

The Difference Is...

Jay Anderson, CPA, CITP, CISA

Principal, Risk Services



314.983.1385
janderson@bswllc.com

Jay is a Principal in Brown Smith Wallace's Risk Services practice, where he has responsibility for providing risk management and internal audit services to the firm's clients. Jay joined Brown Smith Wallace after spending five years as a Corporate Manager, Information Technology Audit for SBC Communications. Prior to SBC, Jay spent more than four years as a senior internal auditor and regional controller for a financial institution and a service management company. Jay's background includes:

- Leads the IT audit teams for all compliance and SAS 70 Audits for diverse clients, including: TPAs, Software as a Service, Hosting, Financial Services, Banking, Credit Unions, etc.
- Manager of the IT portion of the external audit Sarbanes-Oxley review for a major financial services and healthcare service provider. Responsibilities included analyzing system controls, defining and performing mainframe, client server and network security testing and drafting an opinion on IT general and application controls.
- Providing overall leadership on IT audits for a variety of technologies. Duties included development of audit programs, communication of audit results, performing risk assessments, development of auditors and assisted with the maintenance of the risk-based universe of audit subjects for strategic audit planning. Internal financial procedure evaluations
- Assisting in developing IT audit approach to SBC's SOX efforts and led SOX project teams designed to evaluate and strengthen business and IT controls and to develop analysis tools and guidelines for continual monitoring of these controls.
- Supporting various projects involving company-wide implementation of standardized processes relating to change management, mainframe security and maintenance of equipment providing support to SBC data centers.
- Reviewing RACF and UNIX configuration of security settings to ensure logical security was enforced enterprise-wide. Identified best practices to enhance regional security controls for compliance with SOX.
- Reviewing general controls utilized in critical data center facilities. Evaluated physical security, change management, capacity planning, environmental controls, backup and recovery procedures and power diversity and redundancy.