Statement on Risk Management and Internal Control

Pursuant to Paragraph 15.26 (b) of the Main Market Listing Requirements of Bursa Malaysia Securities Berhad (Bursa Securities), the Board of Directors of listed companies is required to include in their annual report, a statement about the state of risk management and internal control of the listed issuer as a group.

Digi Board of Directors (Board) is pleased to provide the following statement that has been prepared in accordance with the Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers endorsed by Bursa Securities. The Statement outlines the nature and scope of risk management and internal control within Digi during the financial year under review.

RESPONSIBILITIES AND ACCOUNTABILITIES

The Board acknowledges its responsibility for the establishment as well as oversight of Digi's risk management framework and internal control systems. The risk management framework and internal control systems are designed to identify, assess and manage risks that may impede the achievement of business objectives and strategies. The Board also acknowledges that the internal control systems are designed to manage and minimise, rather than eliminate, occurrences of material misstatement, financial losses or fraud.

The Board, through the Audit and Risk Committee (ARC) periodically reviews the effectiveness and adequacy of the risk management framework and internal controls by identifying, assessing, monitoring and reporting key business risks with the objective to safeguard shareholders' investments and Digi's assets.

Management is responsible for implementing Board approved policies and procedures on risk management and internal controls by identifying and evaluating risks faced and monitoring the achievement of business goals and objectives within the risk appetite parameters.

RISK MANAGEMENT

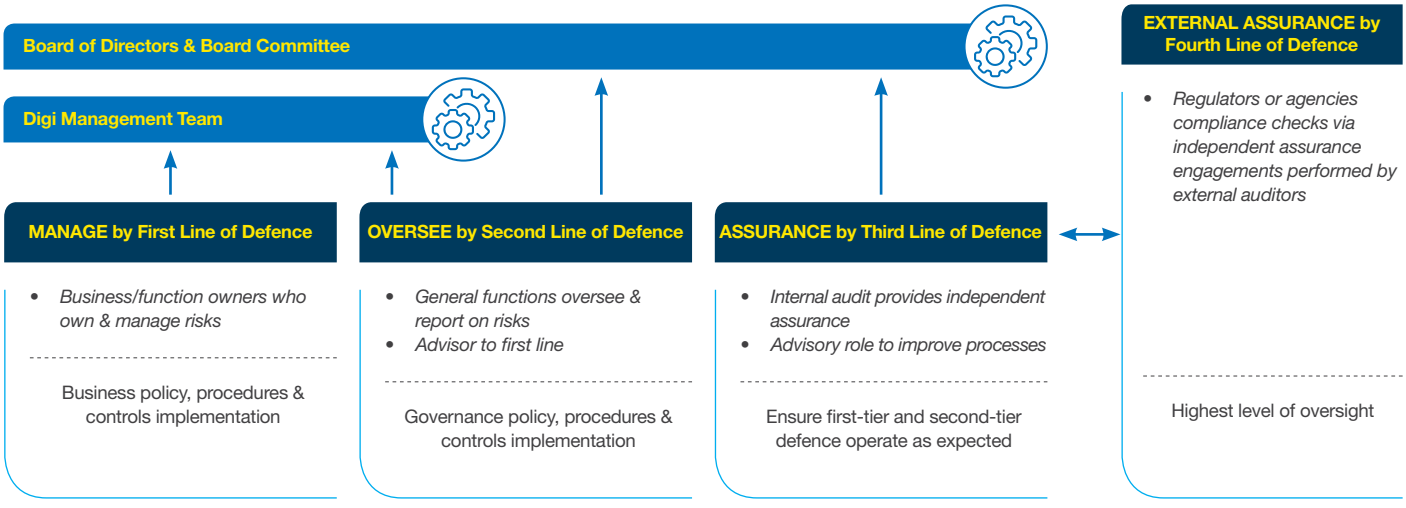
Digi's risk management framework provides the foundation and process on how risks are managed across Digi. Our process is broadly based on ISO 31000:2018.

Risk management responsibilities in Digi are defined in the framework where Risk Management function is responsible to implement the enterprise risk management process.

Digi's Management Team (Management)'s key role is to identify significant threats and opportunities, evaluate the risk profile and drive mitigation strategies on a regular basis. All line managers are required to assume responsibility for risk management within their areas of responsibility and ensure that risk management is embedded in the day-to-day business and decision-making processes.

The diagram below illustrates the roles and responsibilities of risk management practices across Digi.

Roles & Responsibilities of Managing Risks:



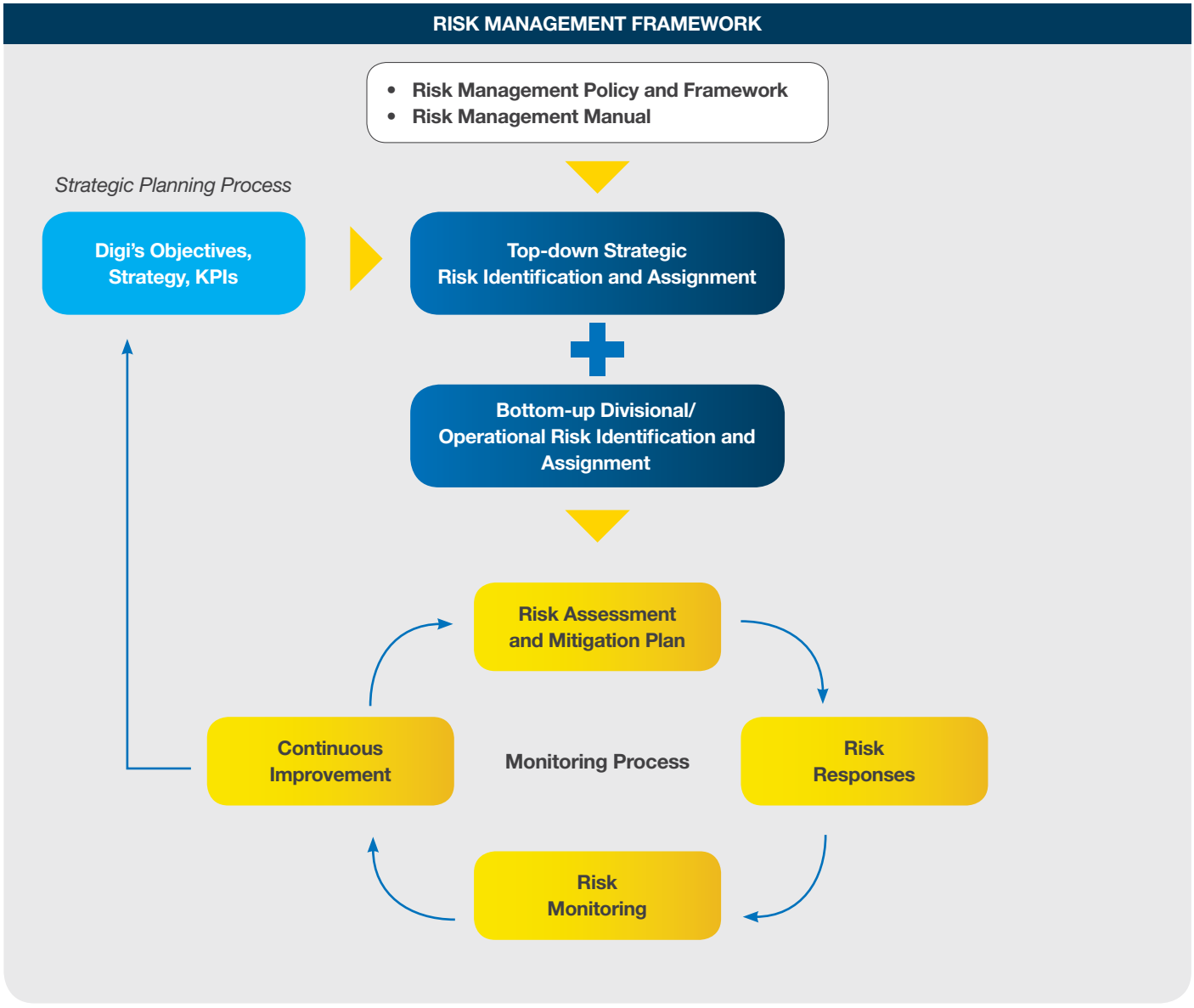
Statement on Risk Management and Internal Control

Digi's risks are identified based on risk assessments performed relative to the organisation's ambition and objectives from our strategic planning process. The identified risks are assessed and deliberated by Management and mitigated through strategies which are monitored for progress to maintain the risk exposure within acceptable level.

As part of risk governance, Management reports Digi's top enterprise risks to ARC in a risk heat map on a quarterly basis for oversight and mitigation status. Material risks identified are reported to the Board annually, via the ARC, to ensure the Board is updated on significant risks and progress of mitigation actions.

To strengthen our risk management framework, we have continuously improved to enhance our risk management practices and increase the scope across Digi.

Refer to the diagram below for an overview of the risk management framework and processes implemented in Digi:



Statement on Risk Management and Internal Control

Risks reported by Management and discussed with ARC and the Board during the financial year are summarised below. As these risks are still relevant, mitigation responses are in place and continuously monitored to mitigate risk exposures.

Market and Competition

Risk on heightened competition level coupled with effects of Covid-19 on the economy are challenging industry and revenue growth

Business Discontinuity

Risk of interruptions in Digi's critical service areas during the pandemic outbreak

Employee's Health and Safety

Covid related impact on employees health and safety, including wellbeing and engagement amidst change in way of work

Capital Allocation and Operational Efficiency Risk

Failure to optimise capital allocation and operational efficiencies on digitisation and network modernisation will impede our competitiveness

Regulatory, Legal and Compliance Risk

Risk of non-compliance by Digi and/or our business partners to applicable industry regulations or requirements on spectrum, access licenses, registration, or responsible business ethics

Data Protection and Risk Management

Vast amount of data is subject to numerous compliance, security, and privacy requirements. Effective data governance is critical to fulfil increased expectation in consumer data protection under the new remote way of work

Cyber Threats and Security Risk

Risk of cyber-attacks with presence of threat actors and exploitation activities due to increased digitisation, high internet usage from remote working during Covid

Responsible Business Commitment Risk

Risk of not fulfilling corporate social responsibility to support the community during Covid; and not gaining consumers' trust and expectations in carbon emission, e-waste and climate change threats on network infrastructure expansion and roll out

Talent and Succession Management Risk

Inability to manage sucession planning risk, attract new talents to promote diversity and inclusion, and retain top talents

Statement on Risk Management and Internal Control

INTERNAL CONTROL SYSTEMS

The key elements of the internal control systems established by the Board that provide effective governance and oversight of internal controls include:

Policies and Operating Procedures

Policies and operating procedures are in place to ensure compliance with internal controls and the prescribed laws and regulations. These policies and procedures provide guidance and direction for proper management and governance of operations and business activities. The documents are reviewed annually and published in the Compliance portal which is available to all employees.

Profitability Assurance

This function minimises revenue leakage by implementing adequate controls and processes through an optimal revenue management framework. It covers the cycle of identification, assessment, mitigation and monitoring. Digi has in place automated controls to ensure that usage and profile integrity between the network, mediation, rating and billing is assured and adequately controlled. Key issues and mitigation actions are reported to Management monthly. The effectiveness and efficiency of processes and controls within the revenue cycle are reviewed regularly. In addition to assuring minimal revenue leakage, the team also works on automation and dashboards for efficient business monitoring.

Security

Digi is committed to reduce the impact of service disruptions by ensuring infrastructure is protected and services are not interrupted, thereby enabling continuous services to its customers.

The Cyber Security and Physical Security functions are responsible for ensuring confidentiality, integrity and availability of information and information processing facilities, including telecommunication systems and infrastructure and to protect against cyber-attacks, fraudulent activities, information loss and other security risks and threats arising internally and externally.

The Fraud Management function manages and mitigates the risk of relevant fraud and related losses. Some of its key activities involve developing and designing internal fraud controls which are regularly reviewed to ensure relevance and effectiveness. Fraud awareness activities, measures and continuous actions are taken to ensure telecommunication fraud is minimised and the requirement for preventive controls are embedded into business processes.

Security Assurance activities performed to ensure network security protection include conducting security awareness sessions, running vulnerability management and security posture assessments, and continuous security monitoring and governance in security compliance audits and risk management. Digi complies with the ISO 27001:2013 – Information Security Management System, ISO 14001: 2015 – Environmental Management System, ISO 45001:2018 – Occupational Health and Safety Management System and Payment Card Industry/Data Security Standard (PCIDSS) standards.

Periodic meetings are held with the Chief Technology Officer to discuss, direct and approve security initiatives, activities, policies and projects driven by the Security department.

Business Continuity Management (BCM)

Digi recognises the importance of providing uninterrupted mission critical and time sensitive products and services to its customers. Hence, disruptive incidents are handled and responded to effectively to ensure a structural recovery that safeguards the interests of its stakeholders, as well as to protect the credibility and reputation of Digi.

The BCM practices adopted in Digi are aligned with ISO 22301: Business Continuity Management. The Management continuously leads the drive to enhance Digi's Business Continuity processes which encompass emergency response, crisis management, crisis communication, business continuity and Network and IT disaster recovery. In addition, Digi has an annual BCM programme which includes awareness, training, review and validation on the efficiencies and effectiveness of BCM.

Controls over Financial Reporting

The Controls over Financial Reporting (CFR) function plays an important role in evaluating and improving effectiveness of key controls surrounding Digi's financial reporting process. Its primary objective is to provide reasonable assurance regarding the reliability of financial reporting and preparation of financial statements. Reviews on internal controls over financial reporting is performed in accordance with Digi's Internal Control over Financial Reporting Framework, which requires assessment based on materiality of significant accounts, and testing and evaluation of the design and operational effectiveness of key controls.

The function adopts a continuous monitoring routine to follow up on unaddressed risks and non-operating controls, including periodic reporting to Management and the ARC on the status of controls over the financial reporting processes.

Statement on Risk Management and Internal Control

Organisation Structure

Digi has established an organisational structure with clearly defined lines of responsibility and accountability, proper segregation of duties and assignment of authority to ensure effective and independent stewardship.

Board and Management Committees

The Board Committees, namely the Audit and Risk, Nomination and Remuneration Committees have been established to assist the Board in executing its governance responsibilities and oversight function. These Board Committees have been delegated specific responsibilities all of which are governed by clearly defined Terms of Reference. The Terms of Reference of these Committees are accessible in the Corporate Governance section of Digi's website at *https://digi.listedcompany.com/corporate_governance.html.*

Various committees comprising key Management members have been established to assist and support the Board Committees to oversee core areas of business operations under their respective documented mandates. These Management Committees are:

Vendor and Investment Committee (VIC)

- Governs the approval process regarding material capital investments, operating expenditure, vendor evaluation criteria and vendor selection, in accordance with Digi's Delegation Authority Matrix (DAM)
- Occurs bi-weekly or ad hoc sessions where necessary
- Chaired by the Investment Controller with the VIC members as assigned / depicted in the Investment approval manual, in accordance with Digi's DAM to ensure sufficient quorum for all investment approvals

Regulatory Steering Committee (RSC)

- Provides direction and makes decisions on regulatory matters and/or related topics that have a significant impact to Digi
- Meets monthly
- Chaired by the CEO with key Management as RSC members

Risk Management Forum

- Forum members consists of Management who meets quarterly
- Reviews and deliberates on significant risks (threats and opportunities) in Digi
- Makes decisions on the coordinated action plans to mitigate risks

Responsible Business Forum (RBF)

- Chaired by the CEO, the forum includes the Chief Human Resource Officer, Chief Technology Officer, Chief Corporate Affairs Officer, and other key Management members
- Formulates Responsible Business strategies, policies, and goals
- Monitors and facilitates adherence to the related Responsible Business policies and manuals
- Supports Departments to meet Responsible Business goals
- Conducts Responsible Business awareness and engagement activities
- Oversees Environmental, Social and Governance (ESG) and Non-Financial Reporting (NFR) performances
- Responsible Business is presented to the Board quarterly

Assignment of Authority

The DAM provides a framework of authority and accountability and outlines approval authority for strategic, capital, and operational expenditure. The DAM is reviewed and approved by the Board in line with changes in business needs.

Code of Conduct & Agreement of Responsible Business Conduct

The Code of Conduct (the Code) and Agreement of Responsible Business Conduct (ABC) are a vital and integral part of Digi's governance regime that defines the core principles and ethical standards in conducting business and engagements with all stakeholders, and compliance with relevant laws and regulations. The Code and ABC apply to members of the Board, employees and those acting on behalf of Digi. All employees and business partners are required to confirm that they have read, understood and will adhere to the Code and ABC, respectively. The Group has established communication channels that allow concerns of non-adherence to the Code and ABC to be anonymously reported.

Compliance

The Compliance Officer supports the CEO and the Board in ensuring that:

- The Code and ABC reflect good business practices and relevant laws, regulations and widely recognised treaties
- The Code and ABC are implemented consistently and effectively through sharing of knowledge and measures for quality assurance
- Compliance incidents are consistently and effectively managed
- Reports on material breaches of the Code and ABC are made to the Compliance Committee (comprising members of the Management), members of the Board and ARC on a quarterly basis
- Capacity building for Employees, Business Partners, Management and Members of the Board and ARC on the Compliance requirements of the Group on a regular basis
- The effectiveness of the Compliance programme is periodically reviewed and improved

Statement on Risk Management and Internal Control

- Compliance risk assessment is conducted annually with a view to preventing incidents from occurring through effective remediation and mitigation steps

Management and Board Meetings

Management meetings are held weekly to identify, discuss, approve and resolve strategic, operational, financial and key management issues pertaining to Digi's day-to-day business. Significant changes in the business and the external environment are reported by the Management to the Board on an on-going basis and/or during Board meetings.

Internal Audit

The Internal Audit function is established to undertake independent review and assessment on the adequacy, efficiency and effectiveness of risk management, internal control and governance processes implemented by Management. To maintain its impartiality, proficiency and due professional care, the Internal Audit function reports functionally to the ARC and administratively to the CEO.

The annual audit plan, established using a risk-based approach, is reviewed and approved by the Board annually. Audit reports, including the audit recommendations, Management responses and action plans for improvement and/or rectification are presented and tabled to the ARC on a quarterly basis. The status of the implementation is monitored by the ARC to ensure that they are addressed timely. If deemed necessary, management representative will be required to attend ARC meeting(s) to provide explanation and propose action plans on the significant audit findings.

Further information on the Internal Audit department's activities is detailed in the Audit and Risk Committee Report of this Integrated Annual Report.

REVIEW OF THIS STATEMENT BY EXTERNAL AUDITORS

The external auditors have performed limited assurance procedures on this Statement on Risk Management and Internal Control pursuant to the scope set out in Audit and Assurance Practice Guide 3 (AAPG 3), Guidance for Auditors on Engagements to Report on the Statement on Risk Management and Internal Control included in the Annual Report issued by the Malaysian Institute of Accountants (MIA) for inclusion in the Annual Report of the Group for the financial year ended 31 December 2020, and reported to the Board that nothing has come to their attention that cause them to believe the statement intended to be included in the Annual Report is not prepared, in all material respects, in accordance with the disclosures required by paragraphs 41 and 42 of the Statement on Risk Management and Internal Control: Guidelines, nor is the Statement factually inaccurate.

AAPG 3 does not require the external auditors to consider whether the Directors' Statement on Risk Management and Internal Control covers all risks and controls, or to form an opinion on the adequacy and effectiveness of the Group's risk management and internal control system including the assessment and opinion by the Directors and Management thereon. The report from the external auditor was made solely for, and directed solely to the Board of Directors in connection with their compliance with the listing requirements of Bursa Securities and for no other purposes. The external auditors do not assume responsibility to any person other than the Board of Directors in respect of any aspect of this report.

CONCLUSION

The Board has received assurance from the CEO and CFO that Digi's risk management and internal control framework is operating adequately and effectively, in all material aspects, during the financial year under review and up to the date of this Statement. Taking into consideration the assurance from Management and relevant assurance providers, the Board is of the view that the risk management and internal control practices and processes are operating adequately and effectively to safeguard the stakeholders' interests, shareholders' investment, customer's interests, and Digi's assets.