State-sponsored cyberattacks, such as those from North Korea, are another threat. This combination of criminal and state-sponsored threats increases ASEAN's risk profile, creating obstacles for foreign investment and hampering the growth of the digital economy.

## 1.2 Policy preparedness is still nascent with a lack of institutional oversight and limited funding to fortify digital economies

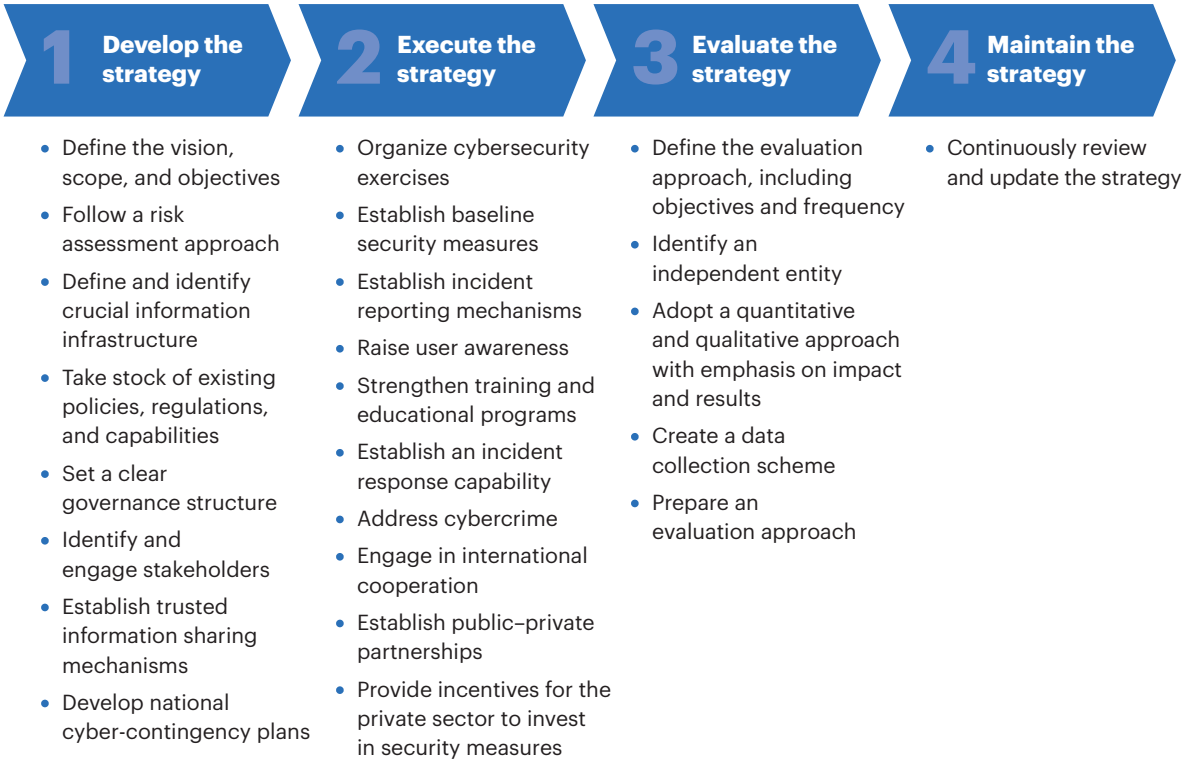
The region's cyber resilience is low, particularly around policy, governance, and cybersecurity capabilities. The absence of a unifying regional governance framework makes it difficult to collaborate and share intelligence within and across countries. Businesses have also underestimated the value-at-risk, resulting in a lack of adequate spending on cybersecurity.

### 1.2.1 Varying levels of cyber readiness, with some countries lacking a strategic mindset about cybersecurity policy and governance

The Good Practice Guide from the European Network Information Security Agency (ENISA) cites four steps in defining and implementing a sound national cybersecurity strategy (see figure 4).

A look at the regional cybersecurity policy landscape reveals varying levels of cyber readiness, particularly around strategy definition and implementation, legislation, and governance (see figure 5 on page 7).[9] See the appendix for more about the current situation.

Figure 4
**Four-phased approach to national cybersecurity strategy development**




Sources: European Union Agency for Network and Information Security; A.T. Kearney analysis

[9] Based on available information in the public domain