Public Sector — Microsoft 365 & Azure Managed Service, Addressing Limited Budgets and Staffing Constraints

KPCS Consulting Case Study

Executive Summary:

The public sector often faces limited budgets and a lack of IT capacity. KPCS Consulting therefore implemented a managed Microsoft 365 and Azure service for a Central European industrial company, enabling stable, secure, and predictable operations without the need for extensive internal IT resources.

By shifting from ad-hoc administration to a structured operational model with continuous monitoring, configuration management, and enforcement of security policies, the client gained a unified management system, standardized endpoint and cloud operations. This solution allows the client to focus on core business while increasing both the security and efficiency of IT operations.

Key Delivered Outcomes:

- **45% reduction** in IT workload
- **60% faster** incident **resolution**
- **40% fewer** security **incidents**
- **35% stronger** security **control coverage**
- **30% fewer user disruptions**
- **Lower operational costs and risk exposure**

1. Client Overview

The client is a Central European industrial services company that streamlines technical sourcing for manufacturers. It coordinates end-to-end delivery of machined components, welded structures, sheet-metal parts, and assembled units, acting as a single accountable partner across multiple technologies and suppliers. The company places strong emphasis on quality, delivery reliability, and logistics, supporting stable availability, controlled supply chains, and reduced internal workload for its customers.

2. Project Overview

KPCS delivered a managed service for Microsoft 365 and Azure to ensure stable, secure, and predictable daily operations without requiring significant internal IT resources. The engagement shifted the customer from ad-hoc administration to a structured operating model with continuous monitoring, configuration governance, and security enforcement.

Scope included:

- Initial onboarding and configuration of Microsoft 365 and Azure services
- Continuous operations and user/device support with defined SLAs
- Security governance (MFA, Conditional Access, identity management, endpoint policies)
- Incident response handling and standardized runbooks
- Regular reporting, reviews, and proactive recommendations

3. Risks & Impacts Before KPCS Involvement

Without a managed operating model, the customer faced several challenges:

- Higher exposure to phishing, account compromise, and unauthorized access
- Slow detection and response due to lack of monitoring and structured processes
- Inconsistent endpoint posture leading to device drift and operational instability
- Growing internal workload tied to manual administration and repeated issues
- Rising "hidden costs" caused by downtime, firefighting, and ad-hoc external support

4. Unique Aspects of the Solution

KPCS delivered a unified operating model connecting security governance, endpoint standardization, and cloud operations under one service. The solution created a continuous control loop—policy, operations, and improvement—so the customer's cloud environment evolves safely and predictably instead of reacting to issues as they arise.

Key differentiators:

- Proactive governance loop (monitoring, risk review, configuration updates)
- Unified security + operations (access policies integrated with day-to-day support)
- Standardized endpoint management at scale
- Structured processes that reduce reliance on internal administration

5. Business Benefits

- **45% reduction in IT workload** — equivalent to reclaiming 700+ hours annually
  - Standardized processes, device governance, and reduced ad-hoc troubleshooting significantly lowered operational overhead.
- **60% faster incident resolution**
  - Single point of contact, monitoring, and predefined runbooks accelerated response and recovery.
- **40% fewer security incidents**
  - Consistent enforcement of MFA, Conditional Access, and device compliance reduced account compromise, phishing impact, and unpatched vulnerabilities.
- **35% stronger security control coverage**
  - Improved baseline adherence across MFA, update compliance, and governed access policies.
- **30% fewer user disruptions**
  - A standardized endpoint posture stabilized day-to-day operations and reduced escalations.
- **Lower operational costs and risk exposure**
  - Less firefighting, fewer outages, and reduced reliance on last-minute external support.

6. Year

2024

7. Next Steps & Contact

KPCS helps global healthcare organizations modernize digital processes, eliminate manual workloads, and unlock AI-driven efficiency.

Contact: info@kpcs-consulting.com | +1 305 307 4462
Website: www.kpcs-consulting.com