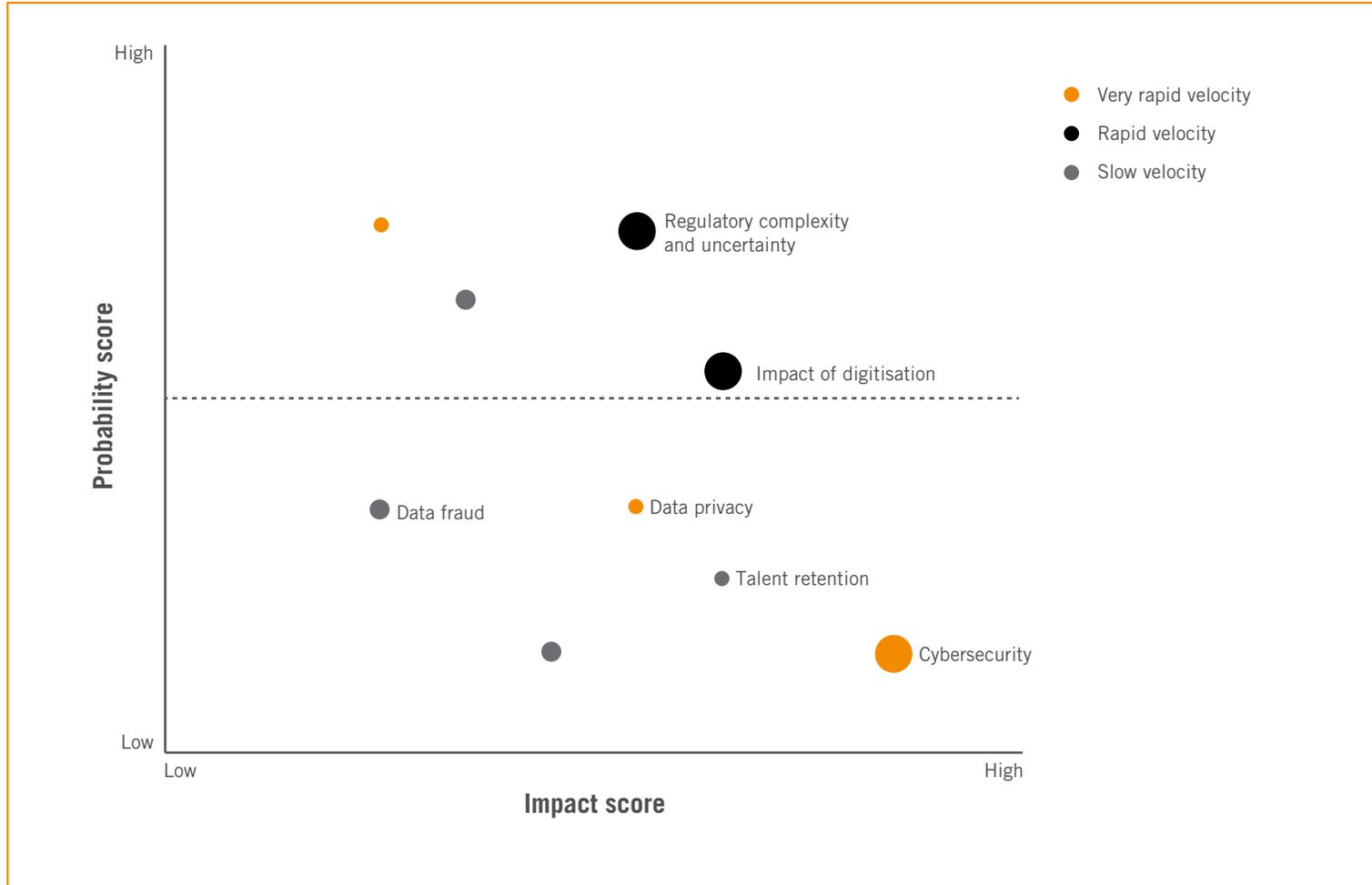


## RISK MANAGEMENT OUTLOOK/EMERGING RISKS FOR THE NEXT 12 MONTHS

The risk outlook detailed below demonstrates the emerging risks which the group has identified could have material business impacts. The board and executive management have ensured that appropriate mitigation strategies are in place, including creating an environment of extensive oversight by the cluster excos.



## RISK MANAGEMENT OUTLOOK/EMERGING RISKS FOR THE NEXT 12 MONTHS *(continued)*

The following mitigating strategies and management actions have been implemented to deal with these emerging risks.

Emerging risks	Risk mitigation strategies
<ul style="list-style-type: none"> <li>Regulatory complexity and uncertainty</li> </ul>	<ul style="list-style-type: none"> <li>Increased collaboration between compliance and legal teams to ensure that revised and new legislation is quickly identified, analysed and assessed for business implications</li> <li>Establishment of a special projects team under group legal with the necessary accountability and authority for implementation of group-wide compliance projects</li> <li>Continuous tracking and monitoring by subsidiary and group Audit and Risk Committees</li> <li>Appointment of a centralised group compliance officer and group anti-money laundering officer</li> <li>Implementation of phase 3 of the group's combined assurance model.</li> </ul>
<ul style="list-style-type: none"> <li>Impact of digitisation</li> </ul>	<ul style="list-style-type: none"> <li>Enhanced cross-business collaboration on IT projects</li> <li>Allocation of single line of accountability for strategic IT projects.</li> </ul>
<ul style="list-style-type: none"> <li>Data privacy and data fraud</li> </ul>	<ul style="list-style-type: none"> <li>Implementation of Protection of Personal Information (POPI) ahead of legislative imperatives</li> <li>Increased encryption strategies for all data entering and leaving the group</li> <li>Increasing the robustness of data security programme.</li> </ul>
<ul style="list-style-type: none"> <li>Cybersecurity</li> </ul>	<ul style="list-style-type: none"> <li>Performing annual penetration testing of systems (bi-annual assessments under consideration)</li> <li>Staff awareness programme</li> <li>Enhance IT governance framework</li> <li>Continuous improvement of the group's IT security strategy.</li> </ul>
<ul style="list-style-type: none"> <li>Talent retention</li> </ul>	<ul style="list-style-type: none"> <li>Continuous monitoring of successions plans</li> <li>Continuous enhancement of leadership development through the group Duke and Harvard leadership programmes</li> <li>Continued implementation of staff retention strategies and annual, independent, staff engagement surveys.</li> </ul>
<ul style="list-style-type: none"> <li>Volatile economic conditions and political and social instability</li> </ul>	<ul style="list-style-type: none"> <li>Consistent monitoring of economic conditions and its impact on the businesses strategic intent</li> <li>Performance of quarterly reviews.</li> </ul>
<ul style="list-style-type: none"> <li>Failure on strategy execution</li> </ul>	<ul style="list-style-type: none"> <li>Introduction and creation of cluster concept to monitor delivery of the group's strategic intent, thereby facilitating quicker interventions where appropriate</li> <li>Capacitation of EPMO to independently track strategic projects and report on a quarterly basis to the relevant governance structures</li> <li>Creation of innovation model to driving continuous improvement.</li> </ul>
<ul style="list-style-type: none"> <li>Key sovereign infrastructure failures</li> </ul>	<ul style="list-style-type: none"> <li>Enhanced business continuity and crisis management frameworks – revalidated and simulated annually</li> <li>Establishment of alternative service delivery and IT recovery sites – contracted and in place.</li> </ul>
<ul style="list-style-type: none"> <li>Regulatory enforcement actions</li> </ul>	<ul style="list-style-type: none"> <li>Expanded compliance risk monitoring plans for all regulated entities</li> <li>Progression of the group's combined assurance framework beyond the existing basic capability.</li> </ul>
<ul style="list-style-type: none"> <li>Extreme underwriting losses</li> </ul>	<ul style="list-style-type: none"> <li>Robust reinsurance programmes in place</li> <li>Robust regulatory capital monitoring and oversight</li> <li>Enhanced stress-testing models to model impacts of extreme scenarios (one-in-200-year event)</li> <li>Development and implementation of internal models to determine capital sufficiency in the event of extreme events manifesting.</li> </ul>