



Proposal Response

RFP 25-014

Information Technology Operational Efficiency Audit

Due Date & Time: February 19, 2025 at 12:00 P.M CT

Proposed to:

The City of North Richland Hills

Electronically Via: www.publicpurchase.com

Submitted by:

Cogent Infotech Corporation

Manu Mehta, President

HQ: 1035 Boyce Road, Suite 108, Pittsburgh, PA 15241

Local Address: 1425 Greenway Drive, Suite 340, Irving, Texas 75038

Email: manu.mehta@cogentinfo.com

Phone: (412) 246-0708

Website: <https://www.cogentinfo.com>



TABLE OF CONTENTS

1	DEMONSTRATED EXPERIENCE, QUALIFICATIONS, AND REPUTATION	2
1.1	Firm Overview	2
1.2	Overview of Similar Services Provided on a Regional and Local Basis	3
1.3	Scope of Operation.....	4
1.4	Relevant Experience	5
1.4.1	Reference #1.....	5
1.4.2	Reference #2.....	6
1.4.3	Reference #3.....	6
1.4.4	Reference #4.....	7
1.4.5	Reference #5.....	7
1.4.6	Reference #6.....	8
1.5	Project Team Structure	8
1.6	Key Personnel Qualifications.....	9
1.6.1	Resume –Mansoor Hussain – Security Consultant	10
1.6.2	Resume –Aaron Molina – Network Consultant	10
1.6.3	Resume –Megan Kelley – IT Audit Manager	11
1.7	Staff Capacity and Project Timeliness.....	11
1.8	Distinctive Attributes and Special Capabilities.....	12
1.9	Sample Project Report	14
2	PROPOSED PROJECT METHODOLOGY	14
2.1	Project Execution Plan	14
2.2	Methodology and Tools	18
2.3	Proposed Timeline (4 Months).....	19
2.4	Deliverables	20
3	PROPOSED PRICING	22
4	REQUIRED QUALIFICATIONS	23
5	APPENDIX A	25
5.1	Resume Megan Kelley – PMP, PMI-ACP, SCPM, SCM, MBA.....	25
5.2	Resume – Aaron Molina.....	34
5.3	Resume – Mansoor Hussian.....	39

1 DEMONSTRATED EXPERIENCE, QUALIFICATIONS, AND REPUTATION

1.1 FIRM OVERVIEW

Cogent Infotech Corporation (Cogent), established in 2003, is a national award-winning **ISO Certified, CMMI Level 3, and AWS Certified firm**. Cogent is a leading IT consulting and solutions firm with over 21 years of experience delivering technology-driven operational assessments, process optimization, cybersecurity solutions, and workforce planning to government and public sector clients. Cogent has built a strong reputation for delivering high quality, scalable, and cost-effective IT services to federal, state, and local government agencies, Fortune 500 companies, and public institutions. We operates as an S-Corporation with no subsidiaries, specializing in IT consulting, staffing, and related services. Cogent serves both the public and private sectors, with an emphasis on government consulting and Information technology solutions. Cogent currently manages major IT & Consulting contracts for state and local governments, including **Texas, Massachusetts, New York, Georgia, Florida, and California**. Cogent has multiple offices across the U.S., including **Pennsylvania, Virginia, Washington D.C., Florida, New York, California, and Texas**, allowing it to provide both regional and local services efficiently.

A key differentiator of Cogent is its proprietary in-house training program, Cogent University, which specializes in upskilling professionals in emerging technologies such as **Cloud Computing, Artificial Intelligence, Cybersecurity, and Software Development**. This initiative ensures that clients receive highly qualified professionals who not only possess the necessary technical skills but also align with industry best practices and regulatory requirements.

Company Description	
Company Name	Cogent Infotech Corporation (Cogent)
Year Established	2003
Headquarters	1035 Boyce Road, Suite 108, Pittsburgh, PA 15241
Business Classification	ISO Certified, CMMI Level 3, AWS Certified
Business Type	Subchapter S – Corporation (No subsidiaries)
Primary Services	IT Consulting, IT Managed Services, Project Management, Cybersecurity and Data Analytics
Number of Employees	500+ professionals
Government Certifications	Small Business; Minority Business Enterprise Certified from NMSDC, DFWMSDC, NY OGS, NYC SBS
Website	www.cogentinfo.com

AREAS OF SPECIALIZATION

Cogent specializes in IT consulting, process transformation, and AI-driven data solutions across Federal, State, and Local Governments. Our Key Service Areas include but are not limited to:

- IT Operational Audits & Process Improvement
- Cybersecurity & Risk Assessment
- Cloud & Infrastructure Modernization
- Data Analytics & Business Intelligence
- Enterprise Resource Planning (ERP) & Digital Transformation
- Project & Program Management

- Application & Software Development
- Help Desk & IT Support
- Artificial Intelligence & Machine Learning
- Procurement & Logistics Optimization
- Human Capital Management

1.2 OVERVIEW OF SIMILAR SERVICES PROVIDED ON A REGIONAL AND LOCAL BASIS

Cogent has a strong track record of providing similar IT operational efficiency, staffing, and consulting services across multiple government agencies, municipalities, and commercial entities at both regional and local levels. Our experience aligns closely with the scope outlined in the solicitation. Below table demonstrates a range of governmental, state, and other entities that Cogent has supported with similar services:

Category	Client	Services Provided
IT Operational Efficiency Audits	State of Vermont	Cogent performed an in-depth IT operational analysis, evaluating project management frameworks, identifying inefficiencies, and implementing workflow automation to enhance service delivery across state departments. Our team developed standardized processes to ensure long-term operational sustainability.
	City of Sacramento	Our team conducted a comprehensive IT process review to optimize digital transformation efforts, aligning IT services with city-wide strategic goals. We assessed application usage, IT service models, and infrastructure support to drive efficiency and cost savings.
	Dallas Fort Worth International Airport	We performed an extensive operational assessment of IT infrastructure, cybersecurity protocols, and network management systems. Our team provided actionable recommendations to enhance system reliability, strengthen data security, and modernize technology processes.
IT Process Improvement Services	State of Texas (DIR)	Cogent evaluated IT workflows, identifying automation opportunities and optimizing processes to align with state-mandated technology policies. We developed a roadmap to enhance service efficiency, resource allocation, and regulatory compliance.
	New York Power Authority	Our team assessed IT processes, identifying inefficiencies in application management, infrastructure operations, and security frameworks. We implemented structured process improvements to enhance IT service delivery and ensure regulatory compliance.
	US House of Representatives (CAO Office)	We performed a comprehensive IT service analysis, evaluating end-user support effectiveness, technology service desk operations, and mobile device management. Our recommendations improved response times, streamlined service ticket resolution, and enhanced user satisfaction.
	Florida Department of Transportation	Cogent re-engineered IT processes, introducing automation to enhance service efficiency and operational continuity. We evaluated existing IT governance models and implemented a framework to ensure seamless service delivery across departments.
Cybersecurity & Disaster Recovery Planning	Baltimore City Information & Technology	Cogent performed a cybersecurity resilience assessment, identifying vulnerabilities, evaluating security measures, and enhancing IT disaster recovery planning. Our team implemented risk mitigation strategies and best practices to minimize system downtime and data breaches.
	Tarrant County, Texas	Our team conducted an IT security audit, assessing cybersecurity frameworks, identifying operational risks, and developing a compliance strategy. We provided recommendations for strengthening IT governance, incident response planning, and system resilience.

Category	Client	Services Provided
IT System & Workflow Optimization	Dallas Independent School District	Cogent optimized IT workflows by identifying inefficiencies in system operations, technology support, and digital education platforms. Our recommendations improved IT governance, streamlined internal processes, and enhanced system reliability.
	State of Georgia	We evaluated the department's IT infrastructure and digital learning platforms, implementing solutions to optimize e-learning systems, improve data security, and enhance technology-driven educational initiatives. Our team provided strategies to ensure seamless IT support and operational scalability.





1.3 SCOPE OF OPERATION

Cogent is a nationwide firm with offices across Texas, Pennsylvania, Virginia, Washington D.C., Florida, New York, and California. For the City of North Richland Hills, services will be provided from the Dallas, TX office, ensuring local compliance, fast response times, and tailored solutions.

Currently, we have six offices in major cities across various States namely TX, PA, CA, NY, FL, and DC. Below are the complete addresses of our offices. Our Texas Office will have the primary responsibility for the execution of this service.

SR NO.	STATE	ADDRESS	TYPE
1.	PA	1035 Boyce Road, Suite 108, Pittsburgh, PA 15241	Headquarter
2.	TX	1425 Greenway Drive, Suite 340, Irving, TX 75038	Local Office
3.	CA	1800 North Vine Street Hollywood, Los Angeles, CA 90028	Office
4.	NY	200 Vesey Street, 24th Floor New York, NY 10281	Office
5.	FL	1800 NW Corporate Boulevard, Suite 130, Boca Raton, FL 33431	Office
6.	DC	4250 North Fairfax Drive, Suite 600, Arlington, Virginia 22203	Office

With over 21+ years of experience in the industry, Cogent has the capability to leverage its partner network to provide a vast resource pool of highly qualified technical, administrative, and management skills with the credentials to work on State and Federal government projects. We are currently engaged in significant State contracts and have previously performed on State and Federal contracts as well where we delivered quality services to enhance performance and maintain customer satisfaction. Below provided table depicts list of various State of Texas agencies to whom we have provided similar IT Services till date.

State of Texas Agencies	
 <p>TEXAS Health and Human Services</p> <p>Department of Health and Human Service Commission</p>  <p>Department of Transportation</p>	 <p>TEXAS Department of Family and Protective Services</p> <p>Department of Family & Protective Services</p>  <p>Texas Workforce Commission</p>
Educational Agencies	

	
Dallas Independent School District	Austin Community College
Local Government Agencies	
	
Austin Energy	DFW Airport Authority
	
Lower Colorado River Authority	Harris County
	
San Antonio Water Systems	Harris Health System

1.4 RELEVANT EXPERIENCE

1.4.1 Reference #1

Client: New York Power Authority (NYPA)	
Reference Details:	Name: Christine Prendergast Phone: (914) 681-6612 Email: Christine.Prendergast@nypa.gov
Period of Performance	08/31/2020 to 01/31/2025
<p>Cogent has been a trusted IT service provider for NYPA, supporting digital transformation, cybersecurity, enterprise software management, and infrastructure modernization. Their contributions include:</p> <ul style="list-style-type: none"> • Enterprise IT System Support & Upgrades: <ul style="list-style-type: none"> ○ Supporting NYPA’s SAP, Oracle, and cloud-based ERP systems. ○ Upgrading legacy applications to modernized enterprise solutions for better efficiency. ○ Providing end-to-end cloud migration support for NYPA’s IT infrastructure. • Cybersecurity & Risk Management: <ul style="list-style-type: none"> ○ Conducting cyber risk assessments to safeguard NYPA’s power grid control systems. 	

<ul style="list-style-type: none"> ○ Deploying Security Information & Event Management (SIEM) tools for real-time threat detection. ○ Implementing Identity Access Management (IAM) solutions to strengthen user authentication policies. ● Application Development & Data Analytics: <ul style="list-style-type: none"> ○ Building custom data visualization tools for real-time power distribution analytics. ○ Enhancing GIS-based energy monitoring systems to optimize energy efficiency. ○ Designing business intelligence dashboards for NYPA’s grid management teams. ● IT Project Management & Business Process Optimization: <ul style="list-style-type: none"> ○ Leading agile development teams for workflow automation and system integration. ○ Supporting business process re-engineering for NYPA’s procurement, finance, and compliance departments.
--

1.4.2 Reference #2

Client: Amtrak	
Reference Details:	Name: Carlton Myers Phone: (215) 349 -1227 Email: carlton.myers@amtrak.com
Period of Performance	03/15/2021 to 12/31/2024
<p>Cogent provides IT, cybersecurity, and business process consulting to Amtrak, helping the organization modernize its IT infrastructure, improve its cybersecurity posture, and enhance digital transformation initiatives. Our key contributions include:</p> <ul style="list-style-type: none"> ● Enterprise Software & Cloud Integration: <ul style="list-style-type: none"> ○ Managed Amtrak’s Microsoft 365 environment, including Exchange, SharePoint, and Teams. ○ Implemented ServiceNow IT Service Management (ITSM) to streamline IT operations and incident management. ○ Supported cloud migrations for Amtrak’s enterprise applications and ticketing systems. ● Cybersecurity & IT Governance: <ul style="list-style-type: none"> ○ Deployed Zero Trust security models to enhance access control and authentication protocols. ○ Performed cyber risk assessments and penetration testing to identify vulnerabilities in Amtrak’s critical systems. ○ Implemented SIEM (Security Information and Event Management) tools for real-time security monitoring. ● Software Development & System Integration: <ul style="list-style-type: none"> ○ Upgraded SAP enterprise solutions for procurement and human resources management. ○ Supported eDiscovery and compliance management for Amtrak’s legal and regulatory teams. ○ Integrated automated ticketing and reservation systems with Amtrak’s digital platforms. ● IT Project Management & Agile Support: <ul style="list-style-type: none"> ○ Deployed Scrum Masters and Agile Coaches to optimize Amtrak’s software development lifecycle (SDLC). ○ Lead cross-functional teams to streamline workflow automation and IT governance. 	

1.4.3 Reference #3

Client: Washington Health Benefit Exchange (WAHBE)	
Reference Details:	Name: Erin Hamilton Phone: (360) 688-1562 Email: erin.hamilton@wabhexchange.org
Period of Performance	02/25/2021 to 12/31/2024

Cogent has played a pivotal role in enhancing IT security, system integration, and quality assurance for Washington’s state health benefit exchange. Services include:

- User Acceptance Testing (UAT) & Quality Assurance:
 - Developed automated test scripts for healthcare claims processing systems.
 - Implemented performance testing and defect tracking for the state’s insurance marketplace platform.
- Cybersecurity & Compliance:
 - Conducted HIPAA and NIST compliance assessments to safeguard patient data privacy.
 - Designed intrusion detection systems to mitigate security breaches.
- Data Migration & Integration Support:
 - Assisted in migrating 2+ million user records from legacy health systems to modern platforms.
 - Implemented AI-driven analytics to detect fraudulent healthcare claims.

1.4.4 Reference #4

Client: Dallas Fort Worth International Airport (DFW)	
Reference Details:	Name: Emil Grosye Phone: (972) 973-5468 Email: egrose@dfwairport.com
Period of Performance	03/25/2019 to 03/17/2024
<p>Cogent has been providing comprehensive IT Audit services and technology support to DFW Airport, one of the busiest airports in the world. Services provided include:</p> <ul style="list-style-type: none"> • Enterprise Software Development: <ul style="list-style-type: none"> ○ Supported MuleSoft API architecture, developing custom applications, and managing integration with airport-wide IT systems. ○ Assisted in designing and implementing RESTful Web Services for various third-party applications used in the airport. • Cybersecurity & Network Security: <ul style="list-style-type: none"> ○ Conducted threat analysis, vulnerability scanning, and system audits. ○ Implemented security automation tools to protect airport networks from cyber threats. • Cloud Infrastructure Management: <ul style="list-style-type: none"> ○ Supported Azure, AWS, and hybrid cloud solutions for airport IT operations. ○ Configured cloud storage and disaster recovery systems for critical airport functions. • IT Project Management & Agile Transformation: <ul style="list-style-type: none"> ○ Deployed Scrum Masters and Agile Coaches to help teams transition to Agile and DevOps models. ○ Lead cross-functional teams to optimize project workflows. • IT Support & Helpdesk Services: <ul style="list-style-type: none"> ○ Offered Tier 1, 2, and 3 support for airport employees and systems, ensuring smooth airport operations. 	

1.4.5 Reference #5

Client: City of Sacramento	
Reference Details:	Name: Mrudul Sadanandan Phone: (916) 808-7894 Email: msadanandan@cityofsacramento.org
Period of Performance	03/06/2024 to 04/16/2024
<p>Cogent has provided IT solutions to multiple city departments, ensuring high-quality government services. Our services included but are not limited to:</p> <ul style="list-style-type: none"> • ERP Implementation & System Modernization: <ul style="list-style-type: none"> ○ Supported the City’s transition to a modern ERP system for finance, procurement, and HR functions. • Cybersecurity Risk Assessment & Incident Response: <ul style="list-style-type: none"> ○ Conducted penetration testing and vulnerability scanning of city networks. ○ Implemented multi-factor authentication (MFA) and endpoint security solutions. 	

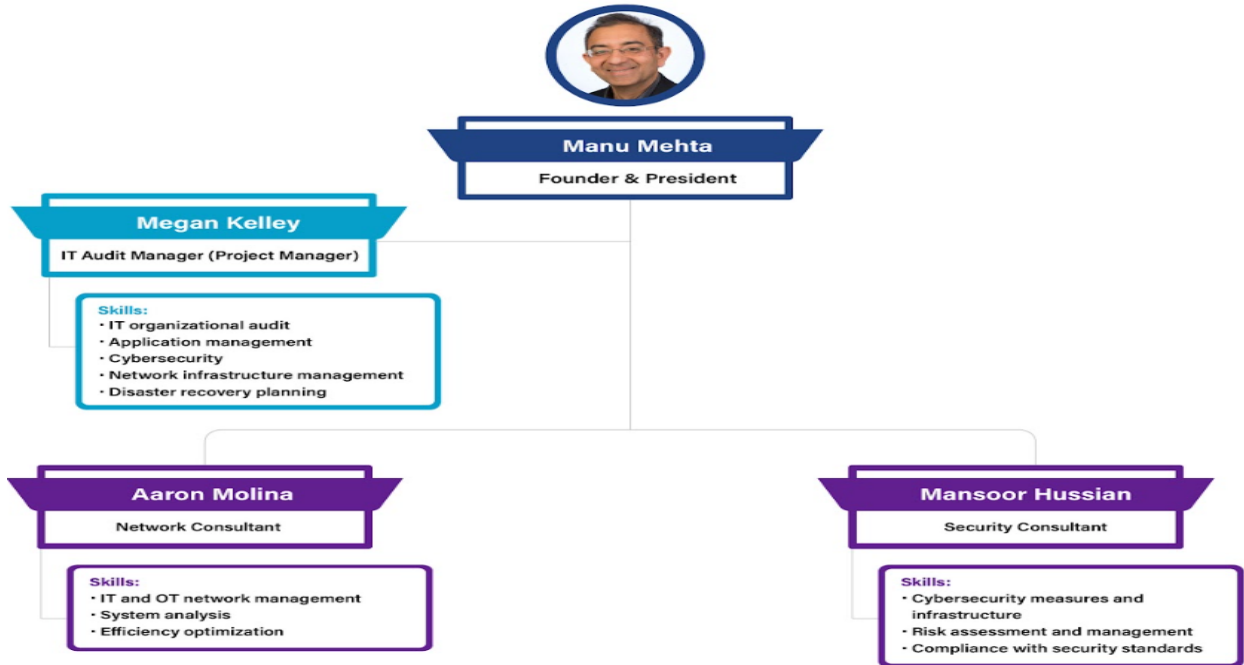
- Technical Support & Help Desk Services:
 - Provided 24/7 IT help desk support for city employees and critical public services.

1.4.6 Reference #6

Client: New York City Housing Authority (NYCHA)	
Reference Details:	Name: Patricia Lindo Phone: (212) 306-2807 Email: Patricia.Lindo@nycha.nyc.gov
Period of Performance	01/14/2019 to 12/31/2024
Cogent provides mission-critical IT support to NYCHA, the largest public housing authority in the United States. Our services included but are not limited to: <ul style="list-style-type: none"> • IT Infrastructure Management: <ul style="list-style-type: none"> ○ Provided technical specialists to upgrade, maintain, and secure NYCHA’s IT infrastructure. ○ Implemented automated monitoring and incident response to improve system resilience. • Enterprise Software Development: <ul style="list-style-type: none"> ○ Supported Oracle and SAP enterprise applications, including financial and property management systems. ○ Built data visualization dashboards for NYCHA’s public safety and tenant management platforms. • Cybersecurity & IT Compliance: <ul style="list-style-type: none"> ○ Implemented NIST 800-53 and FISMA-compliant security protocols to enhance IT security. ○ Conducted cyber risk assessments and training NYCHA employees on data privacy best practices. • Help Desk & End-User Support: <ul style="list-style-type: none"> ○ Provided on-site and remote technical support to NYCHA employees. ○ Managed hardware and software deployment across multiple NYCHA offices. 	

1.5 PROJECT TEAM STRUCTURE

Cogent has extensive expertise using Information Technology Infrastructure Library (ITIL) compliant project management services to provide thoughtful organizational assistance to our clients. We have a streamlined management structure that will allow us to quickly address any potential management difficulties. Our recommended organizational structure will ensure that the Agency and contract team have clear lines of communication. Our staff will be efficiently trained to do their jobs and, as part of our management strategy, cross-trained to undertake additional duties. Our contract manager will be the single point of contact (POC) between the Agency and Cogent for the duration of the contract. This method guarantees that contract operations are coordinated and planned. Our planned Team structure and relationships among the proposed on-site staff members are depicted in the diagram.



Our designated key personnel will dedicate 100% of their time to the project throughout its entire duration.

Candidate Name	Role	Estimated Efforts (Hours)
Megan Kelley	IT Audit Manager (Project Manager)	240
Aaron Molina	Network Consultant	80
Mansoor Hussain	Mansoor Hussain	640
Total Estimation Effort (Hrs)		960

1.6 KEY PERSONNEL QUALIFICATIONS

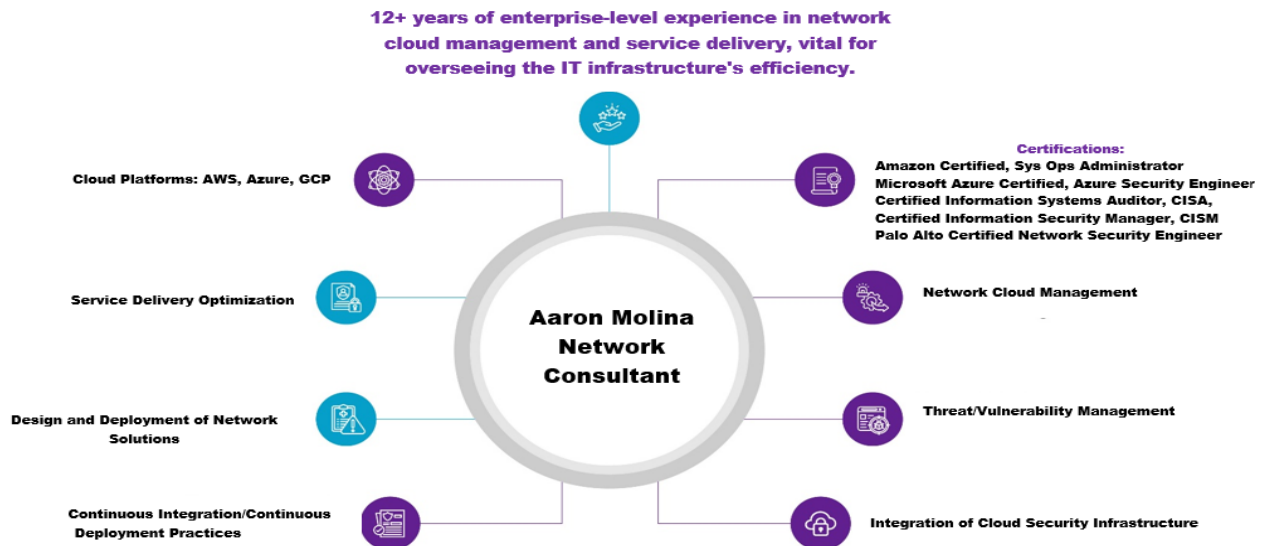
Cogent brings effective and efficient methods and methodologies, innovation, and synergy to City. Our technical and management experience over the past two decades within the Public Sector has afforded us unique expertise to manage and maintain workflows in ever-changing organizational and operational environments. We implement clear and unambiguous lines of communication, responsibility, and authority. Cogent’s organizational methodology demonstrates transparency from the corporate level to the program management/operations level, to the project task execution level. We are proposing **Megan Kelley** who will serve as the **IT Audit Manager and Project Manager**. With expertise in IT organizational audits, application management, cybersecurity, and disaster recovery planning, Megan will oversee the project's strategic direction. She will evaluate IT processes, recommend improvements, and lead the presentation of findings to city leadership. **Aaron Molina** as our **Network Consultant**, specializes in IT/OT network systems. Aaron will analyze the City's IT infrastructure, focusing on cloud usage and overall system performance. His technical analysis will identify potential enhancements and optimizations, to ensure robust and efficient network operations. **Mansoor Hussian**, the **Security Consultant**, brings extensive knowledge in cybersecurity, network security infrastructure, and operational continuity planning. His efforts will center on strengthening the City's IT security posture through comprehensive evaluations and strategic security enhancements. **We have provided the detailed resumes of our**

key personnel in the Section 5: Appendix A. They will be focused on supporting City from the first day of the contract execution.

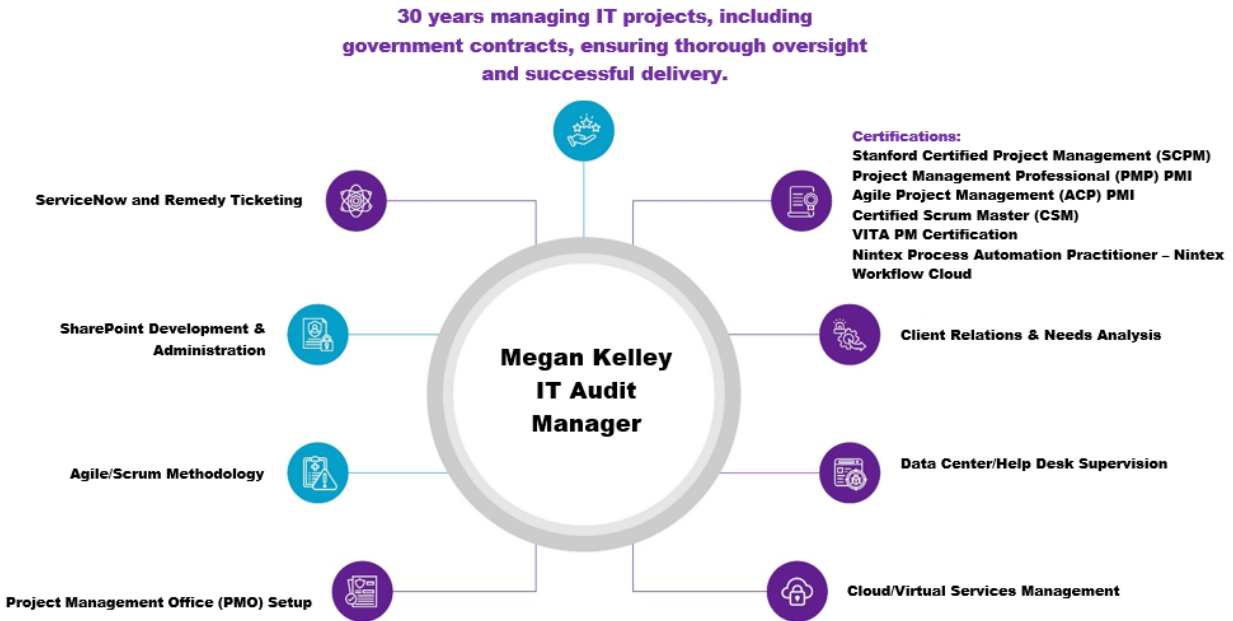
1.6.1 Resume –Mansoor Hussain – Security Consultant



1.6.2 Resume –Aaron Molina – Network Consultant



1.6.3 Resume –Megan Kelley – IT Audit Manager



1.7 STAFF CAPACITY AND PROJECT TIMELINESS

Cogent possesses the workforce capacity, technical expertise, and project management structure to efficiently execute the IT Operational Efficiency Audit for the City. Our structured resource allocation, multi-project management expertise, and commitment to timely delivery ensure we can conduct the audit thoroughly while balancing ongoing engagements. Our dedicated IT consulting and operational audit teams are experienced in delivering large-scale assessments across government entities. Cogent ensures timely execution of projects by assigning dedicated teams that do not have overlapping workloads with other engagements. We have the ability to begin the audit immediately upon contract award, utilizing predefined audit frameworks tailored for City’s IT operations. Our agile methodologies allow us to track iterative progress while maintaining stakeholder alignment throughout the audit process. By leveraging automated process analysis tools and IT service management metrics, we ensure rapid data collection, workflow mapping, and efficient project tracking through platforms like ServiceNow, JIRA, and Microsoft Project.

**About
Cogent Infotech**

Founded in 2003, Cogent Infotech is a trusted, award-winning firm with **21+ years** of experience, **150+** government contracts, **10,000+** projects, and a 96% employee retention rate. Recognized as an SBA Small Business and MBE-certified, we deliver excellence through diverse talent, AI-driven recruitment, and cooperative contracts like NASPO Value Point and TIPS-USA.

Our scalable staffing model ensures that we can dedicate specialized personnel to this project without straining existing commitments. With a pre-vetted talent pool of over **4 million professionals**, we can deploy high-caliber experts within five to ten business days. Our structured workforce planning and **AI-driven resource management systems** allow us to anticipate and allocate resources dynamically, ensuring optimal utilization of our personnel. This enables us to

handle multiple large-scale projects concurrently, without compromising quality, deadlines, or client-specific objectives.

We operate within a disciplined and results-driven project management framework, leveraging **Agile and Scrum methodologies** to ensure incremental progress, continuous stakeholder engagement, and rapid issue resolution. Our **automated workload tracking and real-time performance dashboards** provide clear visibility into project milestones, allowing us to identify bottlenecks before they occur and take preemptive corrective actions. Every engagement is supported by contingency staffing strategies to mitigate unforeseen challenges, ensuring seamless execution and adherence to strict deadlines.

Cogent's proven success in IT governance, operational audits, and business process optimization is evident in our past engagements with large public sector entities, including the **New York City Housing Authority, Tarrant County, and Washington Health Benefit Exchange**. These projects required rigorous efficiency assessments, IT security audits, risk mitigation strategies, and workforce evaluations, all delivered on time and within budget. We understand the unique operational constraints of government IT environments and tailor our solutions to maximize efficiency, minimize disruptions, and enhance service delivery.

To further reinforce our commitment to excellence, we integrate comprehensive quality assurance mechanisms into every phase of the project. Our approach includes **real-time progress monitoring, stakeholder alignment, risk assessments, and adherence to ITIL and NIST frameworks**, ensuring that our recommendations are actionable, scalable, and sustainable. Our compliance with industry standards ensures high-quality outcomes. As a CMMI Level 3 and ISO-certified firm, we adhere to internationally recognized best practices. We implement ITIL frameworks for service management assessments and maintain strict adherence to Key performance indicators (KPIs) and service level agreements.

1.8 DISTINCTIVE ATTRIBUTES AND SPECIAL CAPABILITIES

Cogent possesses a unique set of capabilities that extend beyond traditional IT consulting firms, making us an exceptional choice for the City of North Richland Hills' IT Operational Efficiency Audit. Our special capabilities lie in our ability to transform an IT audit into a strategic roadmap for long-term operational success, rather than just a compliance exercise or a list of recommendations.

1. Beyond Traditional Auditing – Data Driven, AI Powered Analysis

Most IT efficiency audits focus on manual assessments and subjective evaluations. At Cogent, we redefine the audit process by incorporating AI-driven analytics, predictive modeling, and automated performance tracking to identify inefficiencies before they become critical bottlenecks. Our ability to integrate machine learning and data visualization dashboards allows us to deliver real-time insights rather than post-project reports, ensuring that the City's leadership can act on recommendations while the audit is still in progress.

2. Real-Time, Agile-Focused Execution – No Waiting for Results

Unlike traditional firms that deliver findings only after an audit, Cogent employs agile methodologies to provide incremental insights and immediate value. Through our iterative reporting model, the City will see tangible improvements throughout the project lifecycle, rather than waiting until the end of the engagement. This enables leadership to implement quick wins,

gain immediate cost savings, and fast-track efficiency improvements, setting us apart from firms that operate with rigid, outdated assessment models.

3. Transforming IT Operations beyond Just Cost Savings

Many IT audits focus solely on reducing operational costs but Cogent takes a holistic approach that emphasizes service enhancement, risk mitigation, security hardening, and workforce alignment. By identifying not only inefficiencies but also opportunities for automation, digital transformation, and strategic investment, we help municipalities like North Richland Hills future-proof their IT operations, ensuring that the City's IT department remains resilient, secure, and agile in the face of evolving technology landscapes.

4. Unparalleled Speed, Scalability, and Resource Readiness

A critical factor in government IT projects is the ability to execute efficiently without disrupting ongoing operations. Cogent maintains a permanent bench of IT experts, allowing us to rapidly scale resources and deploy specialists within days not weeks or months. With **500+ core professionals** and access to a **vetted talent pool of 4 million experts**, we can instantly address staffing gaps, integrate new technologies, and support IT teams with highly specialized expertise, ensuring that projects move quickly, seamlessly, and with minimal downtime.

5. Government IT Expertise – Deep Understanding of Regulatory & Compliance Needs

Public sector IT operations are subject to strict compliance, cybersecurity mandates, and evolving state and federal regulations. Cogent's work with **federal, state, and local government agencies** has given us unmatched expertise in navigating IT governance frameworks such as **NIST, ITIL, FISMA, HIPAA, and CJIS standards**. Our compliance-first approach ensures that every recommendation aligns with regulatory requirements, cybersecurity best practices, and risk mitigation strategies, allowing the City to strengthen its IT posture while improving operational efficiency.

6. Long Term Engagement, Not Just a One Time Audit

Our engagement does not end with an audit report. Cogent's commitment to long-term success ensures that we provide:

- **Post-audit implementation support to drive real-world improvements.**
- **Executive training and workforce upskilling to ensure sustained efficiency.**
- **Change management strategies to help IT teams adopt new frameworks seamlessly.**

POSITIVE FEEDBACK & TESTIMONIALS FROM CLIENTS

- **Boeing Distribution Inc.:** *Cogent Infotech exceeded all expectations and consistently performs at the highest levels – Rohan Dass (Director), Phone: 352-484-9917*
- **ThermoFisher:** *Cogent leadership is a fantastic partner within the program. They are quick to act on escalations and provide timely feedback when requested – Zakhoury Adams (Associate Director), Phone: 484-460-6408*
- **Amtrak:** *Customer is very satisfied with Cogent's performance as it relates to personnel placement in terms of managing substantial FRA-funded railway station renovations which went beyond their useful life and presented possible danger – Kelly McCoy (Senior Construction Manager), Phone: 631-682-6212*

- **ThermoFisher Testimonial:** *Since joining the program, Cogent has become a great remote supporting supplier. Their headcount has increased as we've had the volume increase and they have been added to our Tier 1 category, along with increasing our diversity spend. Their leadership team is great to work with at both the high level and individually driving day-to-day operations – Zakhoury Adams (Associate Director), Phone: 484-460-6408*
- **New York City Housing Authority:** *Cogent currently serves as one of NYCHA's top vendors and has actively provided excellent Project Management services. This agency has assisted NYCHA in recruiting temporary staff, who demonstrate exceptional customer service and data entry skills.*

Cogent Infotech are courteous and professional service provider and is very responsive to our needs. They continue to showcase their efforts to fulfill open positions with qualified candidates and do an exceptional job meeting the required standards. The staff at Cogent has always been professional, cooperative, and proactive.

Without hesitation, I would recommend their services to anyone who is looking for a high-quality provider of temporary staffing services – Patricia Lindo (Assistant Director), Phone: +1 (212) 306-2807

These testimonials highlight the positive feedback and strong performance of Cogent in various aspects of its partnership with different clients, showcasing our capabilities and value as a partner.

1.9 SAMPLE PROJECT REPORT

Cogent is attaching the sample project report as separate attachment titled as “Cogent's Sample Project Report”

2 PROPOSED PROJECT METHODOLOGY

2.1 PROJECT EXECUTION PLAN

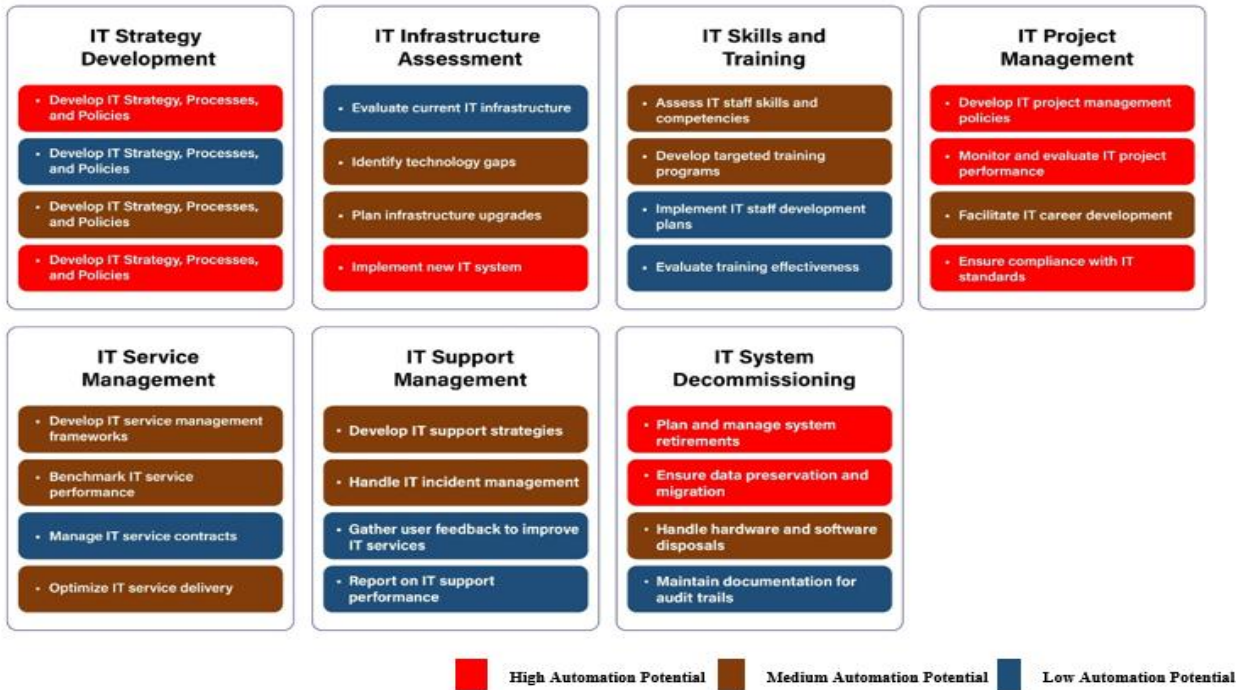
Cogent brings over **21 years** of experience in optimizing IT operations for municipalities, government agencies, and public sector organizations. Our team combines deep expertise in **IT process improvement, cybersecurity, disaster recovery, and operational continuity** with a proven track record of delivering measurable results. For North Richland Hills, we propose a tailored, data-driven approach to conducting the IT operational efficiency audit, ensuring alignment with the City's strategic objectives and operational needs. Our methodology emphasizes actionable recommendations, stakeholder engagement, and sustainable outcomes. By leveraging industry best practices, advanced analytics, and our proprietary framework for IT optimization, we will deliver a Work Plan.

PHASE 1: ORGANIZATIONAL AUDIT – ALIGNING IT WITH STRATEGIC GOALS

The first phase focuses on evaluating the IT Department's organizational structure, processes, and alignment with the City's strategic objectives. We will begin by conducting structured interviews with key stakeholders, including the **IT Director, department heads, and end-users**, to understand roles, responsibilities, and decision-making processes. These interviews will be supplemented by a comprehensive review of documentation such as **organizational charts, mission statements, vision documents, IT policies, and disaster recovery plans**. To ensure alignment, we will map the IT Department's mission, vision, and goals against the City's broader

strategic objectives. This includes assessing how well the department supports critical functions like **public safety technology, network infrastructure, and GIS systems**. Also, we will evaluate internal processes and workflows to identify inefficiencies, redundancies, or bottlenecks.

Cogent’s IT Operational Efficiency Heat Map: Visualizing Priority Areas for Process Improvement in North Richland Hills IT Department



Our proposed approach includes the use of process **heat maps – visual tools** that highlight areas of high complexity, resource drain, or inefficiency. These heatmaps will provide a clear, data-backed foundation for identifying opportunities to streamline operations, enhance communication, and optimize resource allocation. We will also assess the alignment of IT infrastructure components (e.g., computational resources, network infrastructure, cybersecurity measures, and cloud services) with current and future operational needs. Using a **scalability matrix**, we will evaluate the adaptability of the IT infrastructure to support evolving service delivery requirements, particularly as the City grows or adopts new technologies.

Deliverable: A comprehensive organizational audit report, including **visual process heatmaps and scalability matrix findings**, with actionable recommendations for improving alignment, processes, and infrastructure.

PHASE 2: STAFFING ANALYSIS – BUILDING A RESILIENT WORKFORCE

Cogent will conduct a detailed analysis of the IT Department’s staffing levels, technical expertise, and skillsets. Using **competency modeling**, we will benchmark the department’s workforce against industry standards and peer organizations. This analysis will identify skill gaps, redundancies, and areas where additional training or hiring may be needed.

A key differentiator in our approach is the integration of **predictive workforce analytics**. By analyzing historical data on service demands and projecting future trends (e.g., increased reliance on **GIS systems** or cybersecurity threats), we will recommend optimal staffing levels and a skill

mix that ensures the department can effectively meet its operational needs. We will also evaluate the feasibility of leveraging external partnerships, such as **managed service providers (MSPs) or service level agreements (SLAs)**, to address specific skill gaps without overextending the budget.

Deliverable: A staffing analysis report with **predictive workforce analytics, competency models**, and recommendations for optimal staffing levels and skill mix.

PHASE 3: PROJECT MANAGEMENT ANALYSIS – DRIVING ACCOUNTABILITY AND SUCCESS

This phase focuses on evaluating the IT Department’s project management methodologies, tools, and processes. We will assess the effectiveness of current practices in project planning, execution, monitoring, and closure using **project health assessments – a proprietary tool** that evaluates projects based on key metrics such as timeline adherence, budget compliance, and stakeholder satisfaction.

We recommend a hybrid project management framework that combines agile methodologies for iterative development with **traditional waterfall approaches** for large-scale projects to enhance project delivery and success rates. This framework will include templates, checklists, and governance structures to standardize project management practices across the department. We will also provide guidance on selecting and implementing project management tools that integrate seamlessly with the City’s existing systems, ensuring real time visibility into project performance.

Deliverable: A **project management assessment report, hybrid project management framework**, and tool recommendations.

PHASE 4: OPERATIONAL CONTINUITY AND DISASTER RECOVERY PLANNING – STRENGTHENING RESILIENCE

Cogent will conduct a comprehensive evaluation of the organization’s disaster recovery and incident response plans. Using **risk scenario modeling**, we will simulate potential disruptions (e.g., cyberattacks, natural disasters) to identify vulnerabilities in the IT infrastructure and test the effectiveness of recovery procedures. A standout feature of our approach is the **development of a tiered redundancy strategy**. This strategy prioritizes critical systems (e.g., public safety technology, network infrastructure) for failover systems and backup infrastructure, ensuring continuous operation during outages or disruptions. We will also identify single points of failure and recommend improvements to enhance system availability and resilience.

Finally, we will provide a playbook for incident response a step by step guide that outlines procedures for identifying, responding to, and recovering from IT incidents. This playbook will include role-based responsibilities, escalation protocols, and communication templates.

Deliverable: A **disaster recovery and incident response evaluation report**, tiered redundancy strategy, and incident response playbook.

PHASE 5: OPERATIONS AND SERVICE DELIVERY – ENHANCING CUSTOMER CENTRICITY

This phase focuses on assessing the effectiveness of services provided by the IT Department to city staff and residents. Using **service maturity assessments**, we will evaluate the maturity of key service areas such as **help desk support, network management, application support, and cybersecurity services**. This assessment will highlight areas where service delivery can be improved and provide actionable recommendations.

We will also conduct a **cost benefit analysis** of existing maintenance agreements for hardware, software, and cloud services. This analysis will identify overlapping coverage, redundant services, or opportunities for consolidation to optimize costs and improve efficiency. We will assess the organization’s software landscape to identify redundancies and inefficiencies, providing recommendations to standardize tools and platforms across departments.

Deliverable: A **service delivery effectiveness report, cost benefit analysis of maintenance agreements,** and software standardization recommendations.

PHASE 6: PROCESS IMPROVEMENT AND FUTURE STATE DESIGN – ENABLING SUSTAINABLE CHANGE

In the final phase, we will facilitate design thinking workshops with City staff to co-create future state processes. These workshops will focus on identifying process improvements and developing standard operating procedures (SOPs) that are practical, scalable, and aligned with the City’s operational needs.

A unique aspect of our approach is the **development of a change management roadmap**. This roadmap will outline strategies for **training, communication, and stakeholder engagement** to ensure smooth adoption of redesigned processes. We will also provide a performance dashboard template to monitor the implementation of process improvements and track key metrics such as cost savings, efficiency gains, and user satisfaction.

Deliverable: Standard operating procedures (SOPs), change management roadmap, and performance dashboard template.

TIMELINE OF THE PROJECT

Scope	Month 1	Month 2	Month 3	Month 4
Organizational Audit				
Staffing Analysis				
Project Management Analysis				
Operational Continuity and Disaster Recovery Planning				
Operations and Service Delivery				
Project Management Support/Reporting				

CITY STAFF ASSISTANCE REQUIREMENTS

- **Access to Documentation:** Provide all relevant documentation, including organizational charts, IT policies, disaster recovery plans, and maintenance agreements.
- **Stakeholder Availability:** Key IT personnel, department heads, and end-users must participate in interviews, focus groups, and workshops.
- **Validation of Findings:** Engage in validation sessions to ensure accuracy and completeness of our analysis.

- **Implementation Support:** Dedicate resources to execute high-priority process improvements during the implementation phase.
- **Regular Communication:** Schedule bi-weekly check-ins to discuss progress, address challenges, and ensure alignment with project goals.

By combining rigorous analysis, innovative tools, and collaborative engagement, we will provide actionable insights and a clear roadmap for enhancing operational efficiency, reducing costs, and strengthening resilience. Our commitment to excellence and our deep understanding of municipal IT challenges ensure that this engagement will deliver lasting value for the City roadmap that enhances service delivery, reduces costs, and strengthens resilience.

2.2 METHODOLOGY AND TOOLS

Cogent’s methodology is rooted in a structured, data-driven approach to conducting the operational efficiency audit of the City’s Information Technology Department. Our process leverages industry leading analytical tools, proven process improvement principles, and collaborative stakeholder engagement to deliver actionable insights and recommendations. The methodology is designed to address all tasks outlined in the RFP while ensuring alignment with the City’s strategic objectives and operational needs. We will utilize the following industry standard tools and methodologies:

Category	Tools & Techniques
Process Analysis	Visio, Lucidchart, BPMN (Business Process Model & Notation)
IT Service Management (ITSM)	ServiceNow, Jira, Zendesk
Data Analytics & Visualization	Power BI, Tableau, Excel Analytics
Project Management	Microsoft Project, Trello, Monday.com
Process Improvement	Lean Six Sigma (DMAIC), ITIL Framework, Agile Methodology
Security & Infrastructure Assessment	NIST Cybersecurity Framework, CIS Controls, SIEM tools

Below is a detailed description of our proposed methodology, including the analytical tools and techniques we will use, as well as how process improvement principles will be applied to identify and analyze operational inefficiencies.

DETAILED METHODOLOGY, TOOLS, AND TECHNIQUES

Data Collection and Analysis:

- **Structured Interviews and Focus Groups:** Engage with IT leadership, department heads, and end users through interviews to capture qualitative insights on roles, responsibilities, and challenges. Focus groups will help validate these findings and delve deeper into recurrent issues.
- **Document Review and Gap Analysis:** A thorough examination of existing documents (e.g., IT policies, disaster recovery plans) will be conducted. **Gap analysis** will pinpoint deviations from industry standards.
- **Process Mapping and Workflow Analysis:** Tools like **Microsoft Visio and Lucidchart** will be utilized to create process maps and flowcharts, documenting existing workflows and identifying inefficiencies through value stream mapping.

- **Benchmarking and Peer Comparisons:** Leverage tools such as **Gartner IT Score** for benchmarking against peers and industry standards to highlight performance gaps or strengths.
- **Quantitative Metrics and KPIs:** Data on metrics like **help desk response times** will be analyzed using tools like **Power BI**, aiding in the measurement and enhancement of process efficiency.

Advanced Analytical Techniques:

- **Risk Scenario Modeling:** Tools like **NIST Cybersecurity Framework (CSF)** will be used to simulate potential IT disruptions, assessing the robustness of response plans.
- **Predictive Workforce Analytics:** Statistical models and tools like **SAP SuccessFactors** will forecast staffing needs based on service demand projections.
- **Cost Benefit Analysis:** Financial impacts of different technological strategies will be evaluated using **Net Present Value (NPV) and Return on Investment (ROI) calculations**.
- **Heatmaps and Scalability Matrices:** These visual tools will identify high-complexity areas and assess IT infrastructure’s scalability to meet future demands.

Application of Process Improvement Principles:

- **Lean Six Sigma:** The **DMAIC (Define, Measure, Analyze, Improve, and Control) framework and value stream mapping** will be pivotal in identifying and eliminating inefficiencies.
- **Kaizen Continuous Improvement:** Facilitate **Kaizen workshops** to drive incremental and impactful enhancements.
- **Agile Methodologies:** Implement agile practices like **scrum boards and sprint reviews** to maintain flexibility and continuous improvement.
- **Change Management:** Employ the **Prosci ADKAR Model (Awareness, Desire, Knowledge, Ability and Reinforcement)** to ensure smooth adoption of new processes, focusing on awareness, desire, knowledge, ability, and reinforcement.

Task Specific Methodologies:

- **Organizational Audit:** Use **Balanced Scorecard methods** to align IT strategies with the City’s goals.
- **Staffing Analysis:** Assess and forecast IT staffing requirements using tools like **Occupational Information Network (O*NET) and predictive analytics**.
- **Project Management:** Evaluate and enhance project management practices using **the Organizational Project Management Maturity Model (OPM3) and hybrid methodologies**.
- **Operational Continuity and Disaster Recovery:** Enhance disaster preparedness through rigorous testing and strategy development.

2.3 PROPOSED TIMELINE (4 MONTHS)

Scope	Month 1 (M1)	Month 2 (M2)	Month 3 (M3)	Month 4 (M4)
Organizational Audit	Data Collection, Stakeholder Interviews	Process Mapping & Current-State Analysis		
Staffing Analysis		Role & Workforce Evaluation	Optimization Strategy Development	

Scope	Month 1 (M1)	Month 2 (M2)	Month 3 (M3)	Month 4 (M4)
Project Management Analysis	Project Identification & Governance Review	Process Efficiency & Risk Assessment	Implementation Strategy & Best Practices	
Operational Continuity & Disaster Recovery		Risk Identification & Resilience Assessment	Strategy Enhancement & Recommendations Draft	Final Report on Resilience Plan
Operations & Service Delivery		Service Efficiency & SLA Compliance Analysis	Optimization Strategy Formulation	Final Service Delivery Optimization Report
Project Management Support/Reporting	Framework Establishment	Progress Tracking & Stakeholder Reporting	Finalizing Implementation Roadmap	Final Project Review & Closeout Presentation

KEY FEATURES OF THE TIMELINE

1. Efficient Phasing:
 - The project is divided into four distinct phases to ensure logical progression from discovery to implementation.
 - Each phase has clear objectives, tasks, and deliverables.
2. Parallel Activities:
 - Tasks such as organizational analysis and service delivery assessment are conducted concurrently where possible to save time.
3. Milestones for Accountability:
 - Key milestones are defined at the end of each major task to track progress and ensure timely completion.
4. Deliverables for Transparency:
 - Deliverables are clearly outlined for each phase to ensure transparency and alignment with stakeholder expectations.
5. Implementation Focus:
 - The final phase includes hands-on implementation support, ensuring that recommendations are actionable and practical.

2.4 DELIVERABLES

Cogent will deliver a structured and data-driven IT Operational Efficiency Audit for the City of North Richland Hills, providing key deliverables to enhance IT performance, security, and governance. The Current State Assessment Report will evaluate IT workflows, infrastructure, staffing, and service delivery, identifying inefficiencies and benchmarking performance against industry standards. The Gap Analysis Report will pinpoint operational challenges, security risks, and compliance gaps, providing actionable insights for process optimization. The Future State IT Roadmap will define an optimized, scalable IT framework with streamlined workflows, automation strategies, and technology upgrades. The Implementation Plan and KPI Dashboard will present a phased execution strategy with measurable performance indicators to track improvements. The Executive Summary and Final Presentation will consolidate findings and recommendations for leadership decision-making. The Process Automation Strategy Report will focus on integrating IT service management (ITSM) solutions to enhance efficiency and reduce

manual workload. The IT Governance and Risk Management Framework will strengthen cybersecurity, disaster recovery planning, and compliance with regulatory standards, ensuring long-term resilience. Through these deliverables, Cogent will provide the City with a clear, actionable strategy to improve IT operations, optimize costs, and ensure sustainable IT governance.

3 PROPOSED PRICING

Scope	Estimated Efforts (Hours)	Cost (not-to-exceed)
Organizational Audit	160	\$17,920.00
Staffing Analysis	120	\$13,440.00
Project Management Analysis	150	\$16,800.00
Operational Continuity and Disaster Recovery Planning:	120	\$13,440.00
Operations and Service Delivery	160	\$17,920.00
Project Management Support/Reporting	250	\$27,280.00
Total	960	\$106,800.00

4 REQUIRED QUALIFICATIONS

RFP Qualification Requirement	Cogent Infotech Corporation's Response
<p>a. Be a firm, corporation, individual, or partnership normally engaged in the provision of the services as specified herein.</p>	<ul style="list-style-type: none"> ✓ Cogent Infotech Corporation is a nationally recognized IT consulting and staffing firm established in 2003. ✓ Specialized in IT operational efficiency audits, process optimization, and technology transformation for municipal, state, and federal agencies. ✓ Certified firm: ISO 9001, ISO 27001, and CMMI Level 3 appraised for quality and security standards.
<p>b. Have adequate organization, facilities, equipment, and personnel to ensure prompt and efficient service to the City.</p>	<ul style="list-style-type: none"> ✓ 500+ full-time IT professionals, including business analysts, cybersecurity experts, IT project managers, and cloud architects. ✓ Nationwide presence with offices in Texas, Pennsylvania, Virginia, California, Florida, and New York, ensuring onsite & remote support capabilities. ✓ Advanced tools and infrastructure: AI-driven analytics, ITSM software, automation platforms, cybersecurity auditing tools, and cloud-based reporting systems. ✓ Proven ability to deploy specialized teams within weeks for municipal projects.
<p>c. Have demonstrated knowledge of municipal IT operational processes and ways to improve or redesign processes.</p>	<ul style="list-style-type: none"> ✓ Extensive experience working with municipal agencies, counties, and government entities to optimize IT operations. ✓ Specialized in IT workflow optimization, cybersecurity audits, enterprise software enhancements, cloud transformation, and IT governance improvements. ✓ Previous municipal and public sector clients include: <ul style="list-style-type: none"> - Dallas Fort Worth International Airport (DFW) – IT process automation, infrastructure audits. - New York Power Authority (NYPA) – IT governance restructuring, cybersecurity improvements. - Tarrant County, TX – Agile IT service optimization, cloud migration strategy. - City of Sacramento, CA – IT workflow automation, municipal service digitalization. - Amtrak – IT service management transformation, data governance improvements.
<p>d. A minimum of three (3) years of successful operational process review and improvement.</p>	<ul style="list-style-type: none"> ✓ Over 21 years of experience in IT consulting specializing in IT operational process improvement for government agencies. ✓ Proven experience in conducting operational process reviews & improvements: <ul style="list-style-type: none"> - DFW Airport (2018 – Ongoing): IT workflow automation, reducing downtime by 30%. - NYPA (2019 – Ongoing): Digital transformation, data governance optimization. - Tarrant County, TX (2019 – Ongoing): ITSM enhancements, reducing incident response time by 40%. - City of Sacramento, CA (2020 – Ongoing): Municipal IT service standardization. - Amtrak (2019 – Ongoing): Security and compliance upgrades, IT governance improvements.

SIGNED ADDENDUM ONE

Acknowledge receipt of this addendum by inserting this page with your RFP response.
This addendum form is a part of the contract documents, and it so modifies, amends, deletes
and/or adds to the original RFP document.

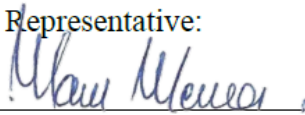
Name and Address of Company:

Cogent Infotech Corporation

1035 Boyce Road, Suite 108,

Pittsburgh, PA 15241

Authorized Representative:

Signature: 

Name: Mr. Manu Mehta

Title: President

Phone: (412) 246-0708

Email: manu.mehta@cogentinfo.com

5 APPENDIX A**5.1 RESUME MEGAN KELLEY – PMP, PMI-ACP, SCPM, SCM, MBA****IT AUDIT MANAGER (PROJECT MANAGER)****Professional Summary:**

- Ms. Kelley is a technically sophisticated analyst, planner, developer, and leader highly skilled in providing overall management of PMOs and project portfolios for a wide range of government and private entities. Dynamic and focused on identifying and addressing business needs, introducing technical solutions, tools, and systems that enhance operational quality, productivity, data sharing, communication, training, and cost effectiveness. Expertly drive all project phases from concept, planning and acquisitions to design, development, testing, quality control / assurance, implementations, documentation, and training. Strong communicator with all levels of technical specialists as well as management and clientele.

Technical Skills:

- Project Management Office (PMO)
- Project/Program/Portfolio Management
- Client Relations / Needs Analysis
- IT / IS / Telecom Products & Services
- Client Relationship Management
- Regulatory Compliance
- Agile/Scrum Methodology
- Sr. Requirements Analysis
- Full Project Lifecycle Management
- PMI Mentor/Protégé Program Mentor
- ServiceNow and Remedy Ticketing
- Network Architecture/Installation
- Provider Integration
- Cloud/Virtual Services
- Data Center/Help Desk Supervisor
- AWS migrations
- SharePoint Development
- SharePoint Administration
- Policies / Procedures Development
- Financial Analysis / Control
- Staff / Trainer Training
- Audits / Certifications / Accreditations
- Section 508 SME
- Test Management
- Expert Level Technical trainer for MS SharePoint, MS Project and Section 508 Compliances
- Workfront and JIRA Admin
- Asset Management
- Risk Analysis
- Proposal/Technical Writing
- Data and VM Migrations

Education:

- Master of Business Administration, American Intercontinental University
- Bachelor of Science in Management – Magna Cum Laude, Park University, Fort Myers, Virginia

Certificates:

- Stanford Certified Project Management (SCPM), Stanford University, California
- Project Management Professional (PMP) PMI
- Agile Project Management (ACP) PMI

- Certified Scrum Master (CSM)
- VITA PM Certification
- Nintex Process Automation Practitioner – Nintex Workflow Cloud
- Nintex Process Automation Practitioner – Office 365
- SCRUM Immersion – PMI

CLEARANCE:

- Security Clearance: DoD Secret (inactive), FBI TS / (inactive), DIA: SCI (inactive), TS / NATO (inactive), DHS HQ / CBP / USCIS Suitability (inactive)

Additional Coursework:

- ISO 9001:2000 Certified Internal Auditor
- ISO 27001
- DoD SharePoint Site Owner Certification
- DoD SharePoint User Training
- DoD NATO Certification
- SCRUM Skillsoft Coursework (20 hrs)
- FEMA Certifications for IS-00700 / IS-00800 / IS-00100
- Operations Security
- Anti-Terrorism Force Protection Level 1
- Privacy Act Awareness
- Selenium IDE/Browsemall coursework
- JIRA coursework
- Visual Studio coursework
- Information Assurance Awareness
- Counter-Intelligence Awareness and Reporting (CIAR)
- SharePoint Designer 2010: Levels 1 & 2
- SharePoint 2013 Designer
- InfoPath Designer 2013
- Dashboard Designer 2013
- Advanced Office 2013
- FISA Standards
- ITIL V3.0 Certification prep
- CISSP Certification prep
- ISTQB Certification prep
- Agile Training for PMI-ACP
- Powershell training
- Workfront Administrator
- Power Platform Training
- Salesforce Training
- Scrum Master Course

Military Training / Courses:

- Army 88M School, Camp Eustis, VA
- NCO Leadership Course, USMC Leadership School, MCLB Albany, GA
- Office Automation Certificates, Coleman Computer Tech College, Escondido, CA
- Personnel Administration School Certification, USMC Administrative School, Camp Lejeune, NC
- Planned Certification Training: Current Training: PL-900 Power Platform, Azure Fundamentals, CBAP
- 2025 Training: Azure Architecture, Azure Administrator, PHR, SPHR, ASQ / CMQ, CKM, ITIL, CISSP, ISEB; ISTQB, CISA; CISM, MCSD, MCP

Professional Experience:**COGENT INFO (9/16/2024 – Present)****Role: SharePoint Modernization Consultant/Sr. PM**

- State of Vermont Department of Transportation. SharePoint Modernization project consultant. Created more than 50 training documents for Basic Users, Power Users, Site Owners, Super Users and Site Collection Admins. Migrated over 280 SharePoint sites from classic to modern ensuring all Power Automate, Forms and

content using ShareGate. Redesigned to Hub and Spoke for Intranet, Documentation, and Project Hub with multiple spokes. Drafted all project documents. Establishing Governance, Community of Practice and automations of multiple manual tasks.

LIVANTA, REMOTE NIGHTS/WEEKEND POSITION (9/23/2023 – 6/28/2024)

Role: Atlassian JIRA Admin/SharePoint/Teams Engineer Help Desk/Sr PM (Nights/Weekends/EST hours). ; Internal Help Desk support (nights/weekends/EST hours).

- Support Infrastructure projects as their dedicated Project Manager: gathering requirements and business analysis; creating testing scripts; and performing technical training documentation for all projects. Primary role was administrator for Atlassian JIRA Software, JIRA Service Management, Confluence, SharePoint Cloud Admin, Teams Admin and Implementation. I also worked as Sr. Project Management designing new processes and reviewing SDLC documentation to redesign the JIRA Project Software screens, workflows and interactions with Confluence. In addition I worked on all JIRA, OneDrive, SharePoint issue. I was a valued member of the ICTF Task Force regarding all Tools used by Livanta and created numerous training documents. I worked with ISO 27001 and CMMI audits. Worked on Atlassian JIRA Service Management; JIRA Software Management; Confluence; DelTek; and ServiceNow.

RADGOV (1/22/2024 – 4/19/2024)

Role: Sr. Project Manager (Temporary)

- VDOT Planning Project Management (Contract), TM-ESS Dot Net and Miscellaneous Technologies upgrades project and HR Works Legacy migration. Successfully passed VDOT PM coursework. Developed Gate review documentation; checklists; presentation materials and miscellaneous project management activities. Worked with CRMs, Enterprise Architects and other key personnel to migrate projects from planning to execution. Worked on Project Server; SharePoint Planner; Teams; and custom applications.

UST, REMOTE POSITION (5/17/2023 – 12/4/2023)

Role: BPaaS Product Manager/SharePoint Admin/Sr. PM; ADVANTASURE. SR. PROJECT MANAGER (Contract)

- Managed the BPaaS clients Change Requests. Change Requests ranged from data changes, new fields to full projects from the governing agency for regulatory changes in Medicaid/Medicare such as Real Time Messaging of BlueCard. Assigned as the PMOs SharePoint Administrator for all PMO SharePoint. Was the primary Trainer, Mentor and documented all Client funded change request process documents. Facilitated the beginning part of a trade off study comparison for the UST Timesheet versus the Planview PPM Pro tool for cost savings opportunities. JIRA management for Project Change Requests. UST acquired Advantasure and cut all contractors and most US based resources by end of 2023 to achieve more cost savings for the company.

CBTS CONSULTING, REMOTE POSITION (1/8/2020 – 9/1/2023)

Role: Sr. PM/Sr. SharePoint Specialist/Azure SP Admin; GE AVIATION. SR. PROJECT MANAGER (Contract)

- Managing cloud migrations for AWS for Virtual Machines (VM), NAS, and gateway data migrations. Working with customers to facilitate new VMs and migrating legacy physical servers to cloud. Documenting and creating training and presentation materials for all Project Managers. Facilitation of govcloud content. Conducting new employee training and mentoring. ISO 27001; Daily Scrum sessions and weekly touchpoints for each site across the US. Facilitating support for offshore migrations of public sites. ServiceNow ticket management. ServiceNow project facilitation and ATF for application deployments. Worked on Atlassian JIRA Service Management; JIRA Software Management; Confluence; Box; Smartsheets; PPM Pro; Power BI; and ServiceNow.

SYNCHRONY FINANCIAL.

Role: Tier I Help Desk Support Lead.

- Managing onshore and offshore Tier I SharePoint and MS Teams tickets to ensure each support resource has an equal number of tickets. Facilitating customers Service Now tickets for Nintex and SharePoint issues. Act as escalation for other Tier I team members. Liaison between server admins and Tier I support. Building customer and Tier I training documents. Facilitate Tier I training and OneNote materials to make sure all Tier I support team members can provide same level of service. Provide metrics to senior executives on non Service-Now customer requests. Working with PMs, PMO and Users on how to hook-in or purpose of Workfront in Marketing PM. Supporting PMO dashboard development. Act as PM/BA requirements gathering for Special Projects. Azure level SharePoint Admin working within Teams, O365 account issues, Active Directory and OneDrive. Worked on both SharePoint on-premise and O365 products. Worked with migrations from on-premise to O365 platform. ServiceNow project facilitation and ATF for application deployments.

SLAIT CONSULTING, REMOTE POSITION (3/13/2018 – 3/31/2020)

Role: Sr. SharePoint Developer/Azure Admin/PM SME/Portfolio Manager (Contract)

- ANTHEM INC. In charge of all O365 and on-premise Voyager2020 transition SharePoint site collection administration; ISO 27001. Creating new site collections, sites and sub-sites in O365 and on-premise environments; developing all new workstream sites; lists; libraries; workflows and migrating data to offshore testing site collections. User Management of all SharePoint users. NDA facilitation. Nintex workflows, InfoPath forms. 24/7 Help Desk support of all vendor, anthem and partner corporations' issues involving SharePoint. Liaison with MS Premier Support. Completed all development and transition to facilitate the new IngenioRx company which dealt with Medicaid, Medicare and BCBS claimants. Onshore support for Ingenio on all things Medicare/Medicaid within the IngenioRx tenant due to offshore access restrictions. 12 TB Azure E3/P1 environment. Workfront administrator. Trained and facilitated Project Management training for Workfront Leads. Trained how to use Workfront. Act as Workfront Admin for Anthem and IngenioRx staff. Help Develop and implement a Marketing Project Management templates on Workfront. Global Admin for Full IngenioRx tenant within O365. Worked with Security resource to maintain all aspects of the O365 platform and tenant administration acted as single POC for all things SharePoint Online. ServiceNow project facilitation and ATF for application deployments. Worked on Atlassian JIRA Service Management; JIRA Software Management; Confluence; Workfront; and ServiceNow.

THE BUFFALO GROUP, DEPARTMENT OF HOMELAND SECURITY

RESTON, VA (4/25/2018 – 6/30/2018)

Role: Sr. SharePoint Developer/PMO (Contract)

- Developed Buffalo Group home site and maintained new SharePoint site development. Supported SharePoint training. PMO Dashboard development. PM support. Developed technological architecture recommendation documents for azure security and customer portfolio dashboarding. Worked with Salesforce integrations. Develop PMO dashboards and support Project Managers with PM recommendations and processes within Agile. Required surgery so unable to continue working 2 jobs. Worked on both SharePoint on-premise and O365 products. Worked on Atlassian JIRA Service Management; JIRA Software Management; Confluence; Salesforce; Tableau; and ServiceNow.

DAYZIM, US MARINE CORPS CAMP PENDLETON, REMOTE POSITION (EVENINGS) (12/04/2018 – 12/14/2018)

Role: Sr. Project Manager (Contract)

- Short term support for Windows 10 migration for installers. Developed a standard status report excel template and conducted nightly reporting.

SC3, US DEPARTMENT OF ARMY

FORT BELVOIR, VA (12/18/2017 – 3/13/2018)

Role: Product Manager/Salesforce/Sr. SharePoint Developer (Contract)

- Worked on contract bridge waiting on new contracting firm. Assigned to Help Desk Tier II support of existing SharePoint sites and management of minor updates allowed during the contract bridge. Supported Salesforce dashboards. Worked on SharePoint on-premise products. ServiceNow project facilitation and ATF for application deployments. Worked on Atlassian JIRA Service Management; Confluence; Salesforce; Tableau; and ServiceNow.

TYGART

Crystal City, VA (3/13/2017 – 12/31/2017)

Role: Sr. SharePoint Developer/Sr Project Manager (Contract)

- FBI and PBGC. Designed and developed cloud based SharePoint Scheduling tool to assist in the installations for Windows 10 Upgrade project. Developed communications material. Coordinated with end users to ensure timely scheduling of their Windows 10, Office 2016 and SharePoint 365 suites. Developed multiple FAQ and end user support guides and helpful training in support of Windows 10. Troubleshooting Cloud SharePoint 365 issues and worked with Service Desk to resolve SharePoint issues and outages. Identified and developed Business Change document for identified Microsoft patching issue resolution. Supported Portfolio Management Tool SharePoint initiative. Day to day management of multiple SharePoint environments; Section 508 testing and compliancy, Development of Workflows, InfoPath forms, Pivot Tables and Business Intelligence Center tools such as Reporting Services. Worked with Salesforce integrations. ISO 27001, SOP development, Agile Dashboard facilitation and automation to recreate JIRA like environment within SharePoint. Requirements analysis for new development initiatives. Tygart lost contract. Worked on both SharePoint on-premise and O365 products as well as migrations to the AWS platform (O365 Azure on Virtual

Network). Worked on Atlassian JIRA Service Management; Confluence; Salesforce; Smartsheets; and ServiceNow.

AMPCUS**Chantilly, VA (11/17/2016 – 3/10/2017)***Role: Sr. Project (Product) Manager (Contract)*

- Pepco Holdings. Temporary support while Project Manager is attending terminal mother. Project Management coordination of 5 developer, 1 tester, 1 Business Analyst provisioning the transformation from Lotus Notes forms and applications to SharePoint 2013. Coordinated developers cloud architecture and test bed for automated tools Proof of Concepts. Coordinated end customer administrative access. Performed customer and stakeholder requirements gathering sessions. Developed SharePoint technologies training. Worked with Salesforce financial modules. Created CMMI level 4 templates and provisioned Portfolio Management Portal dashboard within SharePoint 2013 cloud infrastructure. Day-to-day facilitation of customer and senior executives from Pepco and Exelon.

CKA LLC, HQ Department of the Army, CCSA**Dulles, VA (10/17/2016 – 11/07/2016)***Role: Deputy Program Manager/JIRA Admin/ServiceNow Admin (Contract).*

- Temporary support to bring help Program Manager catch up on workload. Conducted day-to-day operations of O&M staff of 40 while Program Manager dealt with engineering requirements. Managed customer expectations, Supported Human Resource activities, Weekly status updates of over 75 projects and attended customer meetings. Supported provisioning of CMMI level 4 deliverables. ServiceNow project facilitation and ATF for application deployments. Worked on Atlassian JIRA Service Management; JIRA Software Management; Confluence; DelTek; and ServiceNow.

TECHNICA CORPORATION**Dulles, VA (8/2015 – 7/22/2016)***Role: Sr PM/Product Manager/Sr Requirements Analyst/Sr Tester (Contract)*

- FBI Behavioral Analytics Unit 4 Adult/ViCAP. Responsible for Bug identification; daily audit and error log review and analytics; JAD Board facilitation; recommendations for enhancements, fixes, and new technologies; Project management activities for new development environment within FBI internal Cloud; facilitation and interaction with CJIS Operations (to include SA, DBA, and infrastructure tickets). Development of User Guides, training and project documentation to include but not limited to Configuration Plan, Master Test Plan, Testing scripts, and architecture documentation. Support SharePoint users with advance development efforts for Business Intelligence Center, Pivot Table, Performance Point, Excel Services and general page layouts. Identify new and existing bugs, record keeping within JIRA ticketing system for JAVA/JQuery web application and SharePoint sites. Facilitation for cloud environment set up, research on SOLR technologies. Facilitated transition of new development, staging and production in the Justice Cloud. Facilitate ViCAP trouble tickets for local, state, and federal law enforcement and case support. Additional Agile PM support as required. Worked within Subversion (SVN) Versioning software. Developed MS Project Schedules; conducted project management analytics, developed Quad and project reports for Scope, schedule, resources, requirements, issues and risks. Developed Project specific policies, processes and methodologies for cloud application and development environment. Provided mentorship for SharePoint and Project Management related skills as needed. Worked on Atlassian JIRA Service Management; JIRA Software Management; Confluence; Peoplesoft; Tableau; and ServiceNow.

Key Contributions:

- Responsible for the identification of multiple critical bugs and researched root causes for several areas within ViCAP application that would have resulted in full application failure.
- Project Management efforts which lead to the procurements, facilitation and support of infrastructure applications that were unable to be provisioned in a timely manner
- Cross-team facilitations for SOLR and VM migration from FAST Linux based solution.
- Support Directors Office with new SharePoint Business Intelligence Center, Excel Services, and Pivot Table development and responded to architectural requirements.
- Learned and developed training handbooks for over 6 new applications within 1 months' time on top of normal job duties. SQL Fundamentals and Advanced Querying, Browsesmall, Selenium IDE, etc.

SRA**Chantilly, VA (8/2014 – 8/2015)**

Role: Product Manager/Technical Research & Analytics Manager/SharePoint Administrator/Proposal Development (Contract)

- Trail-blazed the FBI Enterprise Data Analytics Section and IT Applications & Data Division (ITADD) Content Administration for redesign, development, and implementation of the SharePoint 2013 across multiple SharePoint architectures. Supporting the OTD Lead Content Administrator in migrating SharePoint and CRM sites into the new SharePoint 2013 platform. Master Page modifications workarounds due to limited permissions by using JQuery, HTML and ASP.net snippet codes. Collecting page layout approval from Branch level resources. Developed multiple automated data calls workflows for Senior Management. Worked with Salesforce. Created the FBI's 508 training documentation utilized for Web Development of Applications, SharePoint and 508 compliant documentation. Conducted enterprise wide training for both SharePoint and 508 across FBI HQ IT Branch. Developed multiple Surveys, InfoPath Designer 2013 forms, and workflows for Security. Designed and developed Project Management Plans; Requirements Management Plans and Design Document templates for FBI Agile SharePoint projects. Acts as liaison between OPA, Branch and Help Desk resources. Conducted advanced SharePoint training to User, Site Owner and Content Managers across the Division. Developed SOPs for new Divisional processes. Created multiple SharePoint sites for customized Programs. Acted as Section 508 Subject Matter Expert. Developed MS Project Schedules and analyzed utilization of MS Project Servers within SharePoint 2013 environments. Worked with SRA Corporate on developing SharePoint Community of Practice training. Worked on Atlassian JIRA Service Management; JIRA Software Management; Confluence; Peoplesoft; Tableau; and ServiceNow.

Key Contributions:

- Created baseline communications and training for SharePoint 2013 and Section 508 utilized across FBI.
- Designed and Developed Operational Dashboards and Executive Management external data source reporting utilizing SharePoint 2013 Business Intelligence Center. Developed prototype SharePoint 2013 Business Intelligence Center Dashboard for automated Portfolio Management Office utilizing full PMBOK, CMMI and ISSO best practices using project templates, processes, workflows, and policies that I created in line with CMMI level 4 process improvement methods.
- Conducted wide scale data streamlining across multiple platforms for data optimization eliminating over 1 Terabit of outdated documentation.
- Managed, maintained and implemented SharePoint 2013 for over 100 Divisional sites, 1200 web pages, and managed over 1TB of documents
- Migrated Divisional SharePoint assets from SharePoint 2010 to 2013 and Developers through the migration of Office 2013. Identified multiple critical bugs during Beta testing.
- Manage and conducted basic to advanced training to all Divisional Site Owners, 130 Content Managers on SharePoint 101 and Section 508 training.
- Developed PMO standards and the dashboard/website displays within SharePoint 2010/2013 for Budget, Schedule, Scope, Risk, Change, Issue, Task, Personnel, Quality and Inventory Management. Automated the majority of manual Portfolio reports for streamline executive management near real time visibility.

INSIGHT GLOBAL INC.

McLean, VA (2/2014 – 8/2014)

Role: Project (Product) Manager/Portfolio Subject Matter Expert/SharePoint Development/Proposal Development (Contract)

- Delivered expert project management services to clients: Freddie Mac – IT Security, MITRE Corporation – Corporate Communications & Public Affairs. Orchestrated design and development of multiple new PM Portal SharePoint sites that encompassed methodologies; risk management; change requests; workflows; project management support; system migrations; and creation of online tools. Managed the Migration from SharePoint 2007 to 2013 of all sites working with each site stakeholder to identify all issues, risks, workflows, custom development or code unique to their site. Developed and conducted all training for beginner, intermediate and advanced SharePoint users. Facilitated all Help Desk requests and reporting. Worked diligently coordinating with the Community of Practice users to ensure continuing training and support once contract was completed and supported modification of their charter to allow for an increase in their scope and funding.

Key Contributions:

- Positively impacted project management practices with the design of portfolio PM methodology dashboards, workflow, roadmaps, controls, and communication strategies.
- Minimized ramp-up time of new project managers with the creation of comprehensive training program covering topics highlighted throughout leadership surveys.

- Elevated end-user performance on a global level by collaborating with all levels of staff and management in the establishment of new policies, processes, and training tools.

ASD**Pentagon, VA (8/2013 – 11/2013)***Role: ITIL Problem Manager/JIRA Admin (Contract).*

- Assigned to DoD Joint Chief of Staff to provide overall outage management, including preventative maintenance impact assessment / audits, trend remedy ticket analysis, long-term solutions development, PMO support, outages briefings, and cross-functional training. Worked with Project Server and SharePoint 2010/2013 front end and back end. Supported a team of Knowledge Engineers and Project Managers for PMO skills and training expertise. Acted as a IV&V Quality Gate for all Operations Change Management activities as a part of their internal Change Control Board efforts. Ensured review of all Procedures, Policies, Processes that impacted Operational Readiness for optimization capability and coordinated with stakeholders for effective changes to ensure process improvement. Worked on Atlassian JIRA Service Management; JIRA Software Management; Confluence; and ServiceNow.

Key Achievements:

- Minimized outages and potential threats through innovative troubleshooting and introduction of process improvements to enhance assets and configuration management.
- Generated significant advances in problem management platforms through development and rollout of documentation as well as workflow, status reporting, quad chart analysis, project management, and support plans.
- Mentored Project Managers and Project Staff for Risk, Scope, Schedule, Quality, and Issue Management
- Conducted monthly training sessions

MYMIC / INSIGHT GLOBAL INC.**Pentagon, VA (5/2013 – 8/2013)***Role: ITIL Knowledge Engineer/Azure SharePoint SME/PMO (Contract)*

- Charged with DoD Joint Chief of Staff contract focused on the completion as well as implementation of NATO, SharePoint User, and Site Owner courses to comply with DoD access regulations. Recommended process improvements, communication plans, automation opportunities, status reporting, problem resolution procedures, training tools, IT solutions, data management enhancements, knowledge management sites, and support blogs / chat rooms. Worked with Project Server and SharePoint 2010/2013 front end and back end. Supported a team of Knowledge Engineers and Project Managers for PMO skills and training expertise. Developed Program Reports for Joint Staff Executive Management for display on SharePoint sites in relation to multiple General or Congressional Data Call Change Requests, many times having to review and analyze full regulations and compliancy policies for issues or conflicts with directives. Worked on Atlassian JIRA Service Management; JIRA Software Management; Confluence; and ServiceNow.

Key Achievement:

- Facilitated training and development of Knowledge Engineers and Quality Control Specialists through new instructional programs (including train-the-trainer), policies, and procedures.
- Accommodated staff reductions in timeliness for check-in / check-out process through implementation of changes and improvement plans.
- Developed PMO standards and the dashboard/website displays within SharePoint 2010/2013 for Budget, Schedule, Scope, Risk, Change, Issue, Task, Personnel, Quality and Inventory Management.
- Developed training for Project Managers and Knowledge Engineers on Requirements, Testing, Knowledge Management Sharing, SharePoint 2010/2013, Customer Relationships, and Issues/Risk Traceability

LOCH HARBOUR GROUP**Washington DC (9/2012 – 5/2013)***Role: Senior Project (Product) Manager/Proposal Manager/ Subject Matter Expert (Contract)*

- Directed SharePoint development and operations maintenance for customer's CIO – DHS S&T. Created timelines, schedules, and SharePoint Agile task dashboard. Performed needs assessment, proposal preparation, testing, design development, future upgrades planning, and policies / procedures development. Handled status reports. Organized user acceptance testing; coordinated releases and prepared user documentation. Provided risk assessments and problem management / resolution.

Key Contributions:

- Developed Enterprise level Communications and Program Plans and Policies for customer approval

- Provided support, mentoring and training facilitation for Project Managers for Agile methodologies and processes/procedures/templates. Developed modified templates in line with clients methodologies and practices for Agile project management. Integrating the key stakeholders to be part of each SCRUM review to minimize Scope creep and increase customer satisfaction.

SCI GROUP**Reston, VA (2/2012 – 8/2012)***Role: Acquisition Consultant / Project (Product) Manager and Subject Matter Expert (Contract)*

- Supported NTT Data / DHS CBP in overall IV&V as well as acquisition of IFT program. Key expert in project lifecycle management, training program development, acquisition presentations, and overall documentation in configuration management, quality assurance, and risk management. Counseled team members in regulatory compliance, project leadership, and strategy planning.

CORTECH**Reston, VA (8/2011 – 1/2012)***Role: CRM Program Manager (Contract)*

- Spearheaded redesign, development, and implementation of Customer Relationships Management customer-facing portal and Wiki for Sprint. Analyzed and revised process documentation for all units interacting with CRM group. Created training guides. Designed and authored the first external quarterly newsletter for CRM organization and presented it to the company's IP executive management team.

IMTAS**Washington DC (12/2010 – 8/2011)***Role: Senior Project (Product) Manager/Proposal Development/Portfolio SME (Contract)*

- Assigned to the FBI to provide expert development of program / process documentation as well as monthly PMRs, weekly quad report maintenance, and integrated master schedule and sub-schedules. Created Portfolio Management standards in line with PMBOK, CMMI and ISSO quality standards. Developed Requirements for internal Portfolio Management tool utilizing information from the MS Project Servers, Performance Point, Timesheet, and Contractors Performance systems to provide Director of FBI with full Portfolio Management level visibility for Cost, Scope, Schedule, Issues, Risk as requested.
- Additional contributions included creation of portfolio dashboard, reviewed and recommended updated project management policies / procedures, Cloud technology evaluations, requested to be the FBI's PMI representative liaison for PM training, developed PMP presentations, PM workbooks, training programs, portfolio metrics, R&D plans, and feasibility analysis. Completed trade-off studies of COTS and telecommunications equipment.

ADDITIONAL CONTRACTS:

- **ASI Government – Senior Portfolio Manager Consultant (9/2010 – 12/2010):** Provided US Aid with management of project managers, engineers, and testers. Mentored, Managed and Trained over 10 Project Managers. Prepared all templates and designed Potfolio Management audit documentation, developed automated tools, and provided staff mentoring and acquisition support.
- **Macro Solutions – Senior Project (Product) Manager Consultant (6/2010 – 8/2010):** Provided assigned customer DIA with project, quality assurance, and configuration management expertise with a strong focus on QA / CM functions.
- **RAC Management – Senior Project (Product) Manager (4/2009 – 6/2010):** Serviced multiple customers (DIA / RACMS Corporate) in project and testing management. Led creation of contract management system technical requirements, training programs, automation plans, and compliance as well as QA / QC documentation.
- **ACE Info Solutions – Senior Project Manager (5/2007 – 4/2009):** Delivered expert project management services to customers, including Ace Corporation, USDA, FAS, USDA FSA, ATF, EPA, and DHS. Provided PMO, project, program, portfolio support, QA, ISO auditing, implementations, requirements, certification & accreditation, best practices, documentation, and training management. Single handedly stood up full USDA PMO to include policies, procedures, processes, websites, training, templates and guides within 6 months (over 110 technical documents and guidelines for the PMO to choose from dependent on which of the 4 programs the project fell under).
- **InDyne Inc. – Senior Project (Product) Manager (6/2006 – 5/2007):** Assigned to provide NASA Headquarters with project and program management support of over 50 simultaneous project initiatives. Led QC / QA, requirements gathering, regulatory compliance, vendor audits / evaluations, procurement, portfolio management reporting, and training. Completed all projects on time and within budget. Facilitated implementation of MS Project Server.

- **AT&T, Government Solutions – Program Manager (7/2005 – 6/2006):** Delivered expert program and project management to USMC and AT&T GSI. Managed special projects, portfolio analysis, proposal development, requirements gathering, QA / QC, IMS / WBS design and maintenance, staff coordination, training, evaluations, and knowledge management. Marine 4 Life Website; MCCDC Portfolio Management
- **Pelican Technologies – Product/Test Manager (6/2005 – 7/2005):** Provided the Federal Reserve Bank with testing documentation, process development, and staff management focused on Financial, Benefits, and Credit Card systems.
- **Dynamic Animation Systems Inc. – MATREX Program Analyst (3/2004 – 6/2005):** Assigned to Customer DoD (Joint Virtual Battlefield Next Generation) MATREX M&S Program.
- **Lockheed Martin – Senior Project Planner / Project (Product) Manager (10/2003 – 3/2004):** Serviced customer DISA Computing Services on the SIPR/NIPR Implementation program.
- **M.J. Kelley Consulting Inc. – Program Director (8/2000 – 12/2002):** Assigned to Kristin Brooks Hope Center’s Technology Enhancement Program focused on the organization’s 1-800-SUICIDE Hotline Evaluation Linkage Project (HELP).
- **Project Management Institute – Special Projects Director (7/2000 – 2/2003):** Volunteered services in Quality Help Desk, High Tech, and Cross-Functional Task management.
- Prior experience includes **military roles in Transportation and Operations Management – US Army National Guard, and Personnel Management – US Marines, HQMC.**
- Prior experience includes **Security Guard roles in American Security Programs (DCJS #107738) Unarmed (Active 2/2016) & Armed (Expired 2014)**
- Also served in **temporary project leadership roles for PEC Solutions Inc. – US Patent & Trademark Office SIRA, Kelly IT Services – Booz / Allen / Hamilton, Arrowhead Space & Telecommunications – Embassies / DoD / Corporate, Cayenta Inc. / Sapphire Technologies, Vista RMS – MCI WorldCom, DynCorp / New Boston Consulting – Treasury Communications System, New Boston Systems Falls – American Red Cross, Norrell Consulting Services – Teletrac Inc., New Boston – Pension Benefit Guarantee Corporation, and America Online**

ADDITIONAL SKILLS:

PROFESSIONAL AFFILIATIONS

- Mentor / Trainer: PMI’s 2014 Mentorship Program Mentor; FBI Content Administrators Community of Practice; and Freddie Mac SharePoint Community of Users
- PMI Member 2000 – Present
- Manchester Who’s Who 2006 –2009

PUBLICATIONS

PMI Symposium 2001: Automotive/Manufacturing SIG ”Trading your time for Results: Comprehensive Six Sigma Trade off Studies”

COMPUTER EXPERIENCE

Hardware:

- IBM Desktops, DB2 Mainframes, Unix, Oracle, Windows, and Linux Servers

Software:

- Adobe CS6 Suite, Adobe Photo Shop, Adobe Acrobat Professional, AS400, AutoCad, Azure Admin portal, Banyan Vines, Bluezone, CASR, Citrix, ComprizonSuite versions 8.3 – 8.9 (.Buy, .Award, .Request, .GPC, .MIPR), Compass, Computron, Confluence, Crystal Reports, DBASE IV, DelTek, DOORS, EMAX, Formfiller, Groupwise, HEAT, HP OpenView, Infomaker, INMS, IPS, ITIL ServiceNow, JIRA, Kronos, Lotus Notes, Lotus Suite, MS DOS, MS Editor, MS Frontpage, Lawson, Lotus Notes, MS Mail, MS Office, MS Outlook, MS Excel, MS PowerPoint, MS Project, MC Project Server, MS Word, MS Works, MS Visio, Nintex workflows, Norton Utilities, Novell 3.x, Oracle STEM, Paint Shop Pro, Paradox, PCLaw, Peoplesoft, Planview, PMD, Power Automate, Power BI, Prism, ProComm, PVCS, Quintus, Rational Rose Suite, Resolve, Selenium IDE, SharePoint 2010 - 2019, SharePoint Designer 2010/2013, SharePoint InfoPath Designer 2010/2013, SharePoint Dashboard Designer 2013, SharePoint O365, SnapIt 11, Snap32, Spectrum, SQL, Subversion (SVN), System Tools, TRS, Visual Studios 2013, WinCap, WinZip, Windows 3.x, 95 & NT, WordPerfect, Unix, Numerous customized relational front-end programs and proprietary programs.

Programming Languages:

- HTML, CSS

Database Management Systems:

- ODIE, Oracle, TCS Service Request Database (Workflow), Serena Teamtrack, SQL

Operating Systems:

- Microsoft Windows 95, 98, 2000, 2013, XP, NT, DOS, and Linux

Communications:

- Telecommunications Protocols or Standards Knowledge: Treasury Communications Systems (ATM & Frame Relay), PBX Switchboards, Alpha/Numeric Paging. Platforms knowledge: OC-48, OC-12, OC-3, ATM, Frame Relay, VPN, Cable Modem, MIMO, Wireless Networks, SONET, etc. within the Treasury Communications Systems Cloud configuration, PBX Switchboards, Alpha/Numeric Paging, Broadband, VOIP, SaaS, and INMARSAT.

5.2 RESUME – AARON MOLINA

NETWORK CONSULTANT

Professional Summary:

- Security Cloud Architect with extensive 12+ years of enterprise-level experience in Network Cloud Management and Service Delivery.
- Cloud Platforms: Versed in AWS, Azure, and GCP ecosystems. Hands-on experience in writing complex Cloud formation templates and developing AWS pipelines.
- Cloud Security: Knowledgeable of Cloud security infrastructures and integration of Source Fire with network (Cisco, Net screen, Checkpoint, IP Tables). Experienced configuring Web Application Firewalls and CSP applicable DDOS tools.
- Infrastructure as Code: Experience with Continuous Integration/Continuous Deployment (CI/CD) practices. Developing scripts to deploy policies and tags for cloud environment management (using tools such as AWS Cloud Formation, PowerShell, Python and Ansible, including use of remote APIs.
- Threat/Vulnerability Management: Knowledgeable of SME Threat/vulnerability management tools, reporting, and incident response. Supported development teams and DevOps in migration to new technologies ensuring that our same level of security oversight is maintained.
- Policy and Compliance: Experienced in developing policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities. Firm understanding of risk management processes. Versed with NIST Cybersecurity Framework Center for Internet Security - Critical Security Controls.
- Technical Leadership: Provided technical leadership in the design, development and deployment of software and hardware solutions. Tracked industry trends and maintains knowledge of new technologies to better serve the enterprise's needs.

Technical Skills:

- Operating Systems: Windows Server 2022, Ubuntu 20.04, Debian 11, CentOS 8, Cisco IOS 15.9, Junos OS 21.1, VMware ESXi 7.0, Citrix Hypervisor 8.2
- Hardware: Cisco - Cisco ACI, Cisco Nexus 9000 Series. Cisco ASR 9001, ASR 9006, and ASR9010, Cisco ISR 4321, ISR 4331, and ISR 4451 Fortinet: Forti Manager 5000F and 6000F 3700D 4200F and 7060E Palo Alto Networks: Panorama M500, PA-7080, PA-5260, and PA-5280 Sonic Wall: Sonic Wall Network Security Manager NSM 9200 and NSM 9600, NSA 4650, NSA 5650, and NSA 6650 Cisco Aironet 3800 Series, Aruba 7000 Series Mobility Controllers, Aruba 7200. Check Point MDM, Check Point 1400 Series thru Check Point 1600 Series. Juniper SRX3000 Series - SRX5000 Series Adtran NetVanta 4000 and 5000 series. Arista 7000 Series, 7280R Series - 7500 Series.
- Software: MQ 5.3, VNC Viewer, Terminal Service Client, Net brain, Aviatix, Case maker Tele mail operations, LDAP operations and Tivoli Storage Manager, C++, Java, Fog light, Wire shark Monitoring, Apache, UNIX Systems Monitoring, Remedy, Work Load Manager, Jira, Service Now, Zscaler ZPA and sb ZIA
- Technologies & Protocols: DNS, DHCP, Remote Desktop, SIP, IIS, VPN, NAT, H.323, TCP, IP, ICMP, VLAN, 802.11x, 802.1X, VPN, FTP, HTTP, HTTPS. SSL, BGP, MPLS, SSH
- Connectivity & Hardware: Juniper SSG, Juniper SRX, Sonicwall (All Models), Cisco ASA (all models) Direct Connect Edgemark, IAD, Cisco 1841, 2500, 2800, 3845, ASR, Catalyst 1900, 2950 2960 3500 3750G 9000, Routers, Switches, Wireless, Ethernet, Fast Ethernet, Gigabit Ethernet, Netopia 3347, Polycom 330, 331 601, 650, 4000 Cisco IP phone 7960, VG224

Certification:

- Amazon Certified, Sys Ops Administrator, Atlanta, GA
- Microsoft Azure Certified, Azure Security Engineer, New York, NY
- Certified Information Systems Auditor, CISA, Atlanta, GA
- Certified Information Security Manager, CISM, Atlanta, GA
- Palo Alto Certified Network Security Engineer, PCNSE, Atlanta, GA

Education:

- Morris Brown College, BS – CIS, Atlanta, GA 2011
- Keller Graduate School of Business, MBA – Atlanta, GA 2009

Professional Experience:**NTT Global****Plano, TX, (March 2021 – Present)***Role: Security Cloud Architect*

- Cloud Platforms: Versed in AWS, Azure, and GCP ecosystems. Hands-on experience in writing complex Cloud formation templates and developing AWS pipelines.
- Cloud Security: Knowledgeable of Cloud security infrastructures and integration of Source Fire with network (Cisco, Net screen, Checkpoint, IP Tables). Experienced configuring Web Application Firewalls and CSP applicable DDOS tools.
- Infrastructure as Code: Experience with Continuous Integration/Continuous Deployment (CI/CD) practices. Developing scripts to deploy policies and tags for cloud environment management (using tools such as AWS Cloud Formation, PowerShell, Python and Ansible, including use of remote APIs.
- Threat/Vulnerability Management: Knowledgeable of SME Threat/vulnerability management tools, reporting, and incident response. Supported development teams and DevOps in migration to new technologies ensuring that our same level of security oversight is maintained.
- Policy and Compliance: Experienced in developing policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities. Firm understanding of risk management processes. Versed with NIST Cybersecurity Framework Center for Internet Security - Critical Security Controls.
- Technical Leadership: Provided technical leadership in the design, development and deployment of software and hardware solutions. Tracked industry trends and maintains knowledge of new technologies to better serve the enterprise's needs.
- Cloud Network Environments: Performed assessments of Cloud network environments, identify gaps and implement performance improvement opportunities.
- SPLUNK Experience: Proficient in using SPLUNK for data analysis and visualization.
- Threat Analysis: Skilled in conducting comprehensive threat analysis to identify potential security risks and develop mitigation strategies.
- SOC Team and Operations: Experience working in a Security Operations Center (SOC) environment, collaborating with teams to monitor, detect, analyze, and respond to security incidents.
- Email Analysis - Proofpoint: Experienced in analyzing email threats using Proofpoint, a leading cybersecurity and threat management tool.
- Cybersecurity: Developed cybersecurity policy, programs, and guidelines for implementation. Created, updated, and maintained, editing and review state cybersecurity policies, providing guidance to C-Level, staff, and end users.
- Scripting and Programming: Experienced with scripting languages – JSON, POSTMAN and PYTHON.
- Firewall Configuration: Experienced with Firewalls: AlgoSec, Checkpoint, CISCO FTD/FMC, ASA, Silver Peak, Fortinet and Palo Alto. Directed others in performing capacity and resource planning, assesses risks, and creates contingency plans for high complexity systems.
- Web Vulnerability Scanning: Experienced with Web vulnerability scanning: Rapid7. Demonstrated effective risk management skills to include appropriately identifying and mitigating weaknesses in cloud resources as needed.
- Network Intrusion Detection: Experienced with Network intrusion detection tools such as Snort, Security Onion and Solar Winds Security Event Manager. Proficient in Full Packet Capture and experienced using/integrating SIEM technologies.
- Virtualization and VPN: Experienced with Virtualization, Sonic Wall, Palo Alto, MS Azure, and AWS. Experience with configuration and support of client-to-site VPN tunnels.

- Cloud Network Strategy: Developed Cloud network strategies for architecture and engineering solutions from concept through implementation. Analyzed and provided recommendations for emerging Cloud network technologies and CSP advancements.
- Incident Detection and Response: Experienced with Incident Detection and Response (Security Hub, Guard Duty, Inspector, Config, Cloud Watch, Cloud Trail).
- Product Management: Versed with Product Managers/Owners to plan and prioritize technology focused backlog items for the architecture runway to enable business epics/features and expand into new opportunities.
- Policy and Standards Writing: Experienced writing policy, standards, guidance, and guidelines adhering to all security posture frameworks.
- Cybersecurity Applications and Appliances: Versed with deploying and maintaining Cybersecurity related applications and appliances. POC new Cybersecurity tools and appliances.
- Client-to-Site VPN Tunnels: Experience with configuration and support of client-to-site VPN tunnels.
- Firewall Platforms: Duties included device installation, management, troubleshooting, and maintenance/upgrades for all firewall platforms (Cisco FMC/ASA, Junos-Space, SRX, Palo Alto, Fortinet, and Sonic wall).

Fiserv**Alpharetta, GA (Nov 2017 – Jan 2021)**Role: Network Security and IT Infrastructure Support Engineer III

- Experienced implementing controls within cloud (Azure or AWS) to achieve and evidence compliance to HIPAA, FFIEC and SOC2 requirements.
- Experienced of cloud security capabilities and tools (Azure or AWS) and leveraging these to achieve compliance.
- Experienced implementing large-scale infrastructure solutions with a proven track record of success.
- Provided technical leadership in the design, development and deployment of software and hardware solutions.
- Tracked industry trends and maintains knowledge of new technologies to better serve the enterprise's needs.
- Made contribution strategies and system deployment consistent with company objectives and generally accepted principles.
- May serve as technical lead, for the resolution of highly complex problems.
- Contributed to the development of procedures and process for routine tasks.
- Experienced in reviewing architectures for security and compliance and offering expert advice on methods for achieving compliant and secure architecture.
- Experienced hosting/providing compliance consultations with Line of Business relating this back to cloud-based technologies and capabilities.
- 15+ years of working experience in network engineering, systems administration, or related field; experience managing engineering and technical employees.
- Experienced with matrix management of engineers or other technical personnel; experience managing infrastructure projects; cross-functional collaboration.
- Strong communication skills ability to facilitate technical conversations with non-technical stakeholders.
- Facilitated the establishment of standards and guidelines for technology solutions.
- Ensured efficient and reliable functioning of integrated systems.
- Reviewed current and proposed business practices for management, backup, recovery, archival technology and procedures.
- Developed and implements changes through normal change control process.
- Proficient performing gap analysis, articulating risks and issues and remediation activities.
- Management, administration and provide Senior level technical support for the Dell Secure Works' Managed Security Services Firewall offerings such as Checkpoint firewalls (IPSO/SPLAT), Cisco PIX/ASA (6.x,7.x ,8.x and 9.x), Juniper SRX (JUNOS) Proventia, Palo Alto, Fortinet, Multi-Vendor IDS/IPS, Net screen and Sonic wall firewalls to enterprise-level customers.
- Worked on improvements including the development of new tools, automation, and integration within AWS and Azure ecosystems.
- Worked with cross-functional application and infrastructure teams to design and architect infrastructure (network, OS, databases) and applications to protect against potential attackers.
- Cloud hands-on technical specialist, handled complex and detailed technical work necessary to establish and maintain secure cloud & data center security for AWS and Azure.

- Worked closely with system admins, Application owners, and network engineering teams in determining remediation and vulnerability intrusion(s).
- Made cloud recommendations to help improve security posture within the cloud as an organization.
- Assess and reviewed cloud network configurations from a security angle; as well as fix any vulnerabilities utilizing the best practice approach.
- Worked closely with functional-area specialists, cloud architects, and security specialists to designing, configuring and/or developing security solutions.
- Managing and troubleshooting firewall management consoles NSM (Net Screen Security Management), Site Protector (IBM ISS Proventia management console) Panorama (Palo Alto Security Management) and FortiManager (Fortinet Security Management).
- Conducted continuous monitoring on base events using SEIM /ArcSight ESM to determine internal or external escalations.
- Automated cloud security solutions and controls.
- Worked on improvements including the development of new tools, automation, and migrations to the cloud.
- Versed of the AWS and Azure ecosystems.
- Knowledgeable of Cloud security infrastructures.
- Examined current cloud security practices and identified key risks, while working with the BU to execute programs to address security flaws and vulnerabilities.
- Experienced multi-vendor IDS/IPS solutions.
- Developed technical plans for integrating complex solutions into enterprise environments.
- Deployed on Premise Firewall migrations for Configuration Management and Patch Management lifecycle
- Conducted continuous monitoring on base events using SEIM /ArcSight ESM to determine internal or external escalations.
- Duties include device installation, management, troubleshooting, and maintenance/upgrades for all firewall platforms (Cisco PIX/ASA, Net screen, SRX, Palo Alto, Fortinet, Multi-Vendor IDS/IPS and Sonic wall)
- Extensive work with High Availability technologies on all major firewall platforms using VRRP, HSRP.
- Extensively involved in creating, managing and troubleshooting VPN tunnels (site to site and client to site) for enterprise customers using Cisco PIX/ASA, Netscreen, SRX, Palo Alto, Sonicwall and Fortinet firewalls.
- Analysis of network topologies to assist customers with security recommendations for their network.
- Develop new documentations, tools, trainings and procedures to improve the quality of services of Security Operation Center (SOC). Interface with external groups such as Product Managers, Provisioning Engineers, SOC, and customers to complete projects and implement new procedures.
- Extensive usage of packet sniffers like TCP Dump, Snoop, fw monitor and debugs to analyze network traffic and solving complex application communication problems.
- Working experience with centralized authentication / authorization service (RSA SecurID)

Dell Secure Works

Atlanta, GA (Nov 2013 – Sept 2017)

Role: IT Network Infrastructure Security Sr. Advisor (Lead)

- Responsibilities include firewall administration; switch configuration and deployment, network troubleshooting, Network video, creation of network, network documentation, support for system and application integration load balancing, port configuration, firewall policy and network security:
- Evaluate data network health, analyze traffic patterns, administer firewall and intrusion detection system efficacy.
- Assisted in logging case notes, monitoring and managing issues through the process to provide RCA.
- Tier 3 Support Engineer for immediate technical escalation path for Tier 1
- On-site Engineer that works in a fast-paced environment with world-class engineers, scientist and customers; Utilizing, the latest cutting-edge technology on a daily basis to ensure the client always has access to their critical data applications via managed networks.
- Responsible for supporting scalable enterprise network designs, solutions, policies, and recommendations in partnership with the technical sales team.
- Catalogue all network configuration items to ensure swift recovery in the event of an outage.
- Identify research, evaluate and recommend both network tools and emerging network technologies.
- Provide Out the box thinking to constantly improve both product and processes.

- Provide primary functionalities of a network analyzer or a packet-sniffer program for traffic captures such as Packet Mon, Smart Sniff and Wire Shark.
- Provide communication skills with ability to clearly explain ideas and influence decisions
- Provide technical RCA (Root Cause Analysis) articles outlining problems resolution and troubleshooting
- Provide technical oversight to customer's global data and voice network architecture.
- Monitor both uptime availability and performance to meet and/or exceed our business Service Level Agreements (SLA's).
- Support fault tolerant and high availability networks providing 99.999% uptime.
- Support the management of the Internet/WAN/LAN/ Voice and Network Security
- Support all data centers and corporate offices.
- Work closely with Video and Network Engineering management in design, test and trial phases.
- Provide an integral role in deployment and turn up of network components in production environments.
- Work with other Operations groups on monitoring and support requirements.
- Provide a 24x7 (on-call) Tier III Operational Support role for Service Delivery Networks and Services.
- Perform upgrades, analyze trends and assist in capacity planning.
- Create & maintain Operational documentation related to contractual SLA's
- Facilitate process to ensure intervals are met.
- Support customer's global network.
- Become an integral part in the Development and Growth of the Video Operations group and the support of Service Delivery Networks and Services.
- Review all service and non-service affecting outages to determine best practices and recommended improvements to reduce future potential service interruptions.
- Continuously optimize the Video Network to achieve the highest level of Video Quality, Network Reliability, and Performance possible.
- Conduct ongoing security risk assessments including the monitoring, investigation and reporting of security and access violations.
- Evaluate security device logs for possible breaches in security, auditing, and troubleshooting.
- Troubles hooted data and telephony circuit outages including DS3, OC3, T1/PRI, MPLS, circuits.
- Serve as technical advisor to design engineers.
- Responsible for ensuring that our Network/Systems security guidelines adhere to best practice and PCI compliance standards.
- Conduct periodic security audits, risk assessments, and penetration tests across our datacenters.
- Responsible for Change Management and Incident Management for Network infrastructure.
- Provide project oversight and technical direction in satisfying implementation milestones.
- Follow standard operating procedures, carried out team responsibilities, tasks and time-lines.
- Perform requirement needs assessments and proposal development.
- Work rotational shifts and occasional change windows during evenings and weekends.
- Provide emergency on-call support on a rotating schedule.
- Design, implement and troubleshoot large-scale, wide-area and local-area IP-based networks.
- Perform lab validation of hardware and software used in the implementation of the network.
- Clearly articulate network designs and drawings through documentation.
- Evaluate and recommend specific products and platforms to provide cost-effective solutions that meet architectural requirements.

AT&T Corporate (Service Delivery)**Dallas, TX (Apr 2006 – Oct 2011)**Role: Network Engineer

- Provide technical guidance and leadership in the arenas of telephony, networking, and system administration Manage, deliver and deploy aspects of network architecture, design, engineering and detail for new accounts:
- Tier 2 Support Engineer for immediate technical escalation path for Tier 1.
- Technical Subject Matter Expert for support on both the network as well as application service components within AT&T's internal IBM applications.
- Created network architecture designs specifications to migrate clients from current network environment.
- Responsible to either resolve escalated technical issues or qualify the issues before escalating to AT&T Labs.

- Proactively identified delivery problems, client issues, or other problems, which may impact the success or time schedule of the project.
- Developed contact center application and infrastructure architectures to facilitate long-term growth.
- Assisted in logging case notes, monitoring and managing issues through the process to provide RCA.
- Extensive experience supporting technologies in traditional and VOIP call center environments
- Ability to coordinate and create a timeline with sub-contractors
- Created installations documents for OPS personnel to quickly and efficiently install new equipment and the provisioning of new circuits.
- Worked with business partners (Sales Teams, Product Management) in front-end planning role.
- Worked with cross-functional engineering and operation teams to design, implement and maintain services related to the telephony infrastructure and/or systems used by the customers.
- Provided regular reports to Account Executives and Management on Project Status
- Developed and execute plans under a set of implementation and delivery time constraints, optimizing for a complex blend of product cost, service opportunity cost, and ongoing support costs.
- Responsible for timely installation, troubleshooting, activation and service validation associated with provisioning Voice over IP Services.
- Ability to resolve issues with internal divisions such as sales and MIS to deliver service in a timely manner
- Scheduled and Facilitate Project Kick Off, Milestone Meetings and Closing Meetings
- Performed all tests and turn ups of BVOIP Voice DNA circuits and performed all BVOIP Voice DNA circuits cross connects.
- Worked with various AT&T network control centers to troubleshoot any call routing and voice quality issues associated with AT&T IP backbone or VOIP Network.
- Interact with outside developers to test the deployment of new software revisions.
- Worked with on-site technicians to install and troubleshoot client premise equipment (modem, CSU/DSU, Router, Code Switch, IP and TDM PBXs, switches, etc.)
- Coordinated implementations of AT&T VOIP service from small to large business users.

References:

Reference #1

Name: Kedar Shahi

Phone: (443)-554-2118

Email: kedarbikramshahi@gmail.com

Role: Dell Corporation (Manager)

Reference #2

Name: Tun Aung

Phone: (857)-327-0072

Email: ttabu@bu.edu

Role: Microsoft Corporation (Manager)

Reference #3

Name: Terrell Parks

Phone: (240) 217-6340

Email: terrell.parks16@gmail.com

Role: County of Orange (Manager)

5.3 RESUME – MANSOOR HUSSIAN

SECURITY CONSULTANT

Professional Summary:

- 10 years of experience in Information Security, design, and development experience in Information Security, IT risk assessments, and risk remediation activities.
- Established and managed documentation process as per SOC2 audit guidelines
- Hands-on experience with common compliance standards such as SOX, SOC2, PCI-DSS, ISO, GDPR, security frameworks (ISO 27001, NIST), and general security concepts.

- Identifying and exploiting network level vulnerabilities on open ports like SSH vulnerabilities, SSL certificate related vulnerabilities, RDP, FTP, SMTP, and SNMP Vulnerabilities etc.
- Installed and maintained security infrastructure, including IPS, IDS, log management, and security assessment systems. Assessed threats, risks, and vulnerabilities from emerging Security issues.
- Hands on experience in standing up AWS accounts, migrating workloads, enforcing security and automation best practices.
- Setup GCP Firewall rules to ingress or egress traffic to and from the VM's instances based on specified configuration and used GCP cloud CDN (content delivery network) to deliver content from GCP cache locations drastically improving user experience and latency.
- Deployed in the cloud and on-premises using Amazon Web Services (AWS) and Single- Server Support.
- Contribute and maintain a showcase of cloud security solutions covering public (AWS, GCP) cloud and hybrid cloud platforms.
- Good at scripting languages like Python, Power shell, Bash, Groovy and configuration management tools Terraform/Ansible/Cloud Formation and Web Service like AWS.
- Performed incident response management role during major outages and cyber-attacks.
- IOC-driven detection of threats and malicious actors and expert knowledge of existing Threat Actor groups and TTP attribution.
- Perform cyber threat intelligence analysis, correlate actionable security events, perform network traffic analysis using raw packet data, NetFlow, IDS, IPS, and custom sensor output as it pertains to the cyber security of communications networks, and participate in coordinating resources during incidents
- Experience in Vulnerability Management using tools like Qualys.
- Used a variety of IAST/RASP scanning, penetration testing, and performance & quality tools to eliminate vulnerabilities and to achieve sector security governance, risk management, & compliance (GRC).
- Experience with Secure protocols like Vulnerability Management tools (Qualys, Whitehat) and implemented the Kenna reporting tool
- Hands on Experience on vulnerability assessment and penetration testing using various tools like Burp Suite, Fiddler, ZAP Proxy, SQL map, HP Web Inspect and IBM AppScan, HP fortify, to determine the security of web application developed in different platforms like .NET, Java, AJAX, PHP and many others
- Manage Compliance and Audit projects of ISO 27001/2 and its derivatives - (HITRUST, Shared Assessment), SOC 1, SOC 2 Security Trust Principal Audit, Consulting, and collaboration around an ISO 27001 Information Security Management System.
- Implement GRC and Risk Management Framework to ensure best practices and metrics that are practical, attainable, and support business goals across all aspects of the system development lifecycle.
- Experienced in security testing and penetration tools that include: Burp, Kali Linux, Metasploit, Nmap, Wireshark, and Red / Blue team assessment experience
- Experience in different web application security testing tools like Accunetix, Metasploit, Burp Suite, Sqlmap, OWASP ZAP Proxy, Nmap and HP Fortify.
- Experienced with Symantec DLP Policies (DLP templates) compliance and regulation standards such as SOX, PCI, and HIPAA.
- Used a variety of IAST/RASP scanning, penetration testing, and performance & quality tools to eliminate vulnerabilities and to achieve sector security governance, risk management, & compliance (GRC).
- Implement, configure, and maintain security solutions, DLP, antivirus, vulnerability scanners, IPS/IDS, web filters, VPN, SIEM, SOAR, etc. Perform daily security systems monitoring, verifying the integrity and availability of all systems and key processes.
- Knowledge and experience in standard security and regulatory frameworks including ISO 27001/31000, NIST 800 - 71, HITRUST CSF, and PCI DSS.
- Knowledge of information security risk management and GRC industry control frameworks; FISMA, FedRAMP, NIST, FIPS, ISO 27001, ISO 27002, GDPR, COBIT, CMMI, SOX, GLB Act, FCRA, HIPAA, HITRUST, CSA/STAR Alliance, CCPA, NYDFS, ITIL, FFIEC, NIC, PCI DSS, MITRE ATT&CK, etc.
- Experienced and proficient in the Security Framework of OWASP, BSIMM, and Secure SDLC along with expertise in OWASP Top 10, SANS 25, CWE, and CVSS.
- Expertise in the development of Information Security Programs based on frameworks such as NIST, NIST, NIST, ISO 27002, COBIT 5.0, FFIEC, GLBA, SOX, PCI & PII with IT Risk drivers KPI and KRI's to ensure Financial regulatory compliance and data security.

- Performing Confidential KPIs performance Analysis and troubleshooting.
- Responsible for ensuring Anthem Information Systems remains in compliance with Center for Medicare and Medicaid Services CMS, TRICARE, federal NIST, and FISMA regulatory requirements.
- Compliance standards and frameworks such as PCI, NIST 800-53, HIPAA, HITRUST, and Privacy standards and frameworks such as Generally Accepted Privacy Principles (GAPP)
- Perform and document audit activities by professional standards such as COBIT, COSO, and SOX internal control frameworks Audit Project.
- Assuring PCI DSS, PI, Legal, and Regulatory Audit compliance.
- Experience in Archer administration techniques to troubleshoot configure integrations and manipulate data to accurately portray the customers' requirements.
- Expertise in improving the Risk and Control functions against Governance, Risk Management, and Compliance (GRC).
- Ensures security and privacy compliance with the organization's policies (such as FISMA, HIPAA, HITECH, and the RMF), and standards (such as FedRAMP, the NIST 800 Series, SSAE SOC 2, and HITRUST).
- Conducted vulnerability and compliance scans (i.e., Nessus) to determine overall system risk impacts and provide results to the customer and information system owner respectively.
- Experience in different web application security testing tools like Acunetix, Metasploit, Burp Suite, Sqlmap, OWASP ZAP Proxy, HP Fortify and Veracode
- Conduct Digital Forensics research, Malware Analysis, and Cyber Threat Intelligence.
- Deployed in the cloud and on-premises using Amazon Web Services (AWS) and Single- Server Support.
- Supporting for Enterprise customers on Microsoft Azure (IAAS, PAAS, and SAAS).
- Expertise in improving the Risk and Control functions against Governance, Risk Management, and Compliance.
- Maintained security infrastructure, including IPS, IDS, log management, and security assessment systems.
- Utilized Security Information and Event Management (SIEM), Intrusion Detection and prevention (IDS/ IPS), Data Loss Prevention (DLP), forensics, sniffers, and malware analysis tools.

Technical Skills:

- **Security Standards/Frameworks:** ISO 27001, NIST SP /NIST CSF
- **Compliance:** SOX, PCI DSS, SOC2, GLBA, GDPR, FEDRAMP/FISMA, HIPAA/HITRUST, COBIT
- **Security Control:** CIS Top 20, CSA CCM, NIST, OWASP Top 10
- **Security Operations:** SIEM/SIMS, CERT/CSIRT, Incidence, Response, logs, events, Cyber Investigation, BCP/DR, Threat Intelligence, Vulnerability Management, Web Application Scanning
- **Operating Systems:** Windows, Server 2012 R2, Linux
- **Automation Tools:** Power Shell, Python
- MS Office Suite (Word, Excel, Access, PowerPoint, Outlook)

Professional Experience:

New York Life Insurance Company (Remote) (Jul'2020-Till date)

Role: Cyber Security Lead

Responsibilities:

- Managed the third-party assessment process by reviewing vendor assessment questionnaires including Soc 2 reports, SIG, and ISO 27001.
- Conducted Dynamic and Static Application Security Testing (SAST & DAST).
- Act as a defender of critical OT infrastructure, implementing security controls and measures to safeguard industrial control systems (ICS), SCADA systems, and other OT assets from cyber threats.
- Monitor adherence to Risk Mitigation strategies in conjunction with Information Security/Cyber Security, Business Continuity Planning BCP /Disaster Recovery DR and Audit teams to provide direction on usage of the guidelines and/or regulations, maintaining flexibility to accommodate changing needs and threats.
- Worked with Cloud-knox IAM for AWS, Azure & GCP subscription
- Configured Pub/Sub to send logs from Google Cloud (GCP) to IBM QRADAR and Splunk using Terraform
- Implemented all aspects of Google Cloud (GCP) Security including IAM Roles, User and Group Management. 25V/MFA, Securing VPC's, Firewall Rules, Encryption, Vulnerability scanning.
- Worked on dome 9 for compliance and security posture management for AWS, Azure & GCP

- Deployed Unified Threat Management (UTM) and Advanced Threat Protection (ATP) across various network platforms.
- Developed threat-hunting techniques by leveraging Sysmon and Windows logs, understanding the pattern of behavior, and reducing the number of false positives by adhering to MITRE ATT&CK framework
- Responsible for the day-to-day Threat and Vulnerability Management and Threat Intelligence activities
- Red Team/ Blue Team Exercises with post mortem remediation efforts and lessons learned
- Instruct cyber red and blue team curriculum, facilitate Security Operations Center exercise and playbook
- Hands-on with network penetration testing and ethical hacking.
- In-depth internal and external network penetration tests.
- Analyze traffic patterns to determine potential distributed denial of service attacks (DDOS) attacks.
- Threat Actors to prevent cyber - attacks, especially in business and corporate settings by providing immediate investigation and resolution.
- Conduct network/host penetration tests and web application penetration tests.
- Performed pen testing of both internal and external networks. The pen testing scope included O/S (Windows and Linux) and external facing web apps and database servers that store customer confidential information.
- Using Qualys Vulnerability Management tool to aid in manual pen-testing in red teaming work
- Administrating Carbon Black to do host based monitoring for red team.
- Network scanning using tools like MAP and Nessus.
- Conduct network Vulnerability Assessments using tools to evaluate attack vectors, identify System Vulnerabilities and develop remediation plans and Security Procedures.
- Analyzed, designed, developed, coded, and implemented programs in various programming languages for Web and Rich Internet Applications
- Collaborated with API Management platforms to develop APIs, Products, Plans, etc., and conducted thorough testing to ensure reliability and functionality.
- Developed user interface (UI) and API functionality using languages such as JavaScript, TypeScript, and Python.
- Preparation (including Narratives, and RCMs related to SOX processes and audits) for ISO 27001. SOC1 (SSAE16/SSAE18) and SOC2 Audits from Management's Perspective in the Governance, Risk & Compliance (GRC) areas.
- Key skills include control assessment, and governance, risk, and compliance (GRC) solutions utilizing cyber security standards and frameworks (e.g., FedRAMP, COBIT, ITIL, NEI, NERC/CIP, NIST/FISMA, HIPAA, SOX, PCI-DSS, SANS, SDLC, ISO/IEC, CMS, HITRUST).
- Experience in all aspects of the NIST Risk Management Framework and associated System Authorization processes and procedures. Technical experience spans software and system level design, integration, testing, operations, and maintenance of distributed, internetworked, client-server-based, and web-based computer systems.
- Control Risk Mitigation involving approved deviations/waiver request forms
- Reviewed third party software application & IT Controls(s) for in-house development. Performed SOC 1 & 2 Type 1 & 2 review, audits & mapping Complementary User Entity Controls SSAE18/ ISAE 3402, SAS70 I & II to ensure compliance with SOX, and performed remediation where required.
- Reviewed the SOC1 and SOC2 deliverables and documented evidences.
- Reviewed areas identified for improvement by staff and by self, and in conjunction with IT Compliance Management, developed viable business solutions to mitigate the risk.
- Tested compliance with company policies and procedures to ensure they conform to industry standards; such as HIPAA and PCI DSS frameworks
- Conducting threat modelling exercises to identify potential security threats and vulnerabilities to our company's systems and networks
- Conducted Web Application Vulnerability Assessment and Threat Modelling, Gap Analysis, secure code reviews on the applications.
- Skilled using tools like Automatic Scanner, NMAP, Dirbuster, Qualysguard, Nessus, HP Fortify, HP Webinspect, IBM appscan for web application penetration tests and infrastructure testing.

- Conducted vulnerability assessment, Blue team vulnerability employing and intrusion assessments, cyber security inspections and Red Team operations employing internal and external capabilities to provide a systemic view of enclave and IS technical and traditional security posture.
- Conducted security assessment of PKI Enabled Applications.
- Perform threat hunting and threat modelling using MITRE attack framework and other methodologies.
- Responsible in web application vulnerabilities (OWASP TOP 10, SANS, NIST) to review application source code to find its security vulnerabilities (CSRF, XSS, SQL Injection, Privilege Escalation, etc.) and recommend remediation.
- Responsible for implementing monitoring solutions in Ansible, Terraform, Docker, and Jenkins
- Performed penetration testing on CVS infrastructure and vulnerability assessment of application and database servers.
- Conducted security assessment of PKI Enabled Applications.
- Skilled using Burp Suite, Acunetix Automatic Scanner, NMAP for web application penetration tests.
- Good knowledge of network and security technologies such as Firewalls, TCP/IP, LAN/WAN, IDS/IPS, Routing and Switching
- Develop test cases to test web application according to OWASP and mapped every test case to NIST control
- Socialize with control owners and stakeholders to ensure all identified risks are mitigated.
- Liaise with control owners on timeframes for control remediation for identified risk areas during integration.
- Review of enterprise cloud security controls.
- Configured and Monitored Azure Sentinel (SIEM - Security Information and event management tool).
- Working knowledge on cloud security engineering and administrating for SaaS, PaaS, and IaaS (AWS and Azure).
- Lead the configuration of cloud-based network and application firewalls (Security Groups, Network ACLs, AWS Network Firewall, and WAF).
- Involved in maintaining Data Privacy for GDPR, HIPAA, FDR, and lead SOC 2
- Implement SOC2, GDPR and ISO27002 principles according to the client location
- Experienced with implementing, monitoring, and managing Governance, Risk, and Compliance (GRC) Tools.
- Develops cyber security reports and metrics for management presentations on policy exception requests.
- Prepare the Cloud Platform Security (CPS) for audit readiness through coordination with the IT Risk Management group.
- Plan and execute security risk assessments for all third-party vendors/suppliers
- Assured all Personal Information was held in compliance with Privacy and PCI DSS 2.0 Regulations and Guidelines.
- Knowledge in implementing HITRUST CSF as a single benchmark to facilitate internal and external security control measurements that meet requirements of NIST, ISO, PCI, HIPAA, HITECH, and COBIT.
- Performed reviews of Information Flow Control to validate that adequate security controls are in place to meet HITRUST CSF and NIST 800-54 guidelines.
- Collaborate with GRC Team and IT leadership to ensure that the IT Security Control Framework complies with SOX and industry standard operating procedures.
- Performed audit/SOX testing as outlined in the audit/SOX program
- Conducted application program interface security assessments as a crucial part of the API security program.
- Utilized the enterprise SSDLC processes and toolset for efficient and secure development practices.
- Work (Nexpose) to setup, schedule and documentation of a Vulnerability scanning cycle.
- Manages a team of Security Analysts and Engineers in supporting security authorization efforts in vulnerability detection, mitigation, and eradication
- Implement known security methodologies and standards such as OWASP etc.
- Conduct on-site risk assessments based on agreed-upon procedures and guidelines.
- Actively participated red vs. blue teaming exercises for custom built ransomware and malware attack infrastructure to perform Penetration Testing to discover vulnerabilities and breaches in security infrastructure and process.
- Performs network/ host-based intrusion detection using a variety of threat detection tools such as Splunk, Proofpoint Sourcefire, FireEye (HX, NX)

- Review key vendor-provided documentation such as the SSAE 16 Type-II report and review the access control management on the vendor sites.
- Escalate issues of 3rd party vendor non-compliance to the Vendor Risk Management Office (VMO).
- Working with the vendors to ensure risks discovered are remediated within a reasonable time.

CenterPoint Energy**Dallas TX (Feb'2018–Jul'2020)***Role: Cyber Security Engineer***Responsibilities:**

- Managed InfoSec assessment program of Cloud and Consumer Technology organization. Involved in maintaining Data Privacy for GDPR, HIPAA, FDR, and leading SOC 2 and HITRUST Audits
- Implemented all components of AWS, Azure and GCP security standards.
- Significant experience with AWS, GCP and Azure Security.
- Performed penetration testing on infrastructure and vulnerability assessment of application and database servers.
- Working with Red team to do application testing, Web application testing etc.
- Monitor and support compliance initiatives for related 3rd parties (e.g. SOC1,2).
- Preparing Splunk Scripts for forensic investigation, diagnosis the cyber-attacks and incident alerts.
- Develops and submits detailed reports of findings, analysis and recommendations. Researches new vulnerabilities, attacks and exploits
- Maintenance of anti-virus\Anti-malware\Endpoint protection platform, threat hunting, and compliance.
- Manage the Security Incident and Event Management (SIEM) infrastructure.
- Performed threat hunting and incident Response (IR) using Carbon Black Endpoint Detection and Response (EDR). Developed correlation rules and conducted incident analysis using Splunk ES and Exabeam UBA, UEBA
- Performed Threat Vulnerability Management scans through Qualys Guard and Nexpose, as well as App Scan
- Analyzed threats to corporate networks by utilizing SIEM products (QRadar, Splunk) to assess the impact on client environments.
- Conduct threat intelligence analysis on key areas of the Enterprise Defense-in-depth analytics, incident statistics, and other relevant information in creating periodic threat intelligence reports.
- Maintained up-to-date controls, coordinated the control assessments, and identified and escalated the non-compliance issues.
- Monitored activities of IT security systems and applications to ensure compliance with internal policies and procedures including monthly, quarterly, and annual account and activity reviews
- Conduct network/host penetration tests and web application penetration tests.
- Performed Network scanning using tools Nessus and Nmap and generated reports.
- Identifying the risk level (critical, High, Medium, Low) and prioritizing vulnerabilities found in web applications based on OWASP Top 10, SANS 25 and GSEC.
- Assessed threats, risks, and vulnerabilities from emerging Security issues.
- Performed static code reviews with the help of automation tools.
- Training the development team on the most common vulnerabilities and common code review issues and explaining the remediation's, prioritizing the issues found.
- STRIDE assessment of the applications during the design phase, identifying the threats possible and providing security requirements.
- Provide software security support related to Fortify, HP Web inspect and remediation guidance to development teams.
- Identifying vulnerabilities and threats based on client's security policy and regulatory requirements such as PCI, PII, HIPAA, and SOX.
- Performed penetration testing and vulnerability management over the enterprise systems to audit the standards to comply with NIST and ISO 2700x standards.
- Vulnerability Management by scanning, mapping and identifying possible security holes using Qualys Guard and Nessus scanner.
- Management lead and engineer for internal Blue Team Vulnerability Assessment efforts for VAAM and PT
- Reviewing the reports and code removing the False Positives and identify the False Negatives.

- Participates in Blue Team Incident Response team, coordinate with Cyber Security Incident Responder
- Developed comprehensive risk management based on current industry security frameworks to document observations, enterprise risk, remediation, and monitoring using frameworks like NIST 800-53, HITRUST V8, ISO 27001, SAE 16 (SOC 1 and 2), HITECH, COBIT, and SOX.
- Developed risk management program and planned, developed, and modified policies, processes, guides, standards, and procedures and ensured compliance working with appropriate teams.
- Experience in using Kali Linux performing web application assessment to identify, validate and exploit vulnerabilities using tools like Metasploit, DirBuster, OpenVAS, Nikto, SoapUI and Nmap.
- Create develop and test environments of different applications by provisioning Kubernetes clusters on AWS using Docker, Ansible, and Terraform
- Experience working with SQLmap, an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.
- Developed and maintained documentation for projects, APIs, and integration solutions.
- Familiar with the TTP playbook for Incident Response, adhering to the MITRE Industrial Control Systems attack matrix.
- Serving as the Lead Threat Investigations and Incident response person to the SOC team using CrowdStrike.
- Worked in Threat Modelling during Requirement gathering and Design phases.
- Worked on OWASP top 10, SANS 25 and Common Vulnerabilities and Exposures (CVE) identifying, reporting and help developers in remediating the issues.
- Conducting Web Application Vulnerability Assessment, Threat Modeling and secure code reviews on the applications.
- Responsible for deploying various network security & High Availability in Checkpoint Firewall.
- Efficiently performed web application, vulnerability assessment using Burp Suite, HP Web Inspect, Nexpose and IBM AppScan.
- Perform manual security testing for OWASP Top 10 vulnerabilities like SQL Injection attacks, cross site scripting (XSS), CSRF, and Session Management etc.
- Using Qualys Vulnerability Management tool to aid in manual pen-testing in red teaming work
- Network Monitoring and security scanning utilizing Nessus Vulnerability scanning.
- Implemented security controls in accordance to NIST, CIS Benchmarks, ISO 27001 Frameworks.
- Conducted system security assessments based on FISMA, NIST and PCI DSS Compliance.
- Worked on OWASP top 10, SANS 25 and Common Vulnerabilities and Exposures (CVE) identifying, reporting and help developers in remediating the issues.
- Conducting Web Application Vulnerability Assessment, Threat Modeling and secure code reviews on the applications.
- Perform manual security testing for OWASP Top 10 vulnerabilities like SQL Injection attacks, cross site scripting (XSS), CSRF, and Session Management etc.
- Identifying vulnerabilities and threats based on client's security policy and regulatory requirements such as PCI, PII, HIPAA, and SOX.
- Performed penetration testing and vulnerability management over the enterprise systems to audit the standards to comply with NIST and ISO 2700x standards.
- Vulnerability Management by scanning, mapping and identifying possible security holes using Qualys Guard and Nessus scanner.
- Implemented and evaluated SOC1 and SOC2 deliverables
- Work alongside the Compliance Administrator to properly handle and manage the incident and Breach Response events and tickets using One trust.
- Electing and implementing applicable security controls (technical, operational, and management) using NIST SP 800-53 Rev 4 as a guide.
- Complete risk assessments, security requirements analysis, and security testing for existing and new Applications.
- Performed User Access Reviews - Applications impacted by SOX and SOC 2. Conducted walkthrough (UAR) design checklist with key stakeholders to determine if access to applications is role-based and if access has been authorized at the system or server level.

- Developed Vulnerability Scanning process for all environment builds, and ongoing monthly scanning reporting using Nessus.
- Perform HITRUST readiness and certification assessments, including GRC integration into overall business processes
- Reviewed SOC1,2, SIG and other industry standards to assess the Cybersecurity risk and provide recommendations to the contract owner on residual risk and mitigation strategies.
- Performed penetration testing and vulnerability management over the enterprise systems to audit the standards to comply with NIST and ISO 2700x standards.
- Reviewed POA&M, enforced timely remediation of audit issues, and updated system security plans (SSP) using NIST SP 800-18 guidelines
- Regularly evaluate internal/external technical security controls reviews, perform IT audit/risk advisory services for existing or prospective IT systems, technology, applications, medical and IT devices

Applied Material**Austin, TX (Oct' 2015 - Dec'2017)**Role: Security Engineer**Responsibilities:**

- Establish standard operating procedures for embedding Cybersecurity driven processes into the agile Software Development Life Cycle (SDLC).
- Use threat intelligence and models to create hypotheses
- Operational Knowledge in cybersecurity, threat intelligence, threat hunting, or investigative teams.
- Familiarity with common network security threats and vulnerabilities
- Performed risk assessments on the vulnerabilities found during the test
- Evaluates and coordinates the identification of cyber threats, vulnerabilities, and risks to the HRSA IT Enterprise.
- Provide technical analysis to the Risk Management Team
- Contributed to the enhancement of enterprise SSDLC processes, ensuring alignment with industry best practices.
- Created a TTP (Tactics Techniques and Procedure) playbook for Incident Response adhering to the MITRE ICS attack matrix
- Performed Gap Analysis for MITRE Attack evaluation for transferability to ICS environment
- Hands on experience performing security assessment with SAST and DAST using tools like HP Fortify, HP Web Inspect and IBM AppScan.
- Performed Vulnerability Assessments using - Kali Linux / Metasploit / BurpSuite / Paros / SQL map and many open-source tools.
- Maintains network performance by performing network monitoring and analysis, performance tuning, troubleshooting network problems. Skilled using Burp Suite, Acunetix Automatic Scanner, MAP, Dir-Buster, HP Fortify, Qualys-guard,
- Working with red team in SOC to apply security awareness to Cyber Kill Chain management as well as using moving target defense approach.
- Responsible for Source code analysis of multiple teams using Checkmarx and updating the triaged report findings to developers.
- Initiated/run DAST, SAST scans (Fortify, Checkmarx).
- Identify and remediate application security vulnerabilities (OWASP top 10) using Dynamic analysis (DAST), static analysis (SAST) tools such as IBM Appscan, Checkmarx.
- Conducted thorough API security assessments and executed remediation activities as part of the API security program, enhancing the overall security posture.
- Working with Red team to do application testing, Web application testing etc.
- Performed dynamic analysis (DAST) and static code reviews (SAST)with Veracode, extracted reports and opened tickets to track the development efforts using JIRA, and meet with development teams as required and remediate
- Used Sqlmap and Nmap for VAPT, and prepared reports for audit according to OWASP with all issues and their mitigation.

- Experienced on Firewalls Cisco ASA, SonicWall, Palo Alto Networks, Sourcefire, Checkpoint, Juniper Networks, Arista, Huawei, Peplink, and ADTRAN. Tested authentication in OSPF and BGP.
- Proficient in detecting application-level vulnerabilities like XSS, SQL Injection, CSRF, authentication flaws etc both through automation and manual testing
- Authored security control narratives in support of ISO 27001 and SOC 2 framework-based audits
- Created the PCI Audit and Remediation Program (SOC 1&2)
- Established a Security Committee offering ISO 27001 certification guidance while working with external auditors and directing IT security audit procedural policies.
- Facilitated external audits with auditors and stakeholders for ISO 27001, SOC2, and third-party
- Developed a comprehensive risk management program based on current industry security frameworks to document observations, enterprise risk, remediation, and monitoring using frameworks like NIST 800-53, HITRUST V8, ISO 27001, SAE 16 (SOC 1 and 2), HIPAA, HITECH, COBIT, and SOX.
- Perform Risk Assessments for current and/or previously engaged 3rd Party vendors, providing risk recommendations and mitigation based on regulatory compliance guidelines
- Perform Risk Assessments to identify system vulnerabilities and create Risk Assessment Reports.
- Perform Risk Assessments for current and/or previously engaged 3rd Party vendors, providing risk recommendations and mitigation based on regulatory compliance guidelines
- Perform Risk Assessments to identify system vulnerabilities and create Risk Assessment Reports.
- Utilize NIST SP 800-37 methodologies to prepare documents to implement the Risk Management Framework (RMF).

Capital One**Dallas, TX (Feb 2014 – Sep 2015)***Role: Security Analyst***Responsibilities:**

- Assess risk and document all IT mortgage lending systems and their GCC controls. (SOC 1,2)
- Assess agencies' assets for potential and active vulnerabilities and/or risks.
- Performed Network scanning using tools Nessus and Nmap and generated reports.
- Responsible for maintaining, reporting and communication of SIEM between event-sources and endpoints.
- Participates in Blue Team Incident Response team, coordinate with Cyber Security Incident Responder
- Network Monitoring and security scanning utilizing Nessus Vulnerability scanning.
- Handling SIEM events and response in critical environments (Email Threat Analysis, Web Threat Analysis, Malware Analysis, etc.).
- Analyze multiple network and host-based security appliance logs (Firewalls, NIDS, HIDS, Sys Logs, etc.) to determine and apply proper remediation actions and escalation paths for each incident.
- Actively monitored and responded to activity impacting various enterprise endpoints facilitating network communication and data handling (McAfee End Point Security, DLP, and Splunk).
- Assessed filled questionnaires from Third-Party vendors, documented and updated the various artifacts and deliverables based on the GRC Compliance model using NIST Standards, and recommended remediation plans to stakeholders.
- Conducted IT controls risk assessments with NIST 800-53A, including reviewing organizational policies, standards, and procedures and providing advice on their adequacy, accuracy, and compliance with NIST standards
- Conducted compliance assessment, reviews, and analysis and prepared reports Identifying areas of non-compliance
- Conducted risk assessments and evaluations of new and existing 3rd party vendors at Confidential; determining the risk governance and control compliance
- Implement system recovery procedures to minimize losses should an attack occur
- Ensure the organization is complying with all applicable standards and frameworks, such as NIST SP 800-53, ISO/IEC 27001/2, the Cybersecurity Framework, COBIT, and/or PCI/DSS.
- Implement all phases of the RSA Archer GRC (Governance, Risk, and Compliance) platform.
- Implementation of enterprise-wide Cyber Security Risk Management Program based on FISMA and NIST 800 Standards for Information Technology and Industrial Control Systems

- Managed multiple engagements, performing cyber risk assessments and developing response strategies based on current state, developed target state based on NIST 800-53 and ISO 27001, NIST cybersecurity framework (CSF) standards that ensured business continuity and limited the impact of a security breach.
- Managed and delivered IT security and compliance initiatives of PCI DSS, SOX Audit, Enterprise Risk Management, and ISO 27001 –Information Security Management Systems (ISMS) frameworks.
- Review and update System Security Plans (SSP) and Security baselines by NIST, FISMA, NIST SP, and industry best security practices.
- Reported vulnerabilities identified during security assessments utilizing standard WE, CVE, CVSS, WASC, CWE/SANS Top 25 Most Dangerous Programming Errors, and OWASP Top 10 classifications, as well as compliance standards: FISMA NIST SP 800-53.
- Resolved vulnerabilities in the WebEx and FedRAMP GRC environments, POA&M & NIST, using automated scripts created in Python, PowerShell, and Bash.

References:

Name: Edmond Gambles

Company: New York Life Insurance Company

Phone: (786) 453-0681

Designation: PM

Email: Edmond.Gambles12@gmail.com

Name: Paul Brouse

Company: CenterPoint Energy

Phone: (256) 602-7290

Designation: Reporting Manager

Email: pbrouse@gmail.com

Name: Alison Baldwin

Company: Applied Material,

Phone: 551-229-5624

Designation: BA

Email: abaldwin8@gmail.com