protiviti®

Face the Future with Confidence

Enterprise Thinking

Planning the Deployment of Microsoft 365 to Ensure Investment

Internal Audit, Risk, Business & Technology Consulting

Introduction

The Microsoft 365 platform transforms how every member of an organisation chats, emails, shares files and performs the essential tasks inherent to all corporate roles. A comprehensive approach to Microsoft 365 deployment planning will ensure the efficiency, cost saving and employee satisfaction that the Microsoft 365 investment has the potential to deliver.

Widely available guidance for Microsoft 365 deployments focuses on tactical matters and tasks related to the mechanics of application delivery. But because Microsoft 365 implementation touches every function of the organisation and changes the working life of every user, and because Microsoft 365 moves sensitive data to the cloud, Microsoft 365 deployment planning should be considered more deeply, broadly and strategically than mere tactical application installation approaches.

The focus of this paper is on considerations for the planning phase of large or complex Microsoft 365 implementations that ensure security and compliance matters are addressed, that the organisation's users are prepared, and that technical considerations ranging from licence management to application coexistence are addressed early enough to ensure full value for the Microsoft 365 investment.

These recommendations start with stakeholders, then cover the criticality of security, legal and compliance considerations early in planning. They cover ways to ensure cohesive infrastructure and support, starting with early planning, and discuss how to overcome the resistance to change that characterises changes as all-encompassing as Microsoft 365 deployment. Lastly, the paper looks at proven, practical methods for managing a deployment program — methods that will embody the vision, success criteria, timeline and organisational change management activities that define successful Microsoft 365 deployments. For organisations that are further along — those that have launched some components of Microsoft 365 or have already commenced their implementations — the recommendations here will help to correct issues that may have begun to emerge.

Organisations may embark on Microsoft 365 deployments without having had the opportunity to recognise the platform's profound impacts across the organisation. The Microsoft 365 deployment planning process must consider what the business requires and what the technical team needs, while giving priority to security, legal and compliance obligations above all. While this paper touches upon some tactical matters and tasks, its intent is to provide an expanded view of the more strategic, often critical aspects of successful Microsoft 365 deployment that are often overlooked.

Most organisations implement Microsoft 365 applications in discrete implementation "waves" rather than all at once. Their rationales for this may include business, technical, compliance, organisational readiness and legal considerations. In fact, some organisations may not deploy particular Microsoft 365 applications at all.

There is no one "right" way to deploy Microsoft 365, because each organisation's deployment planning decisions must be founded in its own evaluations of its particular business model and culture, security needs, compliance obligations and legal commitments. These factors make each business unique.

The powerful adaptability of Microsoft 365 carries great potential for an organisation, but with that adaptability comes complexity. This makes planning Microsoft 365 deployment a considerable and critical task. Approaching the Microsoft 365 deployment planning process equipped with a proven approach, however, will result in secure, compliant, stable implementations and sustained organisational adoption.

Critical success factors for Microsoft 365 deployment planning

Embodied in all considerations are these critical success factors for Microsoft 365 implementation:

- **Communicate**. Identify Microsoft 365 deployment stakeholders, engage them and keep them aligned and updated throughout the implementation and afterward.
- **Clarify objectives.** Define and understand not only business objectives, but also compliance obligations, security requirements and legal responsibilities. Articulate through design exactly how the Microsoft 365 implementation will address compliance, security, and legal considerations.
- **Analyse the technical environment.** Create a complete and detailed picture of how Microsoft 365 will interact with other solutions in the existing technical landscape, including current infrastructure, mobile devices, and hosted and cloud-based business applications.
- **Anticipate and counter resistance to change.** Embark on a program of organisational change management (OCM) in parallel with the Microsoft 365 deployment effort, commencing with Microsoft 365 deployment planning. Ensure end users and all other stakeholders not only are informed, but also are educated, confident and enthusiastic about coming changes.
- **Enlist dedicated program management** and rely on a repeatable, predictable approach to implementation. An implementation effort of the complexity of Microsoft 365 is best managed by an experienced project leader who is undistracted by other responsibilities. Having a structured approach with proven success defined and communicated at the time of initiation is ideal for managing expectations of stakeholders.

Engaging and aligning stakeholders

At a glance

Implementations are most likely to meet the entire enterprise's needs when planners enlist stakeholder groups early for ongoing participation. For most organisations, key stakeholders represent these functions:

- Applications
- Business divisions/units
- Communications
- Information Security
- Infrastructure
- Risk, Compliance and Legal

Implementation of Microsoft 365 will impact business operations and every end user. Successful Microsoft 365 deployment plans, therefore, start with understanding and engaging stakeholder leadership at an early stage. It is important to establish champions for Microsoft 365 deployment throughout the organisation and to resolve to make decisions collectively, because these practices promote ownership of the results. Without early engagement of stakeholders, perceptions of the deployment are harmed.

Each stakeholder group's interests should be represented in deployment prioritisation decisions, and the prioritisation process should be transparent and understood to avoid any conflict or perception of exclusion.

Stakeholder alignment efforts begin with understanding the organisation's structure, leadership and culture. Stakeholder education should be implemented to help them understand their particular roles and the impact of their contributions to a successful Microsoft 365 implementation. While department names vary from one organisation to another, business operations generally consist of the functions discussed below. It's vital to align these teams in deployment planning so stakeholders can know what's expected and execute their responsibilities effectively. The deployment planning phase is the ideal time to consider every aspect of the system's operation and effectiveness once it's up and running.

- The **Risk, Compliance and Legal** functions will want to consider the implementation of Microsoft 365 in light of governmental and industry regulations with which the enterprise must comply. They will want to evaluate the data Microsoft 365 will be hosting, creating and updating, and consider how relevant policies will translate to implementation specifics that ensure adequate data privacy, comply with standards and regulations, and satisfy legal obligations.
- The **Information Security** function will want to consider the adequacy of existing protections against security threats and data breaches. It will want to evaluate applications, features and new data traffic to the cloud, and ensure that adequate protections are designed in.
- The **Infrastructure** function will want to think about how Microsoft 365 deployments will impact end-user computing, identity management and user account management.
- **Business divisions** and business units must lead the conversation about how Microsoft 365's applications designs align to requirements and to business strategy. Further, leaders from the business are among the best candidates to serve as ambassadors and champions of the Microsoft 365 initiative. They can set the tone among their organisation for an enthusiastic adoption among business users. They can make their best and brightest available to support delivery of Microsoft 365.
- The **Applications** function will want to consider which of the current systems Microsoft 365 will replace in whole or in part and initiate plans for migrations of data to Microsoft 365 from these systems. It will want to think through strategies for the possible coexistence of point solutions with Microsoft 365 equivalents in the future. The Applications function will also want to consider current licences and timing for decommissioning of systems.
- The **Communication** function will want to begin planning its support of the significant organisational change management efforts. Its efforts not only instill the excitement characteristic of the most successful Microsoft 365 implementations but also include the training that results in competent, confident users.

Understanding compliance, security and governance considerations

At a glance

Microsoft 365 applications increase enterprise data mobility and entail migration of sensitive data to the cloud. As a result, security, compliance and legal requirements take precedence over business requirements.

Organisations should give careful consideration to how the Microsoft 365 implementation will meet security, compliance and legal objectives. Selecting an established framework will help ensure cloud security. A governance committee can take charge of information governance planning, resolve cross-application dependencies and establish practices for records retention and electronic discovery matters.

Because implementation of Microsoft 365 applications facilitates access to and movement of data, and entails migration of sensitive data to the cloud, Microsoft 365 deployment planning activities must start with analysing security, compliance and legal considerations along with business needs.

Microsoft 365 affects organisational information — often sensitive information — to travel from group to group, user to user, country to country, and potentially to external parties. For compliance, security and governance specialists, these attributes demand close and careful attention to regulations and compliance. These specialists will want to articulate security, compliance and legal objectives and study in depth how Microsoft 365 will meet those objectives.

Understanding local, global and internal regulatory controls, standards and policies in particular relation to Microsoft 365 deployment is a critical first step. Putting these matters first also conveys a message to all stakeholders that compliance, legal and security concerns will take precedence over every other requirement. These elements will thus become significant guidelines by which business requirements and technical designs are constrained.

The governance committee

Successful implementations of Microsoft 365 are typically accompanied by new, formal governance committees that monitor and manage cross-application dependencies such as identity, data protection, etc. Committees like these take charge of information governance planning and establish internal agreements regarding records handling, retention and electronic discovery matters. Lastly, the committee functions as liaison between the Microsoft 365 implementation team, legal entity compliance officers, data privacy officers and relevant business groups. With these stakeholders, they identify and gather the compliance, legal and security requirements that inform the Microsoft 365 deployment plan and procedures for Microsoft 365 operation.

Recently, a global science and technology company approached Protiviti with concern about the exponential amount of unsecured data in its Microsoft 365 environment. With more than 20 global operating companies and 80,000 employees, the company had confidential information flowing throughout each organisation. Protiviti implemented an information protection strategy with Microsoft Information Protection within the company's Microsoft 365 environment to protect its data, meet internal security objectives and address compliance and privacy requirements across all operating companies and all 80,000 global employees.

The transition of sensitive data to the cloud may require not only business stakeholder authorisation, but also regulator authorisation. For large global organisations, the governance committee can consolidate information about pending compliance obligations and risk management needs. The committee can interview stakeholders from all departments and geographies about business activities. Through these conversations, they will identify data classifications and data handling practices, and can then document data flows and understand each group's expectations for future business operations supported by Microsoft 365. This information will help the project team plan critical path activities. It also will ensure any evidentiary documentation of compliance that's needed is produced in the course of deployment.

Some enterprises will want to engage external experts to lead or coordinate the analysis of security requirements, compliance obligations and legal commitments. These matters will certainly vary depending on the nature of the business, but might include any of the following matters:

- Data localisation
- Data protection
- Global data residency (i.e., multi-geo tenants)
- Internal asset classification
- Records information management

Security frameworks and controls

Cloud security frameworks provide best practices for securing an organisation's environment. Applying a well-established security management and controls framework will help ensure that a Microsoft 365 deployment meets the organisation's confidentiality, integrity and availability needs. Businesses that are not regulated by government or industry authorities will want to adopt best security practices, nevertheless. Security requirements are developed from an authoritative framework, complemented by internal standards, and functional controls are translated to technical specification via Microsoft 365 deployment designs.

Effective and broadly adopted frameworks include:

- International Standards Organisation (ISO) 27001/2
- Committee of Sponsoring Organisations of the Treadway Commission (COSO)
- Control Objectives for Information Technology (COBIT)
- National Institute of Standards and Technology (NIST)
- Health Information Trust Alliance (HITRUST)

Security considerations

Microsoft 365's cloud architecture — and the sensitivity of the data that the software will process — means that any Microsoft 365 deployment will entail a multitude of decisions regarding security, governance and compliance. Some of the following considerations will be applicable to any organisation, while others should be evaluated for particular applicability to a given enterprise. For each of these considerations, ownership and decision-making authority must be clearly identified.

Account management and authentication

- Privileged accounts (e.g., administrative roles for each application)
- Cloud identities, guest accounts, service accounts, generic accounts, etc.
- Multi-factor authentication
- Federation services
- Guest access (across platforms)
- Modern authentication
- Conditional access
- Identity synchronisation
- Identity protection
- Password settings and expiration

Application permissions

- Application and permission governance
- Third-party integrated applications

Data management

- Information protection classification labels and policies
- Data loss prevention (DLP) policies
- External file sharing
- Cloud application security console management monitoring
- Customer lockbox

E-mail security

- Calendar detail sharing
- Common attachment type filtering
- Spam policies
- External email forwarding
- Domain whitelisting
- Advanced threat P\protection (ATP) safe links and attachment policy management
- Anti-phishing policy management

Collaboration tool security

- Classification labels
- Creation, modification, deletion life cycle
- Expiration/disposition

Auditing and monitoring

- Audit log configurations
- Mailbox auditing
- Key reports monitoring
- Incident reporting and escalation

Continued...

Data storage

- Document sharing
- OneDrive sync policy management
- Backup and recovery

Device management

- Mobile device and application management
- Remote wipe
- Data encryption
- Anti-virus
- Firewalls
- Application proxy
- Single sign-on and conditional access
- Policy management

Privacy, legal, and compliance

- Data subject requests
- General data protection regulation (GDPR) policies
- Compliance requirement identification
- Supervision and surveillance
- Data retention and records governance
- Electronic discovery (eDiscovery)
- Compliance scoring and compliance management
- Disaster recovery and business continuity planning (DR and BCP)

Interoperability of infrastructure, applications and devices

At a glance

Once implemented, Microsoft 365 will replace an assortment of applications for the enterprise and will run on a variety of devices. Planning therefore includes understanding the current technology portfolio as well as detailed plans for operating the new platform. Considerations include measuring the capacity of the current network relative to new traffic and establishing processes for user provisioning, disaster recovery and data backup.

Organisations may choose a "big bang" cutover to Microsoft 365 or opt to run current applications in parallel with Microsoft 365 for a time. Successful deployment calls for plans that cover transitioning to the Microsoft 365 implementation's end state for each replaced application and device.

Microsoft 365 will be interacting with other applications in the organisation's environment, as well as with infrastructure and devices. A detailed and clear understanding of Microsoft 365's interactions with the environment is foundational to effective decision-making and organisational adoption.

Technical strategy

Technical strategy begins with an evaluation of the current environmental tools, devices and network capabilities, and should include identification of the opportunities, requirements and recommendations for Microsoft 365 deployment and support to develop a complete picture of the current information technology (IT) landscape. From this exercise, a detailed list of prioritised opportunities, requirements and recommendations will emerge. To evaluate proposed changes, organisations should consider scoring recommendations and opportunities according to effort, complexity and importance.

To formulate a thorough and detailed technical strategy for Microsoft 365 deployment, the following questions should be considered:

- How will Microsoft 365 be distributed to the current inventory of mobile devices?
- How will licencing be managed as employees are onboarded and terminated? How will access authorisations for applications be addressed when employees move from role to role?
- What are the anticipated impacts of Microsoft 365 network traffic on the current network's capacity, and what enhancements to bandwidth must be included in deployment planning?
- How will Microsoft 365 application data be backed up?
- How will the organisation fall back and recover in disaster and outage situations?

Coexistence and application redundancy

The essential nature of the processes that Microsoft 365 supports means that no member of the organisation — from CEO to clerk — finds their working day unchanged by Microsoft 365. Most organisations will have point solutions already in place for chat, file sharing, email and so on. For example, businesses will have adopted a publicly available, web-based videoconferencing platform with each department perhaps making its own choice.

Replacing all point solutions overnight with Microsoft 365 may be the right move for some organisations, but many others will find a wholesale cutover too jarring for users to accept (or for help desks to support). Therefore, it's realistic to consider when, how and even whether various Microsoft 365 applications will be deployed. Some of the most successful implementations may retain one or more point solutions for videoconferencing in coexistence with or even instead of the Microsoft Teams application. Organisations will need to inventory currently deployed point solutions that Microsoft 365 might be replacing and create a complete transition plan for each of them.

Deployment planners may elect to decommission a current point solution as soon as the equivalent Microsoft 365 module goes live. Then again, they might opt to not use the corresponding Microsoft 365 application at all if the organisation is happy with a particular point solution. Planners also might elect to deploy the corresponding Microsoft 365 application to coexist with the current point solution.

Application overload can be a real risk to adoption, however. Deployment planning teams should evaluate the tradeoffs when they consider operating multiple systems for the same purpose. When users have multiple tools to support a single task, it can be difficult for businesses to standardise processes, and can be problematic for IT to support and confusing for users.

Continuing to use a popular point solution in lieu of or in parallel with its corresponding Microsoft 365 application can make good sense if the business has already adopted the current technology. However, application redundancies like these generate new considerations for the deployment planning team. Deployment planning is complicated by application redundancy, because the deployment planning team must address several additional planning and operational considerations for analogous applications running in parallel, including:

- Application security
- Data security
- Data synchronisation
- Device security
- Interoperability with Microsoft 365 applications
- Network bandwidth
- Support issues
- Training issues

Overcoming resistance to change

At a glance

Effective user adoption begins with early messaging to inform and engage end users. Users who are confident about their performance with Microsoft 365 from day one, and who understand the rationale and benefits for the change, will support the implementation with enthusiasm. Different user populations will have different interests and concerns about using Microsoft 365. Organisations should consider training tailored to various user populations.

Organisational change management (OCM) is essential to successful deployment. Deriving full value from the organisation's investment in Microsoft 365 requires ensuring stakeholders are engaged and users are equipped with the skills to be confident and competent in their use of Microsoft 365 prior to launch.

Engaging the business

Effective OCM recognises that end users are human beings and therefore naturally resistant to change. For the strongest possible user adoption, deployment planning can include OCM efforts that ensure users are aware of and excited about the changes Microsoft 365 will bring to their working lives. Ideally, OCM messaging will explain the rationales behind the organisation's decision to implement Microsoft 365. Change is easier for anyone when they understand the reasons for — and benefits of — the transformation. Ideally, business stakeholders will be made available and dedicated to facilitating user adoption and training from early days of Microsoft 365 deployment planning. Helping stakeholders to see the value of Microsoft 365 to the organisation and its processes keeps teams focused on positive outcomes. OCM can include communications and workshops that are designed for specific stakeholder groups.

Each team and function may find value in different features of Microsoft 365. Therefore, articulating the value of Microsoft 365 will result in varied communications depending on the department. Human resources, for instance, will take a greater interest in how applications support onboarding. Communications teams will be interested in new ways to run programs and engage employees. Engineering will be interested in the potential for Microsoft 365 to support workflow and provide an intelligent platform for collaboration.

OCM activities can provide multiple paths for users to learn more about the coming changes. These activities could include offering ample training, so users approach the new technology with confidence. Activities also could include "how-to" documents tailored by application or by employee group. "How-to" documents can integrate business-specific process instruction that clarifies how Microsoft 365 will support specific tasks. OCM efforts like these will work best if stakeholders are enlisted early and change is communicated early and often throughout the deployment effort, starting with the planning phase. Organisations should communicate with business users and other stakeholders about benefits, progress and what to expect next for the life of the project through launch and beyond.

Operations support

A robust plan for technical support of Microsoft 365 solutions, aligned with the organisation's operations support team structure, should be included in Microsoft 365 deployment planning. Effective OCM will take operational support teams' needs into account early. Microsoft 365 feature design and configuration are important information for the help desk. In fact, sharing this kind of information with operational support teams is foundational to their preparation. Microsoft 365 deployment efforts benefit when operations and support teams participate directly in developing production support planning and protocols. Organisations should include a training program designed specifically for the operations support team based on the organisation's particular Microsoft 365 deployment details as part of the scope of Microsoft 365 deployment planning.

In order to ease the transition to Microsoft Teams and Exchange Online, a large nonprofit organisation needed an effective change management plan and training program for their staff. After implementing Microsoft 365, Exchange Online and Microsoft Teams for the organisation, Protiviti conducted a three-week online training program to encourage user adoption across the organisation. "Office hours" were conducted to allow staff to ask questions, discuss capabilities and work through problems in an open forum to remain supported during their transition and change management. Together with the company, Protiviti focused on developing full awareness of the technology's capabilities to enhance interaction and drive adoption.

Managing the deployment program

At a glance

Microsoft 365 implementations are most successful when they include early wins.

- Implementing applications in waves builds the implementation team's confidence, and news of their success can be shared to build interest in and support for the initiative.
- Waves can be prioritised to meet goals related to functionality opportunities or compliance gaps.
- Each wave includes careful consideration of security, compliance and legal requirements with each iteration.

The Microsoft 365 deployment planning phase can culminate in a plan that includes the vision, success criteria, timeline and activities that define the initiative. The deployment plan should meet the business' needs, but it's equally important that information technology, compliance, security and legal team stakeholders contribute their views and are kept informed and aligned.

Deployment plans should ensure activities are sequenced so that all security, compliance and legal requirements are met prior to any migration of information to the cloud. Elsewhere in IT, competing initiatives may also be underway, and effective Microsoft 365 deployment plans will include aligning and coordinating with those projects to minimise disruptions. The Microsoft 365 deployment plan will be used to direct, monitor and report on the progress and attainments of the Microsoft 365 deployment initiative.

Crawl, walk, run: the roadmap

Many organisations benefit from a "crawl, walk, run" approach to deployment. It's ideal to undertake smaller and simpler implementation waves first to help the project team gain confidence and consolidate their skills in Microsoft 365 deployments while securing quick wins that build stakeholder and user confidence.

The roadmap should include a framework for seeing implementations as sequences of applications in successive waves with stabilisation periods for each wave. Sharing the complete roadmap broadly and acknowledging progress against it helps stakeholders understand what will be happening when (and why), so they feel empowered and included.

Early implementation waves are often low risk and high reward by design, so that they demonstrate product capabilities and provide a proving ground to consolidate new skills for the team. Organisations should enlist business stakeholders, as well as compliance, legal, security and IT teams in developing the roadmap. They should also consider the organisation's priorities for the deployment of applications and design of features. It is important to evaluate technical and functional goals to identify what's most needed in the near term and which applications can be implemented first from technical and compliance perspectives.

Analysing gaps and finding opportunities

Microsoft 365 deployment planning additionally should encompass the assessment of gaps between the current state and the desired state of systems and processes. A proven process for comprehensive and effective Microsoft 365 deployment planning starts with the analysis of current systems and processes that will be impacted by Microsoft 365. Thorough exploration could expose gaps between the organisation's vision and standard for security and compliance versus what the current environment embodies. Gaps uncovered in this activity are opportunities to enhance security and ensure compliance through design and configuration of Microsoft 365 applications.

A process for reviewing legal, compliance and security factors should be iterated with every implementation wave. Organisations should survey applicable government regulations and industry requirements pertaining to cloud outsourcing for the organisation's line of business, and then use this information to identify and map all necessary controls and to align with future privacy initiatives.

Conclusion

Microsoft 365 enables collaboration at full speed through enterprise-wide sharing of information. This makes compliance, security and legal considerations the primary concerns for most deployments. Microsoft 365's near-limitless adaptability and its effects on every function of the organisation make intensive and detailed consideration of requirements a necessity. Deployments of all Microsoft 365 applications at once are too much for most organisation to process. Many organisations are ill prepared for the magnitude of change a full deployment would mean, so planning for successive waves of implementation is a better strategy.

For all of these reasons, concentrated attention on Microsoft 365 deployment planning is essential. A Microsoft 365 deployment plan should give careful attention to compliance, legal, security, technical and business requirements. It should encompass a comprehensive OCM program. Plans that are segmented into a roadmap that represents the needs of all stakeholders have helped some of the world's most successful organisations achieve a full return on their Microsoft 365 investment. By adopting a comprehensive and detailed approach to Microsoft 365 deployment planning, these organisations are attaining the efficiency, cost savings and employee satisfaction that constitute only some of the potential advantages of Microsoft 365.

How Protiviti helps

We blend a technology and business-driven approach to Microsoft 365 deployments to accomplish rapid stakeholder adoption, requirements-driven compliance and security, and application of a proven, repeatable process for deployment and support. We seek to maximise the return of cost saving, efficiency and employee satisfaction benefits through strong program management and governance practices drawn from prior experience. Our Microsoft 365 experts bring technology, business process, data and program management skills to deliver efficient solutions across functional areas, Microsoft 365 applications, and various implementation stages.

We help organisations manage their Microsoft 365 deployments through a variety of partnership models. From advisory to implementation to augmentation of a company's in-house teams, Protiviti brings expertise, intellectual property and leading industry tools to deliver successfully on Microsoft 365 implementations for organisations of every size, including global regulated businesses with complex compliance obligations and data security needs:

- Microsoft 365 governance and strategic planning
- Microsoft 365 security and compliance assessments
- Microsoft information protection
- Enterprise mobility + security
- Microsoft 365 content service solutions
- Microsoft 365 application enablement
- Windows 10 deployment services

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

Corey Harrison
+1.312.476.3663
corey.harrison@protiviti.com

Scott Gracyalny
+1 312.476.6381
scott.gracyalny@protiviti.com

Evelyn Zabo
+1-206.262.8385
evelyn.zabo@protiviti.com

THE AMERICAS

UNITED STATES
Alexandria, VA
Atlanta, GA
Austin, TX
Baltimore, MD
Boston, MA
Charlotte, NC
Chicago, IL
Cincinnati, OH
Cleveland, OH
Columbus, OH
Dallas, TX
Denver, CO
Ft. Lauderdale, FL
Houston, TX
Indianapolis, IN
Irvine, CA
Kansas City, KS
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New York, NY
Orlando, FL
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
Portland, OR
Richmond, VA
Sacramento, CA
Salt Lake City, UT
San Francisco, CA
San Jose, CA
Seattle, WA
Stamford, CT
St. Louis, MO
Tampa, FL
Washington, D.C.
Winchester, VA
Woodbridge, NJ

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte*
Rio de Janeiro
São Paulo

CANADA
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

BULGARIA
Sofia

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Chennai
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®