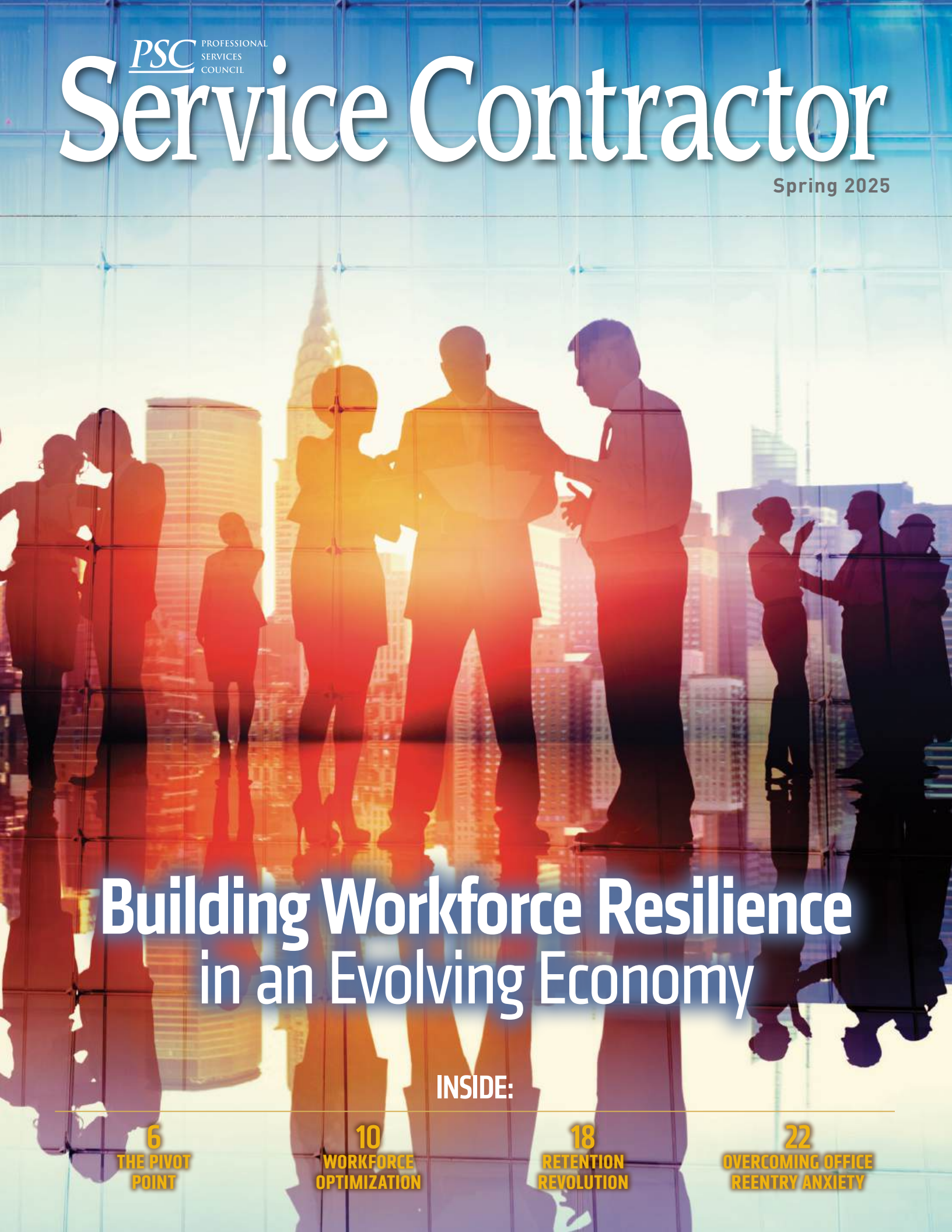
PSC PROFESSIONAL SERVICES COUNCIL

Service Contractor

Spring 2025



Building Workforce Resilience in an Evolving Economy

INSIDE:

Modernizing Federal IT with Zero Trust and Application Portfolio Management

by David E. Crawford, CISSP, PMP

Director, CGI Federal

Federal agencies implementing zero trust frameworks must grapple with a broad range of factors that can influence plans and initiatives. Your application portfolio is a significant aspect of successfully implementing zero trust, and many agencies are at the starting line for analyzing and rationalizing applications.

Application workload is one of the five pillars of zero trust. Applications proliferate so rapidly across organizations that getting a full picture of your application ecosystem is rarely simple. Still, for success with zero trust, it's essential to do so.

A Quick Refresher

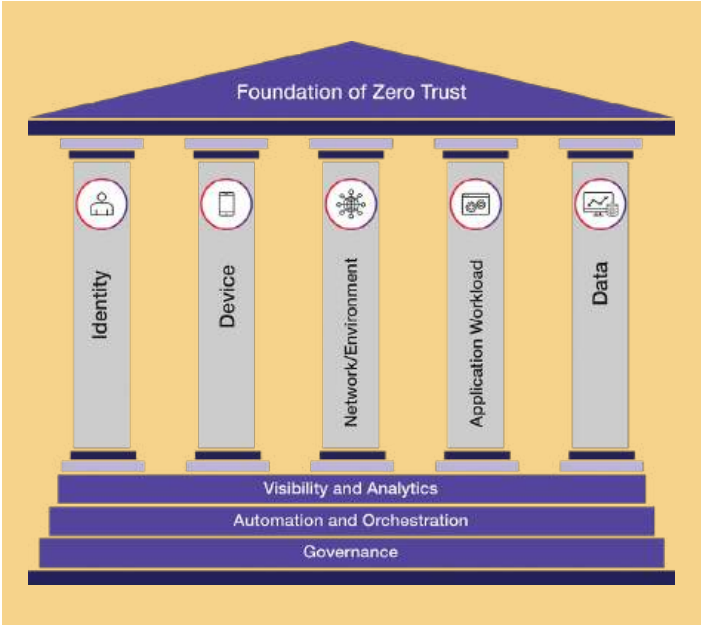
Zero trust provides the foundation for powerful cybersecurity, and any organization with critical assets should consider implementing it. Built on the premise that threats can originate from both outside and within the network, zero trust demands stringent verification measures for every individual and device seeking access to a given asset or resource.

As its name implies, zero trust is a framework to enhance security by granting the least amount of access possible to critical systems and data. Implemented correctly, it ensures that only authorized individuals or systems have access to specific assets—and only to those they truly need.

How Zero Trust and IT Modernization Intersect

An IT modernization initiative often provides an opportunity to implement a zero trust framework. Zero trust reinforces many of the goals of modernization, and the necessary business process reengineering and organizational change management that come with modernization can ease the transition to new security practices.

The goals of IT modernization typically include improving efficiency, agility, scalability, and reducing costs, enhancing security and enabling digital transformation. Zero trust provides a robust security framework that supports these goals.



Application Portfolio Rationalization

Identifying and removing duplicative, outdated or unused applications reduces the organization's potential attack surface while increasing efficiency and reducing software costs.

Evaluate each application in your ecosystem using qualitative data and metrics. Consider the entire lifecycle of each application, from development to retirement. Where possible, leverage investments in existing technologies such as Application Discovery and Dependency Mapping (ADDM), and Application Portfolio Management (APM) solutions. At the end of the analysis, you should have each application categorized as retain, retire, replace or consolidate.

To begin the rationalization process, consider these steps:

Understand there is no defined end state for zero trust—you never truly reach a final destination. It is an information security model that organizations must continuously refine and adapt as new technologies emerge.

1. Catalog Applications:
- **Inventory:** Include details such as application name, functionality, users, and associated costs (licensing, maintenance, etc.).
- **Ownership:** Identify and document both the business owner and the technical owner for each application.

2. Assess Usage and Performance:
- **Metrics Analysis:** Collect usage metrics to determine which applications are widely used and which are underutilized.
- **Performance Evaluation:** Assess the technical performance of each application, including response time, reliability and scalability.

3. Categorize Applications:
- **Platform Dependency:** Categorize applications based on their platforms, such as legacy systems, cloud-based solutions, or hybrid environments.
- **Compatibility:** Identify applications that are incompatible with the current or future IT environment.

4. Identify Redundancies and Duplicates:
- **Duplicative Applications:** Identify applications that perform similar functions and determine whether all are necessary.
- **Nested Applications:** Be alert to applications embedded within larger systems that may not be immediately visible.

5. Evaluate Business Value:
- **Business Impact:** Consider each application's contribution to business outcomes, customer satisfaction and strategic goals.
- **Total Cost of Ownership (TCO):** Calculate each application's TCO, including direct and indirect costs.

6. Research and Plan for Modernization:
- **Legacy Replacement:** Research suitable replacements or modernization options for legacy applications.
- **Modernization Roadmap:** Develop a roadmap to modernize the application portfolio, prioritizing high-impact applications.

7. Identity and Access Management (IAM) Analysis:
- **Current State Assessment:** Evaluate the IAM capabilities of each application, focusing on legacy systems that may have outdated or insufficient IAM controls.
- **Compliance and Security:** Ensure IAM practices meet modern security standards and compliance requirements, such as multi-factor authentication, single sign-on and role-based access control.
- **Integration Challenges:** Identify legacy applications that lack support for modern security solutions and plan for necessary upgrades or replacements.

Appreciating the Big Picture

Understand there is no defined end state for zero trust—you never truly reach a final destination. It is an information security model that organizations must continuously refine and adapt as new technologies emerge.

Application rationalization, as a subset of the larger zero trust paradigm, is also an ongoing effort. With every new application introduced, existing applications may become outdated or redundant. Managing application proliferation is an ongoing challenge, but it is essential to ensure your zero trust framework remains effective.

Zero trust is a critical component of IT modernization efforts, and its creator, John Kindervag, emphasizes that it is intended to be simple. However, as straightforward as it can be, it does require care and attention to detail.

A well-structured approach to all zero trust pillars will lead to a more successful implementation, allowing you to expand and refine your strategy as your organization evolves. For more insight into zero trust, visit Federal zero trust | CGI United States.[1] ■

[1] https://www.cgi.com/us/en-us/federal/cybersecurity/zero-trust