



Cyber cost optimization

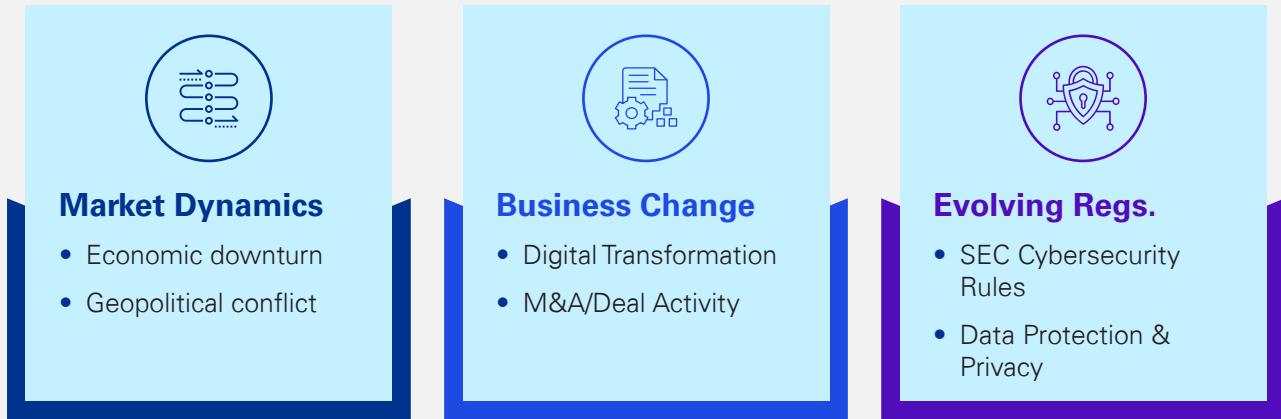
Helping business leadership and CISOs to more effectively and efficiently manage risks which achieving higher returns on security and risk investments.

February 2023

The speed of change in cybersecurity drives the need to optimize costs

Of the family of enterprise risks, cybersecurity is perhaps the most dynamic, with the threat landscape changing by the day or even hour. The effectiveness of cybersecurity strategy, services, and tools is impacted by the business change, which creates a need to remain agile in the face of new and emerging risks. Maintaining readiness usually requires continuous and evolving investment, with many organizations struggling to understand the value and risk reduction delivered by their cybersecurity programs.

Business Factors Influencing Cybersecurity Spend




Balancing cost moderation and unacceptable risk

The financial burden of maintaining an effective cybersecurity program warrants oversight to be sure of prudent investments. However, there must be a balance between a judicious review of spend and a restriction preventing a cybersecurity organization from delivering the services needed to avoid a significant incident or business disruption. Effective control of costs can be achieved with a cooperative approach between financial, cybersecurity, and risk leadership that prioritizes business growth objectives aligned with a risk-based cybersecurity investment strategy.

A coordinated methodology for managing cybersecurity spend

Spend analysis for cybersecurity begins by setting achievable objectives that aren't solely focused on cost takeout. They should consider the need for a stable core of foundational services, the agility to support business change, and the people required to support both.



Common questions about cybersecurity spend.

- How can we optimize the performance of existing cybersecurity investments?
- How can we cut costs without taking on uncomfortable levels of risk?
- How can I work to make cyber spend more predictable and avoid big "refresh" cycles?

Our approach to Cyber Cost Optimization

1. Gain visibility into your cost base and budgetary priorities

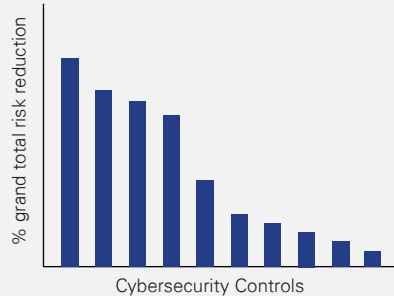
2. Analyze by KPMG Cyber cost optimization hypotheses

High-level, standardized focus areas for opportunity identification

Levels	Cyber investment and expenditure	Organizational rightsizing	Process improvement	Tool rationalization
	Revisit inflight initiatives	Contractor conversion	Process convergence	Tool de-duplication
Hypotheses	Operational expenditure management	High to low cost migration	Process simplification	Tool performance enhancement
	Business chargeback model deployment	Non-core function outsourcing	Manual process automation	
			Self-service and enable business	

3. Evaluate controls effectiveness against risk reduction

Tailored, risk-focused opportunity identification



4. Perform focused deep-dives

Domain specific opportunity identification e.g.

- Identity & Access Management
- Application Security
- Data Protection
- Infrastructure Security
- Cyber Resilience & Response

5. Execute, realize and measure prioritized cost optimization recommendations

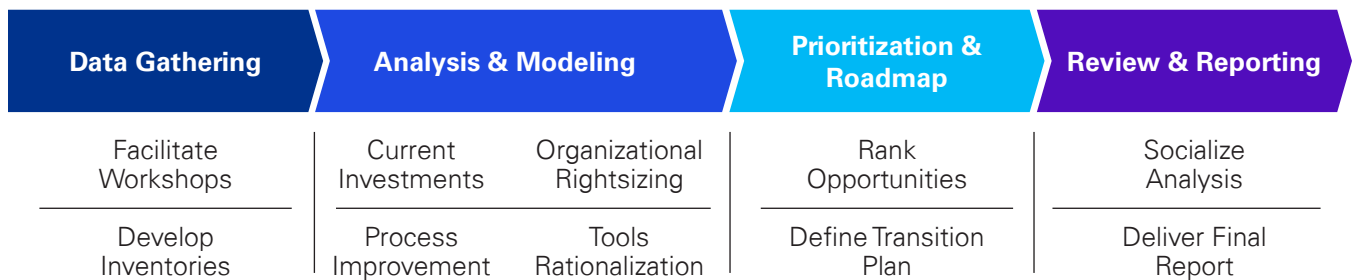
Aligned to KPMG Elevate to transform cost control while preserving risk containment

- Provides a flexible delivery model that can be leveraged for all or part of the framework to address specific needs
- Evaluates organizational design, process, and tools portfolios to deliver insights and action plans for savings and efficiency across enterprise cyber operations

What is Elevate?

Elevate is the firm's enterprise performance transformation offering designed to fundamentally and sustainably improve a business's financial trajectory through a balanced focus on growth and cost.

The rapid assessment model



Data Gathering

- Meet with key stakeholders to understand organizational priorities for cybersecurity
- Inventory spend on people, tools, and service delivery



Analysis and Modeling

- Leverage data-driven insights for organizational rightsizing and working capital optimization
- Identify opportunities for simplification, reduction of redundancy, and support for agility



Prioritization and Roadmap

- Focus on areas of highest impact with dynamic risk management and transition scenario analysis
- Remove complexity, favor automation, and leverage diverse service delivery models



Review and Reporting

- Socialize plans with program sponsors and leadership, confirming cultural alignment
- Deliver final readout and walkthrough of cost opportunities, transition plan, and outcomes

Contact us



Rik Parker
Principal, Advisory
Cyber Security Services
E: rikparker@kpmg.com



Katherine Herbert
Director, Advisory
Cyber Security Services
E: katherineherbert@kpmg.com



Lekshmy Sankar
Director, Advisory
Cyber Security Services
E: lekshmysankar@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. NDP434879