

サイバーセキュリティについて

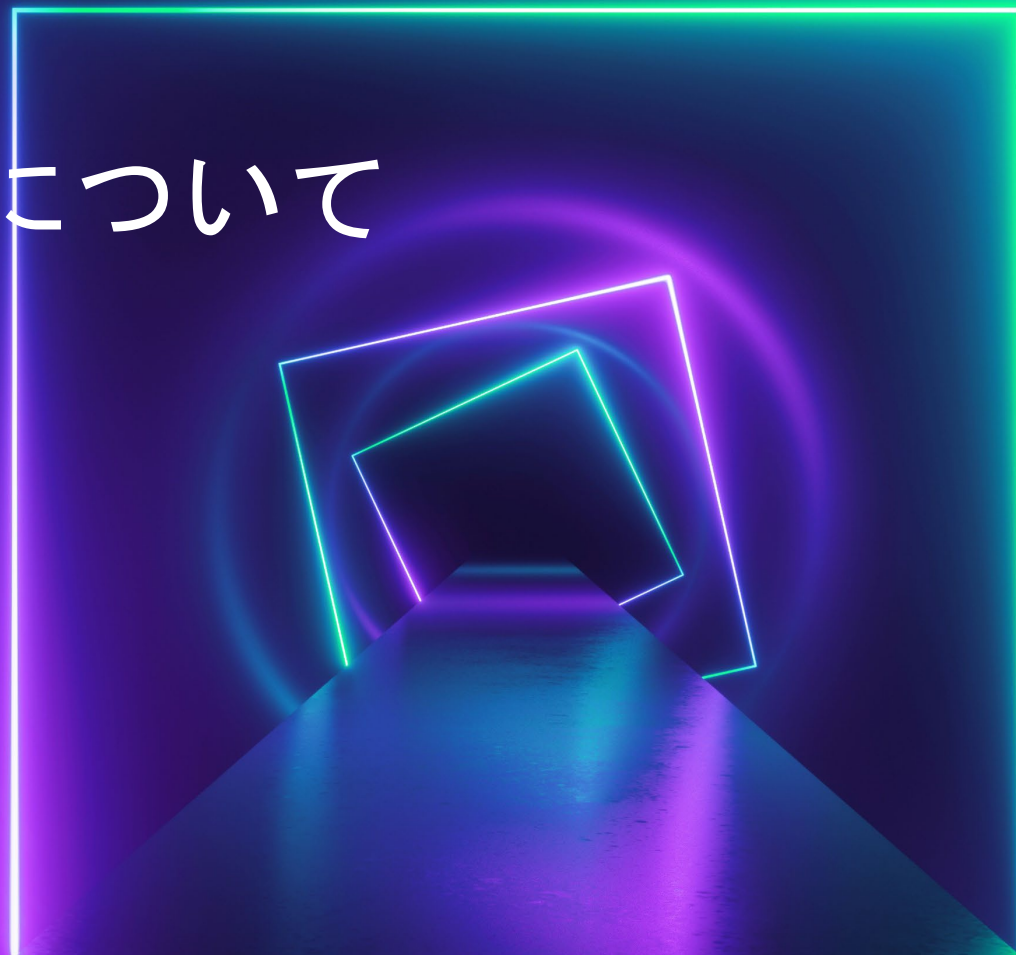
(はじめに)

Introduction

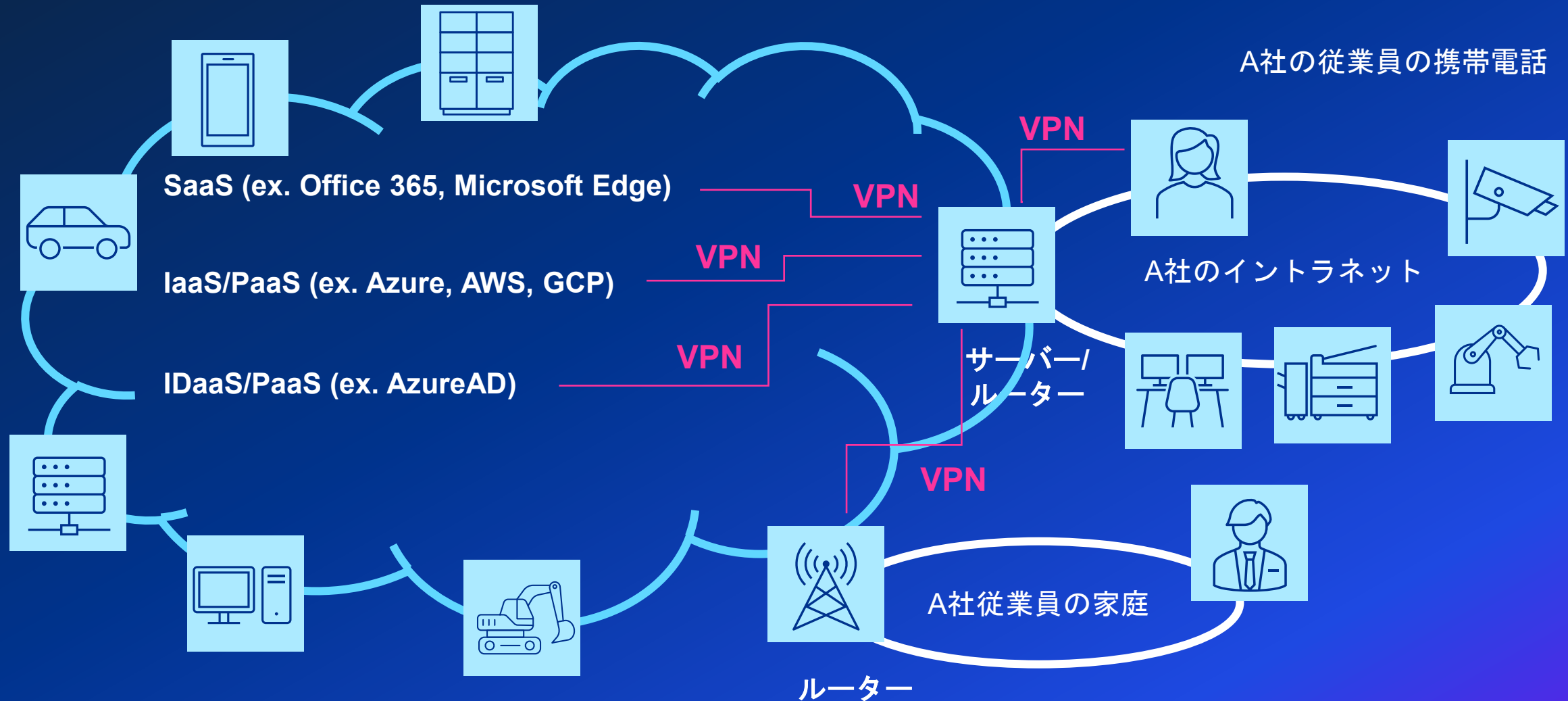
JCC Seminar @ KPMG HU

—

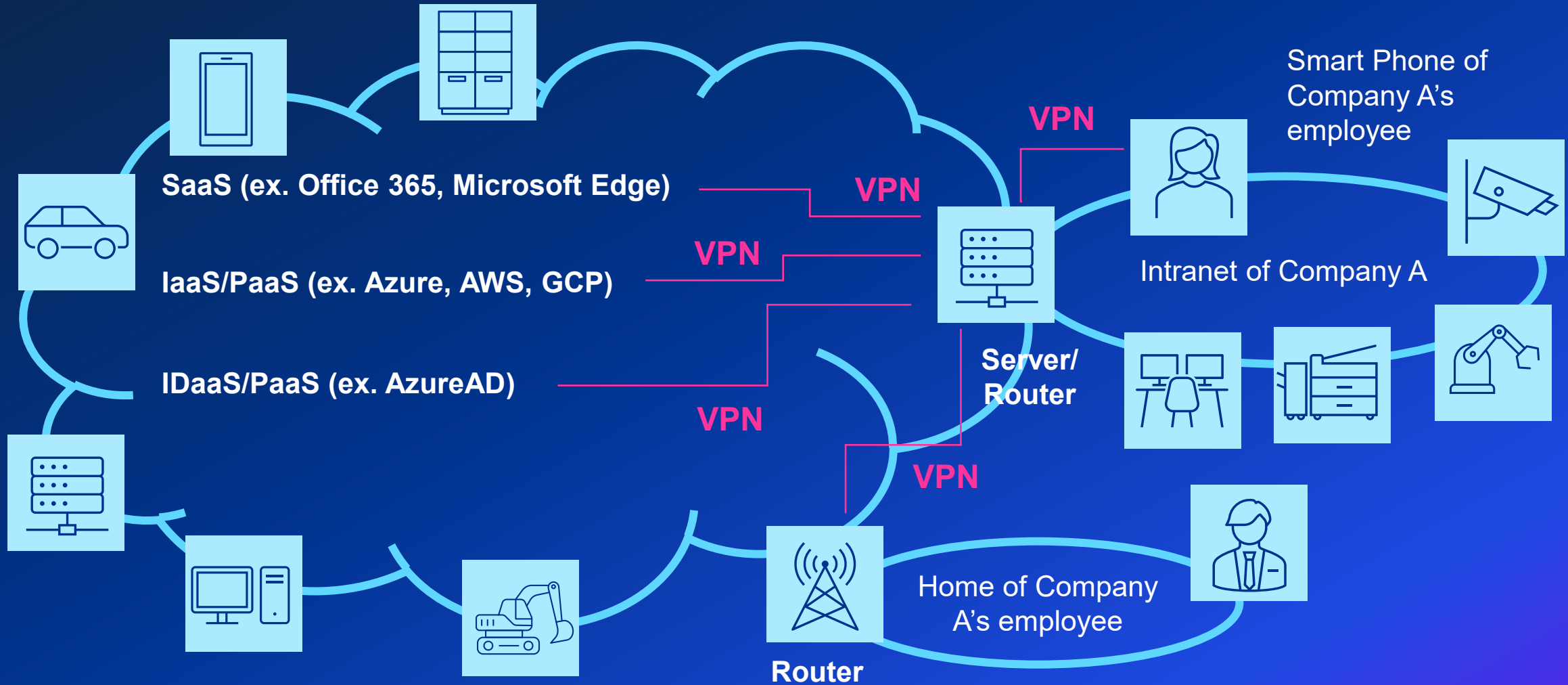
2024



はじめに:サイバーセキュリティの重要性の高まり



Introduction: Why cyber security is gaining attention now?



はじめに:サイバーセキュリティの重要性の高まり

サイバーセキュリティ上の脅威が高まっている主な理由

- クラウドコンピューティングの普及
- 在宅勤務の増加
- サイバー攻撃の産業化 (e.g. ランサムウェアのサービス化、分業化、ダークマーケットやコミュニティの発達)
- 戦争、政治的対立の武器として開発されたサイバー攻撃スキーム、テクノロジーの転用

Introduction: Why cyber security is gaining attention now?

Major factor to increase cyber threat

- Increase of utilization of cloud computing
- Increase of remote working
- Cyber attack is becoming industry (e.g. Ransomware as a service, specialization, dark markets and communities.)
- Cyber attack schemes and technologies are developed through war and political conflict which could be applicable to other targets.

はじめに：キーコンセプト

情報セキュリティの3要素（CIA）

- 気密性（Confidentiality）：
許可された者のみが重要な情報にアクセスできる
>>アクセス制御、主体認証、通信の暗号化
- 完全性（Integrity）：
情報に信頼性があり、改ざんされない
>> ハッシュ関数、暗号化、デジタル署名など
- 可用性（Availability）：
システム、ネットワーク、アプリケーションが稼働すべき時に稼働する。停電、災害、破壊工作（たとえばDoS攻撃など）含む。
>>システムの二重化

クラウドコンピューティング

On-Prem	IaaS	PaaS	ASP	SaaS
Application	Application	Application	Application	Application
Data	Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage	Storage
Network	Network	Network	Network	Network
Physical Env.	Physical Env.	Physical Env.	Physical Env.	Physical Env.

内部運用／開発

外部運用／開発

Introduction: Key Concept

CIA triad

- Confidentiality:
Only authorized people can access to important information assets. >>Access control, authentication, encryption of communication
- Integrity:
Making sure your data is trustworthy and free from tampering >> hashing, encryption, digital certificates, or digital signatures
- Availability:
Systems, networks, and applications must be functioning as they should and when they should. To prepare power outage, disasters, sabotage, such as the use of denial-of-service (DoS) attacks or ransomware. >>redundant networks, servers, and applications

Image of Cloud Computing

On-Prem	IaaS	PaaS	ASP	SaaS
Application	Application	Application	Application	Application
Data	Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage	Storage
Network	Network	Network	Network	Network
Physical Env.	Physical Env.	Physical Env.	Physical Env.	Physical Env.

Internal operations / development

External operations / development

内部運用／開発

外部運用／開発

はじめに：キーコンセプト

境界型防衛

- ファイアーウォール: OSの脆弱性
- IDS(Intrusion Detection Systems), IPS(Intrusion Detection Systems): ミドルウェアの脆弱性、侵入の検知・遮断
- WAF(Web Application Firewall): ウェブアプリケーションの脆弱性
- UTM(Unified Threat Management) Systems: 様々なセキュリティ機能（ファイアーウォール、ウイルス対策、侵入防止）を果たすソリューション

主体認証

- 持ち物による認証：USBのセキュリティトークン、銀行カード、鍵など
- 知識による認証：パスワード、ピンコードなど
- 生体認証：指紋、声紋、虹彩、タイピングスピードやパターン

上記の2つ以上を用いるものを多要素認証という

Introduction: Key Concept

Perimeter security/defense

- Firewall: Vulnerabilities in O/S
- IDS(Intrusion Detection Systems), IPS(Intrusion Detection Systems): Middle ware
- WAF(Web Application Firewall): Web Application
- UTM(Unified Threat Management) Systems: UTMs combine multiple security functions (such as firewall, antivirus, and intrusion prevention) into a single solution

Authentication

- Something the user has: Any physical object in the possession of the user, such as a security token (USB stick), a bank card, a key, etc.
- Something the user knows: Certain knowledge only known to the user, such as a password, PIN, PUK, etc.
- Something the user is: Some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.

Multi-factor authentication: using more than two above.

はじめに：キーコンセプト



マルウェア

- マルウェアとは、コンピューター、サーバー、P Cあるいはコンピューターネットワークを破壊、情報漏洩、不正なアクセス権の取得を引き起こしたり、コンピューターのセキュリティやプライバシーを妨害するように意図的に設計されたソフトウェアを意味する。
 - コンピューターウィルス
 - ワーム
 - トロイの木馬
 - ランサムウェアなど
- マルウェアが配布される主なルート
 - Eメールおよび添付ファイル
 - ウェブサイト
 - USBメモリー
 - VPN
 - リモートデスクトップなど

Introduction: Key concept



Malware

- Malware (a portmanteau for malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy.
 - computer viruses
 - Worms
 - Trojan horses
 - Ransomware
etc.,
- Major route of delivery of malwares
 - E-mail and attached file
 - Website
 - USB memory
 - VPN
 - RDP
etc.,



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

kpmg.hu

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 on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2024 KPMG Advisory Ltd., a Hungarian limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.