Conklin Technology
Security Assessments

Larry Conklin, CISA, CPA, CIA, CFSA
Telephone: 515-491-7457
Email: LConklin@ConklinTechSec.Com

Certifications:

- Certified Information Systems Auditor (CISA)
- Certified Internal Auditor (CIA)
- Certified Public Accountant (CPA) (non-practicing)
- Certified Financial Services Auditor (CFSA)
- Certificated Cloud Security Professional (CCSP)
- Certified Data Privacy Solutions Engineer (CDPSE)
- Cybersecurity Practitioner (CSXP)
- Cybersecurity Audit (CAC)

Education:

Bachelor of Science, Northwest Missouri State University, 1983

Major Accounting
Minor: Computer Science

Technology Knowledge and Audit Experience:

Operating Systems:

- Linux/UNIX – **Detailed**
- Windows 10 – **Detailed**
- Apple MAC – **Baseline**
- VMWare – **Functional**
- IBM zOS - **Detailed**

Databases:

- SQL Server – **Detailed**
- Oracle – **Detailed**
- DB2 LUW – **Functional**
- MongoDB – **Baseline**
- MYSQL - **Baseline**

Experience:

Principal Financial Group - Director, IT Auditor
April 1989 – December 2019
Conklin Technology Security Assessments (CTSA)
January 2020 – Current

Professional Profile:

During my career as a Technology Auditor and Consultant the size and complexity of the Technology architectures and solutions has grown exponentially. I have overseen the continuous modification of the scope and nature of the technology assessment projects performed across the company to meet the changing risk profiles associated with the introduction of each new technology. Work history includes extensive experience and expertise in the assessment of technical risks associated with operating systems, database applications, firewalls/data networks, cybersecurity, and cloud risk governance.

Successfully established positive working relationships with IT management across the company who routinely sought out my expertise and guidance. Consulted with Technology personnel, particularly around security administration, on proposed control changes to ensure that they are evaluating all the potential risk impacts. The audits performed by the IT audit team I directed were risk based and focused on not only the technical configurations and security but also the operational efficiencies and effectiveness as well as the strategic positioning of the technology reviewed within the overall company technical infrastructure.

Experience & Accomplishments:

- Developed and made special topic presentations to the Audit Committee of the Board, Company CIO Working Group, and other Executive Committees as needed.

- Supervised all technical IT audits, ensuring the proper focus on risks for each technology; the staff on each audit possessed adequate knowledge, time and tools and benchmarking authoritative standards (CoBiT, ITIL, NIST, ISO, CERT, etc.) were applied.

Technology Knowledge and Audit Experience (cont):

Networking Technologies:

- Firewalls (Cisco, CheckPoint, Juniper, Sonicwall, Fortinet) - **Detailed**
- Routers & Switches (Cisco) – **Detailed**
- Wireless networks – **Detailed**
- Remote Access (RSA, Xenapp solution) - **Detailed**

Hosting Infrastructure:

- Virtual Network (VMWare Distributed Virtual Switch, Cisco F5, VMWare NSX) - **Functional**
- Middleware (Message Queuing, Message Brokers, Tivoli Workload Scheduler Agent, Java Database Connectors) – **Functional**
- Containers (Docker, Tectonic, Open Shift Container Platform, Rancher) - **Baseline**
- Runtime (WebSphere Application Server, Liberty, .Net Runtime, MuleSoft, WildFly) – **Functional**

Detailed = In depth knowledge and experience with security, configuration, logging, and administrative risks.

Functional = Detailed knowledge of risks related to this technology with limited audit experience.

Baseline = Basic understanding of the risks related to the technology.

- Developed and implemented automated configuration assessment tools to extract and analyze security and configuration settings from key operating systems and database implementations.
- Identified and implemented cost effective vulnerability assessment tools for operating systems, web applications, and networking devices to improve assessment coverage and efficiency.
- Developed a cybersecurity assessment program which provides a structured, independent, objective analysis of a company's cybersecurity program. These assessment templates have been scaled and tailored to address the cybersecurity risk profile based upon the breadth, maturity, and complexity of each IT architecture.
- Developed cloud risk governance and oversight consulting and assessments program based on Cloud Security Alliance Cloud Control Matrix (CSA CCM). Performed and supervised engagements on cloud implementation/adoption projects:
    - Implementation consulting during the negotiation and initial deployment phase to ensure the establishment of risk management roles, responsibilities, and reporting activities for the CSP and the cloud customer.
    - Periodic assessment of the ongoing oversight activities to verify compliance with agreed upon internal controls and procedures and the CSP Service Level Agreement (SLA) fulfillment.
- Annually completed a risk assessment based on audit history, technology materiality to company operations, risk management profile for the technology, emerging threats, and changes to the environment since the last audit.
- Acted as a liaison between IT personnel and regulatory auditor to facilitate and manage the appropriateness of audit information gathering requests. Lead/participated in company internal regulatory compliance self-assessments.
- Co-developer of the first formal corporate risk model introduced into a Fortune 500 company.