# Security through a downturn

## Five strategies for cyber cost optimization

KPMG International

home.kpmg/cybersecurity

# Foreword

Economic uncertainty is driving many organizations to revisit their overall cost efficiency. Depressed revenues (largely resulting from COVID-19) are driving a hunt for operating cost reduction and the preservation of working capital. No organizational function can be expected to be shielded from cost pressure, including cyber security. Chief Information Security Officers (CISOs) should anticipate pressure on their program budgets and proactively identify measures to contain their costs while delicately balancing 'future proofing' the ever-evolving threat landscape.

Widespread budgetary contractions follow a period of significant investment in cyber security, during which organizations rapidly matured their cyber security capabilities to maintain pace with the evolving threat landscape. Indeed, in 2019 the Harvey Nash/KPMG CIO Survey identified the biggest budget increases in 15 years, driven by investments in cyber security (up 14 percent as a board priority). Yet, in 2020 the survey identified only a 5 percent increase, a much slower increase from previous years. This new reality period will likely be the first time many CISOs will face cost pressures.

Achieving cost efficiencies while still maintaining robust cyber security is a complex task at the best of times. COVID-19 has significantly impacted the complexity of this challenge. Not only are CISOs being faced with increased cost pressures, they have also had to quickly adapt their security to defend against adversaries seeking to capitalize on new ways of working, namely employees working from home, and whose home systems may be less well protected.

In this report, we explore five key problem areas and corresponding cost optimization strategies that CISOs should consider. The various approaches depend very much on where you are in the cost optimization journey. Some of these are more tactical, where the focus is on improving performance to generate ongoing efficiencies, and some more structural and strategic, so that while some investment is required, the results will yield a significant return on security investment.

**Akhilesh Tuteja**
Global Cyber Security Leader
KPMG

# Contents

# Five strategies for cyber cost optimization

High Average Low

| | 1. Urgent need for cash preservation | 2. Increasing third-party security spend |
|---|---|---|
| **Challenge** | | |
| **Cost optimization opportunity** | — Pause discretionary spend<br>— Pause 'low-risk' review and testing activities | — Value-driven contract renegotiation<br>— Organizational 'rightsizing' |
| **Examples** | — Temporarily pause 'low-risk' vendor assessments, entitlements reviews/ recertification of non-critical applications, post-mortem incident reviews on low-risk events, code reviews on non-internet-facing applications, etc.<br>— Postpone or cease all discretionary spending, including 'research and development,' non-regulatory-driven initiatives, etc. | — Review third-party spend and contract renegotiation, soliciting ideas on improving operational and financial efficiencies<br>— Transition business-as-usual contingent workers to outcomes-based 'Managed Services' or to permanent full-time equivalents<br>— Perform lookback and adjust Service Level Agreements (SLAs)/Service Level Objectives (SLOs) in Managed Services engagements, e.g., MSSP to achieve cost balance |
| **Speed to realize cost savings** | ↑ | ↔ |
| **Sustainability** | ↓ | ↔ |

| | | | |
|---|---|---|---|
| **Challenge** | **3. Underutilized or overlapping cyber security tools and abundance of projects** | **4. Increasing regulatory and compliance obligations** | **5. Manual, disparate, and siloed security processes** |
| **Cost optimization opportunity** | — Security tool rationalization<br>— Cost versus reward project rationalization | — Unified control framework and governance<br>— Unified compliance management | — Convergence<br>— Automation<br>— Self-service enablement |
| **Examples** | — Identify duplication of capabilities and functions across the technologies<br>— Rationalize security technologies against defined and approved security use cases and target 'Best of Breed'<br>— Rationalization of initiatives, to just focus on remediation of regulatory/ audit issues | — Ground the various regulatory obligations and corresponding controls with a baseline control framework<br>— Embed 'test once, comply (and report) many' compliance management activities<br>— Leverage natural language processing for regulatory mapping and alignment to controls | — Convergence of governance, risk, and compliance (GRC) processes and enablement through GRC<br>— Automate workflows such as security issue management, risk reviews and approvals, incident response, and case management<br>— Deploy user authentication self-service, security code-scanning developer self-service<br>— Enrich threat intelligence data through enhanced data analytics and artificial intelligence |
| **Speed to realize cost savings** |  |  |  |
| **Sustainability** |  |  |  |

# Pausing 'low-risk' activities

Some of the more tactical cost takeout measures for those organizations who are in 'cash preservation' mode are to identify and pause discretionary spend and costs associated with the 'low-risk,' 'noncritical' activities.

We have seen organizations asking staff to take cuts in hours or accept unpaid leave, halt their staff's training budget, limit subscriptions to intelligence feeds, withdraw from consortiums and professional associations, and postpone internal marketing and external marketing activities such as contributions to industry groups and conferences. Some organizations have scrutinized their testing and control activities and have temporarily halted those addressing 'low-risk' or 'non-critical' assets, e.g., performing vendor risk assessments with formal assurance evidence such as SSAE or ISO certifications, conducting security investigations for low-risk events or even postmortem incident reviews, conducting security code reviews on internally facing applications, and performing vulnerability scans on noncritical hosts or assets.

The realization of cost savings is almost immediate, but this should be considered a temporary solution given the ever-evolving threat landscape and changing security risk profiles.

**What you can do**

— Understand and visualize your entire spend including discretionary costs.

— Identify your 'low risk' activities and determine based on your organization's current appetite during the downturn to discern where to temporarily take a pause.

# Seek value and open dialogue when renegotiating contracts — not just fee reduction

Security organizations often look externally for independent insights, cyber experience, or an objective view on their cyber capability. This may include engaging technology providers, trusted advisers, or contractors. However, external resources typically carry a significantly higher price tag than in-house personnel and as such should be engaged sparingly. When cost takeout is urgently required, it is typical for organizations to start with disengaging consultants and contingent workers.

Consultants and contingent workers can provide significant value to organizations embarking on initiatives requiring specialist technical skill sets (for example, security tool technology deployment or enablement). It is also beneficial to periodically obtain independent opinions on the cyber security program, particularly as it contrasts to industry leading practices. Some services being delivered by consultants and contingent workers could be moved to a Managed Security Service Provider (MSSP) where organizations pay for outcomes versus paying for resources.

However, on all initiatives in which external parties are engaged, a plan should be built around returning knowledge and experience to the organization. Alongside this, it is important to challenge consultants, contingent workers, and MSSPs to help identify cost reduction opportunities. Typically, they may have experience with transforming another client's service delivery model to a lower cost base.

**What you can do**

There are various strategies to working with your consultants and contingent workers in achieving cost efficiencies:

- Request ideas for value and cost efficiencies from your suppliers, when renegotiating contracts renewals or amendments.
- Move from 'buying resources' to 'buying outcomes' — identify services being completed by consultants or contingent workers that could be moved to a Managed Services Provider.
- Adjust service-level agreements/service-level objectives to achieve a balance of cost and service.

# Rationalize your security technologies and projects

With the abundance of security tools in the market, many organizations have invested a considerable amount of money in new technologies over recent years, in the effort to stay 'ahead' with the latest security solutions given the ever-shifting land. However, organizations that haven't successfully aligned the cyber security strategy and technology strategy may find themselves having to manage a huge portfolio deploying and operating underutilized or duplicative cyber security tools, wasting valuable security resources.

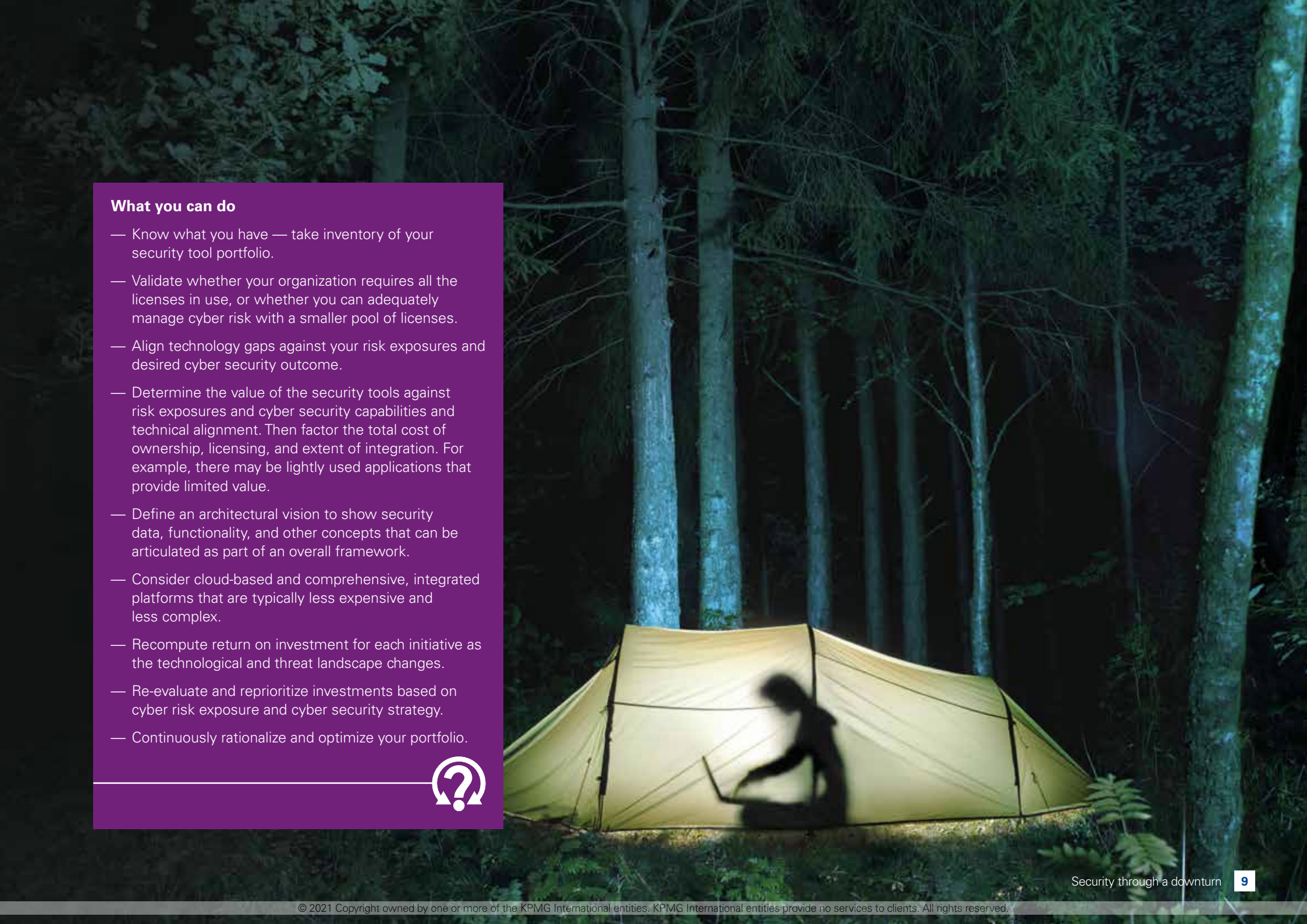
We have seen security roadmaps, many with focus on 'shiny tool deployments' as well as a plethora of remediation activities, process optimization efforts, and tool upgrades. There is little to no alignment back to the broader security strategy, security architecture, or risks and issues. It is critical that these initiatives are accurately assessed for risk versus reward return on investment, to help ensure that they are prioritized in accordance with security requirements.

Across larger organizations, we've seen multiple tool rollouts that have failed to be deployed with the use cases or requirements in mind, rolled out piecemeal, or failed to integrate with other solutions and processes to bring a more cohesive and integrated solution. All the while these organizations are paying significant licensing fees for the tool, as well as costs for ongoing maintenance and support, testing, and frequent updates. Many organizations are reviewing their licenses to assess whether the full functionality is actually being used, and whether an older release would have the same risk reduction impact.

In one client organization, for example, we have seen multiple authentication solutions, multiple identity governance platforms, and entitlement solutions catering for various business units — some purchased, some developed in-house. In another example, we had seen over a dozen tools for data analytics via log data collection.

However, only a handful of leaders analyze how much log data across the environment is actually collected (sometimes just from a fraction of assets) and there may be limited correlation of the data itself. We have seen different technologies (governed by different teams) that enable the same capability but targeted at different assets, e.g., vendor assessments, application security assessments, and business process risk assessments.

Technology total cost of ownership in cyber (e.g., costs associated with tool deployment, updates, licensing, maintenance and continuous testing, training, etc.) is among, if not the highest cost items within a cyber program and rationalizing the toolset can bring about significant savings, not just financially but operationally.



**What you can do**

— Know what you have — take inventory of your security tool portfolio.

— Validate whether your organization requires all the licenses in use, or whether you can adequately manage cyber risk with a smaller pool of licenses.

— Align technology gaps against your risk exposures and desired cyber security outcome.

— Determine the value of the security tools against risk exposures and cyber security capabilities and technical alignment. Then factor the total cost of ownership, licensing, and extent of integration. For example, there may be lightly used applications that provide limited value.

— Define an architectural vision to show security data, functionality, and other concepts that can be articulated as part of an overall framework.

— Consider cloud-based and comprehensive, integrated platforms that are typically less expensive and less complex.

— Recompute return on investment for each initiative as the technological and threat landscape changes.

— Re-evaluate and reprioritize investments based on cyber risk exposure and cyber security strategy.

— Continuously rationalize and optimize your portfolio.

# Unify your control set and compliance management activities

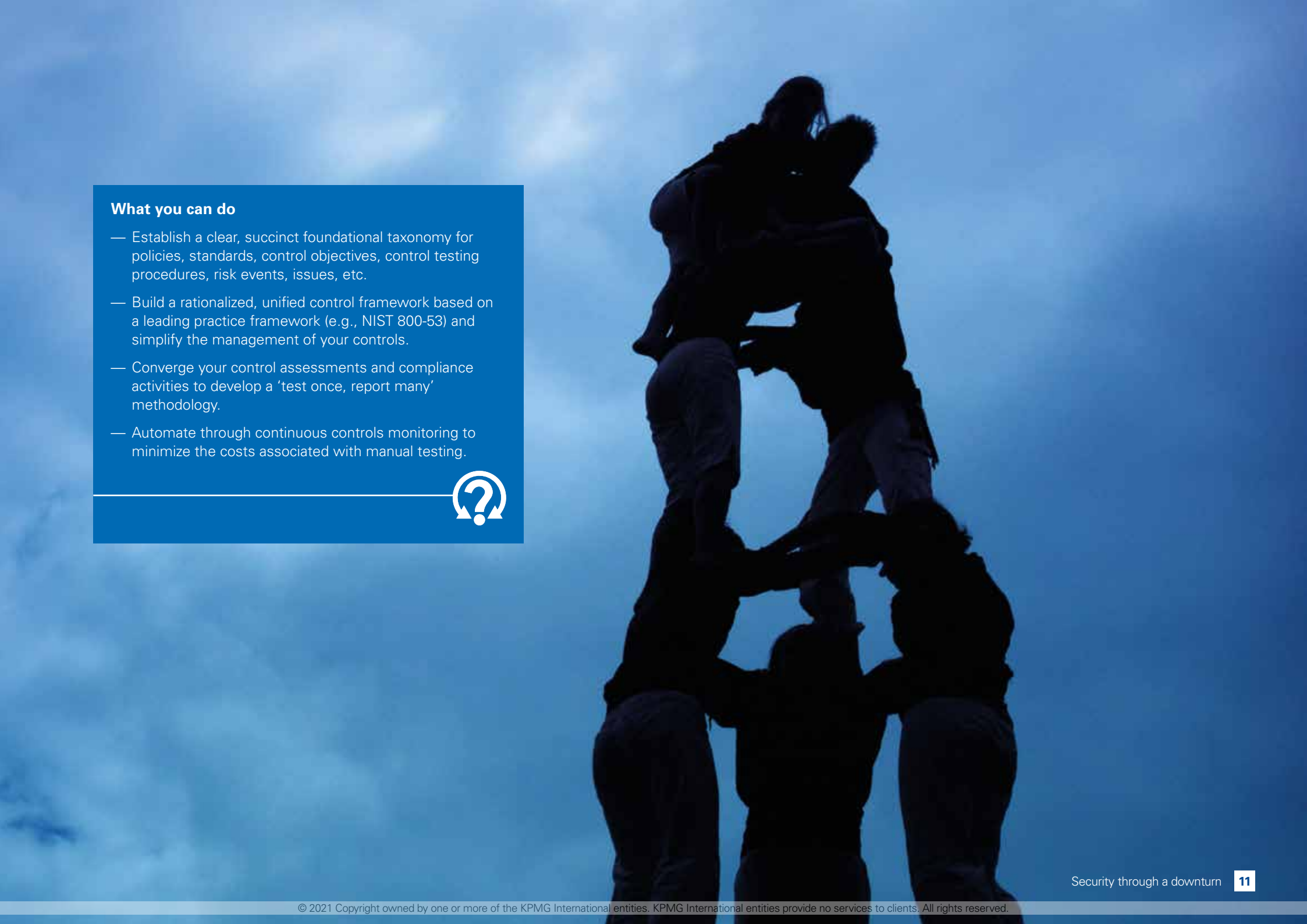
Many industry and government regulators have brought cyber security into their purview. They collectively acknowledge the criticality of cyber security risks; however, their approach to administering oversight varies from regulator to regulator. Different regulators are, understandably, interested in different aspects of cyber security. This has resulted in an array of obligations, ranging from the neatly overlapping to the entirely unique.

In the Privacy space alone, there are numerous different state regulations[1] and various non-U.S. legislation (most notably GDPR) impacting U.S.-based organizations. Efforts to align obligations across discordant regulators (e.g., the Financial Services Sector Cyber security Profile) remain in their infancy and this is unlikely to change in the near future.

Without a foundational risk and control ontology and a defined assessment and issue management process, the bedrock of a 'test once, report many' principle, organizations typically achieve compliance through performing additional, duplicative compliance control assessments. This has created additional workload with no risk exposure limitation upside.

We have seen continuous and disparate requests to assess against various regulations and compliance obligations, when the majority of control objectives do indeed align. As such, efforts to assess, measure compliance gaps, collect evidence, develop reports, etc., are duplicative and redundant.

[1] California's AB375/SB1121 (California Consumer Privacy Act) is signed; Massachusetts' S120, Minnesota's HF2917, Nebraska's LB764 (Nebraska Consumer Data Privacy Act), New Hampshire's HB1680, New York's S224 (Right to Know Act), New York's S5642 (New York Privacy Act), Virginia's HB 473 (Virginia Privacy Act), and Washington's SB6281 (Washington Privacy Act) are all in committee; and Florida's H963 and Hawaii's SB418 are both introduced.



### What you can do

— Establish a clear, succinct foundational taxonomy for policies, standards, control objectives, control testing procedures, risk events, issues, etc.

— Build a rationalized, unified control framework based on a leading practice framework (e.g., NIST 800-53) and simplify the management of your controls.

— Converge your control assessments and compliance activities to develop a 'test once, report many' methodology.

— Automate through continuous controls monitoring to minimize the costs associated with manual testing.

# Simplify, converge, and automate

Highly manual, siloed, and disparate security processes are a clear and obvious focus for optimization. Inefficiencies are often exacerbated by inaccessible or inaccurate data.

Take the example of managing vulnerability scans and patching and remediation of critical and highly exposed applications. All too often, we hear of wastefulness in this process from limited scope and visibility of the scanning and therefore limited visibility of vulnerability exposure, inability to identify the correct application owner for remediation leading to missed SLAs in patching, or lack of risk and impact analysis such that more time is mismanaged, e.g., where much time is spent remediating actual low-risk assets.

Furthermore, we have seen limited integration between this and incident responses processes to allow for effective, quick analysis for incident response. A significant amount of time and effort and associated costs can be saved, through data cleanup and process simplification.

The convergence and automation of governance, risk, and compliance activities is another example of where efficiency gains can be made. Organizations often spend innumerable hours identifying and collating data, following up with individuals for responses, and analyzing information for reporting purposes. This time can be significantly reduced through converging and automating control management and policies, including compliance, audit, and risk activities.

For some of the more mature organizations, we have seen investments in data analytics, robotic process analysis, artificial intelligence, and machine learning. This is intended to transform static or manual legacy processes, which typically consume a significant amount of resource time. Common use cases for these automation investments range from basic conversational bots that answer common security questions, e.g., in information technology support helpdesks, to analysis of log data, vulnerability data, and code that, when aggregated, can improve security incident detection accuracy and accelerate remediation.

Leading organizations are also making use of 'self-service' security consumables. This is where they provide the business with the ability to deal with basic security enquiries using automated tools and portals. It saves money in the security budget—and often accelerates the business processes, saving the business money as well.

In a recent example, a KPMG firm supported a financial services client in developing a learning algorithm applied to aggregated data to identify and detect suspicious IP addresses and accounts (which were either not blocked or not covered by the organization's manual processes). This resulted in a 30 percent improvement against existing baselines in the ability to detect activities that lead to locked accounts due to suspicious activities. Coupled with this was a 60 percent effort saving against manual model tuning.

**What you can do?**

— Strengthen the foundation such as the cleanup, simplification, and accessibility of your data that is integral to your security processes, e.g., assets and ownership, controls, entitlements, security classifications, etc.

— Converge mature security processes that can enrich threat intelligence data, increase visibility of your cyber risks, and enable greater efficiencies in issue or incident resolution.

— Enable the business and users, e.g., building a self-service portal for lines of business to use and access security tools to ease activities around intake and triage.

— Think about the future of your security organization to be more strategic with cost optimization, e.g., extreme automation, data analytics for real-time and on-demand analysis.

— Focus on determining control effectiveness and cyber risk reduction for greater accuracy and focused security efforts.

# Where does this leave the CISO?

**CISOs face inordinate pressures from all angles of their organizations. Business units are continuously requesting exceptions approvals and compliance departments are continuously seeking assurance over the robustness of protected information controls. Adding cost pressure into this mix will likely feel like another strain for the CISO to manage.**

**However, there are various strategies to help achieve cost efficiencies without compromising security posture or decelerating strategic roadmaps. By thinking creatively, CISOs can work proactively with the enterprise to share the burden of cost pressures, wherever the enterprise is in the economic cycle.**

# Our authors


**David Ferbrache**
**Global Head of Cyber Futures**
KPMG

**Tom Nash**
**Manager,**
**Cyber Security Services**
KPMG in the US

**Leah Gregorio**
**Managing Director,**
**Cyber Security Services**
KPMG in the US

**Rik Parker**
**Principal,**
**Cyber Security Services**
KPMG in the US

**Matthew Miller**
**Principal,**
**Cyber Security Services**
KPMG in the US

# Contacts


**Akhilesh Tuteja**
**Global Cyber Security Leader and Partner**
KPMG in India
**E:** atuteja@kpmg.com

**Dani Michaux**
**Cyber EMA Lead and Partner**
KPMG in Ireland
**E:** dani.michaux@kpmg.ie

**Matt O'Keefe**
**Cyber ASPAC Lead and Partner**
KPMG in Australia
**E:** mokeefe@kpmg.com.au

**Prasad Jayaraman**
**Cyber Americas Lead and Principal**
KPMG in the US
**E:** prasadjayaraman@kpmg.com


**home.kpmg/socialmedia**




Designed by Evalueserve.
Publication name: Security through a downturn
Publication number: 137304-G
Publication date: January 2021