Petra Diamonds Information Communication & Technology
(11 October 2022)

ICT Overview

Petra's Chief Technical Officer (**CTO**) who is a member of Petra's Executive Committee (**ExCo**) and Operational Committee, has overall responsibility for Information Communication and Technology (**ICT**) at Petra. The CTO is supported by the Acting Head of ICT that runs the day-to-day activities of the ICT function which consists of 23 in-house skilled certified professionals with experience spanning various specialisms and where required, further support services from external service providers.

The function's key service deliverables include:

- providing a comprehensive ICT service across the Group which includes the development and implementation of a Group ICT strategy and frameworks aligned with Petra's overall business strategy;
- providing ICT strategic and technical advice and support to the operations to ensure adequate security measures are in place over data and information, including the management and maintenance of ICT infrastructure and associated assets to prevent minimal business disruptions; and
- providing internal assurance and, where necessary, seeking external assurance on the adequacy and effectiveness of ICT's internal controls, risk management and governance processes.

ICT Frameworks

Petra deploys widely recognised and well established ICT frameworks to ensure standardised and consistent ICT performance and security standards which incorporate:

- *ITIL 4*: which measures, optimises, monitors and evaluates the overall performance of ICT services;
- *ISO 27001*: this standard sets out the specification for Petra's information security management system by addressing people, processes, and technology systems which is considered a best-practice approach; and
- *IEC 62443*: these series of standards assist Petra in defining requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (**IACS**) including the setting of cybersecurity benchmarks. These standards set best practices for security and provide a way to assess the level of security performance with Petra's ICT and IACS systems.

Legal Landscape

Petra's ICT systems, processes, policies and procedures are designed to ensure compliance with key legislation across all its businesses. The key legislation that Petra is required to comply with includes: General Data Protection Regulations (EU & UK), Protection of Personal Information Act (SA), Electronic Communications Act (SA) and Electronic and Postal Communications Act (Tanzania). Petra implements security measures to protect confidential, sensitive and personally identifiable information against reasonably anticipated threats and unlawful data breaches.

Policies and Procedures

The Group's policies, procedures and processes are developed in accordance with the ICT frameworks and legal requirements set out in the preceding paragraphs with the key purpose of mitigating ICT security risk exposures. Petra's key policies and procedures in this area include:

- Information Communication and Technology Policy & Standards;
- Mobile Phone and Printing Policies;
- Security Policy Third Party;

- Third Party Access Policy;
- Back-up & Restore Policy;
- Disaster Recovery and Business Continuity Policy; and
- Acceptable Use of Information Policy.

Incidents: Management and Response

Petra's information security incident management strategy is to process incidents as effectively as possible and minimize the impact of business interruptions. Petra's incident management and response systems enable all incidents to be logged and/or responded to and/or resolved within 24 hours which is aligned with Service Level Agreements between operations and ICT. Depending on the severity and materiality of an incident, ICT responses including the resolution of the incident may exceed the 24 hour turnaround time.

Petra is in the process of developing an ICT emergency response procedure detailing the responsibility of key role players and processes to manage and restore data and information as a result of potential cyber-attacks, including ransomware or other instances where data integrity and information is compromised. Petra is further evaluating and developing end-to-end processes and protocols in responding to potential cyber-attacks.

Petra has not experienced a material information security breach in the last three years.

Risk Management

ICT conducts risk assessments in accordance with the Group's Enterprise Risk Management Framework. During FY 2022 a risk assessment was performed to identify, assess and evaluate key cyber security risks the Group is exposed to, including an assessment of mitigating controls management has implemented to minimise the occurrence of cyber-security risks. The findings of this risk assessment were reported to and reviewed by the ExCo and the Board's Audit and Risk Committee. Whilst Petra insures its ICT infrastructure and mobile assets, it is in the process of evaluating the cost of insurance cover for data and information losses.

Petra recognises the risks associated with cyber-attacks and continuously implements and assesses the effectiveness of mitigating controls, which includes, user training and awareness, penetration testing and vulnerability assessments. The Group delivers security focused user training on phishing and whaling attacks, amongst others, on an Advanced Thread Protection platform.

Due to the increasing trends and potential material financial impact of cyber-security risk attacks, Petra continually reviews and assesses the adequacy of its investments in ICT security. To increase the awareness of cybersecurity and the impact of cyber-attacks on Petra, dedicated cyber-security training sessions have taken place for ExCo and are scheduled for Petra's Board of Directors during Q2 of FY 2023. Key highlights of the training incorporate an overview of cybersecurity, global trends, effective crisis management plans in responding to cyber-attacks and Director's fiduciary duties and responsibilities and other legal implications regarding cyber-attacks.

Assurance

The Group's Internal Audit function, in conjunction with the ICT function, periodically performs certain internal assurance reviews, while external assurance reviews are conducted by certified independent service providers with the relevant expertise and credibility. These internal and external reviews include the following, amongst others:

- financial systems audit (annually);
- internal and external cyber security vulnerability assessments (annually);
- in-house developed software vulnerability assessments;
- ISO 27001 – level 3 compliance; and
- planned for FY 23: IEC 62443 (assurance over IACS).

Reporting

The ICT function reports material security incidents and responses monthly to all on-mine Management Committees and the Group's Operational Committee. The Operational Committee is made up of Group Heads of Department and is chaired by the Chief Operating Officer. This reporting includes remedial actions and preventative measures that will be implemented to mitigate the reoccurrence of ICT security risks or other incidents.

Petra's Audit & Risk Committee, consisting solely of independent Non-Executive Directors, assists the Board in discharging its oversight and monitoring responsibilities in relation to ICT and its Terms of Reference includes the following responsibilities:

- overseeing the development and implementation of an ICT Governance Charter and policies that are integrated with the business strategy process and which sustain and enhance the Company's strategic objectives, thereby improving the Company's performance and sustainability;
- overseeing the implementation of ICT processes and governance mechanisms, ICT frameworks, policies, procedures and standards, ensuring ICT governance alignment with corporate governance;
- reviewing the information security strategy (including information security, information management and information privacy) and management's implementation of the strategy; and
- ensuring that there are processes in place to enable complete, timely, relevant, accurate and accessible ICT reporting, firstly from management to the Board, and secondly by the Board in the integrated report.

As stated above, the Audit and Risk Committee has recently reviewed a cyber security risk assessment that was conducted in FY 2022 and the Committee will be looking to extend ICT reporting to include updates on key areas of internal controls, risk, governance, incident management and overall ICT initiatives.