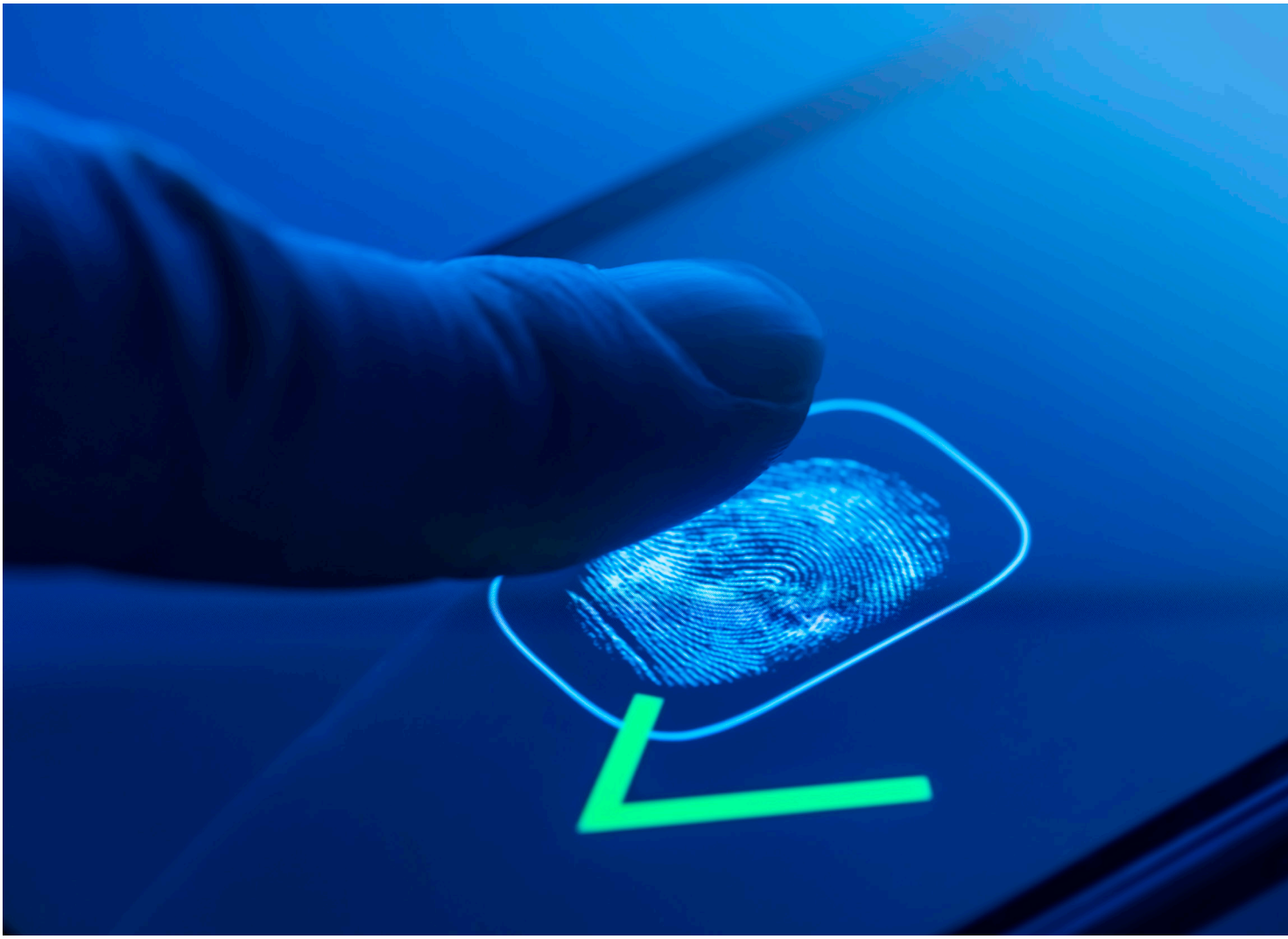
SailPoint

protiviti®

Face the Future with Confidence



What you should know about identity and access management

Five common identity and access management pitfalls to avoid

- Who has access to what?
- Who should have access to what?
- How is that access being used?

Internal Audit, Risk, Business & Technology Consulting

KNOW WITH CONFIDENCE:

- Who has access to what?;
- Who should have access to what? and;
- How is that access being used?

Three benefits of implementing an Identity & Access Management (IAM) solution in an organisation like yours

Secure access management is the path to a secure and confident enterprise. To keep up with today's ever-changing security and compliance landscape, business leaders are starting to understand the strategy evolution needed to govern their users and their access to corporate resources. Leveraging leading edge digital IAM and IGA (Identity Governance and Administration) solutions could enable your company to organise effectively multiple applications, including the associated identities, in a central repository.

Good IAM processes ensures that users are who they say they are, as well as ensuring they have appropriate permissions within the target application (authorisation). A centralised tool can also log all associated changes to user access, easing the ability to pull reports for audits and other executive reports.

In addition, there is a reputational benefit. The central planks of GDPR rest on protecting personal data and respecting consumers' choices on how that data is used. In order meet these two requirements, it's essential that organisations implement the necessary visibility and controls to govern access of users to ensure that only the right people in the right circumstances can access personal data.

A helping hand

Protiviti and SailPoint have proven IAM methodologies and frameworks to help you avoid common pitfalls and integrate IAM as an ongoing service. These frameworks include the whole lifecycle: setting up an operating model, establishing business and security objectives, developing key metrics, roadmaps and prioritising investments to reach a secure and confident IAM environment.

Read our guide to scoping and designing robust, ever-living IAM implementations in your organisation.

Five Common Identity and Access Management Pitfalls

Belton Flournoy, Business & Technology Consultant at Protiviti UK discusses five common IAM pitfalls organisations run into today.

Identity and access management (IAM) is at the forefront of each organisation's overall security strategy. Effective organisations ensure that regulatory compliance and risk management drivers are balanced with business-friendly and effective processes in order to provide users with access to the right resources at the right time.

Organisations that struggle with IAM often do not treat it as an ever-living component of their business. Too often, IAM needs are handled as one-off IT security initiatives due to specific triggers, such as closing an audit finding or improving on a particular business inefficiency. Mature IAM capabilities help meet the demands of initiatives from business and application teams and can potentially reduce costs associated with managing identities and access.

Organisations that treat IAM as a project or series of projects, rather than an ongoing internal service offering, often face issues such as a lack of long-term executive sponsorship, ownership for ensuring the continuous improvement of IAM services and focus needed from multiple parts of the organisation to solve complex IAM problems. Performing one-off IAM initiatives may close gaps in the short term, but doing so leads to decentralised services and potential resurfacing of root causes. Organisations should establish an internal services team or organisation with the mission to continuously improve IAM services to better serve business needs pertaining to risk, compliance, efficiency and competitive advantage to achieve the long-term benefits from the investments made in managing IAM.

In this paper, we discuss five common IAM pitfalls organisations run into today: lack of an effective operating model, lack of meaningful metrics, lack of an IAM roadmap, insufficient business analyst involvement in IAM and technology as the primary focus of IAM investment.

01 Lack of an effective operating model to ensure organisational alignment to continuously improve IAM services

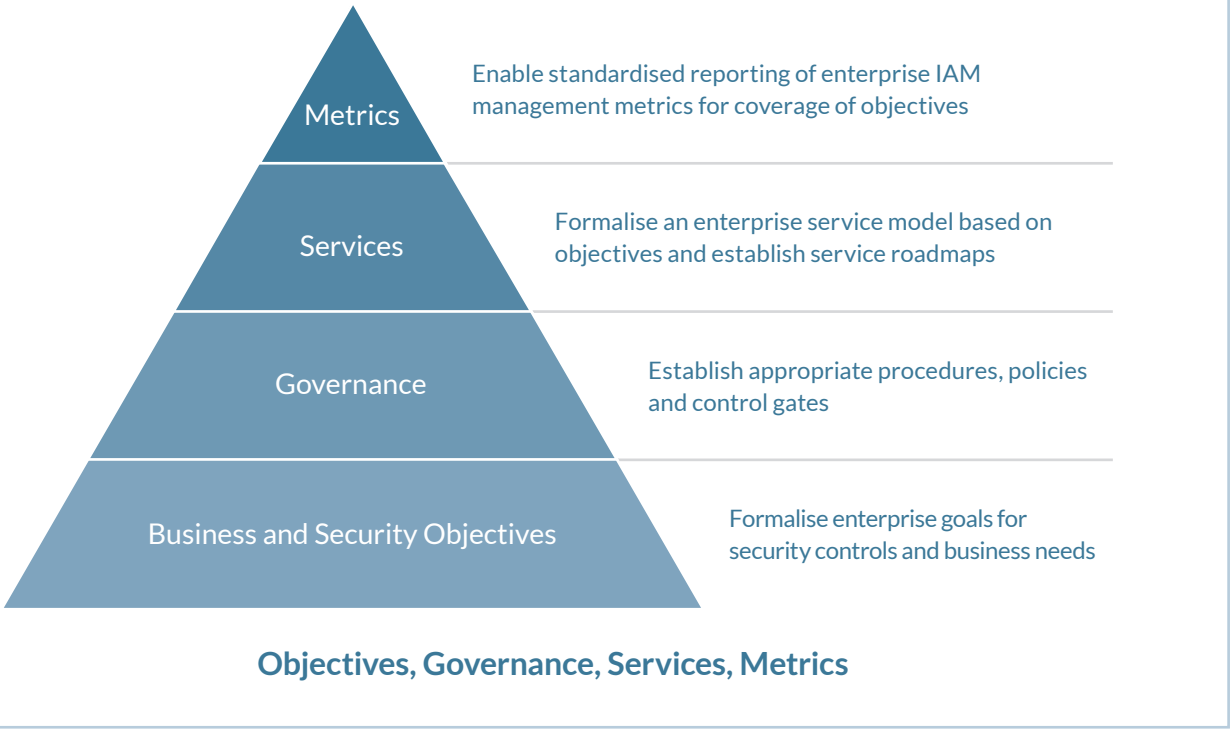
A fundamental mistake for organisations when handling security needs is performing individual, one-off projects to address IAM concerns. Individual projects often lack centralised leadership and provide only temporary solutions to the issue at hand. While a one-off initiative may temporarily close a pointed gap for a specific business area, it may not always align with the enterprise IAM program vision.

A successful organisation treats IAM as an ongoing internal service to the organisation. Setting up an IAM operating model, along with a dedicated internal services team, helps establish IAM as an ongoing service, manage demand from the business and IT, prioritise initiatives, and gauge IAM progress and maturity. An IAM operating model consists of four elements: formalising enterprise goals and control objectives; establishing procedures, policies and control gates to drive governance; formalising an enterprise service model; and standardising reporting of enterprise IAM management metrics.

02 Lack of meaningful metrics

Many organisations lack defined metrics that report on the status and maturity of an IAM environment, such as enterprise service usage and enterprise control objective compliance. Successful IAM programs put focus on common business and security control objectives. The IAM team must work with the business, risk and compliance, and IT teams to define business objectives that will meet the demands of application teams, HR and other business units. Similarly, aligning security control objectives with industry frameworks, such as NIST and ISO, helps define control objectives. (See the first layer of the operating model in Figure 1.)

Figure 1: Protiviti IAM Operating Model



With these enterprise objectives, an IAM program will be able to effectively report on current status, work in progress and what still has to be done. Executive- and board-level utilisation of compliance and coverage metrics will enable better decision-making around investments at tactical and strategic levels and will demonstrate how risk and operational effectiveness are being addressed. Having the ability to measure the progress of IAM initiatives against these objectives is paramount in helping manage the program and deliver services across the organisation to drive risk reduction, regulatory compliance and business efficiencies.

Coverage metrics help show conformance to enterprise goals and compliance progress by risk level. Business-objective coverage metrics serve to show progress toward meeting business needs throughout the organisation, and they tell you which applications are using IAM services and identify gaps in your IAM efficiency. Control-objective coverage metrics, on the other hand, serve to show compliance of applications and systems against IAM control objectives. They tell you which applications are compliant with which control objectives and which risk levels are lagging behind with control compliance.

Performance metrics provide transaction-level reporting to measure efficiency of services and projects. They tell you which IAM services are being used effectively and where improvements can be made to IAM systems or processes.

03 Lack of an IAM roadmap with effective ongoing demand-management practices

Organisations often lack mature roadmaps, creating point-in-time roadmaps but not actively managing or working from them over time. (In other cases, organisations lack a roadmap at all.) A point-in-time roadmap does not accurately reflect ongoing or completed projects, recently adopted technology, or other dependencies. Without a continually updated roadmap, an organisation's IAM team provides limited demand management and reacts to business needs

only as they arise. The lack of demand management leads to IAM investment that is not aligned with true business needs. In order to make the roadmap effective, a demand-management function is needed.

Organisations should look to invest not only in updating a roadmap but also establishing the ongoing demand-management capability to keep the roadmap refreshed over the long term. Managing IAM can be significantly improved with the continual refresh of a mature roadmap that accounts for initiatives in process and governance, enhancements to existing services, and establishment of new services. A roadmap needs to be actively maintained and used to guide initiatives.

Different IAM services should have product managers in place to manage the lifecycle of the service. A product manager is responsible for the management and demand of his or her particular IAM service and managing inputs to the broader IAM roadmap. The manager becomes a key stakeholder involved in maintaining the overall IAM roadmap and works closely with the team delivering IAM services.

04 Insufficient business-analyst involvement in IAM

Organisations often hire technical staff who lack experience in requirements gathering or managing identity services to implement IAM systems. Although technical staff are needed to deploy and maintain the technology, lack of business analysts with IAM teams results in ineffective system deployments that often do not solve the root cause of business needs. Successful IAM programs look to invest in business analysts who work with the business to understand the issue at hand and work alongside technical staff to implement and manage IAM services.

It is important for organisations to have IAM staff who understand how to interface with the business to solicit and document requirements, support testing, and provide education and awareness (training). Good business analysts understand identity and access lifecycles, know how to interface with nontechnical business stakeholders, and work efficiently with the product manager and technical staff.

A business analyst also helps manage the demand pipeline for IAM services and conduct ongoing demand-management activities with business and IT stakeholders. He or she has the ability to understand the needs of applications and identify whether business and security control objectives can be met using existing services, or whether additional investment may be required. The addition of business analyst personnel significantly improves the effectiveness of an IAM program and its ability to provide services to meet business needs.

05 Technology as the primary focus of IAM Investment

Finally, when IAM issues arise, organisations often lean too heavily on implementing technology with the idea that it will solve all issues related to identity and access. This leads to short-term solutions with an incomplete understanding of the real business need and accompanying requirements, and issues often resurface. Organisations investing too heavily in technology often have a limited view on the overall business value of IAM initiatives and thus struggle to realise maximum gains. Successful IAM programs look to focus efforts on the strategy, process and governance of an IAM program first, then tackle technology with all the right requirements in place.

Effective process and governance helps remediate elements outside of technology, such as organisational structure, risk management, and standard procedures and processes. Complying with existing IAM standards, such as managing privileged accounts through an enterprise IAM tool, can be enforced without the use of technology by utilising existing enterprise gates, like change management processes, release management or a system development lifecycle. Root problems often lie within the process and governance in place (or the lack thereof), which make up organisations' IAM. Increasing the focus on establishing IAM methodologies and governance frameworks, reengineering processes, improving standards, and employing playbooks will have long-term benefits to organisations.

SailPoint Case Study: Centralising Identity for a Secure Future

Hear from one of the enterprise-class identity governance customers that have used SailPoint to meet their identity governance and administration needs.

Western Union, a staple of the American economy for over 165 years, needed a full-scale IAM platform to scale with their business and secure access to their enterprise's applications.

CHALLENGE

After Western Union had been through 5 years of IAM and not finding a solution that could scale to their needs and become the fully-fledged platform they required, they were on the hunt yet again for a new solution.

SOLUTION

With SailPoint IdentityIQ, Western Union was able to gain full visibility and control of all user access to all their mission-critical applications (with more on the way), while saving both time and money.

For over 165 years, Western Union has been a staple of the American economy. With a long history of innovation, they transitioned from a telecommunications giant, delivering telegrams across the country, into the money transfer leader we know today. With the advancement of technology, new challenges have arisen that required Western Union to change and adapt, and identity governance has been one of those challenges. Before SailPoint, anyway. Identity and access management (IAM) had been present at Western Union for seven years, but they faced multiple challenges with their previous vendors. Like many others, when Sun Identity Manager was sunsetted, the corporation was forced to find a new solution. They settled on a combination of four vendors to provide the full scope of functionality required.

When Mark Routh, Senior Manager of IDM Operations joined Western Union, he found that the four products they were using to solve their IAM needs were not cost-effective, and not providing the integrated functionality that Western Union needed in their IDM solution. While SailPoint was already implemented to address Western Union's compliance needs, they opted to migrate, deploying IdentityIQ as the sole identity governance solution for the enterprise.

Staying On-Schedule

For a corporation as large as Western Union, time – and capability – is of the essence. They needed to implement and then migrate hundreds of applications, within one year of the initial project date, and SailPoint delivered.

By the end of the first six months, Western Union had deployed IdentityIQ and successfully migrated 81 applications from the old system for their 20,000+ users. By the end of the first year, they expect to have a remarkable 600+ applications integrated.

Six Big Ideas For an Identity Management Clean Up

Mark Oldroyd, Partner Technical Enablement Manager, SailPoint Europe looks at what you should be doing to keep your house in order:

The number of tasks seems never-ending. Summer is not the time of year one often thinks about cleaning around the dusty corners of their identity and access management program. But it's a perfect time. As enterprises move forward, managing their IT, and deploying new technology, how they manage their identities and associated privileges collects cobwebs and technical debt.

It has to be cleaned-up sometime.

There's aging identity management technology stack, existing antiquated workflows, directories that have become a little musty, and identity policies may not be as aligned with to match new regulations. You get the idea: there's never any end to the work that needs to be done. And if it's not done, it just becomes more challenging to do over time.

What should be done? That, of course, will vary from business to business; however, based on recent conversations with identity management executives, I've created a list of common challenges that could serve as starter ideas.

01 Streamline processes

Unless you have already been through the exercise of normalising identity and access management processes across departments, the chances are that each business unit is doing its own thing. They have their own access approval processes, they probably have customised tools, and they likely even have their own names and language when it comes to identity. This works until it doesn't. And the moment the organisation goes to standardise on an enterprise-wide approach, these variations make that a grueling endeavour.

Take a look at the tools and processes in use across the organisation and look for ways to standardise where possible.

02 Automate manual tasks

The chances are high that many of your identity-related approval workflows are managed manually. And identity-related information is likely stored within spreadsheets, and information gathering is conducted through email. Lots and lots of emails. Many of these processes were set up for a good reason. They protect the organisation from granting employees too much access, or they help to maintain compliance with industry regulation.

Of course, these processes are necessary and designed to help protect the organisation — and some processes absolutely always need a human review — many of these processes, however, can be safely automated. An employee requesting access to data that isn't sensitive or regulated may be able to be granted access automatically, just as a new hire can be given access to an established set of applications or services. Increasingly, with the use of AI-driven identity, you can be made aware of low-risk activities that can be safely automated so your staff can focus on more strategic and/or high risk issues that require greater human attention.

03 Rogue bots

The use of enterprise bots is on the rise. According to Forrester Research, the Robotic Process Automation (RPA) market will reach $2.9 billion by the end of 2021. Enterprises are investing in bots to streamline normal manual processes and, increasingly, make low-risk decisions.

Some enterprises are already well underway to formally securing and governing their bots. Those who don't will realise that they have a complex matrix of service accounts that have been established to manage system and service settings, and now that they are automating many of those processes there is a substantial rise in risk. The best way to manage and audit that risk is through identity governance of these bots — but the work needs to start early to be manageable.

04 Get control of non-payroll accounts

Many companies have a firm handle on the identities of those on their payroll. They have likely integrated their HR software with an identity management system, and the identity lifecycle is managed thoroughly for these users. Where many companies are falling short is with their non-payroll accounts. These are the consultants, interns, partners, and others who visit and use the corporate network.

Take a look at how you are managing non-payroll accounts and see if there are ways to clean and streamline there.

05 Orphaned accounts

To this day, orphaned enterprise identities remain one of the most common areas organisations need clean-up. This includes accounts that remain active long after employees leave the organisation or when job changes occur and privileges are not updated accordingly, giving a person more access than they really need to do their job successfully. All of this increases the organisation's attack surface.

Now is the perfect time to dive into the identity environment and weed out unnecessary accounts and privileges.

06 Take an honest assessment of weaknesses in your identity program

Every organisation has a different situation and will need to work on different things when it comes to their identity management late spring cleaning. So, take an assessment of areas where identity management debt exists, such as manual processes that can be automated, or where teams are struggling with outdated identity software and services. Or, perhaps there are classes of users where identities are not being managed as thoroughly as they should. Whatever it is, there are likely several areas that need attention.

Of course, whatever you choose to tackle in identity 'spring cleaning' list, everything doesn't have to be completed all in one year. But if you manage to knock items off the list each year, you'll find the program gets better — and easier to manage.

Why Protiviti and SailPoint: Partners in Identity Access Management and Identity Governance & Administration

Protiviti's Mission: Deliver Confidence in a Dynamic World

Protiviti UK forms part of a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Our consulting solutions span critical business problems in technology, business process, analytics, risk, compliance, transactions and internal audit

As an organisation, we believe that by teaming together, with each other, and our clients, we can see beyond the surface of changes and problems organisations face in this fast changing world to discover opportunities others might miss and face the future with greater confidence.

Our more than 4,500 experts serve clients through the network of Protiviti and independently owned Member Firms in more than 80 offices in over 20 countries, including seven offices in the UK. We have served over 60% of FORTUNE 1000® companies and 35% of FORTUNE Global 500® companies.

Roland Carandang
Managing Director, Technology & consulting
Protiviti UK

Roland has assisted a wide range of companies, from start-ups to regional and global industry leaders in establishing and refining their information security management systems and delivering the overall information security programme and high profile projects. Roland has built a foundation of advanced technical skills in security assessments, configuration reviews and technical audits across a broad range of technology architectures in several large and complex environments. In addition to leading large client accounts, Roland manages the UK vendor relationships with SailPoint and is a recognised leader in cyber security, IAM and PAM offerings.

Protiviti.co.uk

Focused on Identity. Driven by Integrity.

As one of the market leaders with 1000+ global customers, SailPoint works with select partners to provide innovative solutions to business problems and an exciting, collaborative work environment for identity rock stars. Together, we're redefining identity's place in the security ecosystem.

We love taking on new challenges that seem daunting to others. We hold ourselves to the highest standards, and deliver upon our promises to our customers. We bring out the best in each other, and we're having a lot of fun along the way.

Mark Oldroyd
Partner Technical Enablement Manager,
SailPoint Europe

Mark Oldroyd is SailPoint's Partner Technical Enablement lead in Europe and is responsible for all technical pre-sales education and solution training across SailPoint's extensive partner community. Mark has worked in both partner-facing and direct sales engineering roles, so has wide experience of the challenges in both arenas. In addition to managing training programmes, Mark is a technology leader and evangelist, speaking at a wide range of both partner and industry events. Mark has worked with many leading technology vendors and solution providers, and now ensures the delivery of SailPoint's world-class technical services to some of the largest strategic integrators and partners in Europe.

SailPoint.com

THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*
Buenos Aires

BRAZIL*
Rio de Janeiro
Sao Paulo

CANADA
Kitchener-Waterloo
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE & MIDDLE EAST

FRANCE
Paris

GERMANY
Frankfurt
Munich

ITALY
Milan
Rome
Turin

NETHERLANDS
Amsterdam

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
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®