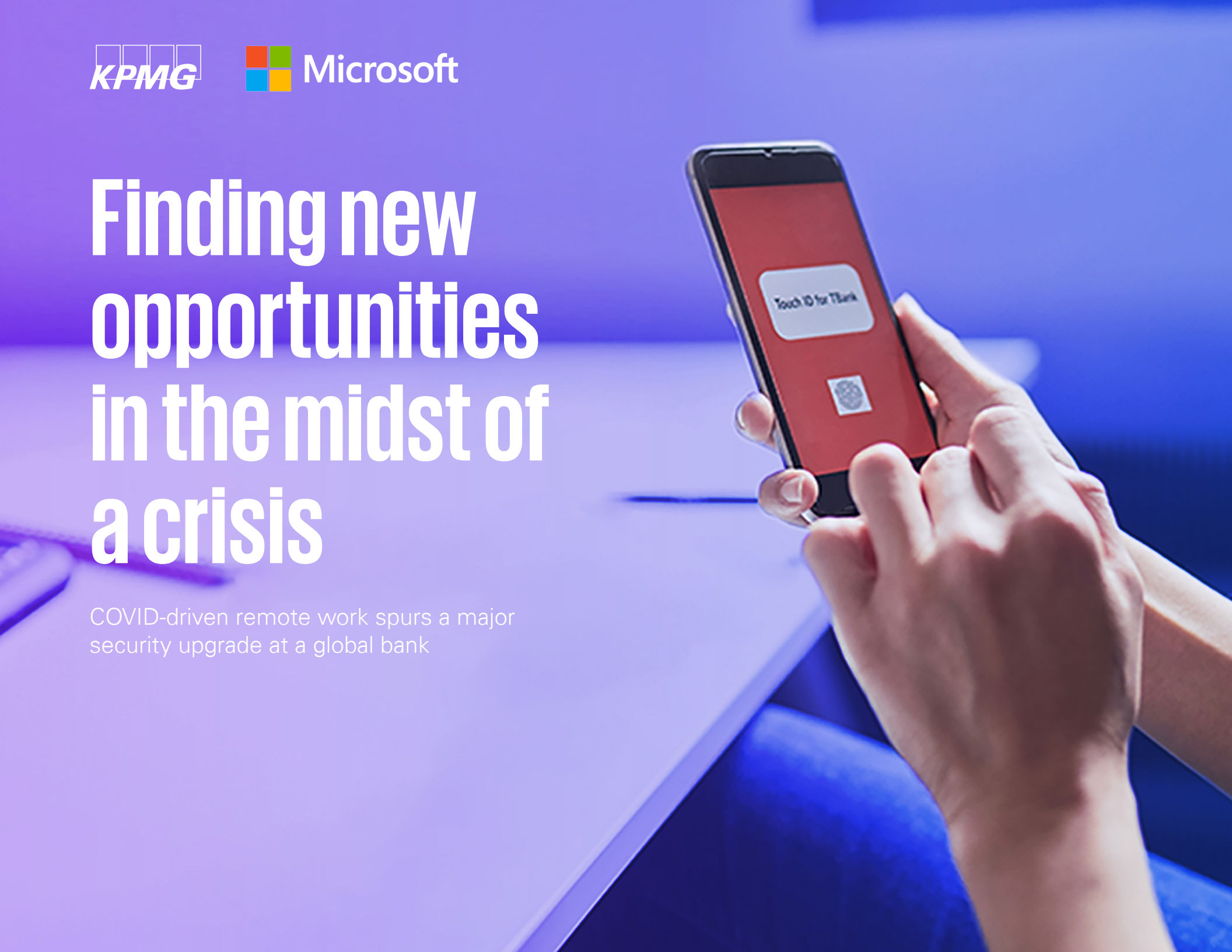
KPMG Microsoft

# Finding new opportunities in the midst of a crisis

COVID-driven remote work spurs a major security upgrade at a global bank



## Key facts

**Client:** A major global bank

**Industry:** Financial services

**Primary goal:** Ensure secure collaboration and controls

**Primary platform:**
Microsoft Azure and Microsoft 365

When COVID-19 forced employees to work remotely, the U.S. subsidiary of a global bank needed to improve the security and compliance of online collaboration via Microsoft Teams. Like so many businesses, our client was stunned by the sudden changes to its workplace. But management also saw that the challenges of remote work were an opportunity to make security upgrades to improve performance and empower employees.

As a longtime adviser on IT issues and cyber security, and as a Microsoft Inner Circle Partner, KPMG was asked to help reconfigure systems to be more secure, collaborative, and efficient.

## Outcome highlights

| | | | |
|---|---|---|---|
| **Key outcomes—overall** | Easier, more secure collaboration | Standardization on a single global platform | Better protection from cyberthreats |
| **Key outcomes—cyber security** | A clearly defined operational model for secure sharing | Full use of Microsoft 365 security and reporting | Lower risk of compliance and regulatory issues |

# Client journey

## Before

**Limited collaboration meets limited security**

The client already used some features of Microsoft 365, but the platform's most important collaborative tools—SharePoint, OneDrive, and Teams—were not rolled out because of security and compliance challenges. All three applications had been launched before but were quickly pulled back after generating a multitude of security red flags.

For office-based workers, collaborating via basic applications like Outlook and Skype was already limiting. But when the COVID-19 pandemic forced more employees to work from home the need for a more functional and secure systems became acute.

And even before the pandemic, the client's CIO understood that the existing operating model and processes for data sharing were too loosely defined and inconsistently applied. In addition to making collaboration difficult, it also meant that responding to possible threats or violations was too slow.

## After

**A clear structure, easier collaboration, better security**

The client has established a clear, enterprise-wide Security Operations model defining a new organization and structure for secure collaboration. Preventative and detective controls have been enabled by using Microsoft Data Loss Prevention (DLP) and Microsoft Defender for Cloud applications, and monitoring is enabled using Sentinel.

In operational terms, the upgraded system lets workers communicate and share data securely from any location or device, including PCs, tablets, or smartphones. Through better controls and automation, response times and reactions to security issues have been reduced significantly. And despite some initial resistance from some employees, extensive training and preparation have built trust and acceptance of the new system across the organization.

And at a higher level, the client is now better protected against cyberthreats, regulatory violations, and potential liability.

## Future

**Going global, reducing costs**

The upgraded policy model and security integrations for Microsoft 365 used in the U.S. will be rolled out to other regions in the near future.

Additional functions and controls will be added to meet local or regional regulatory requirements.

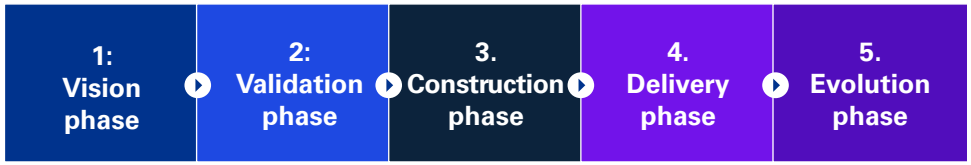
The shift toward fully cloud-based platforms yields cost savings and balance sheet improvements.

"The reason our clients trust us is because we're always on their side. There were many instances during this engagement when the client wanted additional security features that weren't normally supported by our vendor partners. We could have tried to scale back what they were asking for, or tried to find an alternate solution. But we knew it was important to them, so we passed the request on to the vendors and got them to make adding them a priority."

—**Vivek Saxena**
KPMG Engagement Leader

# Phases

**KPMG follows a four-phase approach to better security and collaboration**




### 1. Vision phase
### Getting more out of Microsoft

Our KPMG Powered Enterprise approach to digital transformation starts by working closely with the client to establish a Target Operating Model—a best-case scenario for how new processes and technologies will work together to solve problems and create value.

Despite the previous difficulties with taking secure collaboration beyond email and videoconferencing, the client's CIO understood that Microsoft 365 and Azure already offered nearly all the cyber security capabilities needed—the key would be configuring them correctly. And although some functions in the upgraded system would still be handled through on-premises software, a full migration to the cloud was the longer-term goal.

### 2. Validation phase
### Consensus building at home and abroad

The next stage was to build consensus among the various constituencies within the organization on how the upgraded system should be designed, deployed, and managed. Although the project targeted the bank's U.S. operations, extensive consultation and planning sessions were held with personnel responsible for end-user technology, security, operations and infrastructure at the global level. This made sense not only because a broader international rollout was expected in the future, but because security, risk, and compliance requirements vary by country or region.

### 3. Construction phase
### A better model meets better technology

After conducting a final security assessment, the KPMG team identified gaps in processes and technology and recommended a new Security Operating model for the U.S. that would ensure a high degree of security. The new model was also designed to enhance other IT capabilities such as analytics, lean/agile operations, and cross-functional collaboration. Other important elements included:

- Implementing a new preview feature for Microsoft DLP to meet Information Security requirements
- Allowing remote employees to securely access documents via laptops, tablets, or smartphones without risk of data exfiltration
- Activating security-specific capabilities like data classification, information protection, data loss prevention, and Data Management Platform (DMP) policies
- Improved monitoring and reporting of incidents in which files are shared with unauthorized users
- Creating an end-user training guide to help employees understand the goals of the new system and how to use it effectively
- Adapting Microsoft 365 to create automated custom reports to streamline operations and reduce overhead

And not every part of the final design was immediately available. Thanks in part to our longtime partnership with Microsoft, (and our deep understanding of the client's priorities), our team was able to press for enhanced functions designed to address the client's specific needs.

### 4. Delivery phase
### Test, confirm, and deploy

Since nearly all the U.S. bank's 17,000-plus employees would have access to the new system, advance testing and feedback were required prior to a full rollout. The process started with a pilot launch to about 70 people in late 2021, which yielded valuable responses on everything from usability to documentation for specific features and functions. After incorporating this initial input, a larger trial reaching about 1,000 workers in the IT organization followed. Our team then opened a distribution list for these users to share questions and feedback prior to a full launch in early 2022.

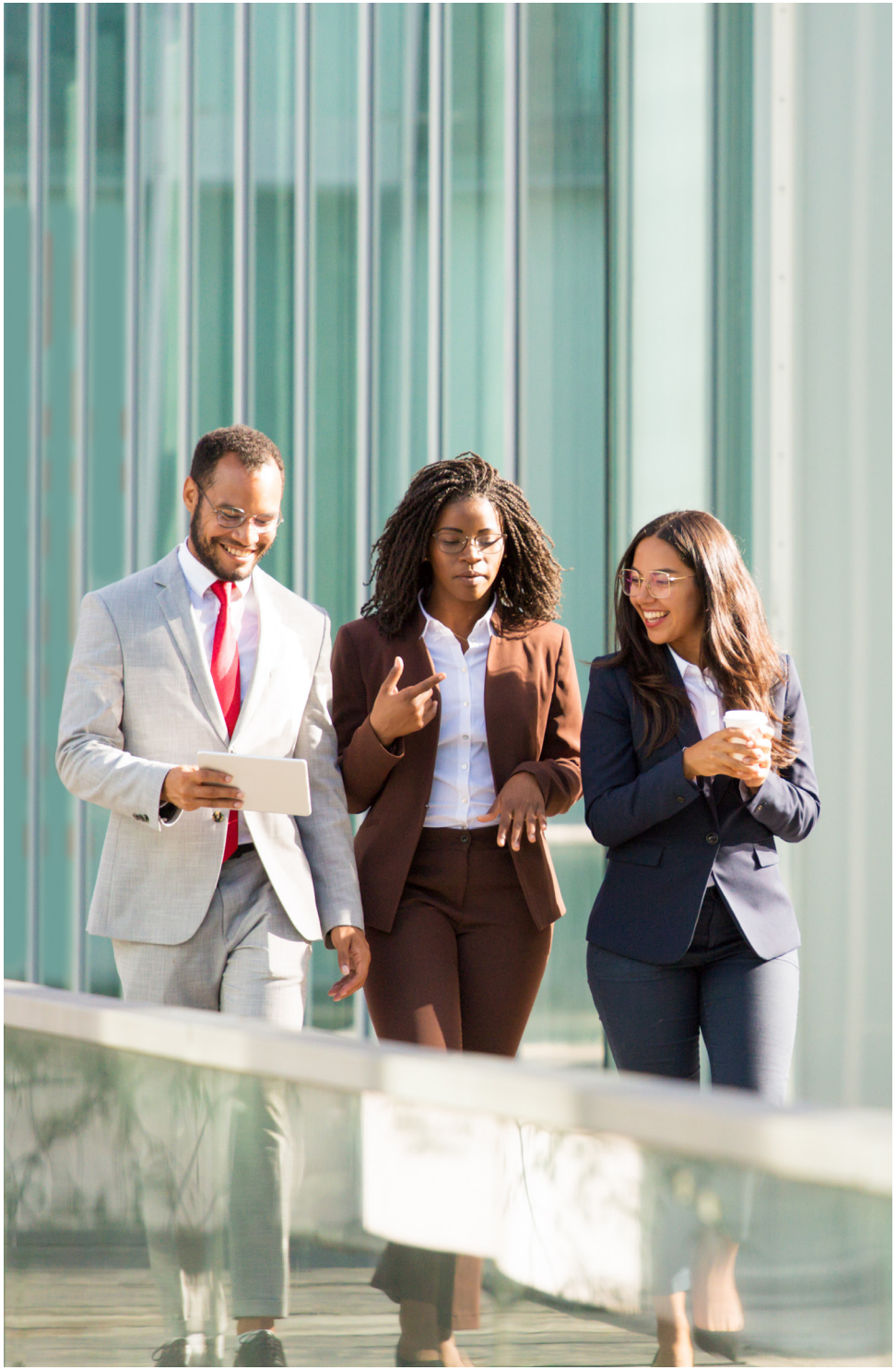
The first result was that we established an interim state during the pandemic which allowed the client to consolidate all collaboration on the Teams platform. Once this solution was in place, we defined a structured path to upgrade security and enable the full range of collaboration features available from Teams.

To date, the response has been overwhelmingly positive, starting with the bank's CIO, who was impressed with the content, ease of access, and controls built into the system. More generally, the full launch produced very little disruption among rank-and-file workers that now able to share data and collaborate more easily. There were zero complaints.

### 5. Evolution phase
### Going global and moving to the cloud

With the deployment of the new security solution in the U.S., KPMG and the client are now planning to replicate its success in other regions. Meanwhile, KPMG continues to monitor the U.S. platform to identify new security issues and add improvements where needed.

Along with better security and more effective collaboration, transitioning to the cloud-based versions of Azure, OneDrive, and SharePoint is allowing the client to retire local on-premises drives and data centers, delivering significant savings and balance sheet improvements.



# Turning insights into opportunity

**KPMG and Microsoft Cyber Security**

Microsoft Azure and Microsoft 365 are continuously evolving to provide greater security to client devices, the Azure cloud platform, on-premise infrastructure and other cloud services. KPMG offers an in-depth understanding of both products as well as the methods and accelerators needed to improve security quickly and prepare to meet future threats. Learn more: https://www.kpmg.us/alliances/kpmg-microsoft/microsoft-cyber-services.html

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

**kpmg.com/socialmedia**



## For smart businesses, managing cyber risk means more than playing defense

Let's talk about where you are now and your goals for the future.

# Start a conversation

**Rajan Behal**
**Advisory Managing Director, Cyber Security Services, KPMG**
**T:** 281-871-9745
**E:** rbehal@kpmg.com

**Vivek Saxena**
**Director, Cyber Security, KPMG**
**T:** 610-263-2876
**E:** viveksaxena@kpmg.com