protiviti®

Face the Future with Confidence

SAP Access Management Governance

Getting It Right, Making It Sustainable

Internal Audit, Risk, Business & Technology Consulting

Introduction

Application security, especially in enterprise resource planning (ERP) systems such as SAP, tends to be complex and fragmented across organizational silos. Because of the lack of ownership and knowledge of associated technologies, security controls are often inconsistent and manually enforced. This complexity increases with the introduction of HANA and Fiori functionality as part of an S/4HANA deployment.

Lack of consistent application security results in increased and unnecessary exposure to many risks, including, but not limited to, internal fraud, data breaches, loss of intellectual property, damage to brand reputation, and compliance violations.

According to the Privacy Rights Clearinghouse, improper access has been a factor in more than 300 data breach incidents in the past five years.[1] And at one leading financial institution, a former vice president in the internal finance department allegedly used his excessive access rights to embezzle more than US$19 million; he was able to quietly transfer the funds between several corporate accounts and his personal account at another financial institution.

Decentralized efforts to assign access, reset passwords and update roles in ERP systems are typically redundant, wasteful and inefficient. This white paper outlines a strategy to improve SAP access management efficiently and establish a structure for governance that standardizes the management process and helps minimize access control risks for the long term. The suggested approach can yield many benefits, including:

- Reducing unauthorized access and fraud across the enterprise
- Limiting the risk that departing employees pose
- Reducing time lost when employee access is changed
- Increasing efficiency of security and provisioning audits
- Streamlining the day-to-day management of access
- Increasing stakeholder confidence
- Motivating compliant conduct in access management

[1] A search of the data breach database at Privacyrights.org, filtered to identify unintended and insider data breaches between 2007 and 2013, and further filtered using "access" as a keyword, returned more than 300 incidents.

1. Getting It Right

The fundamental purpose of SAP access management is to establish an effective segregation of duties (SoD) framework; ensure minimal but appropriate access approvals; and minimize risks related to granting, changing and removing access. To accomplish all of the above, effective organizations often take the following steps:

Design a Foundational SoD Ruleset

Organizations need to define and agree on key business risks and build an SoD ruleset that aligns those risks to associated SAP transactions/authorizations. Some SAP transactions do not need to be combined to pose risk. These stand-alone transactions are defined as sensitive access; these assignments should be restricted and in some cases monitored. These concepts are important, since monitoring for SoD and sensitive access risks is the foundation for role design, role assignments, and risk approval decisions. Definitions of risk level (i.e., high, medium or low) should be agreed upon to understand priority. Also required is a change management process that can be used to maintain the ruleset as business risks, regulations and the organization evolve.

For Users of SAP® S/4HANA Systems

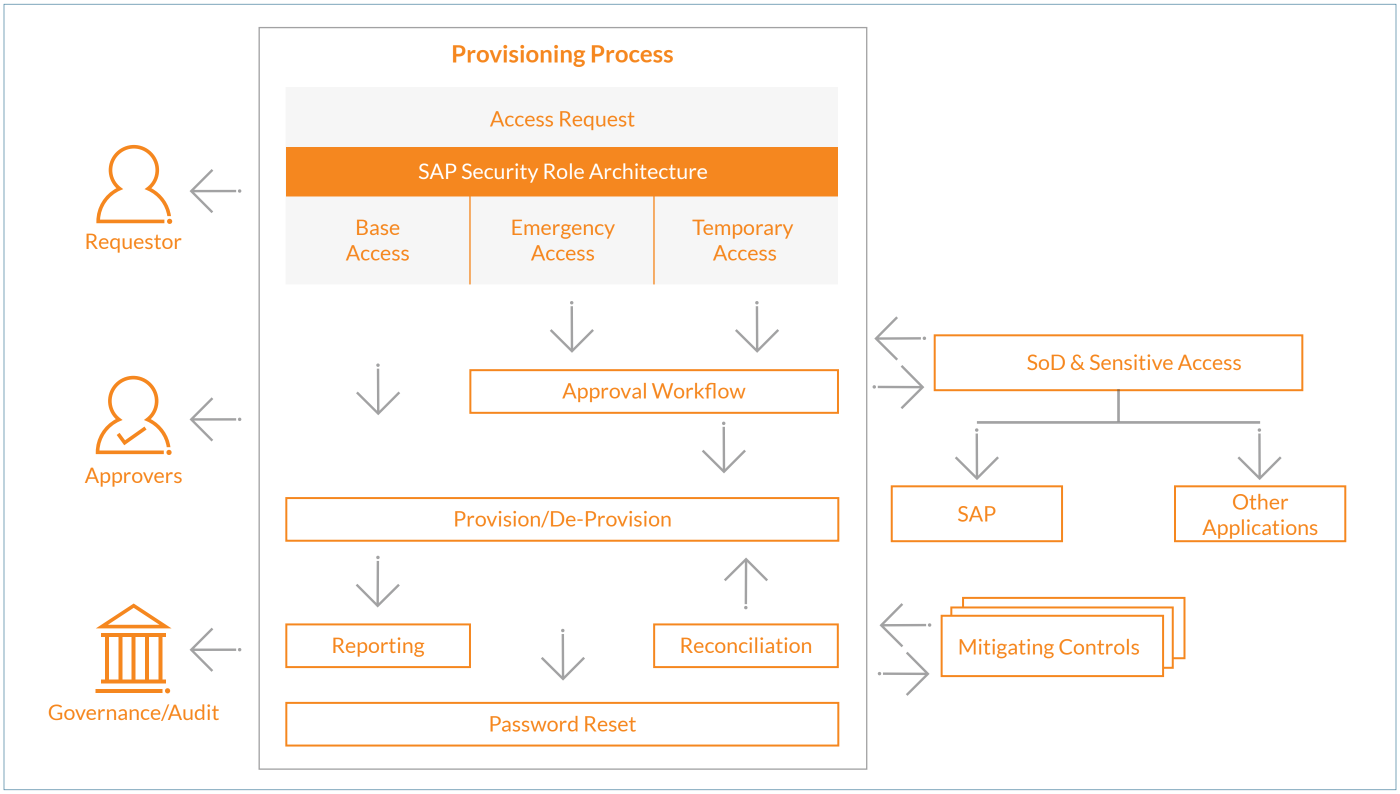
With the introduction of SAP® S/4HANA, the SoD ruleset will have to be reassessed to incorporate changes due to the introduction of new security layers, including over 200 new transactions, and the consolidation/replacement of old transactions and checks (e.g., Simplified Finance & Logistics and Business Partner). Omitting new transactions from the SoD ruleset can drastically reduce its effectiveness in mitigating risks. Overlooking the security updates also could result in inaccurate SoD reports as many real risks may not appear.

Additionally, security at the new presentation layer (SAP Fiori) and database layer (SAP HANA®) may also have to be taken into account when designing the new ruleset.

Create a Centralized and Automated Provisioning Process

Centralizing and automating the provisioning process as much as possible leads to greater efficiency and control (see Figure 1). Most governance leaders choose to deploy a standard access management solution, such as SAP Access Control, which can be complemented with an identity management tool, like SAP NetWeaver Identity Management, to automate user access management tasks and deliver visibility across the enterprise. These tools can help ensure required approvals are consistently and efficiently obtained during the provisioning process, test security changes for potential SoD violations prior to granting access, and apply mitigating controls prior to moving the change into the production environment. In addition, these tools can allow for significant gains in efficiency by automating the creation of users and the associated access once all approvals have been obtained.

Figure 1. Key Elements in the Security Provisioning Process



For Users of SAP® S/4HANA Systems

The SAP Access Control functionality will have to be expanded across the S/4HANA landscape to address the access risks arising with the introduction of new security layers. Changes may need to be made at both the system architecture level (configuring additional connectors) and the Access Control tool functionality level (workflow changes) if users are provided access to Fiori and the HANA database.

Implement an Appropriate SAP Security Role Architecture

The organization's role architecture should be designed to reduce access risks, but also flexible enough to support business objectives (e.g., company growth, mergers and consolidations). A well-designed architecture can help support an efficient provisioning process and assist in the removal of SoD violations from the system.

When defining a security architecture, consider how to balance business priorities, such as the need for flexibility and control, and keep in mind the importance of minimizing the number of security roles to keep maintenance efforts to a minimum. Involving business owners in the design and ownership of roles will help ensure the roles truly reflect business functions and will be sustainable in the longer term.

To help design and keep roles free of SoD conflicts over time, many companies use a security and compliance solution such as SAP Access Control, which can automate the periodic review of users, identify risks within roles before granting access to productive systems, and streamline associated audits and reporting of security risks. It is also important to consider the naming conventions and role groupings. These need to be intuitive not only to IT security experts, but also to business approvers and reviewers.

For Users of SAP® S/4HANA Systems

Security for S/4HANA may encompass security at three layers — database, application and interface:

- With a privilege-based access, authorization at the database level will have to be restricted to technical users (NetWeaver users, developers, data modelers), end users of Fiori, and Business Warehouse clients leveraging HANA's Extended Application Services (XS) engine.
- At the application layer, a universal four-tier approach will help to ensure users get access in a structured way in the ABAP-based system to minimize the potential for risk and excessive access.
- If using Fiori, the ABAP-based roles will have to be mapped to the appropriate groups/catalogs to provide the required application access on Fiori UX.

Control the Use of Emergency Access

It is often necessary to grant temporary SAP access to an employee when an unexpected issue needs immediate resolution; staff resources are limited; or an SoD issue must be mitigated. It is therefore important to have a formal process in place for granting emergency access. The process can be designed to streamline temporary requests, but still minimize risk. There are a number of effective tools available that include emergency access control functionality. The key to controlling emergency access is to ensure logs generated are reviewed by an appropriate person in a timely fashion. Excessive use of emergency access can be a significant risk in itself, so strict governance is needed.

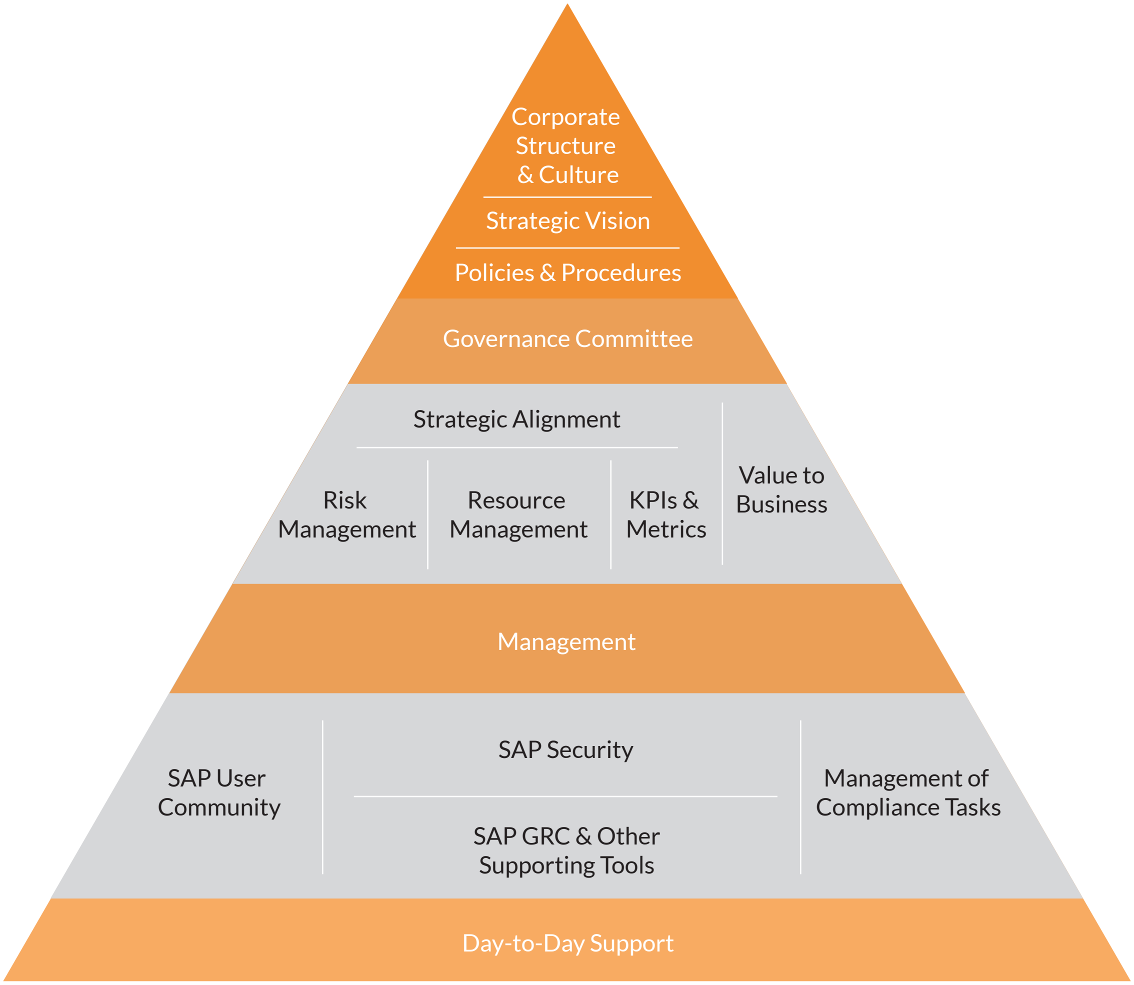
Automate and Secure Password Resets

The first layer of SAP security is the requirement for a user ID and password. So, it is critical to implement standards that help ensure passwords are strong, such as requiring a minimum password length, use of special characters, and use of both lowercase and uppercase letters, and restricting the ability to repeat previous passwords. Deploying a self-service password reset tool that allows users to reset their own passwords and maintains password strength is one approach, as opposed to resetting passwords manually and providing the same initial password to all users. These solutions help ensure standards are in place, passwords are unique, and manual intervention is minimized. A robust tool will enable users to create customizable security questions that are difficult to crack. When passwords are reset, random passwords are emailed directly to the user, minimizing risk. There are a number of password reset products to reduce operational costs and get users back up and running in SAP quickly. The SAP Access Control solution includes Password Self Service functionality.

2. Making It Sustainable

What kind of governance structure and processes can help ensure SAP security will be maintained for the long term? An effective program has several core pillars, as shown in Figure 2.

• • • Figure 2. SAP Access Management Organizational Pillars



The first step to building a sustainable SAP security environment is to develop a strategic vision for access management that aligns with business requirements and risk tolerance. This will enable security to be addressed in an organized, efficient and proactive way, while minimizing exposure to major access management risks.

Organizations also need to identify policies that make access management standards clear, as well as procedures to enforce those standards. It is necessary to check periodically that policies are relevant, understood and followed. This can be accomplished through a policy and procedure survey, which can be automated with a solution such as SAP Process Control.

Key performance indicators (KPIs) and metrics that enable the governance committee to manage the governance process also must be established. Examples include statistics on user SoD violations, role SoD violations, provisioning of service-level agreements (SLAs), and remediation tracking. A few KPIs are:

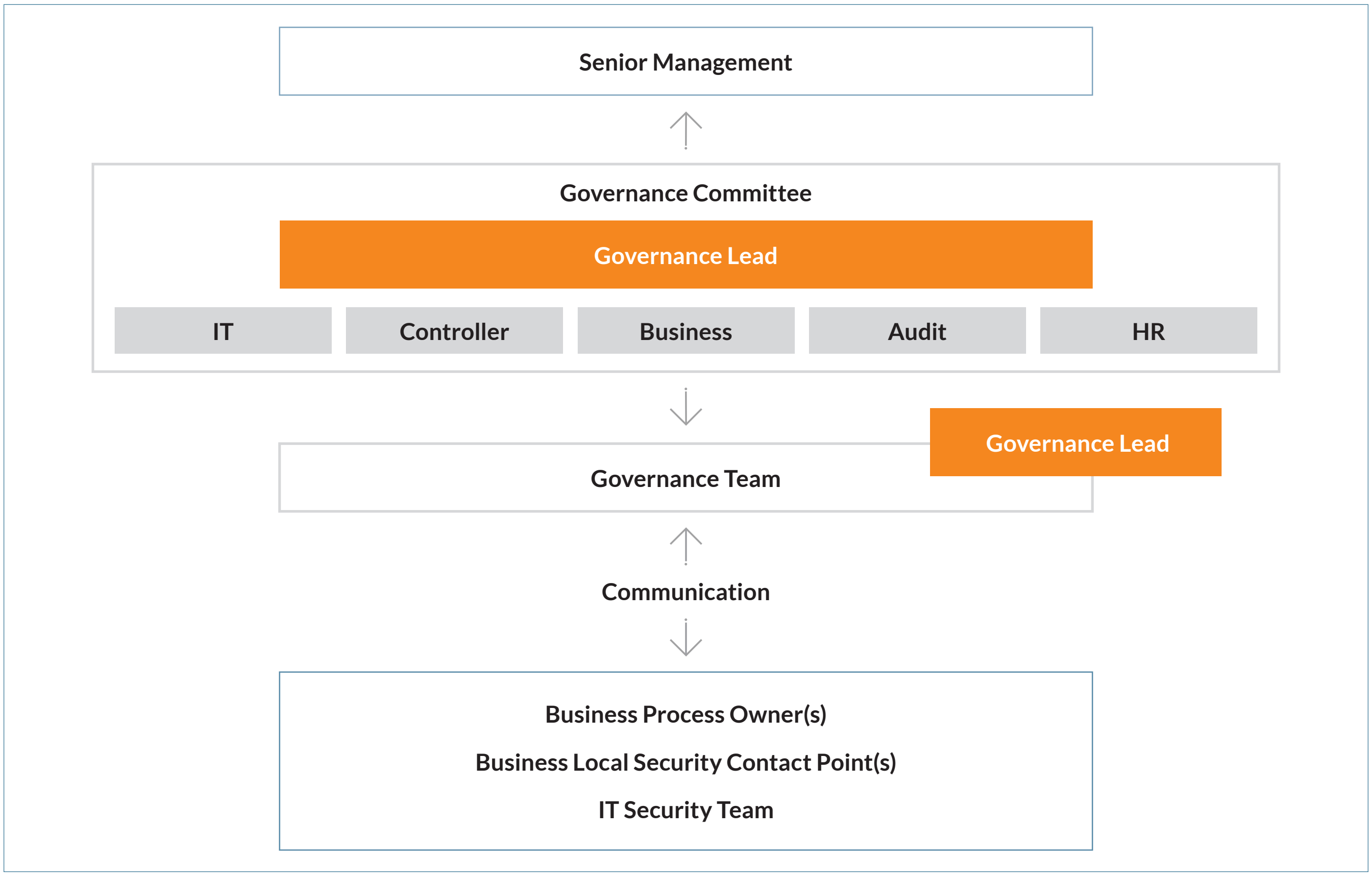
Managing users	• How many users have high/critical SoD violations? • How does this compare from period to period? • What is the average timeline to create, change and remove access requests?
Managing roles	• How many roles have SoD violations built into them? • How many roles have not been assigned to users? • How many duplicate transaction codes are between roles?
Managing emergency access	• How many firefighter and user accounts exist by functional area? • How often are firefighter accounts being used? • Are firefighter logs being reviewed in a timely manner, and are issues addressed appropriately?
Access provisioning	• What access requests are still pending? • What is the average length of time that access requests remain open? • What are the most frequently requested roles?

In addition to the steps outlined above, it is essential to work with business process owners (BPOs) and secure their buy-in throughout the development of the governance process. This helps ensure the governance initiative will add value to the business.

Furthermore, periodic self-reviews of the governance process will ensure it continues to accomplish the core objectives. For example, in addition to monitoring the KPIs above for unexpected anomalies or trending to evaluate the efficiency of performance, there should be a periodic review of each area to evaluate quality of performance (e.g., reviewing a sample of management waivers for SoD risks to determine whether the issue is properly considered and mitigating actions are being taken). Another consideration is whether the reasons for emergency access checkouts are consistent with approved use (or whether elevated access is being abused).

What kind of organizational structure is optimal for the long-term success of access management controls? As shown in Figure 3 on the next page, at its center is a governance lead: a subject-matter expert who reports to executive management. This person drives the day-to-day tasks for access management, coordinates policy changes, and is the primary contact for the business. The governance lead also coordinates the governance committee, which consists of stakeholders from the various organizations, such as information systems (IS), finance, internal audit and the BPOs.

Figure 3. SAP Access Management Governance Organization



The governance team designs, implements and executes controls. It also owns the description of roles and responsibilities. Information from the governance team is communicated to the user community and supported through access management single points of contact within the business and associated BPOs.

For Users of SAP® S/4HANA Systems

With the move to S/4HANA, there may be significant changes in processes resulting from the simplification of the data model, creating a need to assess whether risks are being mitigated effectively and identify new controls. A review of all mitigating controls is recommended to ensure relevancy and accuracy following the changes in processes.

The Potential Rewards of Effective Access Governance and Controls

A sustainable access management governance program requires a strong foundation, including a robust SoD framework, a centralized and automated provisioning process, the right SAP security role architecture that fits current and future organizational needs, controlled and monitored emergency access, and automated password resets. Ongoing input and commitment from all stakeholders involved, such as business users, IT, internal audit and BPOs, are also essential. But once the groundwork is done and a successful program is in place, an organization can realize many benefits, such as:

- Streamlined, enterprisewide processes for managing access that result in cost savings from:
  - Fewer help desk tickets for password resets
  - Little or no staff involvement in the creation, update and removal of access
- Formalized risk management processes that identify high-risk exposures and mitigate them
- Better business results, because controls are driven more by business than by governance needs
- Greater efficiencies and cost savings due to effectively defined SAP security roles
- Enhanced protection of corporate data and assets
- Simplified compliance, improved governance and easier auditing

Access control violations are inevitable. However, with an efficient and effective access management program that includes the foundational elements to get SAP security right, and the correct structure to make processes sustainable, a company's ability to minimize, monitor and mitigate access control risks will be greatly enhanced, even as the organization changes and grows.

ABOUT PROTIVITI

Protiviti 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 independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work 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.

About Protiviti's Enterprise Resource Planning and SAP Technology Practice

We partner with chief information officers, chief financial officers and other executives to ensure their organizations maximize the return on information systems investments while minimizing their risks. Using strong IT governance to ensure alignment with business strategies, we drive excellence though the IT infrastructure and into the supporting applications, data analytics and security. We also facilitate the selection and development of software, implement configurable controls on large ERP installations, implement GRC software applications, and manage implementation risk throughout.

Protiviti is a premier provider of SAP consulting solutions and a long-standing SAP Gold partner. Given our risk and compliance background, we are in a unique position to help companies identify, address and mitigate risks around S/4HANA projects. We bring:

- Optimized S/4HANA business process templates and experienced resources to facilitate your solution design
- Automated tools to assess application security, automated controls and data risks
- Pre-defined library of process and IT controls to consider as part of your S/4HANA solution design
- Expertise in GRC solution implementation related to S/4HANA's impact on SoD rules and automated controls
- Proven methodology and approach to assess project readiness and risks throughout your implementation lifecycle

Contacts

John Harrison
+1.713.314.4996
john.harrison@protiviti.com

Carol Raimo
+1.212.603.8371
carol.raimo@protiviti.com

Aric Quinones
+1.404.240.8376
aric.quinones@protiviti.com

Thomas Luick
+1.312.476.6342
thomas.luick@protiviti.com

Ronan O'Shea
+1.415.402.3639
ronan.oshea@protiviti.com

Steve Cabello
+1.213.327.1470
steve.cabello@protiviti.com

Siamak Razmazma
+1.408.808.3258
siamak.razmazma@protiviti.com

John Livingood
+1.415.402.3682
john.livingood@protiviti.com

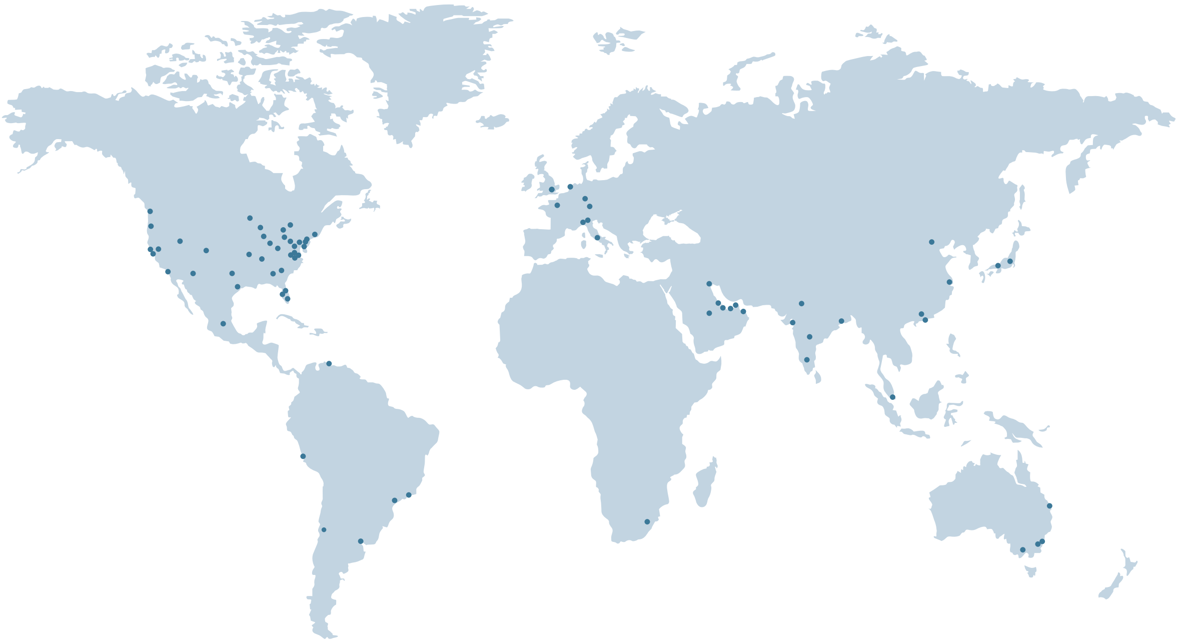
Toni Lastella
+1.212.399.8602
toni.lastella@protiviti.com

Martin Nash
+1.813.348.3374
martin.nash@protiviti.com

Kevin Erlandson
+1.415.402.3682
kevin.erlandson@protiviti.com

Mithilesh Kotwal
+1.312.364.4912
mithilesh.kotwal@protiviti.com

Kyle Wechsler
+1.212.708.6369
kyle.wechsler@protiviti.com



THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Fort Lauderdale
Houston
Indianapolis
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

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE MIDDLE EAST AFRICA

FRANCE
Paris

GERMANY
Frankfurt
Munich

ITALY
Milan
Rome
Turin

NETHERLANDS
Amsterdam

UNITED KINGDOM
London

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

SOUTH AFRICA*
Johannesburg

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

ASIA-PACIFIC

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

INDIA*
Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

*MEMBER FIRM

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.