



# Creating Sustainable Value through Responsible Governance

Guided by strong governance and a steadfast commitment to health and safety, we continue to cultivate a safe and resilient organisation.



## Our Material Topics

Health and Safety	87
Cyber Security and Data Protection	92

**Our commitment to responsible governance guides how we protect our people, secure our operations and build trust with stakeholders, grounded in strong ethics, integrity and accountability.**

## Governance as a Foundation for Sustainable Performance

Responsible governance shapes how we create sustainable value, with our decisions grounded in accountability, transparency and ethical conduct. It strengthens oversight, reinforces trust and supports disciplined management of risks and opportunities, enabling consistent performance as expectations from regulators, investors and society continue to rise.

[Refer to Commitment to Governance on pages 174 to 205.](#)

This approach also informs how we generate and share value beyond financial performance, through contributions to national development and community investments. Strong governance supports resilience across our operations, ensuring safety, reliability and business continuity, while strengthening cyber resilience and protecting data in an increasingly connected environment. Innovation and technology further enhance this foundation, improving operational capabilities, efficiency and decision-making across the business.

[Refer to Key Messages on pages 12 to 15, Health and Safety on pages 87 to 91, Cyber Security and Data Protection on pages 92 to 95, and Delivering Our Strategy on pages 52 to 83.](#)

## HS Health and Safety

### Why This Matters

We operate in the energy industry, where complex projects and geographically dispersed assets create inherent exposure to operational hazards. In this operating environment, health and safety performance depend on consistent decisions across many teams and contractors to support disciplined operational control, technical integrity and real-time risk management. In these conditions, protecting people comes first. Health and Safety performance shapes how safely work is carried out and how effectively risks are managed.

Maintaining safe performance relies on personal accountability at all levels, which makes it challenging to sustain consistent discipline across a diverse workforce and contractor base as operations grow in complexity. Physical health, mental well-being and psychosocial factors influence alertness and teamwork in high-risk settings. This makes occupational health management even more essential to ensure a workforce that is fit to work. Strong performance in these areas supports our business continuity and regulatory compliance.

### Our Focus

We focus on preventing safety incidents, workplace injuries, illnesses and health-related exposure risks through effective Health, Safety and Environment (HSE) management, supported by continuous monitoring, reviews and improvements using the Plan-Do-Check approach.

Preventing Safety Incidents

Preventing Illnesses and Health-Related Exposure

Reducing Workplace Injuries

# Creating Sustainable Value through Responsible Governance

## Our Approach

We manage health and safety through our Safety Management Approach, which is based on Compliance, Culture and Competency. These guide how we manage risk, strengthen accountability and improve safety performance across all operations.

Compliance	Culture	Competency
Drive operating discipline and apply self-regulation to manage risks and meet safety requirements.	Build a Generative HSE Culture and reinforce personal accountability across the organisation.	Strengthen human and asset capabilities to improve HSE performance.

The PETRONAS HSE Policy sets clear expectations to safeguard health, safety and the environment. Our Health, Safety and Environment Management System (HSEMS), aligned with the International Organization for Standardization’s (ISO) 14001:2015 and 45001:2018, translates these expectations into consistent operational controls, defined accountabilities and performance monitoring.

We embed HSE considerations into governance, risk management and operational decision-making through disciplined execution and continuous improvement. Regular leadership reporting enables timely intervention, learning and corrective actions where gaps are identified.

## Our Progress

We strengthened the foundations of health and safety management by reinforcing personal accountability, operating discipline, improving risk visibility, and deepening leadership and workforce engagement.

Efforts concentrated on areas where risks remain most significant, supported by stronger governance, assurance and digital enablement. Continued emphasis on culture and capability supported more consistent application of safe systems of work and earlier intervention where risks were identified.

In 2025, safety indicators showed improvement in process safety and occupational health outcomes, while injury-related metrics indicate the need for continued focus on workforce discipline, hazard awareness and preventive controls.

## 2025 Key Highlights

<b>Fatalities</b>	<b>Total Recordable Cases Frequency (TRCF)</b>	<b>Tier 1 Process Safety Event</b>	<b>Lost Time Injury Frequency (LTIF)</b>	<b>Total Recordable Occupational Illness Frequency (TROIF) – Employees</b>
<b>ZERO</b>	2025 <b>0.34</b> ▲ <i>(2024: 0.30) number per million hours worked</i>	2025 <b>2</b> ▼ <i>(2024: 7) number of cases</i>	2025 <b>0.14</b> ▲ <i>(2024: 0.10) number per million hours worked</i>	2025 <b>0.18</b> ▼ <i>(2024: 0.22) number per million hours worked</i>

In April 2025, PETRONAS responded to a fire incident involving PETRONAS Gas Berhad’s (PGB) Peninsular Gas Utilisation (PGU) pipeline near Putra Heights, Subang Jaya, Malaysia. Investigations by the Department of Occupational Safety and Health (DOSH) and other government authorities identified the cause to be anthropogenic activities in the areas surrounding the pipeline’s Right-of-Way (ROW). This emerging risk highlights the importance of continuous enhancements to our risk assessments, regulatory collaborations and monitoring of third-party activities surrounding the pipeline corridor to mitigate the risk of recurrence.

The incident tested enterprise-wide crisis leadership, with actions focused on safeguarding the public and maintaining supply continuity across the national gas network.

## Compliance

We reinforce safety compliance across our operations by ensuring adherence to applicable national and international requirements. For the year under review, we placed greater emphasis on operating discipline, governance and corrective actions to address identified gaps and reduce risk exposure across the organisation.

## Safety Management

In 2025, we focused on tightening operational risk control through disciplined execution of Safe Systems of Work, improving site supervision, contractor HSE alignment and digital-enabled assurance. We further improved compliance by enhancing the competency of our people in local regulations and international standards. This was supported through collaborations with key stakeholders, including regulatory authorities.

During the year, zero fatalities were recorded, while Total Recordable Case Frequency increased by 13 per cent and Lost Time Injury Frequency increased by 40 per cent. For land transport performance, employees and contractors travelled 44.7 million kilometres, with zero fatal or serious vehicle accidents recorded. For all reported incidents, thorough investigations were conducted with relevant subject matter experts to determine root causes and lessons learnt were shared Group-wide to prevent recurrence.

## Process Safety

Process Safety Management efforts advanced during the year through enhanced asset integrity practices, expanded risk management exposure for new businesses, and stronger process safety ownership and capability, supported by deeper leadership engagement and closer regional collaboration with partners from the Centre for Chemical Process Safety. Key initiatives included improving consistency in flange integrity management to maintain the technical integrity of bolted flange joints and piping systems, thereby minimising Process Safety Events (PSE) across all operating plants. Additional focus was placed on ageing asset management.

Through these targeted interventions, we achieved a 71 per cent reduction in Tier 1 PSE, with zero fatalities recorded during the year. In addition, our initiative to optimise safety critical equipment identification, maintenance planning and resource management received external recognition through the IChemE Malaysia Process Safety Award 2025.

## Self-Regulation

Readiness for Special Scheme of Inspection certification remained central to advancing self-regulation across PETRONAS-owned assets and supporting regulatory compliance. Through these efforts, seven occupiers successfully achieved the Special Scheme of Inspection certification in 2025, maximising plant run length across our integrated value chain.

## Leveraging Digitalisation and Generative Artificial Intelligence in Managing Health, Safety and Environment Risk

We continued to expand our Group-wide HSE risk management capabilities through the progressive implementation of digital and advanced analytics solutions. In 2025, our integrated risk analytics platform, Artificial Intelligence Incident & Risk Analytics (AIIRA), was enhanced with generative AI and machine learning models to deliver more accurate predictive risk modelling and actionable recommendations in mitigating operational risks. These capabilities provide near real-time risk visibility, support enterprise-wide adoption and embed risk intelligence into frontline-to-management usage, enabling earlier risk identification, improved forecasting confidence and timely intervention across our operations. The maturity and impact of AIIRA were externally recognised when the platform was named Country Winner for Malaysia in the Best in AI Ready Platform category at the International Data Corporation (IDC) Future Enterprise Awards 2025.

# Creating Sustainable Value through Responsible Governance

## Culture

Since 2017, we have adopted a Generative HSE Culture, embedding HSE into the organisation's mindset to shape behaviours and decision-making at all levels. Rooted in the principle of care and guided by the mantra of 'Doing the right things right, even when no one is watching,' leaders at every level are entrusted to model and reinforce this culture through daily actions and moments of influence. Supported by targeted engagement programmes and training, more than 7,500 leaders and frontliners have been equipped to champion consistent HSE messaging and uphold safe, responsible and ethical practices as shared organisational values.

Our HSE Accountability and Behaviour Reinforcement framework strengthens our Generative HSE Culture by promoting accountability and safe behaviours at all levels. The framework establishes principles for positive reinforcement, recognising and rewarding employees who comply with HSE requirements.

Our investigation teams review major incidents and non-compliance cases to identify underlying behavioural factors. Structured corrective measures are determined and implemented by each business' HSE Accountability and Behaviour Reinforcement Committee. Through integration with our Generative HSE Culture Leadership Programme and various HSE campaigns, the framework continuously reinforces accountability and proactive safety behaviours across the organisation.

### Protecting Our Workforce's Health and Well-being

We remain steadfast in our commitment to protecting our workforce's right to a safe and healthy working environment, driving resilience and productivity, and supporting sustainable business performance through strengthened Industrial Hygiene and Occupational Health initiatives.

In 2025, Industrial Hygiene focused on reducing occupational noise exposure risk through implementation of engineering controls, improving ventilation requirements and gas testing practices for work within confined spaces, and utilising digital systems with AI to strengthen management of hazardous chemicals. These efforts enabled consistent health risk assessments, improved data visibility and systematic monitoring of exposure-related risks across operations.

Occupational Health focused on supporting business continuity by strengthening and streamlining the capabilities of the integrated Medical Emergency Response and Mass Casualty Incident management across Malaysia operations, particularly in the Southern, Northern and East Coast regions that house multiple operating units. Enhanced interventions and mitigation measures were also implemented to ensure the workforce is physically and mentally resilient, remains fit to work, and is safeguarded against fatigue, substance misuse and occupational illness. Through our holistic occupational health and wellness programme, MESTIfit4health, we equip employees with a proactive approach that fosters healthy behaviours and empowers them to take ownership of their well-being to reduce the risk of occupational injuries and illnesses while enhancing overall workforce performance and resilience.

For the year under review, we recorded an 18 per cent reduction in Total Recordable Occupational Illness Frequency for employees.

## Competency

We develop and enhance the competency of our workforce through training and development programmes to ensure our leaders and frontline personnel possess the skills and knowledge to uphold safety standards and drive operational excellence.

We also participate in a wide range of local and international forums, reflecting our commitment to fostering strong collaboration and sharing knowledge and technical expertise among industry experts.

### Crisis and Incident Management

As a global operator in the oil and gas industry, PETRONAS recognises the various hazards and incidents that our line of business must contend with. To mitigate the disruptive nature of these events, the Group has established a strong management system that effectively addresses crisis and incident risks at every level.

We take proactive measures to prevent recurrence of incidents. We established the Organisational Learning from Incidents portal in 2024, a centralised resource that serves as a one-stop centre to improve accessibility and availability of materials from past lessons learnt and resources on incident management. In 2025, we benchmarked our internal incident governance practices to ensure alignment with industry peers.



Strengthening incident preparedness through on-site inspection.

## Sustainability Impact

Our continued focus on health and safety advances responsible operations through strong governance, disciplined risk management and a clear focus on protecting our people. In 2025, we recorded zero fatalities, with improvements in process safety performance, reflecting the effectiveness of our controls and operational discipline across PETRONAS operations.

Operational resilience was further strengthened through enhanced safe work practices, stronger workforce competency, closer contractor alignment and digital-enabled assurance guided by our Generative HSE Culture. Improved risk visibility, stronger process safety ownership and holistic workforce health initiatives support earlier intervention and safer decision-making across the organisation, contributing to a healthier workforce and more reliable operations that sustain long-term business performance.

# Creating Sustainable Value through Responsible Governance

## Cyber Security and Data Protection

### Why This Matters

As a global energy company with extensive digital integration across our value chain, we operate within a rapidly evolving cyber threat landscape. Threat actors increasingly apply AI to scale phishing, social engineering and ransomware attacks across both information technology and operational technology environments. Deeper digitalisation, cloud adoption and reliance on interconnected suppliers, remote access and personal devices further expand the cyber risk perimeter. At the same time tightening regulatory expectations across jurisdictions, alongside geopolitical tensions, add complexity to oversight and compliance.

A significant cyber incident could disrupt operations, compromise sensitive or proprietary information and undermine stakeholder confidence, exposing the Group to regulatory, financial and reputational consequences. Robust cyber security and data protection are, therefore, essential to protect the confidentiality, integrity and availability of critical information assets and support operational resilience.

### Our Focus

Our aim is to protect our critical systems, data and operations from cyber threats by strengthening resilience, control effectiveness and cyber awareness across the organisation. We monitor cyber security performance through a range of preventive, detective and responsive indicators covering system integrity, workforce awareness, third-party oversight and incident response effectiveness.

### Our Approach

We manage cyber security and data protection through a risk-based, enterprise-wide approach anchored on our Enterprise Cyber Security Governance Framework. The framework drives robust risk management across information technology, operational technology and third-party environments, protecting the confidentiality, integrity and availability of physical and digital information assets.

Our approach integrates regulatory and compliance requirements, supports personal data protection and critical national infrastructure security, and aligns with the PETRONAS Enterprise Risk Management Framework and Risk Policy. By embedding cyber security and data protection into enterprise risk management, we reduce potential financial and reputational impacts while strengthening operational resilience.

### Governance, Policy and Framework

The Board oversees cyber security and data protection through structured governance frameworks, regular reporting and assurance processes, with visibility over the effectiveness of controls across the Group. Oversight is supported by the Enterprise Cyber Security Governance Framework, which standardises controls across business units, information technology and operational technology environments and third-party suppliers, and is reinforced through a three-level Line-of-Assurance model.

Regulatory compliance and critical infrastructure risks form part of Board oversight, with structured reporting on compliance with applicable data protection such as Malaysia's Personal Data Protection Act (PDPA), cyber security laws, National Critical Information Infrastructure obligations and remediation actions. We also fulfil our role as one of three Energy Sector Leads under Malaysia's Cyber Security Act 2024, with the Board maintaining visibility over sector-level responsibilities, assurance activities and related cyber risk exposures.

Cyber security and data protection operate in an integrated manner. The Enterprise Cyber Security Governance Framework, together with the PETRONAS Digital Personal Data Protection Act (PDPA) 2024 Readiness Programme, establishes the personnel, processes and procedures required to protect our systems, assets, data and operations.

<p><b>Enterprise Cyber Security Governance Framework</b></p> <ul style="list-style-type: none"> <li>• Ensures right people, processes and controls protect systems, assets, data and operations.</li> <li>• Establishes Control Framework and Control Standards.</li> <li>• Aligns with the United States National Institute of Standards and Technology (NIST) Cybersecurity Framework.</li> <li>• Applies five core functions: Identify, Protect, Detect, Respond and Recover.</li> </ul>	<p><b>Cyber Security Risk Management Guideline</b></p> <ul style="list-style-type: none"> <li>• Aligns with PETRONAS Enterprise Risk Management Framework and integrates PETRONAS Risk Policy.</li> <li>• Defines standardised approach to assess, respond to, and monitor cyber security risks.</li> <li>• Supports accountability and informed decision-making.</li> </ul>	<p><b>Data Privacy Risk Management</b></p> <ul style="list-style-type: none"> <li>• Integrates data privacy requirements into Cyber Security Control Standards and applies Data Protection Impact Assessments for systems processing personal data.</li> </ul>
---	--	--

**Compliance with Regulations**

We ensure compliance with cyber security and data protection requirements across our operations, supported by strong governance and clear accountability structures, including alignment with the Malaysia Cyber Security Act 2024 (Act 854).

<p><b>Role as National Critical Information Infrastructure Sector Lead (Energy)</b></p> <ul style="list-style-type: none"> <li>• Designate National Critical Information Infrastructure (NCII) entities under sector leadership.</li> <li>• Develop Cyber Security Code of Practice to guide implementation of Act 854 across PETRONAS-designated NCII entities.</li> </ul>	<p><b>Role as a National Critical Information Infrastructure entity</b></p> <ul style="list-style-type: none"> <li>• Align existing cyber incident reporting processes with the Cyber Security Act 2024 requirements into operations, including coordination with the National Cyber Security Agency (NACSA).</li> <li>• Submit PETRONAS' NCII Risk Assessment Report.</li> </ul>	<p><b>Data Protection and Privacy Controls</b></p> <ul style="list-style-type: none"> <li>• Data governance controls aligned with PDPA principles embedded across key digital life cycle processes.</li> <li>• Personal data managed across seven processes through privacy-by-design integration.</li> </ul>
---	---	---

**Measuring Assurance and Cyber Resilience**

We apply the Integrated Assurance framework to provide Group-wide visibility of cyber security controls, compliance and resilience across information technology, operational technology and third-party environments.

<p><b>Assurance and Measurement Approach</b></p> <ul style="list-style-type: none"> <li>• Integrated Assurance framework monitors cyber security control implementation and compliance.</li> <li>• Centralised assurance platform tracks Information Technology and Operational Technology functional checklists across businesses.</li> <li>• Ongoing reporting provides visibility of control effectiveness and gaps.</li> </ul>	<p><b>Measuring Cyber Resilience</b></p> <ul style="list-style-type: none"> <li>• Cyber security resilience assessed through control compliance monitoring, cyber exercises and simulations.</li> <li>• Risk-based metrics informed by World Economic Forum guidance and industry benchmarks.</li> <li>• Key indicators include phishing resilience, vulnerability management and incident response effectiveness.</li> <li>• Metrics integrated into enterprise-level reporting to support Board and management oversight.</li> </ul>
--	--

# Creating Sustainable Value through Responsible Governance

## Our Progress

Our expanding digital footprint across information technology and operational technology environments increases exposure to more sophisticated cyber threats across the enterprise and the wider value chain. In response, cyber security and data protection were strengthened through the application of the PETRONAS Enterprise Cyber Security Governance Framework, reducing vulnerabilities across critical systems, enhancing monitoring and response capabilities, and improving protection of data and intellectual property as digitalisation deepens.

Efforts during the year also focused on people as a key line of defence. Workforce behaviour was treated as an operational risk factor rather than a training topic. Employee awareness and capability building were prioritised to address human-layer risks, recognising that phishing and social engineering remain common attack vectors, with targeted programmes supporting behavioural change and a cyber-safe culture across the workforce. As a result, no major cyber security incidents were recorded in 2025, while the phishing click rate remained below 4 per cent, demonstrating overall cyber resilience in a dynamic threat environment.

## 2025 Key Highlights

Major cyber security incidents

**ZERO**

Phishing click rate under

**4%**



Strengthening cyber resilience through real-time monitoring.

### Strengthening Cyber Resilience

Cyber security controls were enhanced across applications, devices and internet-facing systems, including tighter controls on employee-owned devices covering access rights, downloads, encryption and device usage to reduce exposure and strengthen data protection.

Cyber security performance improved through stronger monitoring and response capabilities. Existing tools, processes and capabilities were optimised, while the cyber security portfolio was streamlined to improve operational efficiency, support continuous monitoring and manage increasing threat volumes.

Board and leadership awareness was raised through the PETRONAS Board Excellence Programme, including live demonstrations on current threats, interactive discussions and a cyber security tabletop exercise to highlight the Board's strategic role and establish a practical understanding of their responsibilities across the organisation's digital and technology agenda.

### Enhancing Data Governance

Data governance controls were embedded across nine critical digital life cycle processes. These controls align with PDPA principles, with privacy-by-design integrated into digital workflows.

Personal data governance was strengthened through updates to Data Governance documentation, which incorporate requirements under the PDPA 2024 amendments. This included classifying biometric data as sensitive personal data in line with updated regulatory definitions and protection requirements, and incorporating updated regulatory terminology and new data subject rights, including data portability, to align with evolving regulatory expectations. These enhancements strengthened alignment with regulatory requirements, and improved clarity and consistency in the classification and handling of sensitive personal data. They also increased organisational readiness to manage personal data responsibly and comply with expanded data subject rights, reducing regulatory and compliance risk.

### Data Privacy Risk Management

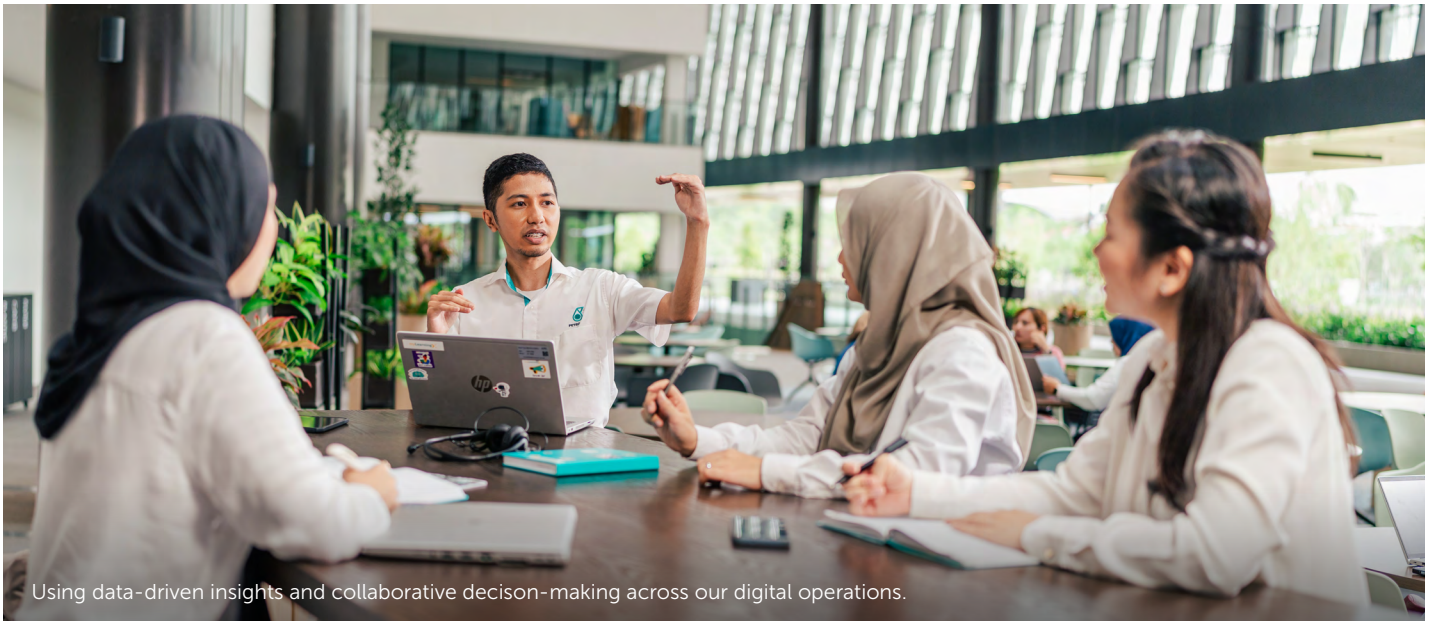
Data privacy risk management was advanced through a pilot PDPA 2024 readiness assessment across 17 targeted applications, covering Tier 1, Tier 2 and Tier 3 personal data categories. The assessment identified gaps, evaluated risks and defined mitigation actions across different data sensitivity levels, including basic personal data limited to business contact information, extended personal data beyond business contacts, and sensitive personal data protected under the PDPA and General Data Protection requirements.

Data privacy requirements were also incorporated into Cyber Security Control Standards, and Data Protection Impact Assessments (DPIAs) were applied to systems processing personal data to ensure consistency in control implementation.

### Building Awareness and Workforce Capability

Training programmes were delivered to inculcate cyber security awareness and behavioural change across the workforce, supported by initiatives such as the Global Cyber Security Month and targeted learning activities. Engagement approaches included communications, targeted microlearning and role-based workshops, as well as participation in industry forums to share insights on safeguarding critical infrastructure. Strong engagement was achieved across training activities, with a high completion rate for the annual cyber security refresher assessment.

Data protection and privacy awareness programmes further supported the application of PDPA requirements and data protection best practices. These programmes equip employees with the knowledge to understand their responsibilities in handling personal data and to apply privacy requirements appropriately in their day-to-day roles.



Using data-driven insights and collaborative decision-making across our digital operations.

### Sustainability Impact

By embedding cyber security and data protection into everyday processes, PETRONAS has strengthened energy-supply reliability, protected critical information assets and bolstered long-term resilience and stakeholder confidence. As digital integration strengthens across operations and partners, enterprise-wide visibility and coordination support consistent readiness and stable performance across the supply chain.

Reduced exposure across applications, devices and internet-facing systems enables safer, more efficient use of digital tools, and streamlined monitoring improves response to rising threat volumes. Greater workforce awareness and tighter supplier oversight foster secure digital behaviours and supply chain readiness, supporting compliant business practices. These ongoing actions reinforce PETRONAS' ability to safeguard critical assets and deliver safe, reliable, sustainable value over the long term.