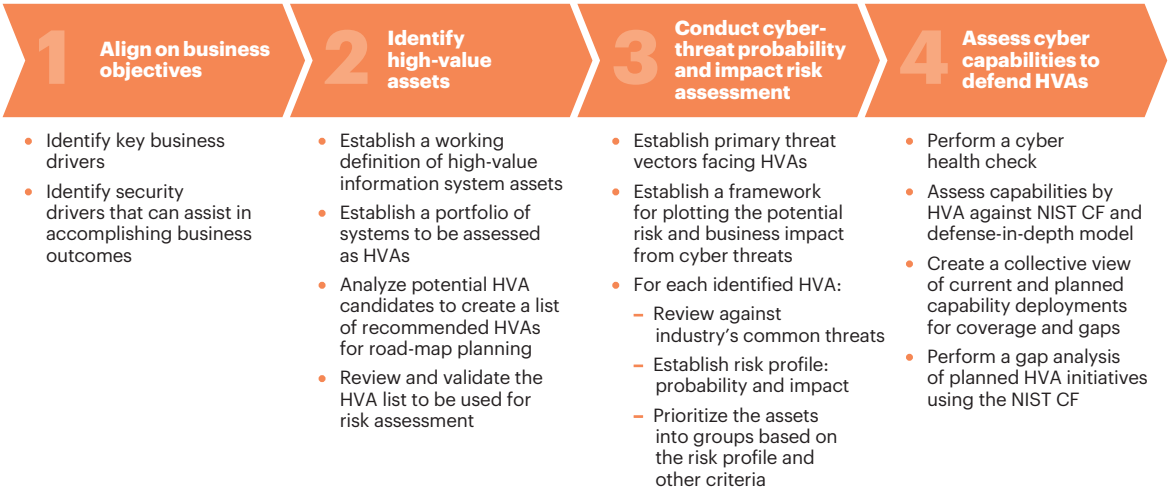
3.3.1 Foster a risk-centric mindset around cybersecurity for the corporate sector

The lack of a holistic approach around strategy, governance, organization, and culture often results in organizations being highly vulnerable despite relying on the best vendors and products. A four-step approach can help companies define their cybersecurity strategy (see figure 24).

Figure 24
Define a cybersecurity strategy with a focus on four areas



Notes: HVA is high-value asset. NIST CF is the National Institute of Standards and Technology Cybersecurity Framework.
Source: A.T. Kearney analysis

The first step is to align on business objectives and raise the profile of cybersecurity as a business risk imperative. Second, high-value assets should be identified and prioritized Third, a cyber threat impact risk assessment should be conducted. Finally, it is imperative to identify cyber capabilities needed to defend high-value assets.

> "We are in the process of setting up the CISO function with an independent mandate to report to the board, distinct from the CIO. We have conducted cybersecurity posture assessments across our major operating companies. This has helped to build awareness, but there is a lot of work to do to build a solid governance framework."
>
> **—major regional telecoms group**

In defining their strategy to enhance cyber resilience, businesses need to consider the value-at-risk. To assess the value-at-risk, businesses could take either an asset- or liability-based view An asset-based view involves valuing critical assets and the potential reputational damage from an attack. Alternatively, businesses could consider a liability-based approach, building scenarios and quantifying the financial and reputational loss Building potential scenarios with a combination of historical data and judgment about the probability of a threat can create a better understanding of the value-at-risk and help allocate resources in a more judicious manner

Businesses should leverage industry best practices and standards such as the NIST Cybersecurity Framework, ISO 27001, and an architecture framework based on risk-centric security (see figure 25).