Leela Karumuri
CRISC and CAIIB
[redacted]; [redacted]
[redacted], [redacted]

IT security and compliance professional proficient in security, compliance, risk, controls and information technology audits such as GLBA and SOX. Worked with IT security, IT audit, IT risk frameworks and standards such as COBIT, NIST, PCI DSS and ISO/IEC. She is experienced in applying critical thinking, analysis, recommendations, solutions to limit risks and ensure accuracy to assist with various processes and IT audits. She has regularly served as the point of contact for multiple departments including IT-Access Controls, BCP/DRP, project management, and core banking project groups with inquiries around segregation of duties, audit follow-up, compliance, and control. Possesses advanced technical skills in Microsoft Office, various core banking applications.

Professional Experience

Manager, IT Risk and Compliance
City of Aurora
Feb, 2019 – present

- Plans, designs and implements an overall risk management process for the organization;
- Conducts risk assessment, which involves analyzing risks as well as identifying, describing and estimate the risks affecting the organization;
- Prepares risk evaluation, which involves comparing estimated risks with criteria established by the organization such as costs, legal requirements and environmental factors and evaluating the Organization's 'risk appetite', i.e. the level of risk they are prepared to accept;
- Prepares risk reporting in an appropriate way for different audiences, for example, to the Executive Committee or the Board of Trustees, so they understand the most significant risks, to business heads to ensure they are aware of risks relevant to their parts of the business and to individuals to understand their accountability for individual risks;
- Handles corporate governance involving external risk reporting to stakeholders;
- Carries out processes such as purchasing insurance, implementing health and safety measures and making business continuity plans, to limit risks and prepare for if things go wrong;
- Ensures the Board of Directors, management and employees follow the rules and regulations of regulatory agencies, that company policies and procedures are being followed, and that behavior in the organization meets the company's Standards of Conduct.
- Conducts audits of policy and compliance to standards, including liaison with internal and external auditors;
- Provides support, education and training to staff to build risk awareness within the organization.
- Assists in performing all tasks necessary to achieve the organization's mission and helps execute staff succession and growth plans.

IT Auditor, Control Audit and Process Department (CAP)

Canadian Western Bank Edmonton, Canada

Feb 2013 – April 2017

Performed risk and control assessments for applications, vendor management and business processes through evidence in Archer, policies, procedures, best practices and professional judgement.

- Project: Enterprise level Access Controls.
  - Identified deficiencies, performed a root cause analysis and recognized lack of procedures and recommended.
  - Lack of communication between various departments was identified as one of the reasons for incidents and enabled communication channels by discussing and arranging meeting between various stake holders.
  - Implementation of procedures in IT Service department has reduced the incidents by 95%.
  - Recognized as an SME on corporate access control risk mitigation and identified as liaison with external auditors.
- Project: Business Continuity and disaster preparedness (BCP / DRP).
  - As an audit observer for annual business continuity process, developed a strategy and recognized by the IT and the business units as an auditor who aligned IT and business operations in BCP/DRP.
  - Became a go to person for all business continuity issues between IT and operations.
  - Reduced the critical observations by 100 percent and only nice to have observations were identified in the 2014 BCP review.
- Project: Regulatory / compliance audits.
  Interac (Canadian Payment Card industry) –
  - Reviewed SOC2 Type 2 reports for 3rd party vendor controls pertaining to payment cards and recommended IT management to identify the control responsibilities between various departments and the 3rd party vendors, which reduced control testing by 50% as vendors are responsible for those controls as per the contractual documents.
  - Project: PCI-DSS- recommended tokenization to one of the subsidiary companies as a solution for PCI-DSS. Eliminated PCI-DSS compliance as credit card information is only obtained from the customers for billing purpose.

  - Project: Canadian Deposit Insurance Corporate-Fast Insurance Determination
    - Identified as subject matter expert on technical and operational issues during the certification process.
    - Risks were identified and ensured that the certification process is completed seamlessly and provided evidence of success to the CFO for the certification

  - Project: Security Audits:
    - Verified and ensured the change management process is in place for all the changes to the firewall configurations.
    - Verified that there is proper segregation of duties in implementing firewall changes and there is a methodology in place to identify unauthorized changes to the configurations.

- Reviewed the emergency change process and ensured that it was properly analyzed by the subject matter experts and the document is reviewed appropriately.
- When considering moving some of the critical applications to cloud as service, performed risk assessment on access management, SDLC, patch management process, release management and exit strategy considerations.
- During application level testing ensured availability of third-party encryption certificates, vulnerability assessments results, SOC reports.

- Project: Steering committee project
  - Conversion of debit cards to chip enabled cards, business VISA cards, core banking application conversion, insurance subsidiary core application conversion, finance application upgrade, trust system conversion, Insurance subsidiary's finance application upgrade, treasury data transfer project, core banking project implementation,.
  - Successfully reduced IT project risks by identifying risks before project implementation.

Investigator, Anti-Money Laundering:

TD Canada Trust Toronto, Canada

June 2006 – Jan 2013

- Processed and reported activities relating to Daily Money Laundering Reporting compliance to FINTRAC/OFAC, including all large cash transactions and suspicious transactions
- Reviewed and processed all declarations relating to all identified Money Laundering files
- Investigated and reported entries on the weekly Terrorist Financing Comparison Reports
- Investigated and updated additions to the Terrorist List to branches
- Completed the weekly and semi-annual Terrorist Financing Comparison Reports
- Processed all Deposit Alerts, Refusals to Open Account or Cash, Govt. Cheques
- Respond to branch enquires with regards to Money Laundering queries
- Reviewed and investigated daily under $10000 cash and Wire Reports and report accordingly

Retail Manager, State Bank of India, Hyderabad:
Feb 2000 – April 2006

Teller, State Bank of India, Hyderabad:
Mar 1988- Jan 2000

<u>Certifications:</u>

- Certified in Risk and Information System Control (**CRISC**)
- Certified Associate of Indian Institute of Bankers (**CAIIB**)

Professional Development:

- Certified Information System Auditor (**CISA**)
- Certified Information System Security Professional (**CISSP**)
- COBIT, COSO

Volunteer Work:

- IIA Edmonton Chapter – Board Member
- JDRF – CWB Team Lead
- Member – CWB Green Team
- Member, Indian Cultural Association, Edmonton, Canada, 2011-2017
- Secretary, Indian Cultural Association, Edmonton, Canada, 2012-2014

Education:

- Graduate in sciences, Andhra University, India
- Post Graduate Diploma in Computer Sciences, CMC, India