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.