance standards.

Performance against targets

Our target of a four-week turnaround time on forensic unit investigations was achieved in 68% of cases (2024: 65%).

Material issues and related principal risks	
Material issue	**Principal risks (PR), emerging risks (ER) and opportunities (O)**
Upholding ethical business conduct and protecting against corruption.	Social licence to operate (PR) People and assets: safety and security (ER).

Disclosure against standards (content index in Supplementary info)		
SASB Mining and Metals Standard 2023-12		
EM-MM-210.3 EM-MM-510a.1		Discussion of engagement processes and due diligence practices with respect to human rights, indigenous rights and operation in areas of conflict
GRI Foundation 2021		
GRI 410-1	14.14.2	Security personnel trained in human rights policies or procedures
GRI 205-1	14.22.2	Operations assessed for risks related to corruption
GRI 205-2	14.22.3	Communication and training about anticorruption policies and procedures
GRI 205-3	14.22.4	Confirmed incidents of corruption and actions taken

INVESTING IN THE SECURITY OF PEOPLE AND ASSETS CONTINUED

Year in review

Tactical response services – business disruptions

Operation	Number of incidents	Average resolution time
PMR	1	**53 min**
All other disruptions	16	**8 min**

We have installed access-control upgrades at certain sites using wave readers – scanners that use touchless hand waves for fingerprint identification.

CCTV with advanced technological capacity has been installed at certain sites.

We have instituted systems to ensure a four-week turnaround time for all GBV and BHVD investigations (see the diversity, equity and inclusion section on pages 54 to 59 for detail on this work).

We have joined and are delivering on our commitments in respect of the Eyes and Ears Initiative (E2), the official joint crime-fighting initiative involving the SAPS, Business Against Crime South Africa, the private security industry and other approved non-private security bodies and law-enforcement agencies.

We completed our tactical response team recruitment drive to reduce contractor costs and operational risks.

We delivered R900 million in last-line-of-defence recoveries in 2025 (2024: R1.3 billion). We also curbed illegal chrome mining at Twickenham.

We have fully implemented security standard operating procedures across all sites this year on the online platform.

Our drone services are currently outsourced, but we are planning a hybrid model to reduce costs.

Focus areas for 2026

We will focus on ongoing compliance.

Loss prevention remains a key priority.

We will enhance operational capability.

We will focus on succession planning.

Der Brochen surface infrastructure

INVESTING IN THE SECURITY OF PEOPLE AND ASSETS CONTINUED

CASE STUDY

Amandelbult flood – February 2025

Amandelbult was afflicted by a severe flood in February 2025, necessitating extensive emergency and recovery efforts and the implementation of a strategy to mitigate against future flooding.

There had been normal seasonal rain until 19 February. However, at 03:00 that day, 85mm of rain fell in just an hour. Over the next 24 hours, a total of 294mm fell. It was designated a greater-than-one-in-10,000-year flood.

Tumela Mine was hit hard and recovery work continued until September when steady-state production resumed. The overflow of nearby river systems, compounded by the collapse of the upstream Bierspruit Dam near Swartklip the following day, caused water ingress in remote areas, which overwhelmed pumping capacity, flooding parts of the underground workings and the main pump station.

The evacuation of Tumela staff was implemented during the morning shift of 19 February and operations were suspended.

Nearby Dishaba Mine was also affected, but to a lesser extent, with operations resuming production after 29 days of recovery.

The emergency recovery initiatives were extensive. New pumping equipment was installed in phases over the following weeks. By 8 March, dewatering was taking place at 7Ml a day. By 17 March, this had increased to 14Ml a day. It took until 11 April, some seven weeks after the flood, for dewatering to be completed. Initial estimates were that it would take eight to 12 months to dewater Tumela and a further four months to return the mine to production. The full recovery of operations in seven months is testament to the incredible work of engineering teams and redeployed operations teams to effect recovery.

It was necessary to airlift essential services due to flooded approaches to the mine. Amandelbult was also asked to use its emergency response teams and equipment to assist local communities that had been badly affected. Helicopter services were extended for rescue operations. Food parcels were airlifted for stranded communities. Mine personnel carried out 30 aviation rescues and six ground rescues.

And that was just the beginning. A short, medium and long-term ‘improvement strategy’ has been designed to mitigate the chances of a repeat of such an impactful flood.

In the short term, among many other elements, the mine’s berm walls – the raised banks or ridges used to divert floodwaters – which had been set to resist a one-in-200-year flood, had to be repaired and it was decided to raise them to meet the standard of a one-in-1,000-year flood. An ‘island’ is also being constructed on top of filled holings in the Bierspruit flood plain. Holings are depressions, pits or trenches that can occur naturally or artificially for drainage.

Regrettably, one life was lost in the community due to the flooding.

An example of a longer-term plan is the creation of 142Ml in storage capacity at Tumela in the underground workings to be used in case of a flood, with pumping capacity to remove the water from underground.

An internal report found that “... the mine demonstrated strong execution of flood response activities. Groundwater monitoring, pumping strategies and communication protocols were effectively implemented. Evidence shows comprehensive planning, resource allocation and coordination.”

“The shaft flooding response was well-managed,” the report concludes.

The insurance claim was initially estimated at US$250 million. Through the impressive emergency response and effective business continuity work, losses were significantly reduced by restoring steady-state production well ahead of initial recovery time estimates, with no loss of life at Amandelbult operations and a significant reduction of loss of life in local communities.

Berm wall constructed at Amandelbult

ADVANCING CYBERSECURITY

Why this matters

Cybersecurity risks for businesses are rising due to increased system connectivity and the growing drive for automation. For the last three years, we have identified cybersecurity as a material risk requiring focused management.

Our approach

The audit and risk committee is responsible for governing information and technology, including cybersecurity risk management. We provide assurance to the committee that this risk remains within defined risk appetite and tolerance levels. Valterra Platinum is implementing a next-generation cybersecurity strategy and organisational model to strengthen resilience against cyber risks. We continuously assess our cybersecurity posture and capability maturity against leading standards, frameworks and industry best practices:

- In 2021, we adopted the National Institute of Standards and Technology (NIST) cybersecurity framework, which guides organisations in preventing, detecting and responding to cyberattacks. Reports based on this framework are submitted to the committee every two years
- We ensure compliance with King IV requirements by aligning technology governance with the Control Objectives for Information and Related Technology (COBIT) framework of the IT Governance Institute
- Additionally, we align cybersecurity management with the requirements of ISO 27001 for an information security management system (ISMS).

Performance against targets

Our goal is to proactively prevent cybersecurity breaches that could jeopardise our business operations and compromise the privacy of our stakeholders, including employees, customers, suppliers and partners:

- The security operations centre managed 931 cyber incidents in 2025
- Compliance monitoring against the acceptable use policy identified 63 violations, including potentially harmful software downloads and access to prohibited content. All these cases were addressed by the security operations centre team
- The team detected and remediated 260 instances of malware and unsanctioned programmes on corporate devices
- The organisation was targeted by over 378 phishing campaigns, impacting 4,443 individuals. Each campaign was identified and mitigated to prevent incidents and further exposure.

Year in review

The information management (IM) function remains focused on the critical task of responsibly separating all IM services from Anglo American. To support this process, an IM transitional service agreement (IM TSA) was developed to ensure joint management and oversight of the separation. A monthly IM TSA survey is distributed to all relevant users, and any indication of service performance below service level agreement standards triggers immediate corrective action. Since the IM TSA launch on 1 June 2025, survey results have consistently confirmed satisfactory service delivery.

In August, Valterra Platinum and Anglo American agreed on a consolidated IM joint separation plan. This includes a dedicated cybersecurity component detailing the transition of cybersecurity services. The process began with a comprehensive review of existing cybersecurity services provided by Anglo American to determine which would transition to Valterra Platinum. Throughout the year, substantial work has gone into preparing and executing the plan to achieve day 1, day 2 and day 3 milestones of the demerger. Full transition of all cybersecurity services is expected by July 2026.

Material issues and related principal risks

Material issue	Principal risks (PR), emerging risks (ER) and opportunities (O)
› Ensuring cybersecurity and data privacy.	› Information and cybersecurity (PR).

ADVANCING CYBERSECURITY CONTINUED

We continue to place strong emphasis on employees being extra vigilant in identifying and reporting suspicious emails. The demerger period introduced increased vulnerability due to the complexity of separating IT systems, data and processes. To manage these risks, extended cybersecurity awareness campaigns were delivered through multiple communication channels, reinforcing the importance of cybersecurity and the responsibility of each employee in safeguarding the organisation. In the reporting period, two data breaches were reported and fully remediated:

- **Incident 1:** an internal confidential document was inadvertently disclosed to a supplier. The supplier agreed to delete the document
- **Incident 2:** a user account was compromised through phishing, resulting in 917 phishing emails being sent externally and internally from the compromised user account. This data breach was reported to the SA Information Regulator.

Artificial intelligence (AI) introduces significant cyber and information risks alongside its benefits. Valterra Platinum is developing a comprehensive AI security strategy encompassing robust data governance to protect sensitive information and mitigate bias by prioritising transparency in AI models. Strengthening the security of AI infrastructure, investing in specialised expertise and establishing clear ethical guidelines are crucial. Regular risk assessments of AI applications and continuous monitoring of the evolving threat landscape are also essential to ensure the secure and responsible adoption of AI technologies.

The annual information management committee risk assessment session in August 2025 identified 13 strategic risks for Valterra Platinum. Dedicated workshops were subsequently conducted with respective risk owners to further analyse each risk, assess risk ratings, define appropriate mitigation actions, assign due dates and document outcomes in the risk register.

Focus areas for 2026

The immediate priority for IM cybersecurity in 2026 is to ensure the responsible and safe separation of cybersecurity services from Anglo American. Key services included in the transition are:

- **Cybersecurity governance:** Valterra Platinum has adopted and adapted Anglo American's existing cybersecurity policies, which are currently under review and being updated
- **Managed security operations centre:** Valterra Platinum currently relies on Anglo American for monitoring, detection and incident response. We are establishing a standalone centre with independent technology, third-party service agreements and separate licensing. The appointment of an appropriate service provider is expected to conclude by March 2026
- **Third-party security risk management:** Valterra Platinum currently uses Anglo American's tool for third-party risk management. We have decided to implement a separate platform, with evaluations underway for deployment in early 2026
- **Cybersecurity awareness and training:** a comprehensive awareness programme is being developed to deliver regular, measurable and role-specific campaigns across the organisation. A new cyber training platform will support this initiative
- Alongside ongoing joint separation plan activities, IM cybersecurity is focused on refreshing and recalibrating the cybersecurity strategy and organisational model, guided by internal business drivers and external ecosystem factors.