KPMG

Redesigning your Target Operating Model as part of a digital transformation?

Don’t overlook data security

kpmg.com/us

Six keys to integrating data security into your TOM

As digital transformation initiatives sweep through the business world, the need to modify and evolve an organization's target operating model (TOM) grows accordingly.

What is often overlooked when redesigning the TOM is updating and strengthening the organization's **data security defenses**. This can lead to grave consequences for an organization in terms of financial loss, data loss, reputational damage, disruption of operations, and potential litigation.

Can't have one without the other

Data security needs to be at the heart of every TOM revamp. The goal of this report is to help your organization bolster its data security capabilities while updating your TOM to support an effective digital transformation.

We will walk you through the data security components of your TOM that should be reviewed and updated. We will also explain how our innovative six-element data security-enabled TOM process is superior to the traditional three element approach (i.e., people, process, and technology).

What's a Target Operating Model (TOM)?

A target operating model, or TOM, is the blueprint of a firm's business vision that aligns operating capacities and strategic objectives. It helps an organization visualize and then apply and execute on its corporate strategy or vision for the business and its operations.

Costs and other impacts of a data breach

These costs include both direct and indirect costs incurred by a breached organization.

- $10.5 trillion – Estimated cost of cybercrime globally by 2025; that's a 15 percent year-over-year increase.
- $9.05 million - Average total cost of a data breach in the United States in 2021, the highest of any country.
- $1.59 million – Cost of average lost business opportunities caused by a data breach in 2021.

Other data breach highlights

- 40 percent – Organizations with more than 10,000 "ghost users" (i.e., former employees who still have active accounts on the corporate network.) These accounts create vulnerabilities that hackers can exploit to access sensitive information.
- 287 days -The average number of days it took to identify a data breach

Source: Varonis, "84 Must-Know Data Breach Statistics" (November 2023).

72 **percent** of CEOs are prepared to radically transform their organization's operating model to remain competitive.

Source: KPMG International, "KPMG Operating Model Transformation: Turning Strategy Into Reality" (January 2023).

The intersection of digital transformation, TOM, and data security

Digital transformation encompasses the use of established and emerging technologies, including cloud computing, the Internet of Things (IoT), ChatGPT or derivative products, artificial intelligence (AI), machine learning (ML), blockchain, data analytics, 5G, robotics, nanotechnology and more. In 2022, spending on digital transformation was approximately $1.6 trillion; by 2026, global digital transformation spending is forecast to reach $3.4 trillion,[1] and there's no indication it will be slowing down any time soon.

These new technologies have the potential to benefit organizations across all markets–financial, manufacturing, agricultural, R&D–regardless of size. When integrated properly, the technology can generate real-time data that provides an organization with better visibility and deeper insights into its operations, which ultimately lead to increased productivity and efficiency.

But this expansion of technology also holds the potential for catastrophic danger for organizations that haven't considered a TOM update alongside the introduction of new technologies. For example, it may lead to:

Exposure of sensitive data: As organizations continue to collect greater amounts of sensitive data, additional steps must be taken to identify where sensitive data resides and how to protect it.

Data breaches: Increasing costs associated with a data breach means organizations need strategies for reducing a breach's overall risk and impact.

Unprotected data in the cloud: Data continues to move to the cloud, often across multiple providers or apps (including ChatGPT). As a result, traditional methods used to secure data on-premises are no longer sufficient and need to be transformed and reinforced.

Regulatory challenges: Legal and regulatory requirements for data security continue to evolve, which means that your organization must take proactive steps to remain in compliance.

Protect your data - or else

At the heart of all digital transformations is data—both human and machine-generated—which is growing exponentially. As data becomes easier for business teams to access and leverage, the need to secure that data is heightened.

What's more, there's no end in sight; if anything, the amount of data generated will be accelerating at an even greater pace. Over the next two years, it's projected that enterprise data will grow at a 42.2 percent annual rate.[2]

[1] Source: Statista, "Spending on digital transformation technologies and services worldwide from 2017 to 2026" (October 2022).

[2] Source: Seagate, "Rethink Data' Report Reveals That 68% of Data Available to Businesses Goes Unleveraged" (July 2020).

Many businesses have learned that significant damages can ensue if data isn't protected properly. While operating models provide a structure for organizations to align its operations with its strategic vision, they often overlook or fail to prioritize the protection of data in favor of accessibility or convenience. This trend began even before the COVID-19 pandemic struck and has only accelerated in the wake of many organizations adopting hybrid working models.

Also, as more companies move to the cloud and away from a secured on-premises office environment, they sometimes overlook mechanisms for protecting data. Unfortunately, this exposes the data–and the companies–to new breach opportunities by cybercriminals or other malicious actors.

With large amounts of data being moved in and out of IT systems from a variety of sources, data security has become even more important–and more challenging. Embedding data security practices into the TOM have become critical in detecting and preventing data breaches as well as unwanted destruction and/or exfiltration of sensitive data. That's why, as an organization progresses in its digital transformation journey and is restructuring its TOM, stronger and more effective data security policies and processes must be efficiently and thoroughly integrated into each element of the TOM.

> Every CEO I meet with asks, 'How do I better drive my business in a digital world while still protecting my data?
>
> – Mark A. Goodburn, Global Head of Advisory, KPMG International

The KPMG TOM: Integrating data security at each stage

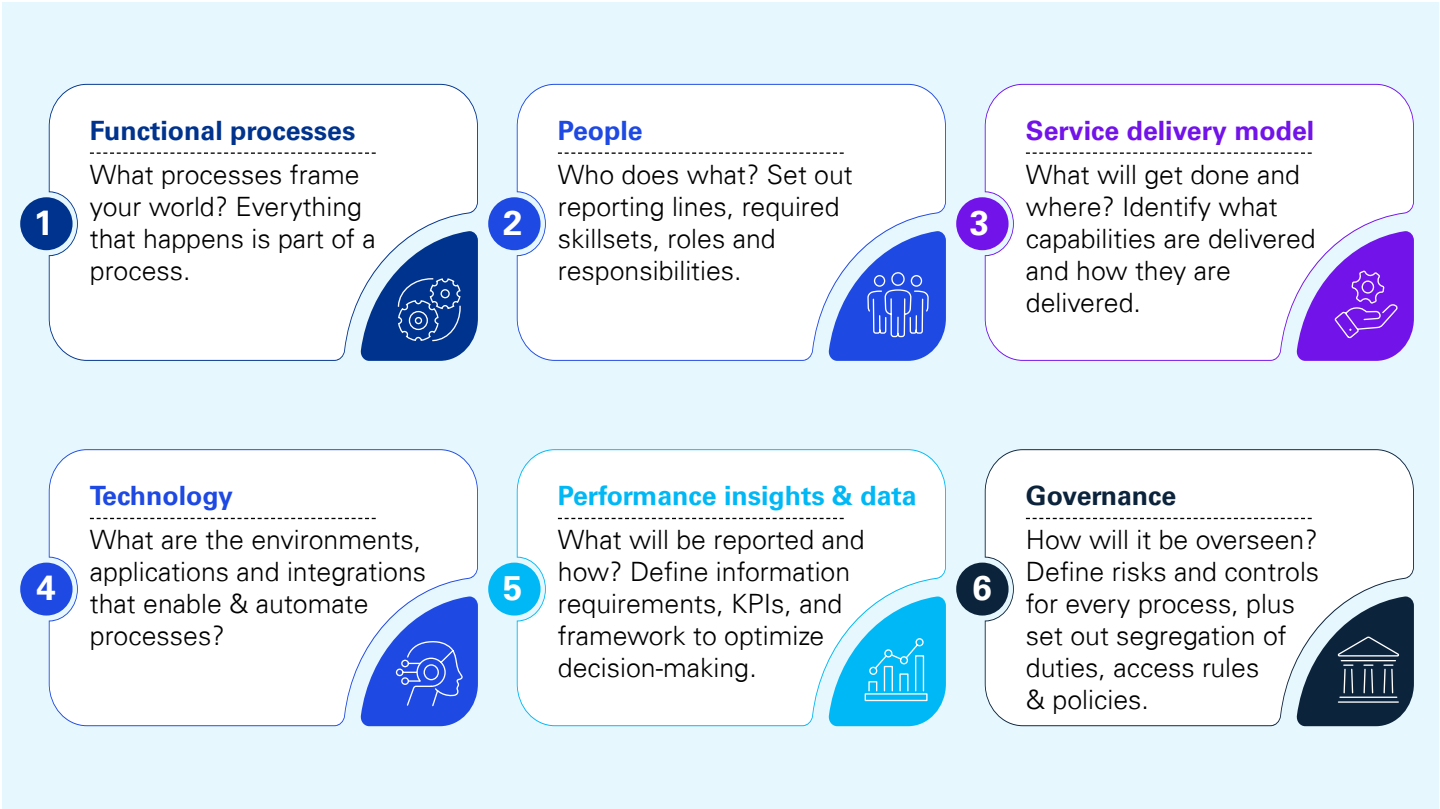
Operating models assist organizations in executing their business strategies and transforming them into operational actions. Without a clear operating model, companies will struggle to meet their goals.

The traditional target operating model addresses the relationship between people, process, and technology. But KPMG has found that this approach often isn't comprehensive enough. For example, it doesn't really deal with: (1) where work will get done, (2) how work will be reported and measured, and (3) how it will be governed and controlled.

To overcome these weaknesses, the KPMG TOM encompasses six "layers," not just three. It covers (1) functional processes, (2) people, (3) service delivery model, (4) technology, (5) performance insights, and (6) governance.

Equally important, we weave data security elements into each of these layers. Our TOM offers a blueprint for rapid and sustainable functional transformation. Each of the six elements contains several predefined "components" that are designed to assist organizations in reaching their end goals sooner.

KPMG Target Operating Model



Here's an overview of how data security can be weaved into each of these six core layers of the KPMG TOM and aligned with an organization's overall business and operations strategy:

Functional processes: Data security must be considered a core business process for companies to function successfully. It needs to be aligned with all other key enterprise-level processes such as sales, marketing, customer service, and product development.

A data security strategy includes data management and data recovery capabilities that utilize people and technology. It also requires security, integration, quality, and scalability to protect data properly and resolve business issues.

Many organizations fail to properly integrate data security requirements with enterprise-level functional processes. Here are some factors to consider so you can avoid this mistake:

- **Strengthen confidentiality:** Safeguard data from unauthorized access attempts by implementing strong control mechanisms and policies that dictate what authorized users can and cannot do with data. The more sensitive the data – and the greater the amount and type of damage that could be done if it fell into the wrong hands – the higher the level of confidentiality required.
- **Secure data integrity:** Maintain consistency, accuracy, and trustworthiness throughout the data lifecycle. Steps must be taken to ensure that data can't be altered by unauthorized individuals or while it is in transit.
- **Ensure accessibility:** Information should be consistently and readily available to authorized parties. This involves properly maintaining hardware, technical infrastructure, and systems that hold and display the information.
- **Enforce accountability:** There needs to be clear accountability that's communicated to personnel to ensure that data use and storage is maintained in accordance with the data security principles listed above.

People: With an increasingly mobile and virtually connected workforce, people in the organization have access to more data than ever before. From data collection to data disposal, protecting data and complying with confidentiality rules has become even more challenging.

While acquiring and utilizing innovative new technology is critical, keep in mind that most data security breaches are the result of human error.[4] Some steps for minimizing the risks of a breach by your personnel include:

- Creating and sustaining a data security culture. This includes defining data security responsibilities for certain roles across the organization that are responsible for handling sensitive data. Enforce rules for violations and publicize when that occurs.
- Encouraging employees to comply with data security policies and best practices. While "sticks" may be appropriate for policy violations, "carrots" should also be awarded for compliance.
- Buttressing encouragement by enforcing data security policies uniformly and taking measures that safeguard people against data security threats. This includes offering data security training and awareness programs for employees and establishing in-house data security expertise.

Service delivery model: Most of the service delivery models used by organizations these days are cloud-based. But there are several other types of service models being utilized – including shared service centers, centers of excellence, and outsourcing – and each of these models may have their own unique data security expectations.

Delivery and data security expectations are established by the parties – which may include contractors and vendors – in service agreements that assign responsibility and potential liability for personal data uploaded on the cloud.

- For cloud-based delivery models, it is crucial to identify the model type – whether it's a service, infrastructure, or platform delivery model – to understand and assign delivery expectations.
- Organizations should implement polices, processes and technology that eliminates – or at least minimizes – the potential for uploading any unprotected sensitive information that can open the door to cyber-attacks or lead to fraud, identity theft or theft of financial information.

Technology: Taking advantage of new, innovative technology is critical to supporting and driving business and an agile way of working. When undertaking a digital transformation, many organizations focus on acquiring newer, faster, more efficient technologies that tend to ingest and analyze more and more data. Unfortunately, the corresponding new and improved safeguards needed to protect this data often take a back seat in favor of getting the new technology operational.

But this is a shortsighted approach. It's essential that organizations build a robust digital infrastructure that includes strong data security architecture with features such as:

- Data discovery
- Data classification
- Data encryption in motion and transit
- Data masking or tokenization
- Data integrity
- Data loss prevention
- Data backup and recovery

Some data discovery/classification tools can automatically identify, classify, and tag both structured and unstructured data in an environment. What's more, these tags can be ingested into other data security tools, like "data loss prevention," to enforce data usage policies.

[4] Source: Verizon; 2022 BDIR Report Master's Guide; Source: IAPP.org , Data indicates human error prevailing cause of breaches, incidents (2018).

Performance insights and data: Key performance indicators (KPIs) are a critical component of every operating model; they help you measure the success–or lack thereof –of your organization operations, reflect on and understand your bottom-line results, and make informed business choices.

KPIs are also used to measure the effectiveness of your data security safeguards within your TOM. The key is selecting the right KPIs to measure so you can evaluate the effectiveness of your safeguards; otherwise, you may end up measuring and evaluating hundreds or thousands of performance indicators that aren't critical to whether you are successfully protecting data.

Examples of data security KPIs include:

- Sensitive data records on "endpoints" (like desktops, laptops and mobile devices) that are particularly vulnerable to hackers.
- DLP violations within cloud apps.
- Outbound emails with sensitive data.

Key stakeholders representing all of your organization's functional business units should be involved in establishing KPIs, including data security KPIs. What's more, as business conditions change and evolve, data security KPIs may also have to change. So, it's critical to periodically review and change them if there are better ways to measure success.

Governance: Governance provisions for your TOM should, among other items, define risks and controls for processes, provide segregation of duties, and detail data handling policies and standards. Effective data governance practices address the availability, use, integrity, management and security of data.

Adherence to these rules should help control data usage and create consistent and trustworthy data. In addition, it also should help avoid the misuse of data and ensure regulatory compliance with data privacy and protection laws, such as the European Union's General Data Security Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

A team of stakeholders from across the organization should be assembled to develop an effective data governance program with standards and policies that include:

- Defining roles and responsibilities for data owners and stewards.
- Specifying how, where and for how long data needs to be stored.
- Maintaining data quality, managing processes and reporting KPIs and other findings.

Final thoughts: Standing still isn't an option

Digital transformation is going to continue unabated, full speed ahead. This means that your organization's operating model will need to evolve to stay ahead of the curve. But equally important will be updating and enhancing your data security strategies, processes and technologies, and integrating them into every phase of your TOM.

As you consider next steps regarding updating your TOM, you should also be sure to evaluate how your data security capabilities currently are layered into it. You need to embrace data security as an essential component of your TOM as your organization navigates an ever-shifting competitive and regulatory landscape.

How KPMG can help you

We are a solutions focused firm that offers sustainable, wide-ranging transformation and strategy. We help enable fast-paced, agile implementation that allows you to manage transformational change while retaining control over your operations and maintaining (if not boosting) productivity. We also work with you to develop an innovative bold, new target operating model that seamlessly allows you to transition to the next level of maturity as your business evolves.

Our integrated, thorough transformation solutions – from strategy to implementation to redesign – include the creation, improvement and delivery of a pragmatic and actionable operating model that is appropriate for your business. We collaborate closely with our clients to enable that the best outcomes are achieved and have a proven track record for helping them attain tangible and lasting improvements in performance.

Connect with us

For more information on establishing or enhancing your operating model or data security process, please go to our website or contact one of our professionals below:

Michael D Gomez
Principal
Cyber Security Services
T: 202-999-9383
E: michaelgomez@kpmg.com

Steven Stein
Principal
Cyber Security Services
T: 312-665-3181
E: ssstein@kpmg.com

Venoth Lal
Director
Cyber Security Services
T: 214-840-4297
E: venothlal@kpmg.com

Andrew Ludwiczak
Manager
Cyber Security Services
T: 415-361-0795
E: aludwiczak@kpmg.com

Rachita Bhattamishra
Associate Director
Cyber-Strategy & Governance
T: 990-380-9351
E: rachitab@kpmg.com

Pallavi Malap
Manager
Cyber-Strategy & Governance
T: 823-714-9892
E:pallavisunilm@kpmg.com

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**