Cyber Assessments

Deloitte Cyber Strategy and Transformation

Introduction

To truly harness the potential of cybersecurity as a business enabler, Chief Information Security Officers (CISOs) should understand the maturity of their security programs and modernize in alignment with business growth objectives, focusing on identifying and mitigating risks in a way that supports their strategic goals.

Table of Contents:

Cyber assessments are not merely a procedural formality; they are a foundational step that can help in understanding your organization's risk profile and determine actions that should be taken to manage these risks effectively as a part of a future-ready cyber strategy.

Copyright © 2025 Deloitte Development LLC. All rights reserved.

The Cyber Landscape is Rapidly Evolving...

Regulatory and compliance scrutiny is growing...

Increasing regulatory and operational pressures (e.g., SEC, PCI DSS) demand increased security rigor, and transparency to satisfy requirements and protect the organization against hefty regulatory fines.

Threat actors are continuously evolving TTPs...

New and sophisticated threat vectors (e.g., artificial intelligence (AI), advanced malware, ransomware, social engineering) may bypass traditional security protections, leading to significant financial losses and reputational damage.

Human-centric security risks are growing...

Employees and extended networks can be weak links in an organization's security posture, heightening the need to foster a culture of security, while implementing safeguards to protect an organization's crown jewels.

AI is changing the face of business and cyber...

AI is rapidly accelerating both business growth and cyber threats. Security strategies must evolve alongside AI adoption, considering the role of human analysis and advance capabilities to protect operations and maintain customer trust.

Inorganic growth introduces integration complexities...

As organizations increasingly seek external growth opportunities, the integration of disparate IT systems, networks, and applications can inherently expand digital footprints, potentially leaving gaps in security coverage.

Economic and geopolitical challenges are influencing cyber policy...

Geopolitical unrest and economic uncertainties may drive the need for increased vigilance against sophisticated threats and adaptability in security operations.

...by proactively identifying gaps in cybersecurity programs, organizations can work to stay ahead of emerging risks, protecting sensitive data, and building digital trust which is accretive to their businesses.

Copyright © 2025 Deloitte Development LLC. All rights reserved.

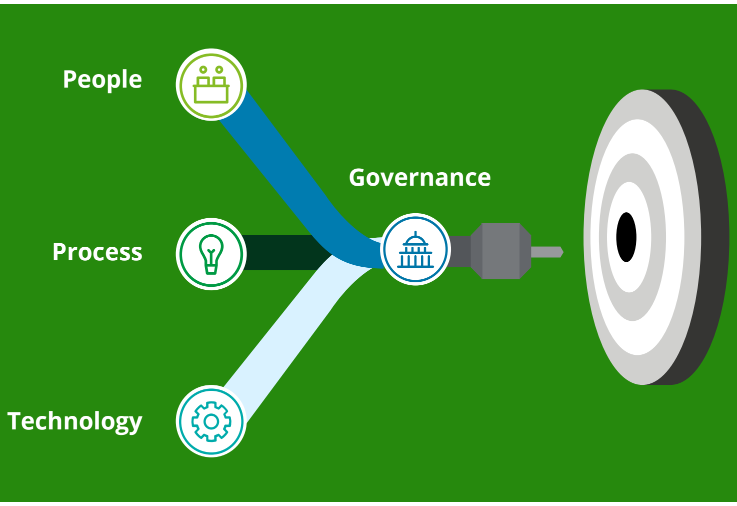
Cyber Assessments can help mature your Security Program

Tailored cyber maturity assessments can help your organization understand its cybersecurity risks and take meaningful actions to secure and accelerate growth.

Cy·ber As·sess·ment

/ˈsībər əˈsesmənt/

An evaluation of an organization's cybersecurity capabilities - considering factors such as business environment, risk appetite, regulatory landscape, and more - from a governance, people, process, and technology perspective, aligned with industry-leading practices.



Supplemented with...

Cyber Frameworks

Leveraging industry-leading frameworks to evaluate your cyber program can lead to a standardized, consistent, and comprising, approach to managing cybersecurity risks.

Risk-Aligned Conversations

Understanding the level and type of risks your organization is willing to accept (i.e., risk appetite) to achieve strategic objectives can help your cyber program prioritize security initiatives and allocate resources effectively.

Industry Comparison

Comparing your organization's cyber maturity against its peers can offer granular, industry-specific insights, providing more relevant and meaningful results and actionable improvement areas.

Can enable you to...

Provide critical insights into **current maturity relative to industry peers** and desired maturity levels

Guage your organization's **readiness to handle cyber threats**

Define **'What Good Looks Like'** beyond your organization

Uncover **immediate and actionable improvements**.

Confidently **pursue digital initiatives and innovation** to consistently demonstrate the strategic importance of cybersecurity

Discover how harnessing AI can position your organization at the forefront of innovation and future growth

Copyright © 2025 Deloitte Development LLC. All rights reserved.

The Deloitte Advantage

Deloitte offers a combination of accelerators and outputs to assist your organization in realizing the full breadth of benefits from cyber assessments.

We are here for every step of the journey

Based on Deloitte's 20+ years of assessment experience, we understand that your organization has unique requirements and will require ***tailored assessment approaches.***

Our ***dedicated practitioners*** and ***subject matter specialists*** look beneath the surface of your organization's cyber program, stitching together ***business, technology, and compliance risks*** into deeper insights of where your security program is and where it should be going.

Leveraging our deep cyber experience coupled with an industry understanding of ***"what good looks like,"*** Deloitte has developed a ***scoring methodology***, that helps your organization accurately reflect its current maturity while developing a future-looking target state.

Deloitte's assessment approach has adopted ***innovative Generative AI capabilities,*** empowering our teams to engage in richer capability conversations.

Deloitte's maturity comparison repository, with anonymized data from ***300+ assessments*** across industries, helps your organization accurately understand its maturity relative to its peers, driving focused discussions around target state goals and objectives.

Our recommendation frameworks have been refined to help you ***prioritize future security initiatives***, identifying investments that provide quick results while simultaneously addressing high-risk areas.

We team with your organization beyond the assessment, connecting with stakeholders across levels to ***uplevel security conversations*** and ***demonstrate the value of cyber as business enabler.***

Copyright © 2025 Deloitte Development LLC. All rights reserved.

Protect Your Digital Future Today

Empowering results through Deloitte cyber assessments, enhancing performance, and delivering differentiated insights.

Deloitte's Assessment Scoping

From the big picture to the nitty-gritty, we've got you covered!

Enterprise

Evaluate the overall cybersecurity posture of an organization or business unit.

Domain

Identify risks within a specific cyber area (e.g., network security, application security, artificial intelligence).

Compliance Readiness & Controls

Evaluate your organization’s readiness to adhere to compliance obligations and examine the effectiveness of security controls.

Set higher goals, set strategic goals

The cyber threat landscape remains *exceptionally complex*, and your organization’s brand and reputation are at stake. The time to act is now.

Engage with our Cyber specialist team

Schedule a consultation with our cyber specialists to discuss your organization’s specific challenges and requirements.

Copyright © 2025 Deloitte Development LLC. All rights reserved.

About the Deloitte Cyber Strategy and Transformation Practice

The ability to innovate, to use new technologies, and to grow securely requires an end-to-end cyber risk strategy driven by an organization's executive leadership.

Deloitte's Cyber Strategy practice is focused on helping our clients to design and implement transformational enterprise programs to reduce and manage security risks. It includes assessments and strategy, security technology risk management, governance risk and compliance, and third-party risk management programs.

Cybersecurity is more than just IT—it's about identifying threats, assessing risks associated with key assets, and understanding your cybersecurity gaps. Our services and solutions provide strategic support in navigating this complex landscape.

Let's Talk

Adnan Amjad

US Cyber Leader
Deloitte & Touche LLP
aamjad@deloitte.com

Giri Chandramohan

USI Cyber Strategy and Transformation
Deloitte & Touche AERS India Private Limited
schandramohan@deloitte.com

Mehdi Houdaigui

US Cyber Strategy Leader
Deloitte & Touche LLP
mhoudaigui@deloitte.com

Ankit Jindal

US Cyber Assessment Center of Excellence (CoE) Lead
Deloitte & Touche LLP
anjindal@deloitte.com

Tiffany Kleeman

US Cyber Strategy and Transformation
Deloitte & Touche LLP
tkleemann@deloitte.com

Ankit Bajaj

USI Cyber Assessment CoE Lead
Deloitte & Touche AERS India Private Limited
ankbajaj@deloitte.com

Contributors

Wyatt Martin

US Cyber Strategy Manager
Deloitte & Touche LLP
wymartin@deloitte.com

Danielle Knell

US Cyber Strategy Senior Consultant
Deloitte & Touche LLP
dknell@deloitte.com

Sandeep Goyal

USI Cyber Strategy Manager
Deloitte & Touche AERS India Private Limited
sandgoyal@deloitte.com

Copyright © 2025 Deloitte Development LLC. All rights reserved.

Thank you.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.