

Mr. Christian Turner

Comprehensive Technical CV & Project Portfolio

Detailed technical expertise documentation and project history

Senior Cloud Architect & DevSecOps Specialist specializing in AWS cloud transformation, government sector compliance, and enterprise infrastructure modernization

Professional Profile

Role Description: Cloud Architect & DevSecOps Specialist

Resource Profile:

Mr. Turner is a Senior Architect and Technology Consultant with over 15 years of Platform Engineering and IT experience. He has extensive experience across multiple vertical and lateral markets and organizations, with a focus on managing change and transforming Infrastructure and IT Business Systems holistically, working with all areas of the technology stacks.

Mr. Turner's expertise in the private sector includes successful project execution and complex migrations to the public cloud, particularly AWS, since 2011. He has worked with highly secure organizations in the Canadian Federal Government, USA Utilities markets, and Health Care markets, ensuring compliance with ITSG, NIST, and HIPAA standards.

He excels in innovating and architecting on-premise, hybrid, and cloud solutions, with a strong emphasis on AWS Cloud services. His proficiency in DevSecOps practices ensures the integration of security into every phase of the development process, enhancing the overall security posture of the solutions.

Mr. Turner drives the implementation of changes to support tracking metrics and KPIs for departmental improvement. He clearly defines vision, strategy, and objectives for change initiatives, ensuring strategic alignment of multiple technical facets with corporate goals.

His experience includes the transformation and integration of Agile processes and methodologies. As a Subject Matter Expert, he works directly with staff, management, senior management, and executives to achieve project success and organizational goals.

Language: English

Professional Development

CERTIFICATION: [AWS Certified SysOps Administrator - Associate](#)

CERTIFICATION: [AWS Certified Solutions Architect - Associate](#)

CERTIFICATION: [AWS Certified Solutions Architect - Professional](#)

CERTIFICATION: [AWS Certified Developer - Associate](#)

CERTIFICATION: [Certified Scrum Master \(CSM - Scrum Alliance\)](#)

Table of Contents

- [PROFESSIONAL EXPERIENCE](#)
 - [13. Project 13 - SSC - Cloud Platform Engineering / Hosting Services Branch](#)

- [Project 13.1 Description - Cloud Services Directorate, Cloud Platform Engineering](#)
 - [Project 13.2 Description - Cloud Services Directorate, Automation and Orchestration Framework](#)
- [12. Project 12 - Agriculture Canada - Cloud Centre of Expertise / Cloud Operations](#)
 - [Project 12.1 Description - Cloud Centre of Expertise / Cloud Operations](#)
 - [Project 12.2 Description - DevOps & AWS Development](#)
- [11. Project 11 - SSC CSD R&D](#)
 - [Project 11.1 Description - Cloud Services Directorate, Cloud Platform Engineering Project](#)
- [10. Project 10 - DND DPDCS SMMS Replacement Project](#)
 - [Project 10.1 Description - SMMS Search and Rescue Replacement Project](#)
- [9. Project 9 - IDS Data Systems \(New Democratic Party\)](#)
 - [Project 9.1 Description - Office 365 Skype Migration - New Democratic Party of Canada](#)
 - [Project 9.2 - Server Workload Cloud Migration - New Democratic Party of Canada](#)
- [8. Project 8 - SSC CITS SMG & CTMS](#)
 - [Project 8.1 Description - SharePoint 2016 Design - July 2018 - February 2019](#)
 - [Project 8.2 Description - Atlassian JIRA Implementation - January 2018 - May 2018](#)
- [7. Project 7 - Brookfield Renewable Energy Cloud Delivery](#)
 - [Project 7.1 Description - Office 365 and Microsoft Azure Cloud Service Delivery Manager](#)
- [6. Project 6 - Lowe Martin DevOps](#)
 - [Project 6.1 Description - Dev Ops](#)
 - [Project 6.2 Description - Office 365 Migration from Exchange & Domino Environments](#)
- [5. Project 5 - HighRoads US Cloud Migration](#)
 - [Project 5.1 Description - Exchange Email Cloud Migration](#)
 - [Project 5.2 Description - Atlassian Project Management Cloud Migration](#)
- [4. Project 4 - HighRoads Canada Inc. Infrastructure Operations Manager](#)
 - [Project 4.1 Description - AWS Cloud Migration \(In-house custom SaaS platform\)](#)
 - [Project 4.2 Description - SaaS System: DevOps Infrastructure](#)
 - [Project 4.3 Description - Infrastructure Decommission & Migration](#)
 - [Project 4.4 Description - Operations Decommission & Migration](#)
- [3. Project 3 - Dymon Corporation - Infrastructure Manager](#)
 - [Project 3.1 Description - Operations Virtualization](#)
 - [Project 3.2 Description - Remote Desktop Services \(RDS\)/ Thin Client Implementation](#)
 - [Project 3.3 Description - Sales Software & POS Infrastructure System Upgrade](#)

- [2. Project 2 - GeoDigital International Inc. Infrastructure Manager](#)
 - [Project 2.1 Description - "PAS - Photo Acquisition Service" SaaS Cloud Application](#)
 - [Project 2.2 Description - Data Centre Migration \(Vancouver, BC - Ottawa, ON\)](#)
 - [Project 2.3 Description - Corporate Private Cloud \(Data Centre Architecture\)](#)
 - [Project 2.4 Description - On-Premise Data Centre Virtualization](#)
 - [Project 2.5 Description - Corporate Hybrid Cloud \(Production & Field Acquisition Systems\)](#)
 - [Project 2.6 Description - Office 365 Cloud Migration](#)
 - [1. Project 1 - Central Wire Industries Infrastructure Manager](#)
 - [Project 1.1 Description - IT Integration of fully automated production systems \(Fond du Lac, Wisconsin\)](#)
 - [Project 1.2 Description - ADP Payroll Systems Migration \(Citrix Virtualization, Platform Upgrade, Database Migration\)](#)
- [TECHNOLOGY INDEX](#)

PROFESSIONAL EXPERIENCE

13. Project 13 - SSC - Cloud Platform Engineering / Hosting Services Branch

Shared Services Canada

Cloud Services Directorate, Cloud Platform Engineering

Role: AWS Cloud Infrastructure as Code DevOps Engineer & Architect

September 2023 - Current

Project 13.1 Description - Cloud Services Directorate, Cloud Platform Engineering

The Cloud Services Platform Engineering team operates within the Hosting Services Branch providing an Enterprise class Tenancy within the Amazon Web Services (AWS) Cloud, supporting AWS ASEA (Secure Accelerator) and AWS LZA (Landing Zone Accelerator) platform designs.

Platform and enterprise services are provisioned and deployed using:

- AWS EKS Kubernetes Service
- GitOps Principles
- Terraform Infrastructure as Code
- Crossplane Infrastructure as Code (GitOps)
- ArgoCD, Argo Workflows, Argo Events

Project Outcomes:

Successfully architected and deployed enterprise-class GitOps platform serving multiple government departments through AWS EKS and ArgoCD. Established Infrastructure as Code standards using Terraform and Crossplane, enabling rapid deployment of NIST 800-53 compliant workloads across SSC's AWS Landing Zone Accelerator platform.

Tasks Performed:

- Needs analysis, defining requirements, defining and maintain deliverable scopes
- AWS and Kubernetes design patterns and architecture
- Design and Delivery Iterations:
 - Concept > Proof of Concept (PoC) > Dev/Test > Minimal Viable Product (MVP) > Production > Continuous Improvements
- Infrastructure as Code development
 - Terraform
 - Crossplane
 - Kubernetes
- Deployment Processes and Implementations
 - GitOps declarative (ArgoCD)
 - Pipeline Promotions (Terraform)
 - ClickOps and Runbooks
- Security By Design patterns and principles
 - Meet and exceed NIST 800-53 & ITSG
 - General Security Best Practices
 - Code Security (Vulnerability and Quality)
- Workload and Application Deployment and Support
 - Deployment Processes
 - Implementation
 - Architectural Patterns
- Implemented Source Code Management, DevOps Toolings, and DevOps Best Practices

Technical Environment:

- **Public Cloud:** Amazon AWS Cloud, Azure DevOps
- **Applications:** Azure DevOps Git, ArgoCD, Argo Workflows, Checkov Security Scanning, JIRA, Confluence,
- **Servers:** Kubernetes (kind, k3d, kubeadm), AWS Linux, CentOS, CIS Hardened Images
- **Languages:** Bash, Python 3.x, Typescript, Golang, Terraform, Crossplane, Helm, CDK, CDK8s

Project 13.2 Description - Cloud Services Directorate, Automation and Orchestration Framework

The Cloud Services Directorate requires comprehensive automation and orchestration frameworks to support enterprise-scale cloud deployments across multiple government departments and regulated sectors. This initiative focuses on developing scalable, compliant, and secure cloud automation solutions through Ottawa Cloud Consulting's federally incorporated consulting services.

Project Outcomes:

Architected 3 multi-account AWS organizations managing 200+ workloads with governance, SCPs, identity models, and compliance baselines aligned to NIST, CIS, and ITSG. Improved deployment frequency by 30% through GitOps automation with ArgoCD and Azure DevOps, managing over 50 microservices. Designed 30+ serverless, event-driven, and containerized workloads reducing operational overhead by 40% and infrastructure costs by \$25K annually. Engineered 3 production EKS clusters achieving 99.9% uptime while reducing Kubernetes onboarding time by over 60% through deterministic automation and developer Golden Paths.

Tasks Performed:

- Needs analysis, architecture design, and implementation of multi-account AWS organizations
- Design and implementation of Service Control Policies (SCPs) and governance frameworks
- Identity and Access Management (IAM) model architecture with compliance baselines
- GitOps automation framework development and implementation
 - ArgoCD deployment and configuration management
 - Azure DevOps integration and pipeline orchestration
 - Microservice deployment automation for 50+ services
- Serverless and event-driven architecture design and implementation
 - AWS Lambda, Step Functions, EventBridge, SQS, SNS
 - Container orchestration with AWS EKS and Docker
 - Cost optimization strategies achieving \$25K annual savings
- Production EKS cluster engineering and management
 - 3 node groups with auto-scaling configurations
 - IRSA (IAM Roles for Service Accounts) implementation
 - Multi-node isolation and security hardening
 - Cilium networking configuration and management
 - RBAC model design and implementation
 - 99.9% uptime achievement through high availability design
- Crossplane and KCL provisioning framework development
 - Modular infrastructure component design

- Versioned OCI bundle creation and management
 - 100+ infrastructure component provisioning automation
 - 75% reduction in deployment errors through standardization
- Developer experience optimization and Golden Path creation
 - Kubernetes onboarding automation reducing time by 60%
 - Deterministic automation workflow development
 - Self-service deployment capabilities
- Observability and monitoring implementation
 - 12 operational dashboards covering metrics, security, compliance, logs
 - Incident response signal integration
 - Multi-organization monitoring across 3 AWS accounts
- Documentation and knowledge management
 - 25+ design specifications and architecture documents
 - ConOps (Concept of Operations) development
 - Runbooks and operational procedures
 - Security models and compliance frameworks
- Compliance and security framework alignment
 - NIST, CIS, and ITSG compliance baseline implementation
 - Automated security scanning and governance
 - Regulatory compliance reporting and monitoring

Technical Environment:

- **Public Cloud:** Amazon AWS Organizations, AWS Control Tower, AWS SSO, AWS Config, AWS CloudTrail, AWS GuardDuty
- **Container Orchestration:** Amazon EKS, Docker, Kubernetes, Helm
- **GitOps & CI/CD:** ArgoCD, Argo Workflows, Azure DevOps, Git
- **Infrastructure as Code:** Crossplane, KCL, Terraform, AWS CDK, CloudFormation
- **Serverless & Event-Driven:** AWS Lambda, Step Functions, EventBridge, SQS, SNS, API Gateway
- **Networking:** Cilium, AWS VPC, Transit Gateway, Load Balancers
- **Security & Compliance:** AWS IAM, IRSA, RBAC, Service Control Policies, CIS Controls, NIST Frameworks
- **Observability:** CloudWatch, Prometheus, Grafana, AWS X-Ray, ElasticSearch
- **Languages:** Python, Golang, Typescript, Bash, YAML, JSON, KCL
- **Package Management:** OCI Bundles, Helm Charts, Docker Images

12. Project 12 - Agriculture Canada - Cloud Centre of Expertise / Cloud Operations

Agriculture Canada

Cloud Centre of Expertise

Role: AWS Cloud DevOps Architect (Part-Time)

January 2021 - September 2023

Project 12.1 Description - Cloud Centre of Expertise / Cloud Operations

The AAFC Cloud Centre of Expertise (CCoE) are focused on providing a secure and scalable managed public cloud environment to internal business users. The AWS Cloud environment is implemented using standard AWS Landing Zone foundations with layers of Infrastructure as Code governance resources deployed to meet both Operational and Security requirements, as well as achieve full ATO status for production workloads.

Project Outcomes:

Achieved full ATO (Authority to Operate) status for Agriculture Canada's AWS Cloud environment, meeting ITSG-22/33/38 requirements. Successfully implemented automated security and governance compliance tooling that exceeded GoC cloud guardrails, enabling secure cloud adoption across the department with integrated Azure AD SSO federation.

Tasks Performed:

- Needs analysis, define requirements, and strategize architecture with AWS team
- Architectural design and Proof of Concept (PoC) implementation for design review sessions
- Infrastructure as Code (IaC) Coding and review
 - AWS CLI, AWS API
 - Infrastructure As Code (IAC) - Terraform, AWS SDK, AWS CLI Scripting
- CI/CD CodePipeline, Azure DevOps Repos, Azure Pipelines/AWS CodeBuild, CodeDeploy
- Implementation of IT Security Program to meet ITSG-22, ITSG-33 and ITSG-38 and TBS driven cloud guardrails and achieve Full ATO
- Secure, implement and support SSO Federation to Azure Active Directory
- Develop and implement Security Control Systems and Posture Management to manage integration of AWS Cloud Identity components, validating against ITSG Controls, and enhanced internal Cloud Centre of Excellence security controls.
- Design and integration of automated Security and Governance compliance tooling, meeting and exceeding GoC ITSG requirements
- Facilitated requirements gathering with technical team, architecture team, and security team to ensure all process and components are clearly captured and defined. Documentation of outcomes and design

are shared with leadership and management.

- Support client workloads with:
 - Needs analysis and POC discussions
 - Architecture and Design
 - Review, Governance and Compliance
 - Technological challenges
 - Implementation and Infrastructure Coding
- Source Code Management within Azure DevOps (Git) Repos
- DevOps integration with DevOps tooling, methodology, and processes
 - Drive Git and Infrastructure Development strategies
 - Drive Event Driven Architecture design
 - Drive Data Driven Infrastructure Coding
- Documentation, Knowledge transfer and cross-training with team, new staff and onboarded clients.

Technical Environment:

- **Public Cloud:** Amazon AWS Cloud (All Services)
- **Public Cloud:** Azure DevOps, Azure Active Directory, Azure Sentinel
- **Applications:** Microsoft Active Directory, Bash, Azure DevOps Git, Azure DevOps Pipelines, CloudFormation, Checkov Security Scanning (BridgeCrew/Prisma), TerraScan Security Scanning (Tenable)
- **Servers:** Microsoft Windows 2019, AWS Linux, CentOS, CIS Hardened Images

Project 12.2 Description - DevOps & AWS Development

The Analytics team are focused on designing, developing and deploying applications for data analysis that operate in the AWS Cloud to meet departmental analytical requirements provided data.

Project Outcomes:

Delivered critical analytics platform supporting border operations through AWS cloud-native architecture for client workload systems. Implemented comprehensive DevSecOps pipeline with automated security scanning and supply chain management, enabling secure data analysis capabilities.

Tasks Performed:

- Needs analysis, define requirements, and strategize architecture with AWS team.
- Architectural design and Proof of Concept (PoC) implementation for design review sessions
- Infrastructure as Code (IaC) Coding and review
 - AWS CLI, AWS API
 - Infrastructure As Code (IAC) - AWS CDK, AWS SDK, AWS CLI Scripting
- CI/CD Pipelines - AWS CodeCommit, AWS CodePipeline, AWS CodeBuild, AWS CodeDeploy

- Implementation and maintenance of CI/CD AWS Resources meeting best practices and agile deployment.
- Security and Governance reporting on Code and IaC to support DevSecOps compliance.
- Continuous improvement of Deployment Practices and Release Management:
 - Source Code Control - GIT & AWS CodeCommit
 - Development Practices - AWS Cloud9 and integrations for development team
 - Code Quality - SonarQube integration and reporting
 - Automation - Pipeline automation and continual enhancements
 - Security - Code supply chain management (container, python & node packages) using JFROG Artifactory
- Developer Tasks
 - Overlapping developer support for AWS Resources and Application Code
 - AWS Glue batch job architecture
 - AWS DMS (Database Migration Service)
 - AWS Serverless architecture
 - AWS Event Drive Architecture design and implementation

Technical Environment:

- **Public Cloud:** Amazon AWS Cloud (All Services)
- **Public Cloud:** Azure DevOps
- **Applications:** Bash, Azure DevOps, Git, Atlassian Jira, Code & IaC Security Scanning, JFROG Artifactory, SonarQube & Dependency Checker, AWS CDK v1.x, AWS CDK v2.x

11. Project 11 - SSC CSD R&D

Shared Services Canada

Cloud Services Directorate, Cloud Platform Engineering

Role: AWS Cloud Infrastructure as Code DevOps Engineer & Architect

September 2019 - January 2021

Project 11.1 Description - Cloud Services Directorate, Cloud Platform Engineering Project

The CSD R&D Project group are focused on generating a set of deployable Infrastructure as Code (IaC) for re-use within SSC and partners. Infrastructure as Code (IaC) supports automation of "CSD Landing Zone" integrating AWS Landing Zone customisation, SAA Security Guard Rails, and generic multi-purpose tools.

Developed and drove success and security achievements to ATO with AWS Secure Environment Accelerator.

Project Outcomes:

First team to achieve ATO status using AWS Secure Environment Accelerator (ASEA), establishing reusable Infrastructure as Code templates for government-wide adoption. Created foundational "CSD Landing Zone" architecture that became the standard for SSC cloud deployments, supporting critical workloads including SCED, DX, and Email systems.

Tasks Performed:

- Needs analysis, define requirements, and strategize architecture with AWS team
- Architectural design and Proof of Concept (PoC) implementation for design review sessions
- Infrastructure as Code (IaC) Coding
 - AWS CLI, AWS SDK/API
 - AWS CloudFormation
 - Terraform
- CI/CD CodePipeline, CodeCommit, CodeBuild, CodeDeploy
- GitLab, GitHub
- Implementation of IT Security Program to meet ITSG-22, ITSG-33 and ITSG-38 and TBS driven cloud guardrails and achieve iATO
- Design, secure and implementation of SSO Federation with Azure Active Directory
- Develop and implement Access Control Program and Posture to manage integration of AWS Cloud Identity components, with validated and acceptable RBAC permission scopes based on Actors, Users and System Role requirements
- Facilitated requirements gathering with technical team, architecture team, and security team to ensure all process and components are clearly captured and defined. Documentation of outcomes and design are shared with leadership and management.
- Client Deployment of AWS Native resources to provide governance and generate iATO evidence packages
- Source Code Management within GitLab
- DevOps integration with DevOps tooling, methodology, and processes
- Documentation, Knowledge transfer and cross-training with team, new staff and onboarded clients.
- Achieve ATO status for AWS Cloud
- Supporting onboarding of workloads (SCED, DX, Vocalls, Email)

Technical Environment:

- **Public Cloud:** Amazon AWS Cloud, AWS VPC, AWS CloudFront, AWS CloudWatch, AWS CloudTrail, AWS IAM, AWS EC2, AWS ECS, AWS SES, AWS S3, AWS RDS, AWS CloudFormation, AWS Service Catalog, AWS Route 53, AWS Systems Manager, AWS Trusted Advisor, AWS VPN, AWS ELB (Load Balancer), AWS ALB (Load Balancer), AWS Transit Gateway, AWS Transit Peering, AWS GuardDuty, AWS WAF & Shield, AWS Inspector, AWS Certificate Manager, AWS Auto-Scaling, AWS EBS Storage, AWS Managed SSO, AWS

CodeBuild, AWS CodePipeline, AWS Organizations, AWS Config, AWS Systems Manager

- **Applications:** Microsoft Active Directory, Bash, GitLab, GitHub, CloudFormation
- **Servers:** Microsoft Windows 2019, AWS Linux

10. Project 10 - DND DPDCS SMMS Replacement Project

Department of National Defence

SMMS Replacement Project, DPDCS

Role: Cloud Architect - Resilient Systems

February 2019 - December 2020

Project 10.1 Description - SMMS Search and Rescue Replacement Project

This project will replace the current SARMASTER software and hardware while providing reliable backup Site capability. It will provide interface capability to accept "live data" and the Geographic Information System (GIS). Lastly, the software will include long term support to ensure continued SAR operational readiness.

Project Outcomes:

Successfully modernized critical Search and Rescue operations system with zero downtime migration to AWS cloud infrastructure. Delivered containerized architecture using Docker/ECS with PostgreSQL, ensuring 24/7 availability for life-saving SAR operations across Canada while meeting stringent DND security requirements.

Tasks Performed:

- Project Management using Agile methodologies, and hybrid reporting
- Needs analysis, define requirements, and strategize high level Cloud Architecture
- Architectural design and PoC implementation with modernization of infrastructure
 - Docker - ECS Containers & externalisation of data strategy
 - AutoScaling - Scale of containers & scale of EC2 instances
 - Monitoring - CloudWatch and EventBridge based Event Driven Architecture and response to events
 - Application - Java, Tomcat/Apache, PostgreSQL applications
- Security Coordination and architectural alignment to required Guidelines (ITSG-33, DND & TSB Cloud Compliance)
- Implementation of IT Security to meet ITSG controls and achieve iATO
- Develop and implement Access Control Program and Posture to manage integration of AWS Cloud Identity components, with validated and acceptable RBAC permission scopes based on Actors, Users and System Role requirements.
- Facilitated requirements gathering with technical and systems team, business team and project

management, external stakeholders (user base,) and security teams. Worked with CONOPS and ISS (In-Service-Support) teams to ensure all business process components are captured and clearly documented.

- Review and realign infrastructure as required from continuous development cycles
- Staged implementation testing of services with inline remediation
- Internal feedback to development and operations for change coordination
- Integration to CI/CD pipeline, automation, and management systems
 - CI/CD - Git, Jenkins, CodePipeline, CodeCommit, CodeBuild, CodeDeploy
- Infrastructure as Code (IaC) deliverables in CloudFormation, deployed as Service Catalog Products for end user 'self-serve' deployment options
- Provide final architecture and documentation
- Pre-migratory testing and security reporting, and failure/high-availability testing
- Migration and cut-over processes
- Documentation, knowledge transfer and cross-training with Operations staff, Development staff, and Management

Technical Environment:

- **Public Cloud:** Amazon AWS Cloud, AWS VPC, AWS CloudFront, AWS CloudWatch, AWS CloudTrail, AWS IAM, AWS EC2, AWS ECS, AWS ECR, AWS SES, AWS S3, AWS EFS, AWS RDS, AWS CloudFormation, AWS Service Catalog, AWS Route 53, AWS Systems Manager, AWS Trusted Advisor, AWS VPN, AWS ELB (Load Balancer), AWS ALB (Load Balancer), AWS Transit Gateway, AWS Transit Peering, AWS GuardDuty, AWS WAF & Shield, AWS Inspector, AWS Certificate Manager, AWS Auto-Scaling, AWS EBS Storage, AWS Service Discovery, AWS Transfer Service (SFTP,) AWS Parameter Store, AWS Secrets Store
- **Applications:** PostgreSQL, Docker Containers, Bash, Terraform 0.12.7, Java 8.x, Tomcat 8.x, Atlassian JIRA, Atlassian Confluence, WSO2, Kafka, PHP, GIT, OpenLDAP, SOGO, ManageEngine Desktop Central, CloudFormation
- **Servers:** Microsoft Windows 2016, AWS Linux, CentOS 7.x

9. Project 9 - IDS Data Systems (New Democratic Party)

IDS Data Systems

Cloud Architect

Role: Cloud Architect

November 2018 - January 2019

This project supplemented the organizations workforce to complete two key cloud migration projects.

Project 9.1 Description - Office 365 Skype Migration - New Democratic Party of Canada

The client was migrating from a traditional distributed on-premise phone system to a fully virtualized Office 365 tenanted system.

Tasks Performed:

- Internal directory configuration reviews
- Migration planning and aligning to tool requirements
 - Active Directory Design and Management
 - Active Directory Federation Services
 - Exchange Online + Litigation/Auditing Features
 - Exchange Online Security Configuration and access policies
 - Microsoft Office Software and deployment strategies
 - Microsoft Skype for Business deployment
- Deployment of Office365 specific features to support Skype for Business
- Manage migration settings and deprecation of Cisco CUCM
- Implementation of IT Security and Cyber Protection to meet required Security Controls for Voice and Unified Communication Systems
- Facilitated requirements gathering with client technical and support teams, governance and security teams, key user stakeholders, and management to capture business process components, and drive documentation and design.
- Office 365 user configurations
- Office 365, Skype for Business, and Microsoft Teams Security and Policy writing
- PowerShell scripting and automation
- Migration Review and end user documentation
- Knowledge transfer and cross-training with internal teams and onboarded client

Technical Environment:

- **Public Cloud:** Microsoft Office 365, Microsoft Skype for Business, Microsoft Office 365 Compliance, Azure PowerShell

Project 9.2 - Server Workload Cloud Migration - New Democratic Party of Canada

The client was migrating a bespoke server workload, comprised of local database, compute functions, and public accessibility into the public cloud from traditional on-premise VMWare 6 infrastructure. The cloud transformation platform selected was Microsoft Azure.

Tasks Performed:

- Project Management using Agile methodologies, and hybrid reporting

- Needs analysis, define requirements, and strategize high level Cloud Architecture
- Architectural design and PoC implementation with modernization of infrastructure
 - Azure ARM, Resource Groups
 - Virtual Machine, Scale Sets, Availability Sets, Machine Images
 - Azure VNET, Load Balancers, Network Security Groups, Application Gateway
 - Azure Storage Accounts, Blob Storage, Block Storage
 - Azure PostgreSQL Database
 - CI/CD Jenkins automation deployment
 - Java, Spring and PostgreSQL application
 - ELK and ElasticSearch Application
 - Azure CLI, PowerShell and Terraform
- Staged implementation testing of services with inline remediation
- Internal feedback to development vendor and client IT operations for change coordination
- Implementation of IT Security and Cyber Protection to meet required Security Controls for data system maintaining voting citizen information, equivalent to Protected B data.
- PowerShell and Azure CLI based deployment automation, change management, and smoke tests
- Provide final architecture and documentation for production "blue-green" deployment
- Pre-migratory testing and security reporting, and failure/high-availability testing
- Knowledge transfer and cross-training with internal teams and support vendor

Technical Environment:

- **Public Cloud:** Microsoft Azure, Azure Resource Manager (ARM,) Azure Resource Groups, Azure Virtual Machines, Azure Virtual Machine Scale Sets, Azure Availability Sets, Azure Images, Azure Virtual Networks, Azure Load Balancers, Azure Network Security Groups, Azure Application Gateways, Azure Storage Accounts, Azure PostgreSQL Database, Cloudflare DNS, CloudFlare CDN
- **Applications:** Java, Tomcat, Apache, Elasticsearch, PowerShell, Azure PowerShell, Azure CLI
- **Servers:** CentOS 6/7, Windows 2012 R2, VMWare 6
- **Security:** WatchGuard (next-gen firewall,) Cloudflare WAF

8. Project 8 - SSC CITS SMG & CTMS

Shared Services Canada

CITS - Infrastructure Security

Role: Senior Business / Technical Architect

January 2018 - February 2019

Mr. Turner worked as a Senior Business and Technical Architect on several projects within the Cyber and Information Technology Security (CITS) Branch at Shared Services Canada. The CITS branch's focus is to protect the Government of Canada's (GC) systems and networks, as well as Canadians' information from cyber threats. SSC also supports Canada's foreign service, military and law enforcement personnel and contributes to national security by defending government systems and delivering information technology (IT) security services.

SSC's role in strengthening cyber and IT security:

- protects Canadians' privacy and information
- protects Canada's networks, systems, and sensitive data
- modernizes the GC's cyber and IT security infrastructure
- achieves broader GC IT security outcomes
- preserves Canada's competitive advantage, economic prosperity, and national security

Project 8.1 Description - SharePoint 2016 Design - July 2018 - February 2019

The client was implementing a SharePoint solution for managing and tracking tasks performed by a number of Security Management and Governance teams. Existing processes relied heavily on Microsoft Excel spreadsheets for reporting, with a non-standardized content.

Tasks Performed:

- Review the 'as-is' implementation and align it with the work methodologies and requirements for all SM&G teams.
- Using a simplified business process mapping and gap analysis strategy, created and refined key workflows to track the process from Business Intake, through Security Assessment (SA) process, and completion with milestone tracking and funding recovery tracking.
- Helped to design the system to standardize meta-data types and vernacular, enforcing data integrity and data value to create reports with meaningful statistics and actionable metrics.
- Implementation of consolidated data project management and reporting system for Security Assessment and Audit of projects across all GC departments, by SMG team.
- Facilitated requirements gathering with management and Director level to understand scope and high-level business process. Engaged with practitioner and assessor teams to provide gap analysis of business process and capture all components. Design and document and align with support team and management.
- Provided knowledge transfer and training to internal FTE staff

Project 8.2 Description - Atlassian JIRA Implementation - January 2018 - May 2018

The client was implementing JIRA for managing and tracking tasks performed by a number of Cyber Security teams. In addition to the JIRA implementation there were complimentary integrated implementations of Confluence and HipChat.

Tasks Performed:

- Reviewed the 'as-is' implementation and align it with the work methodologies and requirements for three teams.
- Created and used a simplified business process mapping and gap analysis strategy and refined key workflows and status types to enable workload management and timely reporting.
- Implementation of consolidated data project management and reporting system for Cyber Threat Management within CITS.
- Develop and implement Access Control Program and Posture to manage integration of CTMS Jira Users, with validated and acceptable RBAC permission scopes based on Actors, Users and System Role requirements for project access, and issue access.
- Facilitated requirements gathering with management level to understand scope and high-level business process. Engaged with business onboarding team, implementation team, and threat assessment hunt teams to map all areas of business process and capture all components. Design and document and align with support team and management.
- Implemented Backlog concepts, daily stand-up meetings, and Kanban for visualization.
- Standardized concepts and practices:
 - The utilization 'Definition of Ready' concepts defined dependencies to be completed before work can commence,
 - 'Acceptance Criteria' concepts defined core task output requirements,
 - 'Definition of Done' standardized the concept of describing a task as 'done' within the team.
 - All concepts were backed by JIRA customization to facilitate checklists to provide visualization and reporting metrics.
- Created and deployed an HA infrastructure into a VMWare ESXI 6 environment.
- Infrastructure was architected using NGINX as a Proxy/Load Balancer with JIRA, Confluence and HipChat instances running behind, backed by a PostgreSQL database on CentOS 7.
- All data volumes were LUKS encrypted, and traffic encrypted with SSL and properly signed certificates.
- Backups were performed daily via Bash Scripts capturing application, data, and database to a remote backup server.
- Provided knowledge transfer and training to internal FTE staff

Technical Environment:

- **Applications:** SharePoint 2016, JIRA, HipChat, Confluence, NGINX, Bash
- **Servers:** VMWare ESXI 6, CentOS 7, PostgreSQL, Windows 2012, GCDOCS, VMWare

7. Project 7 - Brookfield Renewable Energy Cloud Delivery

Brookfield Renewable Energy

Role: Office 365 & Cloud Delivery Manager

September 2017 - December 2017

Project 7.1 Description - Office 365 and Microsoft Azure Cloud Service Delivery Manager

The client was performing extensive internal change, due to growth via Mergers & Acquisition, requiring a change in support vendor. A consolidation of multiple Managed Service Providers was in flight to reduce to a more manageable number and create efficient internal workflows. The primary objective was to provide guidance and governance to the cloud services (Azure and Office365) support vendor, SoftChoice.

Tasks Performed:

- Provide guidance and governance to the cloud services (Azure and Office365)
- Provide management and oversight of vendor cloud architecture
- Oversight and governance for implementation of IT Security to meet NIST controls (eq. ITSG) for both publicly traded organizations and USA Utilities.
- Provided guidance and governance to Access Control Program and Posture to manage integration of Microsoft Office 365/Azure AD components, with validated and acceptable RBAC permission scopes based on Actors, Users and System Role requirements.
 - Office 365
 - Azure Active Directory
 - Microsoft Intune MDM (Mobile Device Management)
 - Azure VNET, VMs, ExpressRoute, LoadBalancing
- Provided guidance and governance to Mobile Security Program and Posture to manage roll-out of Microsoft Azure Intune (mobile compliance) system, with validated and acceptable RBAC permission scopes to published applications based on role and responsibility.
- Facilitated requirements gathering with tiger-team created from all business departments to represent key-users, included technical teams for support and implementation. Map additional processes defined by migration vendor and maintain regular meetings to ensure continuous alignment. Design and document and align with support team and management.
- Oversaw workload and workflow migration to Office365, and Azure Cloud
- Responsible for performance monitoring via standardized KPI's was required
- Provided knowledge transfer and training to internal FTE staff
- Additionally, responsible for day-to-day management of internal requests and tickets. This required management of in-house systems, Active Directory, on-premise E-mail and spam solutions, and Cisco

CUCM.

Technical Environment:

- **Cloud:** Microsoft Office 365, Microsoft Skype for Business, Microsoft Azure Cloud, Azure ExpressRoute, Azure InTune Mobile Device Management, Microsoft PowerShell
- **Servers:** Windows 2008R2, Active Directory

6. Project 6 - Lowe Martin DevOps

Lowe Martin Group

Role: DevOps

March 2017 - September 2017

Project 6.1 Description - Dev Ops

Role: DevOps & Architecture

The client was performing extensive internal change, which required the re-organization of the Software Development team from an unstructured and chaotic team into a fluid Agile and Scrum based team.

Tasks Performed:

- Project Management using Agile & Scrum techniques
- Project Management of IBM WebSphere, Java, and UIX projects
 - IBM WebSphere
 - DB2 Database
 - Java, and .Net application
 - CI/CD Pipeline - Jenkins
- Project Management of WebSphere Individual Customer Web "Store" for each customer, including templating of projects, tasks, and standards
- Configuration and management of Atlassian JIRA and Confluence project and space environments
- Facilitated requirements gathering with tiger-teams created from customer service teams, sales teams, direct client user representatives and senior management to map business process required for Agile workflow. Engaged with secondary team to drive new-scope requirement of ServiceDesk support, as discovered from Business Process documentation and Mapping. Design and document and align with support team and management.
- Implementation of consolidated data project management and reporting system for GC Client Departments. IT Security and Cyber Protection policies implemented to match ITSG, to meet client requirements.
- Provided guidance and governance for Access Control Program and Posture to manage integration of Atlassian JIRA components, with validated and acceptable RBAC permission scopes based on Actors,

Users and System Role requirements. Roles and users access included division of access to internal staff access, and external client access. Specific security planning considerations were made to restrict access and visibility to ticket contents, metadata, and data where applicable.

- Project Planning, Architecture, and Deployment of ITIL based ServiceDesk for integration into manufacturing and Smart-Factory environments
- Provided knowledge transfer and training to internal FTE staff
- Project Planning, Architecture and Upgrade Deployment of Xerox XMPie Suite
 - Implementation and integration of AWS Cloud components
 - Needs analysis, planning and design
 - Architecture and Service creation
 - Integration with internal systems and automation
- AWS Cloud Solution for Imagery Hosting
 - EC2, AutoScaling, Elastic Load Balancing
 - S3 Storage, IAM Policies
 - CloudWatch and Event Driven Architecture Design

Project 6.2 Description - Office 365 Migration from Exchange & Domino Environments

Role: Infrastructure Architect

The client was performing a planned migration from an on-premise mixed environment of Microsoft Exchange 2010 and Lotus Domino 9 to a completely hosted Office 365 environment. The quantity of mail objects was 2000+, including user mailboxes, shared mailboxes, group mailboxes, shared calendars, and resources.

Tasks Performed:

- Internal directory configuration reviews
- Migration planning and aligning to tool requirements
- Deployment of Office365 specific features
- Lotus Domino Migration to Exchange & Manual Migration processes
 - Active Directory Design and Management
 - Active Directory Federation Services
 - Exchange Online + Litigation/Auditing Features
 - Exchange Online Security Configuration and access policies
 - Microsoft Office Software and deployment strategies
 - Microsoft Skype for Business deployment
- Exchange Mailbox and Resource migration processes

- Implementation of IT Security and Cyber Protection Controls to secure and protect public facing mail systems, with relevant log (SIEM) integration. Map to ISO Security Controls.
- Provide guidance and governance whilst reviewing and implement Access Control Program to manage access to Microsoft Exchange Mail System, with integrated Active Directory Access components, with validated and acceptable RBAC permission scopes based on Actors, Users and System Role requirements for Exchange resource provisioning and access, mailbox access rights, and litigation hold access.
- PowerShell scripting and automation
- Migration Review and end user documentation with cross-training and knowledge transfer

Technical Environment:

- **Public Cloud:** Microsoft Office 365, Microsoft Skype for Business, Microsoft Office 365 Compliance, Amazon AWS Cloud, AWS VPC, AWS CloudFront, AWS CloudWatch, AWS CloudTrail, AWS IAM, AWS EC2, AWS SES, AWS S3,
- **Applications:** Xerox XMPie, Microsoft SQL Server 2014, Microsoft PowerShell, Selenium, Bash, Java 8.3, Tomcat 8.0, MySQL, DB2, Atlassian JIRA, Atlassian Confluence, Atlassian HipChat, BitTitan MigrationWiz, Exchange 2013, Lotus Domino 9
- **Servers:** Microsoft Windows 2008R2, Microsoft Windows 2012, RHEL 6.5

5. Project 5 - HighRoads US Cloud Migration

HighRoads (US - Boston, MA)

Role: Cloud Transformation & Cloud Architect

January 2017 - April 2017

Project 5.1 Description - Exchange Email Cloud Migration

January 2017 - April 2017

The client was undergoing extensive internal restructuring, right-sizing staffing and migrating services to the cloud to reduce costs and mitigate risks. The Office 365 was selected as the premium marketplace leader, with rich functionality that could be scaled with simplicity. A fully cloud based environment was supportive to restructuring and streamlining of the internal IT department and facilitating outsourced and offshore support.

Tasks Performed:

- Internal directory configuration reviews
- Migration planning and aligning to tool requirements
- Active Directory upgrades & reconfiguration
- Office365 Tenant Creation and Domain planning
- Deployment of Office365 specific features
 - Active Directory Design and Management

- Active Directory Federation Services
 - Exchange Online + Litigation/Auditing Features
 - Exchange Online Security Configuration and access policies
 - Microsoft Office Software and deployment strategies
 - Microsoft Skype for Business deployment
- Exchange Mailbox & Resource Migration & Cutover Process
- Facilitated requirements gathering with client teams created from multiple sites, with discrete Mail servers and Mail domains from M&A. Align user requirements and processes, including client/user access tools and delegated access types. Gather requirements from executive team for Office365 strategies, permitted apps, and integration into the process. Document complete process, and outcomes to facilitate hand-over to 3rd party support vendor.
- Implementation of IT Security and Cyber Protection Controls to secure and protect public facing mail systems, with relevant log (SIEM) integration. Map to multiple Security Controls - ISO:27001, NIST, and HIPAA.
- Provide guidance and governance whilst reviewing and implement Access Control Program to manage access to Microsoft Exchange Mail System, with integrated Active Directory Access components, with validated and acceptable RBAC permission scopes based on Actors, Users and System Role requirements for Exchange resource provisioning and access, mailbox access rights, and litigation hold access. Additional scope for non-integrated access to MimeCast cyber security services.
- PowerShell scripting and automation
- Migration Review and end user documentation
- Decommission of Exchange Server Services
- Provide documentation, knowledge transfer, and cross-training

Project 5.2 Description - Atlassian Project Management Cloud Migration

March 2017 - April 2017

Client was migrating all on premise services into cloud/SaaS versions to support a change in internal IT Strategy, and re-org reducing IT head count. The Atlassian JIRA and Confluence product was to be maintained, although utilizing the "on demand" cloud version. Primary objective was to migrate new projects into the cloud version, whilst maintaining legacy/historical projects in the on-premise version as read-only. As the project progressed, we strategized that migrating the historical projects into the cloud was a best fit, as the on-premise version could be fully deprecated, and no additional costs would be incurred with the cloud platform.

Tasks Performed:

- Project Management using Waterfall methodologies
- Migration planning and needs analysis

- Production application upgrade path process
- Test driven change management to remediate cloud feature-function manual configurations
- Migration process and cut over
- Bash & SQL Scripting and automation
- Facilitated requirements gathering with tiger-teams created from the organization as a whole, as a global solution. Facilitate meetings and discovery sessions with development teams, QA teams, professional services teams, internal IT Support, Sales teams, business stake holders (TAM's and Product Owners) and external support vendors. Create business process maps and flows to capture end-to-end process and review with end-users to confirm. Perform gap analysis, and document as defined Workflows for implementation
- Implementation of IT Security and Cyber Protection Controls to secure and protect project management and development integration system, with relevant log (SIEM) integration. Map to multiple Security Controls - ISO:27001, NIST, and HIPAA. Additional controls required to secure with use of offshore sub-contractors.
- Develop and implement Access Control Program and Posture to manage integration of CTMS Jira Users, with validated and acceptable RBAC permission scopes based on Actors, Users and System Role requirements for project access, and issue access. Integration of JIRA Directory with Active Directory and assumption of Multi-Factor Authentication
- Migration Review and end user documentation
- End-User enablement for self-serve operations
- Migration of on-premise servers into AWS cloud
- On-premise servers decommission
- AWS Cloud automation for archiving and "auto-build & start" process for legacy system lookups
- Provide documentation, knowledge transfer, and cross-training

Technical Environment:

- **Public Cloud:** Microsoft Office 365, Microsoft Office 365 Compliance, Microsoft Skype for Business, Microsoft Office 365 Compliance, Microsoft SharePoint Online, Amazon AWS Cloud, AWS EC2, AWS RDS, AWS SES, AWS S3, AWS CloudWatch, AWS CloudFormation, AWS CloudTrail, AWS IAM, AWS Certificate Manager, AWS WAF
- **Applications:** MySQL, Exchange 2013, Active Directory, PowerShell, Bash, Atlassian JIRA, Atlassian Confluence
- **Servers:** Microsoft Windows 2008R2, Microsoft Windows 2012, VMWare 5.5, VMWare 6, RedHat 6.5, CentOS 6, CentOS 7
- **Security:** Fortinet FortiGate, Fortinet FortiGuard, Check Point FW, F5 Big-IP LTM, Syslog-NG, ME EventLog Analyzer

4. Project 4 - HighRoads Canada Inc. Infrastructure Operations Manager

HighRoads Canada Inc. (Ottawa, ON)

Role: DevOps, Operations and Cloud Architect; Project Management

June 2015 - December 2016

Project Outcomes:

Migrated 40+ production workloads from VMware to AWS, reducing costs by 35% and improving platform resilience. Delivered active-passive HIPAA-compliant DR architecture meeting strict NIST RTO/RPO objectives. Introduced DevOps and automation practices improving deployment frequency by 50% while operationalizing 3 hybrid AWS/on-prem architectures supporting 100+ workloads. Standardized engineering workflows enabling effective collaboration across 15-person off-shore engineering team.

Project 4.1 Description - AWS Cloud Migration (In-house custom SaaS platform)

December 2015 - December 2016

Architected and managed the migration and implementation of on-premise systems into the AWS cloud platform. This involved right-sizing systems, provisioning micro-service based architecture and leveraging cloud-based security principles. We realized a significant increase in simplicity to manage, time-to-implement and were able to leverage intelligent AWS native solutions for backup and DR.

Project Outcomes:

Successfully migrated 40+ production workloads from VMware to AWS, achieving 35% cost reduction through cloud optimization and improved platform resilience. Implemented AWS-native solutions for backup and DR while transitioning to micro-service based architecture for enhanced scalability and manageability.

Tasks Performed:

- Project Management using Agile methodologies, and hybrid reporting
- Needs analysis, define requirements, and plan migration route
- Architectural design and PoC implementation
 - AWS Cloud, IAM, SQS, SNS, SES
 - AWS EC2; Elastic Load Balancing, Auto-Scaling Groups, Lambda
 - S3 Storage, Elastic Block Store, Elastic File System
 - AWS RDS, EC2 Oracle (BYOD)
 - VPC, CloudFront, Route53
 - CloudWatch (Events & Metrics,) CloudTrail, Config, SystemsManager, Trusted Advisor
 - AWS CloudFormation, TerraForm v0.7, SALT, bespoke scripting, GIT, Bamboo, Jenkins

- Docker - Java/Tomcat Container Applications
- Market compliance under HIPAA & NIST guidelines
- Facilitated requirements gathering with tiger-teams created from the organization as a whole, as a primary product solution. Facilitate meetings and discovery sessions with development teams, QA teams, professional services teams, internal IT Support, Sales teams, business stake holders (TAM's and Product Owners,) external support vendors, and customer representatives. Create business process maps to capture discrete processes for client onboarding, client data and solution maintenance, client special projects, and internal process including IT Support, industry audit processes, financial related processes and people related processes. Document and capture flows as required.
- Implementation of IT Security and Cyber Protection Controls to secure and protect customer facing SaaS solution, with relevant log (SIEM) integration. Map to multiple Security Controls - ISO:27001, NIST, and HIPAA.
- Develop and implement Access Control Program and Posture to manage integration of External Client directories with application-based permission system, with validated and acceptable RBAC permission scopes based on Actors, Users and System Role requirements for project access, and issue access. Additional integration of IT Systems Administration staff with restricted permission sets to non-client data areas, and de-identified data-based shadow and sandbox systems.
- Review and realign infrastructure with cloud offerings
- Staged migratory testing of services with inline remediation
- Internal feedback to development and operations for change coordination
- Provide final architecture and documentation
- Provide documentation, knowledge transfer, and cross-training
- Migration and cut-over processes

Project 4.2 Description - SaaS System: DevOps Infrastructure

June 2015 - September 2016

A traditional hosted customer facing CMS system was in production that was originally designed for an alternate market, with simple web GUI drive access and a cumbersome offline client. Highroads was designing a new "V2" system and was in development as a fully SaaS product with both web GUI access and customer available API access. Infrastructure was required to support the SaaS product, provide reliable operations, secure access, and customer data, and enable customer driven Single Sign-On integration.

Project Outcomes:

Introduced comprehensive DevOps and automation practices improving deployment frequency by 50% and eliminating manual deployment steps through CI/CD pipeline implementation. Standardized engineering workflows enabling effective collaboration across 15-person off-shore engineering team while implementing hybrid AWS/on-premise architecture patterns.

Tasks Performed:

- Project Management using Agile methodologies, and hybrid reporting

- Needs analysis, define requirements, and plan migration route
- Architectural design and PoC implementation with modernization of infrastructure
 - AWS Cloud, IAM, SQS, SNS, SES
 - AWS EC2; Elastic Load Balancing, Auto-Scaling Groups, Lambda
 - S3 Storage, Elastic Block Store, Elastic File System
 - AWS RDS, EC2 Oracle (BYOD)
 - VPC, CloudFront, Route53
 - CloudWatch (Events & Metrics,) CloudTrail, Config, SystemsManager, Trusted Advisor
 - AWS CloudFormation, TerraForm v0.7, SALT, bespoke scripting, GIT, Bamboo, Jenkins
 - VMWare 5.5 & 6.0, Citrix XenServer, Redhat RHEV, RedHat RHEL, Redhat Satellite & Moonwalk
 - Docker - Java/Tomcat Container Applications, Syslog-NG, BMC Insights
- Security Coordination and alignment to required Guidelines (HIPAA & NIST)
- Implementation of IT Security and Cyber Protection Controls to secure and protect customer facing SaaS solution, with relevant log (SIEM) integration. Map to multiple Security Controls - ISO:27001, NIST, and HIPAA.
- Develop and implement Access Control Program and Posture to manage integration of External Client directories with application-based permission system, with validated and acceptable RBAC permission scopes based on Actors, Users and System Role requirements for project access, and issue access. Additional integration of IT Systems Administration staff with restricted permission sets to non-client data areas, and de-identified data-based shadow and sandbox systems
- Facilitated requirements gathering with tiger-teams created from the organization as a whole, as a primary product solution. Facilitate meetings and discovery sessions with development teams, QA teams, professional services teams, internal IT Support, Sales teams, business stake holders (TAM's and Product Owners,) external support vendors, and customer representatives. Create business process maps to capture discrete processes for client onboarding, client data and solution maintenance, client special projects, and internal process including IT Support, industry audit processes, financial related processes and people related processes. Document and capture flows as required
- Review and realign infrastructure as required
- Staged migratory testing of services with inline remediation
- Internal feedback to development and operations for change coordination
- Internal changes to CI/CD pipeline, automation, and management systems
- Provide final architecture and documentation
- Pre-migratory pen-testing and security reporting, load testing, and failure/high-availability testing
- Migration and cut-over processes
- Documentation preparation for Operations staff, Development staff, and Management, knowledge transfer and cross-training

Project 4.3 Description - Infrastructure Decommission & Migration

October 2015 - April 2016

An asset sale required a project to divest software, development environments, QA environments, staging environments, demo environments, training environments, DR environments, and production environments for the "V1" software product. Secondary systems including monitoring, security analysis, edge networking (firewalls, load balancers, etc.,) and backup systems had to be either migrated to the purchasing company with replacements provisioned in Highroads infrastructure, or newly provisioned identical systems provisioned in DirectPath infrastructure. Tertiary systems requiring migration and/or new provisioning included corporate applications (Wiki's, CI/CD software, JIRA, etc.,) physical office installations and office hardware.

To be compliant with the Sale Agreement and Transitional Services Agreement 80% of the work had to be carried out by Highroads with zero down-time to either organization in a timely manner as defined in the sale documentation. A significant percentage of the sale value was held in escrow until completion and approval of the purchasing company.

Project Outcomes:

Delivered active-passive HIPAA-compliant DR architecture meeting strict NIST RTO/RPO objectives while ensuring zero downtime migration of production systems. Successfully orchestrated complex asset divestiture with 80% completion requirement, achieving escrow fund release through comprehensive disaster recovery and business continuity implementation.

Tasks Performed:

- Project Management using Waterfall methodologies
- Stakeholder reporting and meetings with C-Level executives and Board Members
- Needs analysis, define requirements, and plan migration route
- Architectural design and PoC implementation with modernization of infrastructure
 - AWS Cloud, IAM, SQS, SNS, SES
 - AWS EC2; Elastic Load Balancing, Auto-Scaling Groups, Lambda
 - S3 Storage, Elastic Block Store, Elastic File System
 - AWS RDS, EC2 Oracle (BYOD)
 - VPC, CloudFront, Route53
 - CloudWatch (Events & Metrics,) CloudTrail, Config, SystemsManager, Trusted Advisor
 - AWS CloudFormation, TerraForm v0.7, SALT, bespoke scripting, GIT, Bamboo, Jenkins
 - Docker - Java/Tomcat Container Applications, Oracle WebLogic, Oracle 11, Syslog-NG, BMC Insights
- Security Coordination and alignment to required Guidelines (HIPAA & NIST)
- Implementation of IT Security and Cyber Protection Controls to secure and protect customer facing SaaS solution, with relevant log (SIEM) integration into migration target company's data centre. Map to multiple Security Controls - ISO:27001, NIST, and HIPAA.
- Perform "safe" deconstruction and decommission of legacy data centre and hosted solutions, including

safe decommission of data storage and certified destruction client data, hosted application data, and historical log data.

- Develop and implement Access Control Program and Posture to manage migration and eventual hand-over of systems to purchasing company. Define solution to provide interim access to key personnel, based on RBAC requirements with permissions declining based on a combination of timelines and milestones met. Create new Access Control Program and Posture to support 'post-migration' remaining components. Scope includes physical data centre access and secure building access permission sets.
- Facilitated requirements gathering with tiger-teams created from purchasing organization and selling organization as a whole, as a primary product solution. Facilitate meetings and discovery sessions with development teams, QA teams, professional services teams, internal IT Support, Sales teams, business stake holders (TAM's and Product Owners,) external support vendors, and customer representatives. Create business process maps to capture discrete processes for client onboarding, client data and solution maintenance, client special projects, and internal process including IT Support, industry audit processes, financial related processes and people related processes. Additional focus for overlapping process to facilitate legal hand-over period for support, and milestones to capture separation of processes from seller to purchaser to ensure release of funds from Escrow. Document and capture flows as required, and report to senior management.
- Staged migratory testing of services with inline remediation
- Internal feedback to development and operations for change coordination
- Internal changes to CI/CD pipeline, automation, and management systems
- Provide final architecture and documentation
- Pre-migratory pen-testing and security reporting, load testing, and failure/high-availability testing
- Migration and cut-over processes
- Decommission of legacy hardware, separation of hardware
- Project Close-Out, Stakeholder reporting, Legal/Financial reporting for disbursement of Escrow fund compliance
- Documentation preparation for Operations staff, Development staff, Management, and external acquiring company,

Project 4.4 Description - Operations Decommission & Migration

May 2016 - December 2016

In Q4 2016 Highroads announced the closure of their Canadian offices, with subsequent planned closure of the Canadian company. IT Operations was to be fully handed over to various outsourced vendors, physical presence within the Ottawa office was to be immediately deprecated and the closure of the data centre supporting the "V1" application was to be planned. Primary objective was to identify all internal IT Operations functions that we carried out purely from the Ottawa office, and relocate those processes and functions to outsourced vendors. Key focus was placed on risk mitigation from lack of presence and established staff.

Project Outcomes:

Operationalized 3 hybrid AWS/on-prem architectures supporting 100+ workloads with scalable and secure patterns. Successfully transitioned operations to outsourced vendors while maintaining business continuity and ensuring seamless hand-over of production systems to parent operations in Boston, MA.

Tasks Performed:

- Project Management using Waterfall methodologies
- Stakeholder reporting and meetings with C-Level executives and Board Members
- Needs analysis, define requirements, and plan migration route
- Review and realign infrastructure with cloud offerings
 - AWS Cloud, IAM, SQS, SNS, SES
 - AWS EC2; Elastic Load Balancing, Auto-Scaling Groups, Lambda
 - S3 Storage, Elastic Block Store, Elastic File System
 - AWS RDS, EC2 Oracle (BYOD)
 - VPC, CloudFront, Route53
 - CloudWatch (Events & Metrics,) CloudTrail, Config, SystemsManager, Trusted Advisor
 - AWS CloudFormation, TerraForm v0.7, SALT, bespoke scripting, GIT, Bamboo, Jenkins
 - Docker - Java/Tomcat Container Applications, Oracle WebLogic, Oracle 11, Syslog-NG, BMC Insights
- Security Coordination and alignment to required Guidelines (HIPAA & NIST)
- Implementation of IT Security and Cyber Protection Controls to secure and protect customer facing SaaS solution, with relevant log (SIEM) integration. Map to multiple Security Controls - ISO:27001, NIST, and HIPAA. Validation of migrated system, verification to meet HIPAA compliance.
- Develop and implement Access Control Program and Posture to manage migration and eventual hand-over of systems to parent operations in Boston, MA office. Define solution to provide interim access to key personnel, based on RBAC requirements with permissions declining based on a combination of timelines, milestones met, staff onboarding and lay-off structure. Create new Access Control Program and Posture to support 'post-migration' remaining components. Scope includes physical data centre access and secure building access permission sets
- Facilitated requirements gathering with tiger-teams created from the organization as a whole, as a primary product solution. Facilitate meetings and discovery sessions with development teams, QA teams, professional services teams, internal IT Support, Sales teams, business stake holders (TAM's and Product Owners,) external support vendors, and customer representatives. Create business process maps to capture discrete processes in migrated, post deprecation environments, for client onboarding, client data and solution maintenance, client special projects, and internal process including IT Support, industry audit processes, financial related processes and people related processes. Document and capture flows as required
- Staged migratory testing of services with inline remediation
- Internal feedback to development and operations for change coordination

- Internal changes to CI/CD pipeline, automation, and management systems
- Provide final architecture and documentation
- Migration and cut-over processes
- Preparation and planning for decommission of legacy hardware, separation of hardware
- Project Close-Out and handover
- Documentation preparation for Operations staff, Development staff, Management, and external outsourced support company, including cross-training and knowledge transfer

Technical Environment:

- **Hybrid Architecture:** 3 hybrid AWS/on-prem architectures supporting 100+ workloads with scalable patterns
- **Migration Scale:** 40+ production workloads migrated from VMware to AWS with 35% cost reduction
- **Public Cloud:** Amazon AWS (EC2, ELB, Auto-Scaling, Lambda, S3, EBS, EFS, RDS, VPC, CloudFront, Route53, CloudWatch, CloudTrail, Config, Systems Manager), Microsoft Azure, NaviSite Cloud
- **DevOps Automation:** 50% improvement in deployment frequency with CI/CD pipeline automation
- **Compliance:** HIPAA-compliant active-passive DR architecture meeting NIST RTO/RPO objectives
- **Team Collaboration:** Standardized workflows for 15-person off-shore engineering team
- **Private Data Centre:** Tier3 certified data centres Rogers Data Centres, NaviSite Data Centres
- **Applications:** Oracle 10g, MS Exchange, Active Directory, OpenLDAP, PingFed Identity Management, Atlassian JIRA, Atlassian Bamboo, Atlassian Confluence, Atlassian HipChat, Nagios Monitoring, SolarWinds Monitoring, OpManager Monitoring, Observium Monitoring, Syslog-NG, UniTrends Enterprise Backup, Microsoft Project 2013, Gerrit GIT, Apache SVN, SALT, Java, Tomcat, Apache, SOLR, IIS, .NET, Azure PowerShell, Azure ARM, AWS CloudFormation
- **Servers:** RHN Satellite, Windows 2008, Windows 2012, RedHat RHEL / CentOS 5.5/6.0/7, VMWare 5.5, VMWare 6, Citrix XenServer 6.5
- **Security:** Cisco Catalyst, FortiGate Firewall, FortiGate FortiGuard, FortiOS IPS, CheckPoint Firewall, CheckPoint IDS/IPS, F5 Big-IP LTM, Snort, Syslog-NG, rsyslog, Splunk, AlienVault, PFSense SquidGuard, CheckPoint DLP, Nagios, SolarWinds, Tenable Nessus

3. Project 3 - Dymon Corporation - Infrastructure Manager

Dymon Corporation

Role: Operations and Infrastructure Architect

December 2014 - June 2015

Project 3.1 Description - Operations Virtualization

December 2014 - May 2015

The Dymon corporate infrastructure was operating on unique physical hardware per server and per service. We identified 8 physical servers of identical capacity that were running at less than 20% utilization, in one instance 0% utilization. Switching and network was analyzed, and we identified 3 totally unused Layer 3 switches with zero utilization. An architecture was created to migrate to a fully virtualized infrastructure, segregate corporate traffic with various VLANs to support operations, POS systems, publicly accessible web services, CCTV data, and credit transactions in addition to iSCSI traffic, virtualization traffic, monitoring traffic, and Building Automation traffic.

Tasks Performed:

- Stakeholder reporting and meetings with CIO
- Needs analysis, define requirements, and plan migration route
- Review and realign infrastructure plan with budget limitations
 - HP ProCurve Switching with Cisco Top-of-Rack Switches & Sophos UTM
 - HP Switching and MPLS Integration
 - WhiteBox Server Hardware Cluster
 - Citrix XenServer Clustering & Replicated NAS Storage
 - Linux CentOS Workload Servers
- Security Coordination and alignment to required Guidelines (PCI Compliance)
- Implementation of IT Security and Cyber Protection Controls to secure and bespoke hosted Self-Storage system, with compliance to PCI-DSS 3.0.
- Facilitated requirements gathering within organization with consideration to distributed workforce, with varying internal business offerings and processes. Capture processes for discrete line of businesses (storage, residential healthcare, construction, solar.) Map high-level business processes and engage with user base to verify and perform gap analysis. Document processes and utilize for defining security and risk points as well as general strategy and architecture.
- Staged migratory testing of services with inline remediation
- Migration and cut-over processes
- Preparation and planning for decommission of legacy hardware, separation of hardware
- Project Close-Out and handover
- Documentation preparation for Operations staff, and training, including cross-training and knowledge transfer

Project 3.2 Description - Remote Desktop Services (RDS)/ Thin Client Implementation

January 2015 - June 2015

The Dymon Health Care retirement residences were operating with heavily aged systems that incurred excessive amounts of downtimes, ran various operating systems and various versions of software. A frequent churn of nursing staff required unique profiles to be created on each system repeatedly. We identified a number of different solutions, with selection being given to a Terminal Server (RDS) / Thin Client solution where roaming profiles were available to each staff member, and data was centralized into the corporate servers away from the local desktops. Our objective was to leverage technology to reduce the overhead of managing systems, and staff related issues, whilst consolidating services, centralizing data, and incorporating into corporate backups.

Tasks Performed:

- Stakeholder reporting and meetings with CIO & Health Care COO
- Needs analysis, define requirements, and plan transformation
 - Citrix XenServer Virtualization Cluster & Defined NAS Storage Cluster for RDS User and centralised data
 - Windows 2012 R2 Remote Desktop Services Cluster
 - Active Directory design and management for isolation of RDS Users
 - WyseTerminal Hardware & Virtual Terminals on existing hardware
- Security Coordination and advisory process
- Staged migratory testing of services with inline remediation
- Migration and cut-over processes
- Implementation of IT Security and Cyber Protection Controls to secure and bespoke hosted Self-Storage system, with compliance to Canadian PIPEDA
- Preparation and planning for repurposing or decommission of legacy hardware
- Project Close-Out and handover
- Documentation preparation for Operations staff, and training, including knowledge transfer and cross-training.

Project 3.3 Description - Sales Software & POS Infrastructure System Upgrade

May 2015 - June 2015

A vendor driven change to end-user credit transaction PIN pads required Dymon Storage to update their credit transaction software, Line of Business integration module, merchant banking authentication and physical handsets with zero downtime realized to storage facilities. The POS Upgrade object was to replace the PIN pads, upgrade and reconfigure each unit and complete a site within 45 minutes. Pre-testing verification was performed, followed by installation testing a transaction verification of the installation, with post-implementation reporting verified the back-end allocations.

Tasks Performed:

- Stakeholder reporting and meetings with CIO, COO, and Chief Accountant
- Needs analysis, define requirements, and plan transformation
- Security Coordination and advisory process
- Lab-based PoC testing
- Migration and cut-over processes
- Implementation of IT Security and Cyber Protection Controls to secure and bespoke hosted Self-Storage system, with compliance to PCI-DSS 3.0.
- Facilitated requirements gathering within organization with healthcare operations, operating as three discrete businesses and organizations. Capture processes for discrete businesses, plus centralized roll-up reporting into parent company.
- Map high-level business processes and engage with key team-leads to verify and perform gap analysis. Document processes and utilize for defining security and risk points as well as general strategy and architecture.
- Project Close-Out and handover
- Documentation preparation for Operations staff, and training including cross-transfer and knowledge transfer

Technical Environment:

- **Public Cloud:** Microsoft Office 35
- **Private Data Centre:** Physical on-premise locations
- **Applications:** Active Directory, SpiceWorks Helpdesk, SysAid ITIL Helpdesk, ManageEngine OpManager Monitoring, Symantec Backup Exec, UniTrends Backup, Microsoft Project 2010 Server, Sage Timberline Suite, IIS, .NET, Shift4 Payment Processing, DHL Total Recall ERP
- **Servers:** Physical Servers, Citrix XenServer, VMWare 5.5, CentOS, Windows 2003, Windows 2008, Windows 2012, Windows 2008 Terminal Services, Windows 2012 RDS
- **Networking:** Cisco Switches, HP ProCurve
- **Security:** Sophos UTM (NextGen FW,) rsyslog, Syslog-NG, SolarWinds, ME OpManager Monitoring

2. Project 2 - GeoDigital International Inc. Infrastructure Manager

GeoDigital International (GeoSpatial Engineering)

Role: Operations and Infrastructure Architect

September 2011 - December 2014

Project Outcomes:

Successfully designed and deployed GIS SaaS platform on AWS serving 500+ global clients across 15 countries with 99.5% uptime. Engineered 1-2 TB/day data ingestion pipeline improving engineering timelines by 50%, while managing infrastructure operations for 8 production and engineering environments supporting 25+ engineering staff with 99.8% data processing reliability.

Project 2.1 Description - "PAS - Photo Acquisition Service" SaaS Cloud Application

May 2012 - December 2014

GeoDigital created a market pioneering SaaS application utilized by premium US insurance companies to provide a Photo Acquisition Service (PAS) system to provide on-the-fly imagery and extrapolated engineering metrics for roofing claims. API integration provided the customer's agents the ability to receive zip bundles of imagery along with PDF descriptors of building dimensions, including pitch, slope, and height via single click integration to customer's proprietary Line of Business (LoB) application. Primary objective was to design, architect, and develop a fully sustainable and scalable SaaS infrastructure that could grow vertically and horizontally as utilization increased with growth of customer of customer base, and could grow in feature functionality as additional market requirements were serviced. The Application was deployed with a cloud-first initiative delivering integration with client desktop delivery with a hybrid-cloud backend.

Project Outcomes:

Successfully deployed market-leading SaaS platform serving 500+ global insurance company clients across 15 countries with 99.5% platform uptime. Delivered scalable cloud-first architecture supporting real-time imagery processing and automated PDF report generation, enabling single-click integration with client Line of Business applications.

Tasks Performed:

- Project managed and deliverables tracked with Agile Project methodologies and Sprint based cadences
- Needs analysis, define requirements, and identify cloud provider (AWS & RackSpace)
- Architectural design and PoC implementation with alignment to cloud services
 - AWS EC2 Linux Instances & AWS EC2 Windows Instances
 - AWS ELB Load Balancers & AutoScaling & AWS CloudFront
 - AWS S3 Storage & AWS EC2 EBS
 - AWS CloudWatch & AWS SNS & AWS SES
 - "Secure" data links & delivery redirected to On-Premise Datacentre
- Security Coordination and alignment to required Guidelines (NERC, FISMA & NIST)
- Implementation of IT Security and Cyber Protection Controls to hosted SaaS platform for US Markets. Compliance required for ISO:27001, NERC and NIST.
- Facilitated requirements gathering within organization R&D team for new application process. Created tiger team with primary customer, as an early adopter, to drive product and process maps for

consumption. Facilitated interactions with internal support teams, development teams, sales and business teams, and finance teams to capture business process requirements. Created documentation and performed transformation functions to move to operational model.

- Develop and implement Access Control Program and Posture to manage operations access for SAAS application, based on RBAC requirements with integrations from internal departments and external vendor support. Provide guidance and governance for directory creation to support customer access types, with application data management roles.
- Staged build and deployment of cloud infrastructure and on-premise infrastructure
- Internal feedback with development and operations for coordination
- Internal integration to CI/CD pipeline, automation, and management systems
 - Automation Scripting (Bash, Python, MS Batch)
 - Hudson-Jenkins CI/CD Tooling
 - Visual SVN Subversion Version-Control System
- Generate final architecture and documentation
- Pre-migratory pen-testing and security reporting, load testing, and failure/high-availability testing with alignment to customer requirement reporting
- Go-Live and release
- Documentation preparation for Operations staff, Development staff, and Management including cross-training and knowledge transfer

Project 2.2 Description - Data Centre Migration (Vancouver, BC - Ottawa, ON)

May 2012 - September 2012

The client required the migration of physical data centre from Vancouver On-Premise location to Ottawa Tier 2 Data Center. Architecture migration of 750TB production IBM FC SAN storage, IBM FC SAN & Tivoli System 200TB Backup/Archival Storage, 2000 Windows 2008R2 Servers, and VMWare 5.0 IBM Cluster. An expedited timeline was in place due to the termination of facility contracts, and no local staff. Additional risk was identified due the size of data, and GIS Airborne Acquisition data loss would require the physical re-flight of areas and financial exposure and damage to the organization.

Tasks Performed:

- Project Management using hybrid Agile and waterfall methodologies
- Needs analysis, define requirements, and extreme risk with project
- Vendor Selection Advisory and Vendor Engagement
- Vendor Management & Project Management with focus to high risk and severe impacts
- Provisioning of supporting infrastructure and data centre services
 - IBM SAN & Brocade FC Switch Fabric

- IBM Tivoli Backup System & IBM SAN & LTO5 Tape Array
- IBM VMWare HyperVisor Cluster & Microsoft Windows 2012 Cluster
- Child Workload VM's of various nature (LiDAR Processing & related)
- Dell PowerConnect Network Switching & Cisco Top of Rack Switching
- Coordination and advisory services to organization departments (Sales, PMO, Production, Acquisition, and Executive Teams) for impact and expected interruption
- Generate final architecture and supporting documentation
- Pre-migratory planned tasks, including risk mitigation processes
- Migratory cut-over including on-site management and advisory with receiving data centre
- Post-migration management of changes and integrations
- Implementation of IT Security and Cyber Protection Controls to hosted SaaS platform for US Markets. Compliance required for ISO:27001, NERC and NIST.
- Facilitated requirements gathering with tiger-teams created from the organization. Facilitate meetings and discovery sessions with development teams, QA teams, professional services teams, internal IT Support, Project Management teams, Sales teams, business stake holders (TAM's and Product Owners,) external support vendors, and customer representatives. Create business process maps to capture discrete processes for field LiDAR acquisition and transfer, QA processes, LiDAR engineering production processes, backup and maintenance processes, data archival processes, and client delivery processes, as affected by the migration. Transform previous process workflow to a new 'post-migration' workflow.
- Develop and implement Access Control Program and Posture to manage operations access for remote production infrastructure stack, based on RBAC requirements with integrations from internal operations staff, production 'super-user' types, automation systems, and external vendor support. Integration with local directories, and external vendor based ticketing system for automated reactive maintenance.
- Documentation preparation for Operations staff, Production staff, and Management including cross-training and knowledge transfer

Project 2.3 Description - Corporate Private Cloud (Data Centre Architecture)

September 2012 - August 2013

As a multi-petabyte data handling organization, GeoDigital required a robust and richly featured solution for handling data archiving, data retention, and data integrity. Leveraging Tier II and Tier III secure data centres with enterprise scale storage platforms for automated scaling data storage management this project served the identified requirements of all Business Units. The solution had to create and manage a complete 'corporate software directory' of internal tools for workflow maximization based on business requirements, providing fully self-serve managed environments.

Tasks Performed:

- Project Management using hybrid Agile & Waterfall methodologies

- Stakeholder reporting and meetings with Executive teams and operations teams
- Needs analysis, define requirements for project
- Advisory services for technology selection and cloud provider integrations
- Architectural design and lightweight PoC implementation
 - Dell PowerConnect Network Switching & Cisco Top-of-Rack switching
 - Dell PowerEdge Server Clusters & Bespoke Dell PowerVault Rack
 - NexentaStor Software Defined Storage Cluster presenting Block Storage Volumes and Object Storage Shares with automated snapshotting and intelligent data-tiering
 - Redhat Linux RHEL & CentOS Linux Cluster and Virtualization (Xen & KVM)
 - Integration with AWS Cloud for off-site replication and storage-bursting using AWS S3 buckets
- Security Coordination and alignment to required Guidelines (NERC, FISMA & NIST)
- Implementation of IT Security and Cyber Protection Controls to hosted SaaS platform for US Markets. Compliance required for ISO:27001, NERC and NIST.
- Facilitated requirements gathering with tiger-teams created from the organization. Facilitate meetings and discovery sessions with development teams, QA teams, professional services teams, internal IT Support, Project Management teams, Sales teams, business stake holders (TAM's and Product Owners,) external support vendors, and customer representatives. Create business process maps to capture discrete processes for field LiDAR acquisition and transfer, QA processes, LiDAR engineering production processes, backup and maintenance processes, data archival processes, and client delivery processes, as affected by the migration. Transform previous process workflow to a new 'post-migration' workflow.
- Develop and implement Access Control Program and Posture to manage operations access for remote production infrastructure stack, based on RBAC requirements with integrations from internal operations staff, production 'super-user' types, automation systems, and external vendor support. Integration with local directories, and external vendor based ticketing system for automated reactive maintenance.
- Vendor Selection Advisory and Vendor Engagement
- Vendor Management & Project Management
- Provisioning of supporting infrastructure and data centre services
- Staged integration of new services with existing infrastructure, and inline remediation
- Manage internal feedback to operations for change coordination
- Manage internal changes automation, and management systems
- Provide final architecture and documentation
- Build, deploy and integrate process
- Project Close-Out,
- Documentation preparation for Operations staff including knowledge-transfer and cross-training

Project 2.4 Description - On-Premise Data Centre Virtualization

September 2012 - August 2013

Due to growth by corporate acquisitions, the client operated multiple physical locations without a centralized standardized IT Infrastructure platform. This project managed the migration from physical servers and unstructured virtual servers, to a standardized virtualization platform leveraging Hyper-V as a single vendor platform. It provided full license management and auditing, ensured right-sizing of resources for daily operations and future growth. Mr. Turner steered strategy to ensure maximization of virtualization platform and resources.

Tasks Performed:

- Project Management using hybrid Agile & Waterfall methodologies
- Stakeholder reporting and meetings with Executive teams and operations teams
- Needs analysis, define requirements for project
- Advisory services for technology selection and infrastructure integrations
- Architectural design and structure planning
 - Dell PowerConnect Network Switching & Cisco Top-of-Rack switching
 - Dell PowerEdge Server Clusters & Bespoke Dell PowerVault Rack
 - NexentaStor Software Defined Storage Cluster presenting Block Storage Volumes with automated snapshotting and intelligent data-tiering to on-prem data centre
 - VMWare 5,x Virtualization Cluster
 - Integration with AWS Cloud for off-site replication and storage-bursting using AWS S3 buckets
- Security Coordination and alignment to required Guidelines (NERC, FISMA & NIST)
- Implementation of IT Security and Cyber Protection Controls to LiDAR and engineering production IT Infrastructure platform for US Markets. Compliance required for ISO:27001, NERC and NIST.
- Develop and implement Access Control Program and Posture to manage operations access for remote production infrastructure stack, based on RBAC requirements with integrations from internal operations staff, production 'super-user' types, automation systems. Integrations via Active Directory systems.
- Facilitated requirements gathering with tiger-teams created from the organization. Facilitate meetings and discovery sessions with development teams, QA teams, professional services teams, internal IT Support, Project Management teams, Sales teams, business stake holders (TAM's and Product Owners,) external support vendors, and customer representatives. Create business process maps to capture discrete processes for field LiDAR acquisition and transfer, QA processes, LiDAR engineering production processes, backup and maintenance processes, data archival processes, and client delivery processes, as affected by the migration.
- Vendor Selection Advisory and Vendor Engagement
- Vendor Management & Project Management
- Provisioning of supporting infrastructure and data centre services
- Staged integration of new services with existing infrastructure, and inline remediation

- Manage internal feedback to operations for change coordination
- Manage internal changes automation, and management systems
- Provide final architecture and documentation
- Build, deploy and integrate process
- Project Close-Out,
- Documentation preparation for Operations staff

Project 2.5 Description - Corporate Hybrid Cloud (Production & Field Acquisition Systems)

December 2013 - September 2014

The client expanded operations and business markets out of North America and into the Australasia region. The client requirement was to limit expansion, and cost, to only airborne data acquisition teams without incurring any significant support staff, or production staff footprint. Leveraging public cloud partners in Sydney, Australia (RackSpace,) cloud partners in North America (Amazon AWS US,) colocation Data Centre partners (Rogers) and on-premises data centre to create an holistic and end-to-end data management system for hands-off and lights-out management of acquisition data. Data was acquired in Sydney, Australia at the rate of 1TB per day, and handed off by GIS field staff to RackSpace Cloud's data centre personnel. Data was then processed via automation scripts and replicated across cloud partners and to on-premises sites for production staff.

Project Outcomes:

Engineered automated 1-2 TB/day data ingestion pipeline improving engineering processing timelines by 50% through multi-cloud architecture spanning Australia, North America, and Asia. Achieved 99.8% data processing reliability across global cloud partners while managing 8 production and engineering environments supporting 25+ engineering staff.

Tasks Performed:

- Project Management using hybrid Agile and waterfall methodologies
- Needs analysis, define requirements, and identify cloud providers
- Architectural design and PoC implementation with multi-vendor integration
 - RackSpace Compute Instances & Database Instances
 - RackSpace Data Ingestion (Up to 2TB per day on bare drives) at Sydney data centre
 - Automated Data validation, manifest validation and replication into AWS Cloud
 - AWS EC2 Linux Instances
 - AWS ELB Load Balancers & AutoScaling & AWS CloudFront
 - AWS S3 Storage & AWS EC2 EBS
 - AWS CloudWatch & AWS SNS & AWS SES
 - Data replication from AWS to off-shore data analysts in Asia and in-house data analysts in California USA, Minnesota USA, British Columbia CA, & Ottawa CA.

- Security Coordination and alignment to required Guidelines (NERC, FISMA & NIST)
- Implementation of IT Security and Cyber Protection Controls to hosted client data processing platform for US Energy and Utilities Markets. Compliance required for ISO:27001 and NIST.
- Facilitated requirements gathering with tiger-teams created from the organization. Facilitate meetings and discovery sessions with development teams, QA teams, professional services teams, internal IT Support, Project Management teams, Sales teams, business stake holders (TAM's and Product Owners,) external support vendors, and customer representatives. Create business process maps to capture discrete processes for field LiDAR acquisition and transfer, QA processes, LiDAR engineering production processes, backup and maintenance processes, data archival processes, and client delivery processes, as affected by the migration. Transform previous process workflow to a new 'post-migration' workflow.
- Develop and implement Access Control Program and Posture to manage operations access for remote production infrastructure stack, based on RBAC requirements with integrations from internal operations staff, production 'super-user' types, automation systems, and external vendor support. Integration with offline remote directories, and external vendor based ticketing system for automated reactive maintenance.
- Staged build and deployment of cloud infrastructure and on-premise infrastructure
- Internal feedback with development and operations and GIS Acquisition for coordination
- Internal integration to CI/CD pipeline, automation, and management systems
- Generate final architecture and documentation
- Pre-migratory pen-testing and security reporting, load testing, and failure/high-availability testing with alignment to customer requirement reporting
- Go-Live and release
- Documentation preparation for Operations staff, Development staff, and Management

Project 2.6 Description - Office 365 Cloud Migration

September 2011 - December 2012

The client intended to manage risk and centralize mail management into a streamlined cloud platform after growth through mergers and acquisitions. With various offices having been integrated from separate companies and organizations a number of mail systems, and mail domains were operating in stand-alone silos. A targeted strategy was created to consolidate mail and migrate directly into the new Office 365 platform, with a zero-mailbox loss, and zero interruption requirement.

Tasks Performed:

- Project Management using hybrid Agile and waterfall methodologies
- Internal directory configuration reviews
- Migration planning and aligning to tool requirements
- Active Directory upgrades & reconfiguration
- Office365 Tenant Creation and Domain planning

- Deployment of Office365 specific features
- Exchange Mailbox & Resource Migration & Cutover Process
- PowerShell scripting and automation
- Implementation of IT Security and Cyber Protection Controls to secure and protect public facing mail systems, with relevant log (SIEM) integration. Map to ISO:27001 and NIST Security Controls
- Provide guidance and governance whilst reviewing and implement Access Control Program to manage access to Microsoft Exchange Mail System, with integrated Active Directory Access components, with validated and acceptable RBAC permission scopes based on Actors, Users and System Role requirements for Exchange resource provisioning and access, mailbox access rights, and litigation hold access
- Facilitated requirements gathering with tiger-team created from all business departments to represent key-users, included technical teams for support and implementation. Map additional processes defined by migration vendor and maintain regular meetings to ensure continuous alignment. Design and document and align with support team and management.
- Migration Review and end user documentation
- Decommission of Exchange Server Services
- Operational support and maintenance

Technical Environment:

- **Public Cloud:** Amazon AWS (EC2, S3, ELB, AutoScaling, CloudFront, CloudWatch, SNS, SES), RackSpace Cloud, Microsoft Azure, Microsoft Office 365, Google GCP
- **Multi-Region Deployment:** 15 countries globally with cloud-native architecture
- **Data Processing:** 1-2 TB/day automated ingestion pipeline with 99.8% reliability
- **Platform Scale:** 500+ global clients with 99.5% uptime across 8 production environments
- **Private Data Centre:** Physical on-premise location, Rogers Tier 2, ATT Tier 3
- **Applications:** Multiple GIS Platforms, SharePoint, QuickBase, Salesforce, MS SQL, MySQL, MS Exchange 2010, Active Directory, ManageEngine ServiceDesk Pro, ManageEngine OpManager Monitoring, Symantec BackupExec, Veeam Backup, Microsoft Project 2010, VisualSVN
- **Servers:** Windows 2008 R2, Windows 2012, VMWare 5.5, Linux KVM, RedHat RHEV, Microsoft Hyper-V, Citrix XenServer
- **Networking:** Cisco Catalyst, Cisco IOS Routers, Dell PowerConnect
- **Security:** Cisco ASA, FortiNet FortiGate, Snort, F5 Big-IP LTM, Nagios, Solar Winds, New Relic Monitoring, ME OpManager Monitoring

1. Project 1 - Central Wire Industries Infrastructure Manager

Central Wire Industries

Infrastructure & Operations

Role: Operations and Infrastructure Management

May 2007 - September 2011

Project 1.1 Description - IT Integration of fully automated production systems (Fond du Lac, Wisconsin)

January 2010 - March 2011

Central Wire Industries, as a \$500 million annual revenue enterprise, expanded its operations with purchase of a smart-factory requiring integration of all aspects of automation, including IT Systems, ERP and MRP systems. This project required the introduction of GE Fanuc Smart Automation, and various smart SCADA systems into the manufacturing process, configuration of smart-factory automation platform software, and integration via scheduled interfaces and data transform XML process into centralized AS/400 based Lawson Movex (M3) and Info BPCS ERP/MRP suites.

Tasks Performed:

- Project Management using waterfall methodologies
- Needs analysis, define requirements, and trusted vendors
- Identify additional requirements to support "lights-out" manufacturing plant supported by only skeleton crew personnel
- Vendor Management and advisory services for integration
- Management and facilitation of on-premise automation system configuration with Plant Manager
- Architect, design, and implement IT automation routines for data transfer to centralized AS/400 systems and business applications
- Integration of SNMP monitoring to smart-factory systems plus regular IT Infrastructure
- Fail-over testing planning and testing to verify on-site documentation comprehensiveness for non-technical staff
- Facilitated requirements gathering with between facility production team, facility management, corporate production team, material purchasing team, external vendors, and IT teams. Map process and define requirements, and document.
- Implementation of IT Security and Cyber Protection Controls to manufacturing ERP systems, data systems, general IT Infrastructure, and facility automation (Smart-Factory) including provisioning for client data to satisfy United States NOFORN classification, for US DOD. Compliance required for ISO:27001 and NIST.
- Generate final architecture and documentation
- Go-Live and release

Project 1.2 Description - ADP Payroll Systems Migration (Citrix Virtualization, Platform Upgrade, Database Migration)

January 2010 - March 2011

The client had expanded its market share and physical locations by an increase of 60% over the previous few years, seeing a growth in staff with the final onboarding of nine physical sites across the United States of America and Canada. ADP was selected as the corporate vendor for providing consolidated payroll services across the company, requiring the implementation of new infrastructure to support a significantly larger application cluster. Corporate directive required that the physical infrastructure be managed from Canada, with HR and Finance Payroll staff operating from USA locations, and corporate finance operating out of Canada.

Tasks Performed:

- Project Management using waterfall methodologies
- Needs analysis, define requirements, and vendors requirements
- Vendor Management and advisory services for integration
- Architectural design and implementation planning
- Security Coordination and alignment for finance and payroll requirements
- Vendor Engagement and coordination
- Provisioning of supporting infrastructure and Citrix Desktop streaming services
- Staged integration of new services with existing infrastructure, and inline remediation
- Manage internal feedback to operations for change coordination
- Manage internal changes automation, and management systems
- Cutover and migration of data and access
- Facilitated requirements gathering with between HR teams, finance teams, US Finance executives, Canadian Finance executives, external vendors and IT teams. Map process and define requirements, and document.
- Implementation of IT Security and Cyber Protection Controls to manufacturing ERP systems, data systems, general IT Infrastructure. Compliance required for ISO:27001 and NIST.
- Provide guidance and governance whilst reviewing and implement Access Control Program to manage access to Corporate HR Systems and Payroll systems, with integrated Active Directory Access components, with validated and acceptable RBAC permission scopes based on Actors, Users and System Role requirements for HR Processes.
- Provide final architecture and documentation
- Build, deploy and integrate process
- Project Close-Out,
- Documentation preparation and training for Operations staff, HR Staff, and Finance Staff

Technical Environment:

- **Private Data Centre:** Physical on-premise location
- **Applications:** SharePoint, Salesforce, MS SQL, MySQL, Oracle 9, MS Exchange 2007, Active Directory,

ManageEngine ServiceDesk Pro, ManageEngine OpManager Monitoring, Symantec BackupExec, Lawson MOVEX (M3), Info BPCS, Infor Syteline

- **Servers:** Windows 2003, Windows 2008, SCO Unix, AS/40, IBM WebSphere
- **Networking:** Cisco Catalyst, Cisco IOS Routers,
- **Security:** Cisco ASA, Nagios, Solar Winds, ME OpManager Monitoring, rsyslog, Syslog-NG

TECHNOLOGY INDEX

Comprehensive alphabetical reference of all technologies with project cross-references

A:

- **Active Directory** - Projects 1, 2, 3, 4, 6, 7, 12, 13
- **ADP Payroll Systems** - Project 1
- **AlienVault** - Project 4
- **Apache** - Projects 2, 8, 9
- **Apache SVN** - Project 4
- **ArgoCD** - Projects 14.1, 14.2
- **Argo Workflows** - Projects 14.1, 14.2
- **Atlassian Bamboo** - Project 4
- **Atlassian Confluence** - Projects 4, 6, 8, 9, 14
- **Atlassian HipChat** - Projects 4, 6
- **Atlassian JIRA** - Projects 4, 6, 8, 9, 11, 14
- **AWS (Amazon Web Services)** - Projects 2, 4, 5, 6, 9, 10, 11, 12, 13, 14
- **AWS Certificate Manager** - Projects 10, 11
- **AWS CloudFormation** - Projects 10, 11, 12, 13
- **AWS CloudFront** - Projects 6, 10, 11
- **AWS CloudTrail** - Projects 6, 10, 11, 14.2
- **AWS CloudWatch** - Projects 6, 10, 11, 14.2
- **AWS CodeBuild** - Project 11
- **AWS CodePipeline** - Project 11
- **AWS Config** - Projects 11, 14.2
- **AWS Control Tower** - Project 14.2
- **AWS ECS** - Project 11
- **AWS EKS (Elastic Kubernetes Service)** - Projects 14.1, 14.2

- **AWS GuardDuty** - Projects 11, 14.2
- **AWS IAM** - Projects 6, 10, 11
- **AWS Lambda** - Projects 13, 14.2
- **AWS Organizations** - Projects 11, 14.2
- **AWS RDS** - Project 11
- **AWS S3** - Projects 6, 11
- **AWS SES** - Projects 6, 11
- **AWS SSO** - Projects 11, 14.2
- **AWS Systems Manager** - Project 11
- **AWS Transit Gateway** - Projects 11, 14.2
- **AWS VPC** - Projects 6, 10, 11, 14.2
- **AWS X-Ray** - Project 14.2
- **Azure** - Projects 4, 7, 8, 12
- **Azure Active Directory** - Projects 12, 13
- **Azure CLI** - Project 8
- **Azure DevOps** - Projects 11, 12, 13, 14
- **Azure ExpressRoute** - Project 7
- **Azure InTune** - Project 7
- **Azure PowerShell** - Projects 4, 7, 8
- **Azure Resource Manager (ARM)** - Projects 4, 8
- **Azure Sentinel** - Project 13

B:

- **Bash** - Projects 2, 4, 6, 8, 9, 10, 11, 12, 13, 14
- **BitTitan MigrationWiz** - Project 6

C:

- **CDK (AWS Cloud Development Kit)** - Projects 11, 14
- **CDK8s** - Project 14
- **CentOS** - Projects 3, 4, 8, 9, 10, 11, 12, 13, 14
- **Certificate Manager (AWS)** - Projects 10, 11
- **Check Point** - Projects 4, 6
- **Checkov Security Scanning** - Projects 12, 13, 14
- **Cilium** - Project 14.2

- **Cisco ASA** - Projects 1, 2
- **Cisco Catalyst** - Projects 1, 3
- **Cisco IOS** - Project 1
- **CIS Hardening** - Projects 12, 13, 14
- **Citrix XenServer** - Projects 1, 2, 3
- **CloudFlare** - Projects 8, 9
- **CloudFormation** - Projects 10, 11, 12, 13
- **CloudFront** - Projects 6, 10, 11
- **CloudTrail** - Projects 6, 10, 11, 14.2
- **CloudWatch** - Projects 6, 10, 11, 14.2
- **Crossplane** - Projects 14.1, 14.2

D:

- **DB2** - Project 6
- **Docker** - Projects 9, 14.1, 14.2
- **Docker Images** - Project 14.2

E:

- **EKS (Elastic Kubernetes Service)** - Projects 14.1, 14.2
- **Elasticsearch** - Projects 8, 14.2
- **Exchange** - Projects 1, 5, 6

F:

- **F5 Big-IP LTM** - Projects 1, 2, 4, 6
- **FortiGate** - Projects 1, 2, 4, 6
- **FortiGuard** - Projects 4, 6
- **FortiOS IPS** - Project 4

G:

- **GCDocs** - Project 8
- **Gerrit GIT** - Project 4
- **Git** - Projects 9, 11, 12, 13, 14
- **GitLab** - Projects 10, 11, 14
- **GitHub** - Project 11
- **GitOps** - Projects 14.1, 14.2
- **Golang** - Projects 14.1, 14.2

- **Grafana** - Project 14.2

H:

- **Helm** - Projects 14.1, 14.2
- **HIPAA Compliance** - Project 4
- **HP ProCurve** - Project 2

I:

- **IIS** - Project 4
- **Info BPCS** - Project 1
- **Infor Syteline** - Project 1
- **Infrastructure as Code (IaC)** - Projects 10, 11, 12, 13, 14
- **ITSG Compliance** - Projects 11, 13

J:

- **Java** - Projects 4, 6, 8, 9
- **Jenkins** - Project 14
- **JFROG Artifactory** - Project 11
- **JSON** - Project 14.2

K:

- **Kafka** - Project 9
- **KCL (Configuration Language)** - Project 14.2
- **Kubernetes** - Projects 14.1, 14.2
- **kubeadm** - Project 14
- **kind** - Project 14
- **k3d** - Project 14

L:

- **Lawson MOVEX (M3)** - Project 1
- **Load Balancers** - Projects 8, 14.2
- **Lotus Domino** - Project 6

M:

- **ManageEngine** - Projects 1, 9
- **Microsoft Office 365** - Projects 5, 6, 7, 9
- **Microsoft PowerShell** - Projects 4, 6, 7, 8

- **Microsoft Project** - Project 4
- **Microsoft SQL Server** - Projects 1, 6
- **Microsoft Windows** - Projects 1, 2, 3, 4, 7, 10, 11, 12
- **MySQL** - Projects 1, 6, 9

N:

- **Nagios** - Projects 1, 2, 4
- **.NET** - Project 4
- **New Relic** - Project 2
- **NIST Compliance** - Projects 4, 10, 11

O:

- **OCI Bundles** - Project 14.2
- **Office 365** - Projects 5, 6, 7, 9
- **OpenLDAP** - Projects 4, 9
- **OpManager** - Projects 1, 2, 9
- **Oracle** - Projects 1, 4

P:

- **PHP** - Project 9
- **PingFed Identity Management** - Project 4
- **PostgreSQL** - Projects 8, 9
- **PowerShell** - Projects 4, 6, 7, 8
- **Prisma** - Projects 12, 13, 14
- **Prometheus** - Project 14.2
- **Python** - Projects 9, 14.1, 14.2

R:

- **RDS (Remote Desktop Services)** - Project 3
- **RedHat RHEL** - Projects 4, 6
- **RHN Satellite** - Project 4
- **rsyslog** - Projects 1, 2, 4

S:

- **SALT** - Project 4
- **SCO Unix** - Project 1
- **Selenium** - Project 6

- **SharePoint** - Projects 1, 8
- **Skype for Business** - Projects 6, 7, 9
- **Snort** - Projects 1, 2, 4
- **SOGO** - Project 9
- **SolarWinds** - Projects 1, 2, 4
- **SOLR** - Project 4
- **SonarQube** - Project 11
- **Sophos UTM** - Project 2
- **Splunk** - Project 4
- **Symantec BackupExec** - Project 1
- **Syslog-NG** - Projects 1, 2, 4, 6

T:

- **Tenable Nessus** - Project 4
- **TerraScan** - Project 12
- **Terraform** - Projects 9, 14.1, 14.2
- **Tomcat** - Projects 4, 6, 8, 9
- **TypeScript** - Projects 14.1, 14.2

U:

- **UniTrends** - Project 4

V:

- **VMware** - Projects 1, 2, 3, 4, 8
- **VMware ESXI** - Projects 4, 8

W:

- **WatchGuard** - Project 8
- **WebSphere** - Project 1
- **Windows Server** - Projects 1, 2, 3, 4, 7, 10, 11, 12
- **WSO2** - Project 9

X:

- **Xerox XMPie** - Project 6

Y:

- **YAML** - Project 14.2