Healthcare and Life Sciences

Cyber diagnostic assessment

Are healthcare organizations getting real value from cyber-security tool investments?

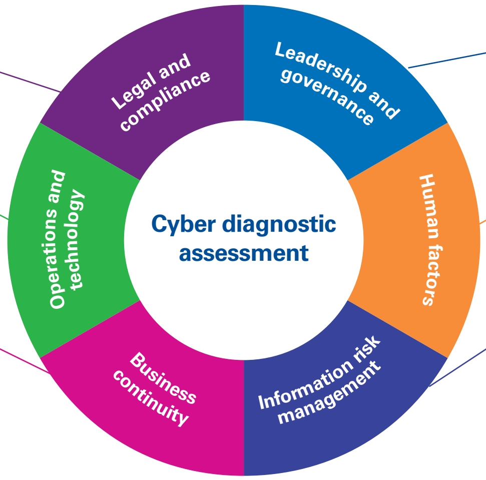
Healthcare and life sciences organizations are under attack every day from hackers, cyber-criminals, and industrial spies. We see the evidence of this in daily media reports. The industry has experienced a number of significant breaches and many organizations have elevated cyber security to a strategic imperative. However, with political uncertainty and other demands for resources, the industry as a whole still lags behind others in cyber-security investments. There are a number of key challenges:

- The political climate promises changes to the "business of healthcare." How it will change and when are still unclear. Therefore, most healthcare entities are focused on tangible changes that will directly improve their bottom lines, limiting cyber efforts to the most vulnerable systems and applications.
- Healthcare providers are increasingly seeking vendor partnerships that will help them provide innovative services to patients. However, vendors delivering everything from Electronic Health Records (EHR) to revenue cycle software increasingly handle sensitive patient data. To minimize cyber risks, provider organizations have not been vigilant enough about ensuring that these vendors have impeccable records.
- Life sciences has an untold amount of intellectual property to protect. It is the life blood of their organizations. Some hostile nation states have publically stated that they want to be world leaders in this area in fewer than 10 years. They are looking to take advantage of weak cyber-security programs at U.S. life sciences organizations to jumpstart their efforts.

Organizations need a clear line of sight into current cyber-security capabilities and weaknesses. The consequences for an organization can be significant with impacts on the bottom line, brand reputation, and patient security. Cyber security must be an enterprise-wide initiative so that all functions throughout the organization are protected. In light of this, KPMG recommends that organizations take a multi-faceted approach to cyber security.

Cyber risk management

A framework for exercising oversight responsibility


Legal and compliance
Leadership and governance
Human factors
Information risk management
Business continuity
Operations and technology
Cyber diagnostic assessment

Legal and compliance
— Cyber insurance
— Legislative and regulatory compliance
— Compliance program

Operations and technology
— Threat and vulnerability
— Physical security
— Network security
— Identity management

Business continuity and crisis management
— Business continuity
— Disaster recovery
— Cyber incident response

Leadership and governance
— Leadership roles
— Cyber strategy and vision
— Policies and procedures

Human factors
— Culture
— Training and awareness
— Talent management

Information risk management
— Enterprise risk appetite
— Asset management
— Third-party management
— Data sharing

What is a cyber diagnostic assessment

KPMG's cyber diagnostic assessment (CDA) provides a foundational overview of an organization's ability to protect its information assets. The KPMG CDA is a high-level, holistic assessment of the common domains that may comprise an organization's cyber security program.

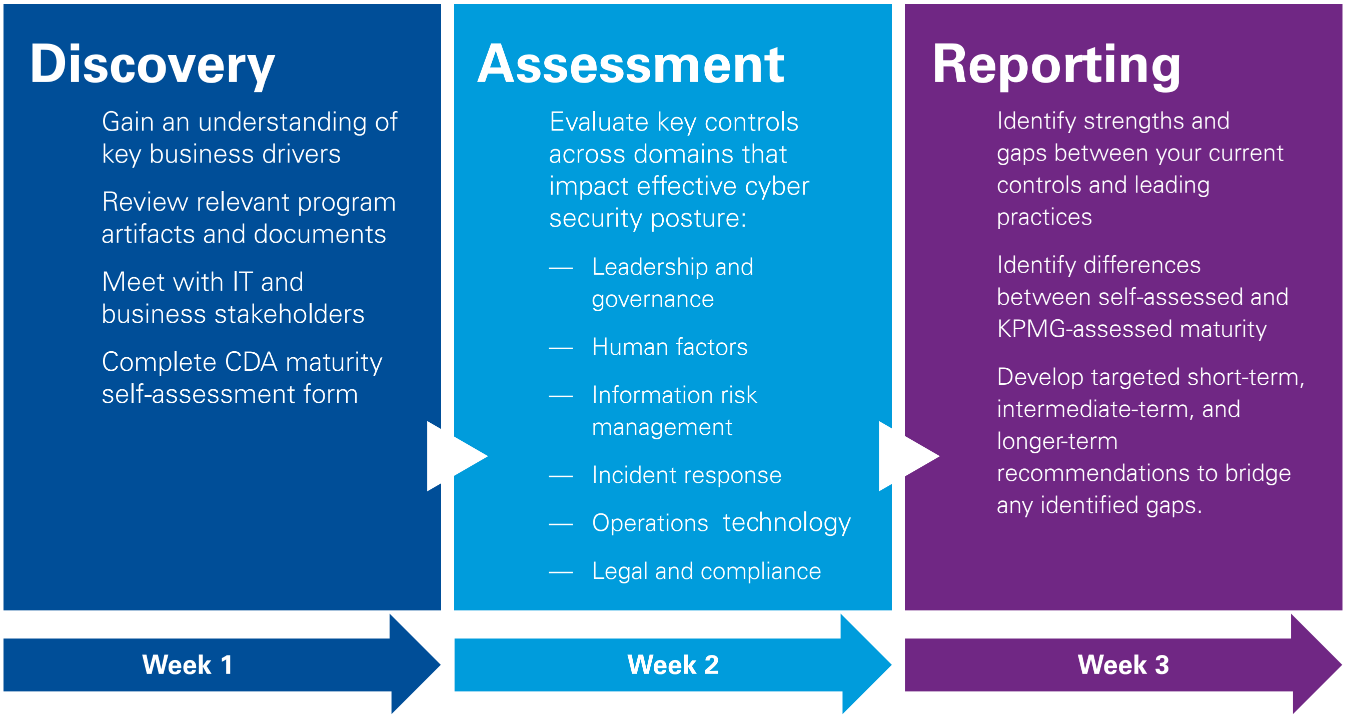
In developing our approach, KPMG used industry leading information security standards and frameworks (including ISO 27001, NIST CSF, NERC CIPv5, COBIT 5) and other such standards, as well as our global teams dedicated to risk management, cyber security, governance, and people and processes.

Through a combination of specific stakeholder interviews and review of information security policies, procedures, and processes, the CDA rapidly:

- Assesses cyber security maturity against defined key controls in the KPMG CDA framework
- Identifies potential gaps in cyber maturity
- Reports key findings and provides actionable recommendations to enhance your organization's cyber maturity and remediate any identified gaps in your environment.

In short, the KPMG CDA is a quick, economical, off-the-shelf approach to identify gaps in your enterprise cyber security program. The output includes tangible deliverables that your organization can leverage to improve your cyber maturity journey.

KPMG will perform the CDA over three weeks. We will discover information through stakeholder interviews and review of information security policies, procedures, and processes. We will assess your cyber security maturity against defined key controls in the KPMG CDA framework and identify potential gaps. We will report to your management on key findings and provide actionable recommendations to enhance your organization's cyber maturity and remediate any identified gaps in your environment.



Discovery

Gain an understanding of key business drivers

Review relevant program artifacts and documents

Meet with IT and business stakeholders

Complete CDA maturity self-assessment form

Assessment

Evaluate key controls across domains that impact effective cyber security posture:

- Leadership and governance
- Human factors
- Information risk management
- Incident response
- Operations technology
- Legal and compliance

Reporting

Identify strengths and gaps between your current controls and leading practices

Identify differences between self-assessed and KPMG-assessed maturity

Develop targeted short-term, intermediate-term, and longer-term recommendations to bridge any identified gaps.

Week 1

Week 2

Week 3

During the CDA's discovery phase, KPMG will interview key stakeholders from process areas throughout the organization to gain an understanding of the current state of cyber security including business drivers. A representative list of stakeholders are listed below.

Stakeholder individuals/process areas*
Chief information security officer
Security engineering and operations
Chief information officer
IT engineering and operations
Human resources
Business continuity
General counsel
Internal audit

From project start to delivery of the final report, KPMG can provide you with:

— Prioritized recommendations to remediate critical gaps

— Gap analysis in current controls versus leading practice

— Analysis of self-assessed maturity versus KPMG benchmarks.

Why KPMG?

The CDA is one component of KPMG's Cyber Transformation Services. Our cyber transformation service brings together specialists in information protection and business continuity, risk management, privacy organization design, behavioral change, and intelligence management. These combined skills are utilized to tailor an approach relevant to your risk appetite and the cyber threats your organization faces.

KPMG member firms are:

— Global – The network of KPMG member firms employ over 189,000 professionals in 152 countries. KPMG cyber security industry professionals have deep knowledge and can offer insight to you wherever you operate.

— Acknowledged leaders in cyber security – KPMG International has been named a leader in the Forrester Research Inc. report, the Forrester Wave™: Information Security Consulting Services, Q1 2016, achieving the highest score for current offering and strategy.[1]

— Shaping the cyber agenda – Through I-4 (the International Information Integrity Institute), KPMG firms help the world's leading organizations to work together to solve today's and tomorrow's biggest security challenges.

— Committed to you – KPMG's client relationships are built on mutual trust and long-term commitment to providing effective and efficient strategies.

[1] Source: Forrester Wave Q1 2016 Report

Contact us

For more information on the Cyber Diagnostic Assessment or KPMG's Cyber Transformation Services please contact one of our healthcare and life science practitioners or visit us at https://advisory.kpmg.us/kpmg-cyber.html

Michael D. Ebert
Partner, KPMG,
Cyber Security Services
T: 856-404-2764
E: mdebert@kpmg.com

Mark M. Johnson
Managing Director, KPMG,
Cyber Security Services
T: 615-830-8438
E: mmjohnson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and thier affiliates

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.