

### Strategy 5: Integrity Governance

Key Action Aspects	2024 Performance	Short-term targets (2025)	Medium-term targets (2026-2030)	Long-term targets (2031-2050)
<p><b>1.</b> Uphold anti-corruption and integrity in business operations and implement internal control mechanisms</p>	<p><b>Uphold integrity governance</b> Maintained integrity governance through the implementation of avoidance of conflict of interest in accordance with Article 206 of the "Company Act"; strengthening the fiduciary duties of board members so as to scrupulously avoid unjust enrichment; strict legal compliance to ensure the soundness of board functions; and the establishment of multiple whistleblowing mechanisms.</p>	<p>Notify directors and supervisors to comply with the "Integrity Governance Principles for Directors and Supervisors;" continue to require directors and supervisors to strictly avoid conflict of interest and unjust enrichment.</p>	<p>Continue to require directors and supervisors to strictly avoid conflict of interest and unjust enrichment in accordance with the "Integrity Governance Principles for Directors and Supervisors."</p>	<p>Strengthen the supervisory function of the board and improve management efficiency.</p>
<p><b>2.</b> Strengthen information security management to ensure operation continuity</p>	<p><b>Strengthen information security</b> In addition to compliance with the "Cyber Security Management Act" and relevant laws, BSI has been commissioned to review the ISO 27001 ISMS certification every six months.</p>	<p><b>1</b> Comply with the "Cyber Security Management Act" and relevant laws, information security policies of the FSC, plus ISO 27001 and other international standards.  <b>2</b> In accordance with the FSC's reference guide on financial zero trust architecture, the TWSE will assess the industry's familiarity with the model, formulate a blueprint for introducing zero trust architecture, and promote its adoption.</p>	<p><b>1</b> Continue to comply with the "Cyber Security Management Act" and relevant laws, information security policies of the FSC, plus ISO 27001 and other international standards.  <b>2</b> Continue to follow the FSC's reference guide on financial zero trust architecture and gradually introduce zero trust architecture into high-risk areas of information safety control.</p>	<p>Continue to comply with the "Cyber Security Management Act" and relevant laws, information security policies of the FSC, plus ISO 27001 and other international standards.</p>

