Audit & Risk Committee responsibility for Kenmare Information Technology Security Risk

The scope of the Kenmare Audit and Risk Committee includes responsibility for information security and all members of this Committee are independent Non-Executive Directors. The Financial Director has relevant information security experience and attends the Committee meetings during which information security matters are discussed. Management briefs the Board and the Audit and Risk Committee on security matters at least twice per year and all material issues discussed by the Audit and Risk Committee are elevated for Board consideration.

Management briefing of the Audit and Risk Committee covers material developments on information security matters at each Audit and Risk Committee meeting and typically focus on information security during at least two meetings per year. In addition, information security is considered by management and the Audit and Risk Committee during the annual risk-review process. The Group does not currently hold information security risk insurance.

The Group employs external independent information systems and security consultants to support the Kenmare information technology teams. The scope of work undertaken by these independent consultants covers both support and security audit services. The principal external consulting group is a GDPR Compliant ICT Partner Data Processor, and the consulting group adheres to ITIL 4 for ICT Service Management and ISO/IEC 27001 Information Security Management. They provide independent systems review and assurance services for the Group and these independent reports are used to update the Kenmare Audit and Risk Committee and the Board.

The Group's Information Communication and Technologies (ICT) systems are designed, implemented and supported to comply with a wide variety of regulatory compliance reporting specifications, including the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of confidential, sensitive, and personally identifiable information and protect against any reasonably anticipated threats, hazards, or disclosures of sensitive data or personally identifiable information not permitted by statutory guidelines or regulations. The systems are designed to ensure compliance with General Data Protection Regulation ((EU) 2016/679) and applicable national implementing laws, regulations and secondary legislation in Ireland relating to the processing of Personal Data and the privacy of electronic communications, including the Privacy and Electronic Communications Directive (2002/58/EC) and the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI 336/2011).

In June 2020, the Audit and Risk Committee received a presentation by the Kenmare Internal Auditor covering the results of a network audit undertaken by an independent cyber security consultant. As a result, the Group established an ICT Taskforce with Kenmare's principal external information systems and security consultancy partner to proactively manage the Group's ICT assets through a Security Information and Event Management (SIEM) solution which globally manages over approximately 500 Company assets. The principal consulting group employed to advise Kenmare comprises highly trained and certified professionals and services include Proactive Managed Services, Data Infrastructure, Cloud Technologies, Networking & Security, Consultancy Services, GDPR / ISO consultancy, and compliance services.

The Group's information security and data protection team meet regularly with the Group's independent information systems and security consultants to support the information technology teams throughout the Group. The scope of work undertaken by these independent consultants covers the proactive monitoring, support, and security auditing services for the Kenmare Group. The ICT Taskforce conduct regular Security & Data Protection Impact Assessment reviews. These assessments involve identifying risk and vulnerabilities in the organisation's information processing systems based on the NIST Cybersecurity and ISO-27001 Frameworks. Kenmare recognises the risks associated with cyber-attacks and invests appropriately in cybersecurity mitigation controls and training, which includes, vulnerability testing, dark web monitoring, cybersecurity monitoring and staff cybersecurity awareness training programmes.

Audit and Risk Committee briefings also cover management of data protection. During the past three years, briefings to the Audit and Risk Committee covered two information data breaches, both of which were not material and resulted in no commercial loss, the most recent of which was discovered on 10 June 2020.

The Group has an information security training and compliance program for all employees that is at least annual. The Group operates a training programme which incorporates information technology security, including phishing and other cyber security threats. This programme forms part of induction and annual refresher training courses. The programme includes ongoing testing and response tracking of email for users which is designed to increase user awareness of online security threats.

For further information, please see the Audit and Risk Committee Report.