Virtual CISO

(Chief Information Security Officer)

Leverage the benefits of highly experienced senior consultants to set, develop and operationalize your information and cybersecurity strategy

What is a Virtual CISO?

The Virtual CISO role embeds senior security leadership into an organization and brings the security lens to the organizations vision. The role hits the ground running whether in a small to medium size business or in a large enterprise with existing security functions in place. As the role is that of an external advisor, an objective view is always presented.

BSI have expert capability to supplement existing security teams in operationalizing the culture of security into the organizations Business as Usual operations and culture. At BSI, we believe the approach to making the security journey successful is to work collaboratively with existing teams, ensuring that security is balanced in a meaningful way to:

- facilitate delivery of business objectives
- meeting compliance obligations
- enabling secure ways of working, without stifling innovation and rapid delivery

What does the VCISO look like in practice?

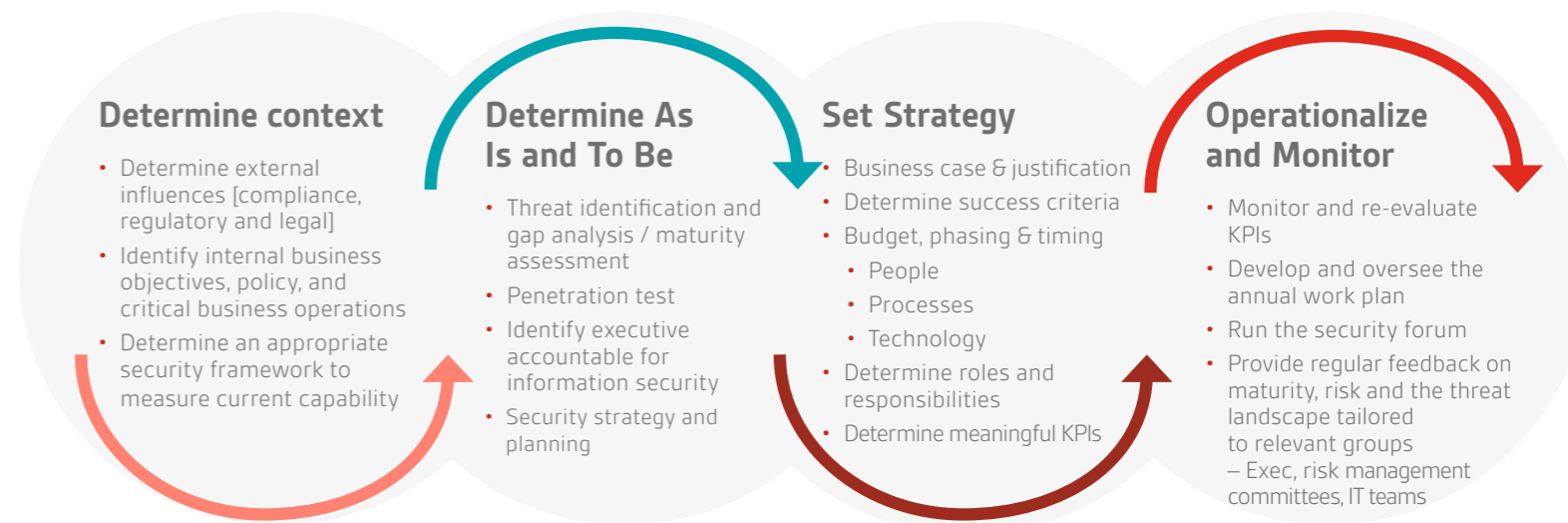The diagram on the right represents a sample end-to-end VCISO engagement leveraging the BSI model.

We work with our clients to find the right balance of resources required here, often these are front loaded across the first three phases into continuous blocks of time, which taper down as operational security functions mature. The Senior CISO role focuses then on monitoring KPIs and continuous improvement and adaption to the threat landscape.

Challenges

- A challenge encountered with the VCISO role, is that often a lot of richness of detail is missed by not being constantly present. While this is certainly true, the complete absence of any security presence means that progressing the cyber security agenda is almost certainly halted and effective leadership to drive the security agenda is absent. This is a balance that is agreed when understanding your organizational need.

- To overcome this challenge, specifically where there is a need for a full time on-site CISO, BSI deploy resources into that role and drive the security agenda, while also leading the hiring process to identify fit for purpose full-time replacement.

- Another effective alternative approach is to deputize or hire a capable but less senior staff member to fulfil certain security related obligations in the absence of the part time CISO, this ensures a level of continuity and continuation of the security agenda.

Benefits

- Lower financial barrier to entry to gain access to high quality security experienced advisors and services, compared to hiring a full time high-quality CISO.

- Delivery of objective feedback on current risks and security maturity .

- Provides insight to the wider security landscape due to being involved in multiple industries and organizations.

- Increases information security resilience and decreases likelihood of successful attack.

Determine context
- Determine external influences [compliance, regulatory and legal]
- Identify internal business objectives, policy, and critical business operations
- Determine an appropriate security framework to measure current capability

Determine As Is and To Be
- Threat identification and gap analysis / maturity assessment
- Penetration test
- Identify executive accountable for information security
- Security strategy and planning

Set Strategy
- Business case & justification
- Determine success criteria
- Budget, phasing & timing
  - People
  - Processes
  - Technology
- Determine roles and responsibilities
- Determine meaningful KPIs

Operationalize and Monitor
- Monitor and re-evaluate KPIs
- Develop and oversee the annual work plan
- Run the security forum
- Provide regular feedback on maturity, risk and the threat landscape tailored to relevant groups – Exec, risk management committees, IT teams

If you would like to hear more

bsi.