Empowering the business to embrace opportunities securely and confidently

A strategic guide for CISOs

2025

Proactive investment in effective cybersecurity protections is an urgent priority

In today's rapidly evolving landscape filled with sophisticated cyber threats, Chief Information Security Officers (CISOs) are tasked with an urgent dual challenge: safeguarding their organization's infrastructure while also supporting business innovation.

With an ever-expanding attack surface driven by rapid technological advancements—particularly artificial intelligence (AI)—CISOs must establish a robust cybersecurity program. Emerging threats like deepfakes and advanced social engineering, coupled with the shifting complexities of cloud environments, regulatory pressures, and a scarcity of financial and human resources, further complicate security management. Increased reliance on external suppliers and services introduces both efficiencies and additional risk complications.

The importance of proactive security measures cannot be overstated. This report illustrates how CISOs can leverage the KPMG integrated suite of cybersecurity capabilities to invest in the right cyber controls, help their teams remain prepared to protect their environment; keep small, isolated issues from becoming big, protracted problems; and fortify robust business continuity and disaster recovery plans.

The CISO's perpetual challenge

An organization's cyber defenses are the only line of protection against increasingly sophisticated adversaries. If those defenses are breached, would the business be able to withstand the blow?

While many CISOs are clear about their primary mission, developing a comprehensive vision of what their security programs should encompass would strengthen their overall approach to cybersecurity. KPMG LLP views cybersecurity from a client-centric perspective, aiming to achieve three primary goals:

Manage risk

Ensure compliance

Establish trust

This should be the CISO's North Star.

The time for action is now

Each moment of delay is an opportunity lost. As cyberattackers leverage AI and machine learning to elevate the sophistication of deepfakes, social engineering, and malware, organizational defenses must evolve in tandem. A proactive stance is essential to organizations' ongoing security. This is about readiness and resilience and moving beyond the fear that can cause inertia and tentativeness.

Indeed, the results of a pair of recent Gartner surveys make the case.

A 2025 Gartner® survey found that "85 percent of CEOs say cybersecurity is critical for business growth." The study also found that 61 percent of CEOs are concerned about cybersecurity threats, driven in large part by AI's growing role in commercial activity and the political debates about the sourcing and use of advanced technologies.[1]

However, the other study found that only 14 percent of security leaders successfully balance data security and business objectives.[2]

We believe that the disconnect these results illustrate places in sharp focus the need for strategic investment in cybersecurity controls and perspective on the role of emerging technology to bridge the gap between merely understanding risk and vigorously mitigating risk.

[1] Gartner, CEO and Senior Business Executive Survey, April 22, 2025

[2] Gartner, Security & Risk Management Survey, February 11, 2025

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved

Implementing a strategic roadmap for proactive cybersecurity

Time is of the essence. We recommend that CISOs employ a six-step action plan to effectively protect and empower the business:

Step 1

Proactively invest in the right controls and protections

Don't wait for a breach to test your network defenses.

Identity and access management (IAM). The cornerstone of security, automated IAM is essential for maintaining control over who, or what, can enter the system, reducing manual efforts and enhancing the efficiency and visibility of digital assets.

Cloud security and data privacy. Forward-looking organizations are developing proactive data protection strategies before moving sensitive assets to the cloud by embedding security, privacy, and regulatory compliance in their target operating model.

Step 2

Identify and prioritize vulnerabilities and security events

Don't let system flaws go unchecked.

Enhanced vulnerability management. Prioritize vulnerabilities of your most critical assets across applications, cloud containers, and legacy infrastructure scanner.

Security operations automation. Utilize AI to automate repetitive security incident triage processes to filter out the noise, create better security incident ticket fidelity, and escalate what matters faster.

Step 3

Stay ahead of increasingly sophisticated attackers through advance planning

Don't let emerging threats such as deepfakes and social engineering infect your environment.

Threat intelligence and response. Develop a robust threat intelligence program to stay ahead of advanced tactics by identifying and responding to threats with proactive threat hunting capabilities.

Training and awareness programs. Continually educating the workforce about evolving threats not only reduces the risk of advanced attack methods but also serves to prioritize and embed a strong cybersecurity culture in which every individual within the organization actively participates in effectively managing cyber risks.

Step 4

Ensure the extended ecosystem is secure

Don't allow third-party vulnerabilities to be an open gateway for cyber adversaries.

Third-party risk management. Ensuring critical suppliers maintain robust security postures characterized by stringent access controls and continuous monitoring is a critical imperative for organizations across virtually every industry.

An incident management framework. Establishing clear incident reporting protocols is essential for ensuring third parties know how and when to report security breaches or compliance lapses.

Step 5

Verify every individual and device and grant the least privileged access necessary with Zero Trust

Don't miss the cyber forest for the trees.

Security architecture and engineering. Adhering to Zero Trust can achieve data and application security through microsegmentation, continuous authentication, and endpoint security.

Automation and analytics. Combining AI-enabled technologies, systems, and processes to enforce Zero Trust principles across the network is key to enhancing internal and external functions across both strategic and operational ecosystems.

Step 6

Maintain cloud and data security

Don't make cloud security an afterthought—make it foundational.

Cloud security posture management (CSPM). Automating CSPM tools to preconfigured policy checks mapped to specific regulatory regimes helps to identify cloud-related misconfiguration issues and compliance risks and help maintain visibility and control over cloud environments.

Data loss prevention (DLP). Implementing cloud-specific DLP solutions to safeguard sensitive organizational and customer data from unauthorized access and exfiltration can provide full-scale assistance in the identification of basic protection objectives and implementation of a supporting strategy that matches your organizational business needs.

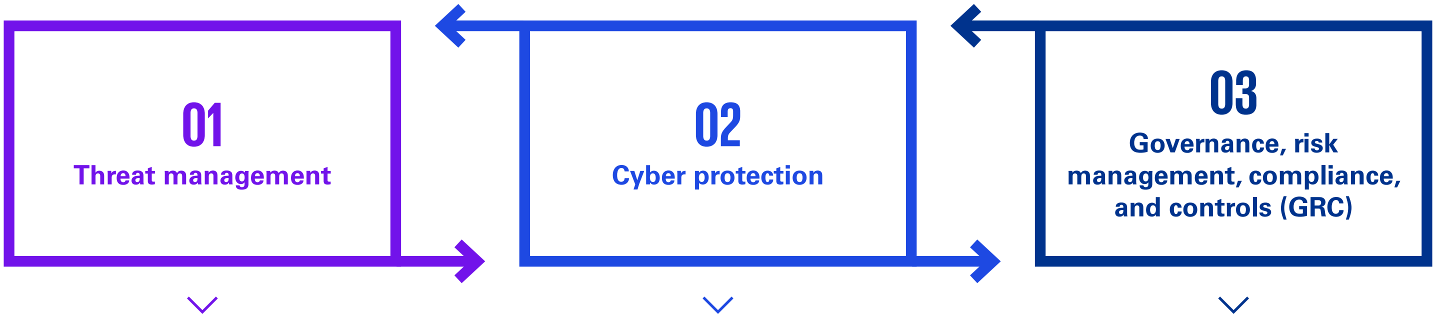
A framework for proactively and strategically empowering the business to embrace opportunities securely and confidently

While CISOs today work very closely with many counterparts across the business, they must speak in one unified voice to manage risks while supporting and empowering the organization’s commercial interests.

The ideal solution set is designed to help CISOs and their teams detect signals around attack vectors, identify and address business and industry risks, respond to threats, and establish appropriate controls. Whether regulatory or situationally driven, these controls safeguard an organization’s digital network against vulnerabilities.

To activate the solutions roadmap in a manner that is agile, efficient, and fit for purpose, KPMG offers a thorough suite of solutions designed to help CISOs effectively govern and protect their environment, report on key risks, and maintain regulatory compliance while managing cyber threats using the appropriate technologies.

The KPMG perspective hinges on an effective operating model supported by a corresponding solutions-based capabilities framework that can be activated, as needed, for various use cases. The focus is on a consistent risk management structure that can be utilized for increasingly advanced needs as maturity levels increase.



01
Threat management

02
Cyber protection

03
Governance, risk management, compliance, and controls (GRC)

Cyber defense, device and Internet of Things security, incident response and recovery, and, ultimately, resiliency.

Identity and access management, cloud and platform security, and third-party supply chain security.

Developing and enforcing strategic cybersecurity policies, continuous risk assessment, and ensuring regulatory compliance through continuous controls monitoring.

This thorough, integrated approach to managing cyber risks, building trust, and helping ensure compliance is designed to help CISOs proactively address both day-to-day and unexpected issues. It aligns cybersecurity initiatives with business objectives, regulatory requirements, and risk management strategies, combining leading technologies with strict, yet flexible governance structures to establish and maintain a resilient cybersecurity environment.

We view this solutions-oriented structure not solely in relation to risk quantification and mitigation. Rather, we believe it supports an understanding of the organization's portfolio of cybersecurity solutions—and recasts them as capabilities—ultimately helping CISOs prioritize and rebalance their overall investment.

KPMG Cyber Managed Services: Transforming mission-critical work

Forward-looking organizations are integrating managed services into their cybersecurity strategies. They seek providers who offer all-encompassing solutions, from strategic consulting to implementation, ongoing enforcement, continuous monitoring, and evolution. The perception of modern managed services is shifting from isolated transactions to transformational partnerships where providers become strategic allies in the journey towards cyber success.

The increasing role of cyber managed services

Cyber managed services play a crucial role in solidifying a holistic view of security. By integrating identity controls, application security testing, and detection and response capabilities, these services address the sophisticated tactics employed by today's threat actors.

Proactive cybersecurity solutions that go beyond everyday challenges

Cybersecurity is inherently complex. Organizations require a broad range of skills to effectively implement cyber tools and services. Maintaining a skilled staff and keeping up with evolving threats is a significant challenge for many businesses.

The KPMG Cyber Managed Services team offers a broad suite of services that provide operational, technical, and governance knowledge that many organizations don't have internally. Our managed services deliver deep insights into the cybersecurity landscape, providing support beyond what can be easily acquired overnight.

Why choose KPMG Cyber Managed Services?

KPMG Cyber Managed Services provide organizations with a strategic advantage in addressing complex cybersecurity challenges. By collaborating with KPMG, organizations can leverage:

A multifaceted talent pool

Access to a diverse range of cybersecurity skills and experience

Industry insights

First-hand knowledge of market trends and leading practices

Holistic solutions

From strategic consulting to real-time threat monitoring and response.

Our managed services also deliver:

Continuous improvement

Enhance security measures and reduce risk through ongoing advancements

Operational efficiencies

Streamline processes and improve overall efficiency

Global support

Benefit from the experience and resources of a leading global cybersecurity provider

24/7 access

Around-the-clock support from skilled KPMG teams.

A robust suite of managed cybersecurity solutions

Our Cyber Managed Services capabilities are categorized into several categories, each addressing a specific aspect of cybersecurity operations:

Digital identity management

Helps businesses control access to digital assets through enhanced visibility and efficient identity governance.

Cyber risk exposure management

Aims to minimize vulnerabilities by identifying, prioritizing, and confirming security exposures in applications and infrastructure before they can be exploited.

Cyber threat management

Focuses on early detection of cyber risk, intelligent response, and proactive defense.

Make KPMG your adviser of choice

Choosing the right adviser is essential for making strategic cybersecurity investments that incorporate the right controls and protections, enabling your business to confidently embrace new opportunities. KPMG is committed to providing value-added solutions that are strategically integrated to align with those priorities. Below is a deeper look at the overarching inputs.

Threat management

Proactive threat detection and response involves utilizing the SOC for real-time, 24/7 monitoring and managed detection and response (MDR) services for 24/7 incident response. Thorough incident response plans and regular simulations help ensure rapid threat mitigation and resilience in the face of disruptions.

Key services include:

Application and cyber defense testing: Continuous validation to identify and remediate vulnerabilities

Security architecture design: Building and managing resilient infrastructures that adapt to threats

Advanced threat detection and response: MDR: Thorough monitoring and response:

- Utilize the SOC to monitor, detect, and respond to security threats in real-time
- MDR for 24/7 threat monitoring and incident response
- Protection of all endpoints and connected devices

Business continuity and disaster recovery:

- Development and testing of business continuity and disaster recovery plans to maintain operations with minimal impact during and after a cyber incident
- Quick restoration of critical systems and data
- Structured response protocols

Incident response:

- Immediate action to manage and contain incidents, followed by detailed forensic investigations to understand root causes
- Detailed incident response plans
- Regular incident response training and simulations.

Cyber protection

Securing interactions with third parties and implementing robust IAM solutions and Zero Trust principles helps ensure secure access, least privilege enforcement, and data security. Thorough data and cloud security measures, including threat intelligence and automated response, protect against advanced cyber threats.

Key services include:

Third-party and supply chain security

- Securing interactions with third parties and the supply chain
- Assessing and verifying that third-party vendors adhere to security standards

Identity management and Zero Trust implementation

- Implementation of robust IAM solutions for secure access and least privilege enforcement
- Continuous verification and validation of users and devices according to Zero Trust principles

Data and cloud security

- Secure use of cloud platforms
- Encryption and DLP to protect sensitive information
- Establishment of appropriate cloud security posture to protect data in distributed cloud environments

Emerging threat management

- Advanced threat intelligence and automated response for threats like deepfakes.

Governance, risk management, compliance, and controls

Governance structures help ensure accountability and support proactive risk management, while continuous risk assessments enable informed decision-making. Leveraging trusted AI systems helps mitigate AI-driven threats like deepfakes. Helping ensure regulatory compliance through continuous monitoring reduces legal and reputational risks.

Key services include:

Strategic investment in controls

- Develop a risk-based approach to strategic allocation of resources and investment in controls
- Align cybersecurity initiatives with organizational goals for effective resource utilization

Governance and oversight

- Establish a robust governance structure to oversee cybersecurity efforts and maintain accountability
- Implement policies and procedures that support proactive risk management and strategic decision-making
- Strategically deploy cybersecurity investments focusing on critical vulnerabilities

Ongoing risk assessment and management

- Conduct continuous risk assessments to identify and quantify risks, enabling informed decision-making
- Develop and implement risk response and remediation plans to address identified vulnerabilities

Trusted AI

- Strategically deploy cybersecurity investments focusing on critical vulnerabilities
- Proactively manage AI-related vulnerabilities and inform tailored AI governance strategies through strategic decision-making

Regulatory compliance

- Prepare for regulatory changes and respond/remediate as needed
- Adhere to relevant laws and regulations, thus preventing legal and reputational risks
- Utilize continuous controls monitoring to automate compliance testing and reporting processes
- Adhere to relevant laws and regulations, thus preventing legal and reputational risks

Vulnerability prioritization

- Implement vulnerability management programs to identify, prioritize, and remediate critical vulnerabilities
- Use risk assessments and advanced analytics to focus on the most critical

Controls management

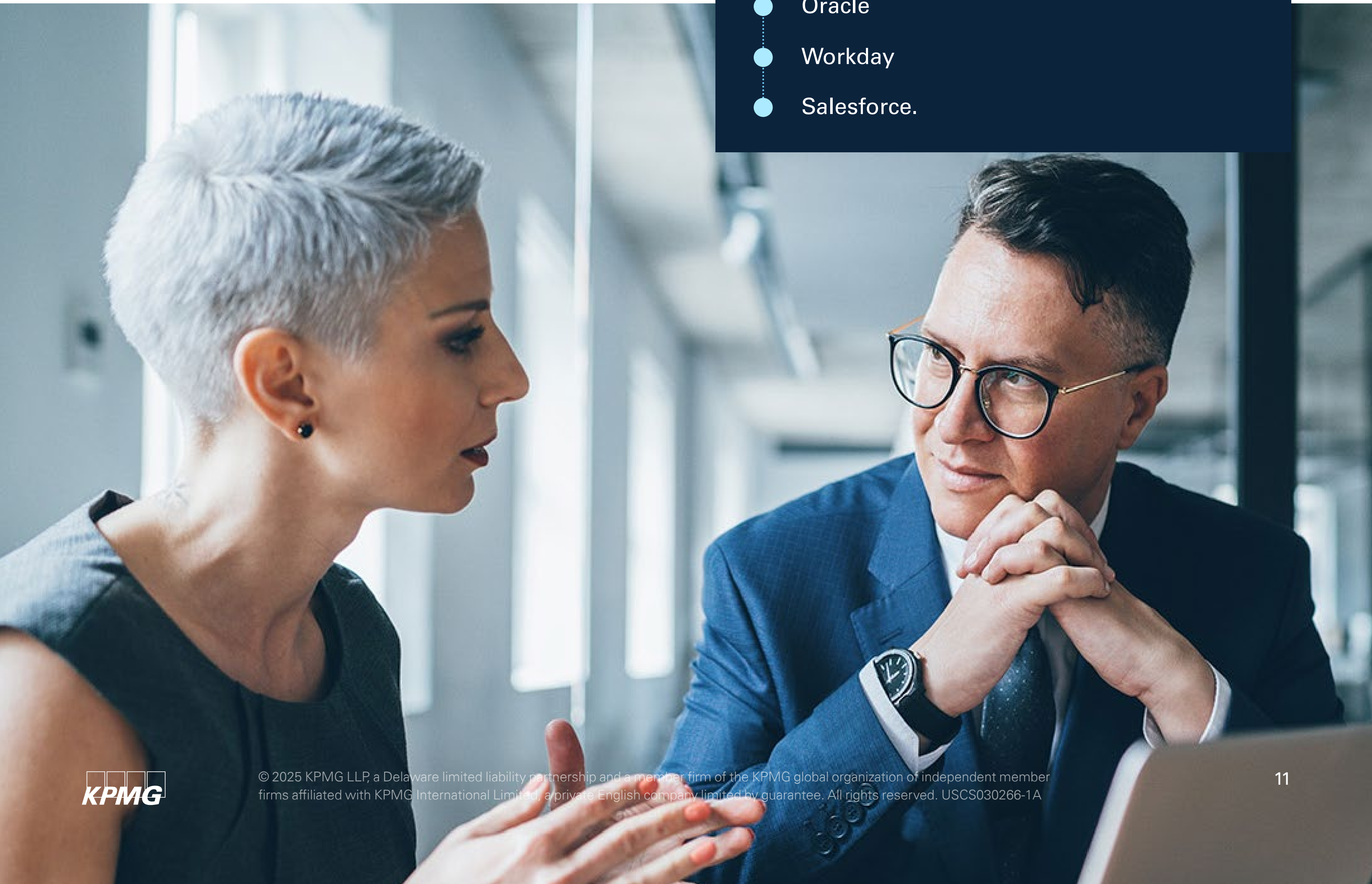
- Systemic identification, testing, and remediation
- Ongoing monitoring to maintain control effectiveness.

Innovate with leading technology advisers

At KPMG, we strive to complement our deep business and technology knowledge and specialized industry perspective by joining forces with leading technology providers. These strategic alliances enable our teams to deliver innovative and scalable solutions that help clients unlock strategic value, drive quicker ROI, and overcome challenges to create new business value.

Our Technology-driven cybersecurity alliances, including partnerships with industry leaders such as Microsoft and Google, enable us to deliver leading solutions that address today's complex cyber challenges and help maximize your cybersecurity investment.

- Google Cloud
- Microsoft
- Servicenow
- SAP
- Oracle
- Workday
- Salesforce.



KPMG can help fortify your cybersecurity program

Proactive measures taken today help ensure a more secure future. At KPMG, we think like you think. We understand your pain points and your challenges. We know cyber, but beyond technical knowledge, we know your business, we know your market and we know how to help you stay ahead of the competition. Our goal is to empower you to operate securely and confidently, ultimately shaping a more trusted digital world.

KPMG professionals provide strategic alignment of cybersecurity with business priorities, advanced digital solutions, ongoing risk management, and effective incident response. No matter where you are in your cybersecurity journey, KPMG can help you reach your destination.

As leading providers and implementers of cybersecurity, KPMG professionals possess the experience to apply industry-leading security practices and innovate new ones tailored to your needs. Our progressive approach means you will work with specialists who understand the markets in which you operate as well as the evolving technology landscape.

Whether you're entering new markets, launching new products and services, or interacting with customers in novel ways, KPMG professionals are here to help you anticipate future challenges and operate more efficiently with secure and trusted technology. We combine technological proficiency with deep business insight and a passion for protecting and building stakeholder trust.

For specialized guidance and detailed methodologies, contact us to develop a customized plan tailored to your organization's unique requirements.

KPMG. Make the Difference.

Learn more at kpmg.com/cybersecurity

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

Learn about us: | **kpmg.com**

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.