AICPA & CIMA

Private Companies Practice Section

IT set–up and security when outsourcing or offshoring

We highly recommend consulting with your IT Provider or Managed Service Provider to ensure your systems are set up correctly. The following information is for informative purposes only and your trusted IT professional should be contacted to ensure a secure connection is set up between you and an outsourcing vendor.

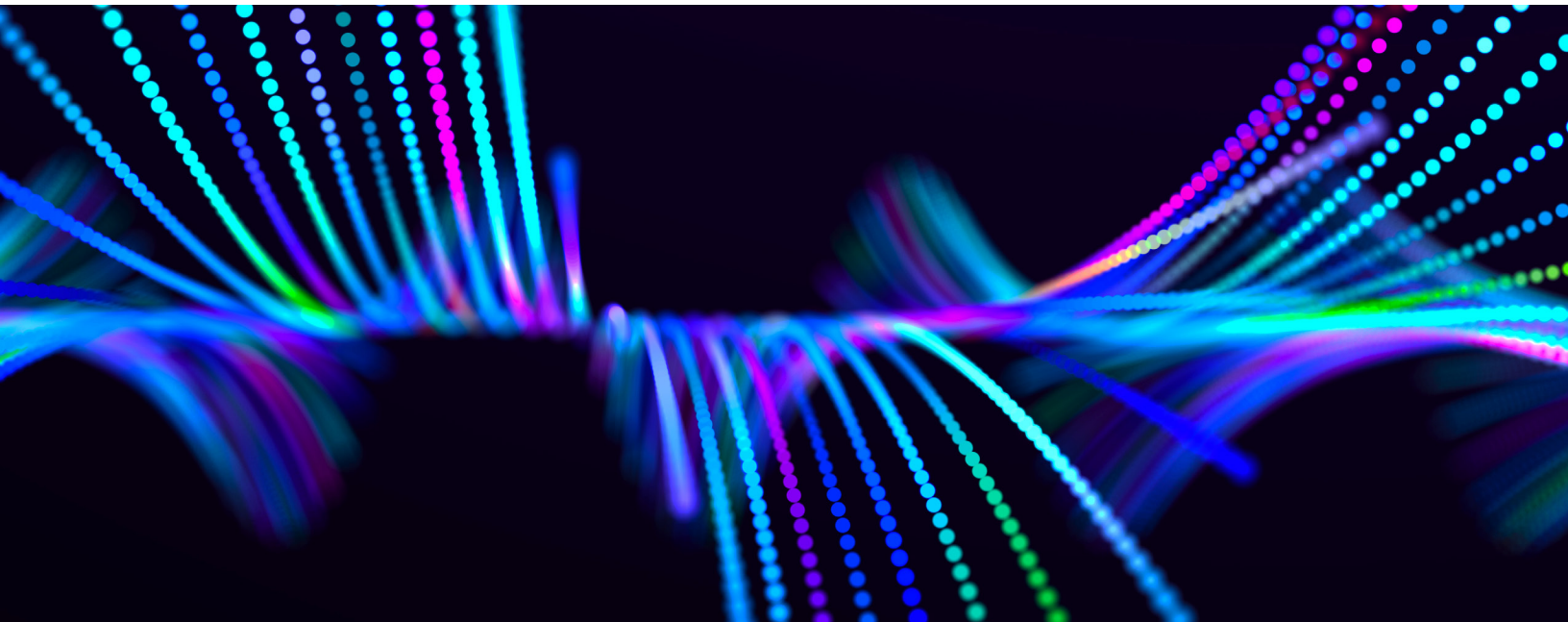
When considering IT aspects of outsourcing and offshoring, the paramount concern is to establish a secure environment. This involves restricting user rights to enhance cybersecurity, ensuring no user has excessive system access. Adherence to the IRS's 7216 regulation for tax outsourcing is crucial, requiring the segregation of returns and access for clients who haven't consented to disclosure. It's safer to deny access for client files of those who haven't signed the consent, rather than risking unauthorized access. Incorporate them into your network so your IT department has control over access rather than housing information offshore.

Commonly, firms utilize cloud-based systems like Citrix Workspace, VMware Horizon, or Microsoft Azure. Alternatively, some use a locally hosted network (possibly managed by an IT provider). Connecting an outsourcing firm or a third-party service is similar to integrating a remote employee. Implementing Multi-Factor Authentication (MFA) is advisable for access control, and limiting access by IP addresses adds an extra layer of security.

Restricting user access to specific system areas is essential for risk reduction and improved control. It's vital to ensure that the third party has robust cybersecurity measures, including antivirus, anti-malware, and firewalls. Compliance with ISO, SOC II, Cyber Essentials, or GDPR, and undergoing audits and certifications, are highly recommended.

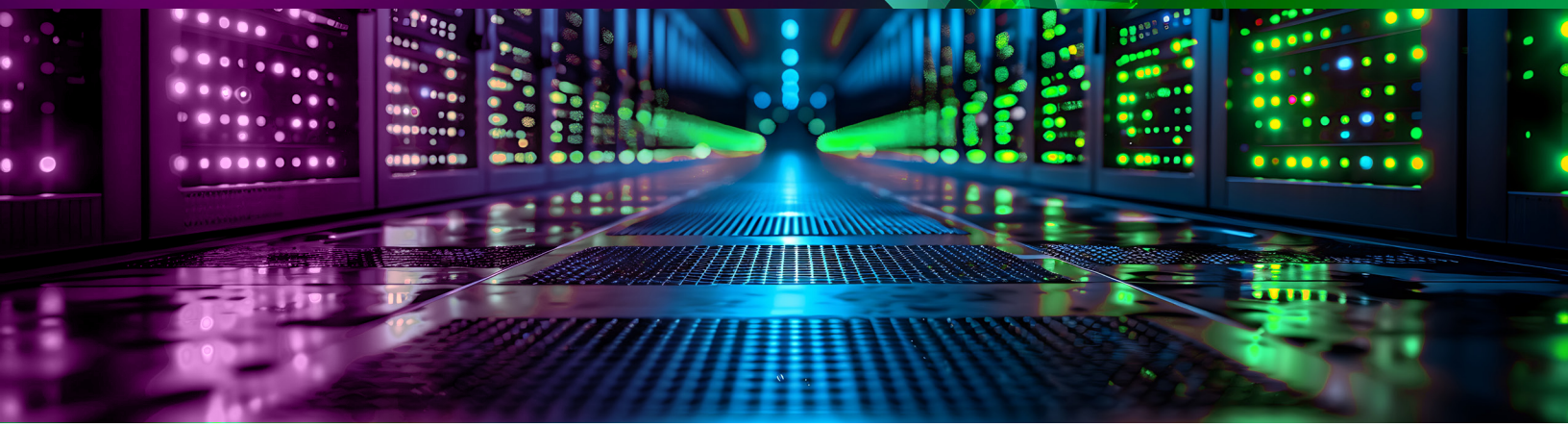
Make sure to integrate all necessary software, typically including accounting, tax, audit, practice management, time/billing, payroll, and document storage applications. Implementing backup and disaster recovery protocols is crucial to regain access to your data in case of emergencies.

For hardware, enforce strict controls such as limited internet and email access, disabled USB ports, and restricted LAN connections or specific Wi-Fi networks. Essentially, create a tightly controlled, risk-averse environment for optimal security.



IT set–up and security when outsourcing or offshoring

Private Companies Practice Section



IT Infrastructure and cybersecurity

1. Secure protocols: ensure secure data transmission.

- **Strong Authentication:** Use certificates or two-factor authentication to authenticate users accessing the network.
- **Access Control:** Limit VPN access to necessary resources only, preventing access to the broader network.
- **Limit Access:** Limit access to a specific IP Address.

2. Software and hardware standards

- Use licensed and up-to-date software to reduce vulnerabilities.
- If possible, provide company-owned hardware with pre-installed security measures.
- Don't ship hardware from the US but ensure it is a trusted provider getting the hardware.
- Lock down access to USB Ports.

3. Cloud-based access

- **Secure Cloud Services:** Choose a reputable cloud service provider with strong security measures (e.g., AWS, Azure, Google Cloud).
- **Data Encryption:** Ensure that all data stored in the cloud is encrypted both at rest and in transit.
- **Identity and Access Management (IAM):** Implement strict IAM policies to control who can access what data and applications in the cloud.
- Implement identity and access management (IAM) solutions to manage user identities and permissions effectively.

4. Facilitate in-person collaboration:

- Contact your software provider to understand the most effective and secure method to set up access to a remote employee. (Some may have international access restrictions that need to be unlocked)
- **Software as a Service (SaaS)**: Consider using cloud-based accounting software with built-in security features.
- **Restricted Access:** Configure software to limit user actions based on their role and necessity. For instance, some users may only need read access, while others may require full access.
- **Audit Trails:** Ensure the software provides comprehensive audit trails for tracking all user activities.

IT set–up and security when outsourcing or offshoring

Private Companies Practice Section

5. User rights management

- **Role-Based Access Control (RBAC)**: Implement RBAC to define what resources a user can access within the network or software based on their role.
- **Least Privilege Principle:** Grant users the minimum level of access needed to perform their job.
- **Regular Review of Access Rights:** Periodically review user rights to ensure they are still appropriate and adjust as necessary.

6. Incident response plan

- Have a well-defined incident response plan in case of a security breach.
- Ensure the offshore firm has its own response plans that align with your standards and federal law.

7. Cybersecurity measures

- **Firewalls:** Deploy both hardware and software-based firewalls to act as a barrier against external threats.
- **Antivirus and Anti-Malware Solutions:** Install and regularly update antivirus software on all devices.
- **Regular Security Audits and Penetration Testing:** Conduct to identify and remediate vulnerabilities.
- **Employee Training:** Regularly train offshore staff on cybersecurity best practices and awareness.
- **Backup and Disaster Recovery:** Implement a robust backup strategy and a disaster recovery plan to mitigate data loss risks.

8. Compliance and data protection

- **Regulatory Compliance:** Ensure that your offshore provider is not only familiar with but also certified in key regulations such as GDPR, SOC II, Cyber Essentials, and other relevant cybersecurity standards to improve compliance and security.
- **Data Localization Laws:** Store data onshore. You want to keep control of all information and limit sending information off your system.
- Define clear terms and conditions regarding network and data access in your contract with the outsourcing firm.
- Establish clear policies and procedures for handling sensitive data and ensure the offshore staff is trained on these.

9. Regular audits and monitoring

- Conduct regular security audits of the offshore vendor's practices.
- Implement continuous monitoring of their network and system activities.

AICPA & CIMA
Together as the Association of International Certified Professional Accountants

IMPACT GLOBAL SOLUTIONS