

1.4 INFRASTRUCTURE TRANSITION MANAGER STAFF QUALIFICATIONS

INFRASTRUCTURE TRANSITION MANAGER					
PART 1 – RÉSUMÉ					
Contractor	Accenture LLP				
Candidate Name	Miguel O. De Ramas, Jr.				
Position in the Company	Mobilization Associate Director	Length of Time in Position	1 year		
Project Position & Responsibilities	Infrastructure Transition Manager Miguel meets the requirements as defined in RFP section 12.1.3.6.4.				
Skills & Qualifications for Project Position	<p>Skills: Miguel is an experienced transition manager who uses his skills in transition management, project management, change management, transformation, and collaboration to help clients complete IT-based transitions to new and modernized platforms and systems. Miguel is a planner who creates transition approaches (methodology, description of work streams, activities, and deliverables) that lead to stable transition execution. He is a leader of cross-functional delivery teams and a collaborator who works beside his clients during transitions.</p> <p>Qualifications: For 18 years, Miguel has managed and delivered operational transition activities on projects involving large and complex IT systems (MQ I-S15: Exceeds) for clients in government, resources, and products industries. He has delivered transition programs with complex transformational and technology shifts using waterfall and agile delivery methods. He has delivered transition-related services across major offering segments—platform, cloud, end user, service management, human resources, network, security, and next-generation services. Miguel manages the successful transition of large and complex IT systems from one company or contract to another, and he has done so on more than two projects. We highlight five projects here, each lasting longer than three months (MQ I-S16: Exceeds). He has led projects and programs in major industries with highly complex operating environments, applications, infrastructure build, migration to cloud, operations establishment, and service desk integration.</p>				
Relevant Experience (Add additional tables as needed)					
Project Title	Huntsman IT Managed Services				
Position Title	Transition Manager				
Begin Date	09/2022	End Date	02/2023	# of Months	4 months (through Dec 2022)
Scope and Description of Responsibility	<p>Scope: Miguel managed the successful transition for the Huntsman IT Managed Services project, a multi-tower engagement (application outsourcing and infrastructure outsourcing (AO/IO), security, and service desk) across multiple geographic locations.</p> <p>Responsibility: Miguel led a global transition team of more than 500 personnel utilizing Information Technology Infrastructure Library (ITIL) and Scaled Agile Framework (SAFe) program management principles. Miguel trained personnel on tools and processes and conducted analysis of risks and issues associated with the transition.</p>				

INFRASTRUCTURE TRANSITION MANAGER

Skills Utilized and Experience Attained	Skills Utilized: Miguel used his skills in program management, Agile delivery methods, and communication to lead the transition in a highly complex operating environment. Experience Attained: Miguel managed the end-to-end execution of the transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of transition execution activities.				
Project Title	McCormick Transition				
Position Title	Transition Manager				
Begin Date	10/2021	End Date	03/2022	# of Months	6 months
Scope and Description of Responsibility	Scope: Miguel managed the overall transition for the McCormick Transition and managed communications with the McCormick team, provided transition solution support, and created a new transition governance structure. Responsibility: Miguel led a global transition team of over 200 personnel, utilizing ITIL, and SAFe program management principles. He coached and upskilled his mobilization team members and new joiners and worked closely with McCormick leadership to maintain and update project timelines and deliverables.				
Skills Utilized and Experience Attained	Skills Utilized: Miguel used his expertise in transition management, project management, and change management to manage and lead the transition. Experience Attained: Miguel established a strong governance structure between Accenture and McCormick leadership teams and met with McCormick leadership daily and maintained an accurate transition timeline.				
Project Title	State of Arizona, Health-e-Arizona Plus (HEAPlus) Maintenance and Operations (M&O)				
Position Title	Transition Manager				
Begin Date	10/2020	End Date	06/2021	# of Months	9 months
Scope and Description of Responsibility	Scope: Miguel managed all infrastructure transition-in activities to deliver a successful transition of infrastructure, applications, security, and IT services for the State of Arizona Health-e-Arizona Plus (HEAPlus) Maintenance and Operations (M&O) Project. Responsibility: Miguel led a global transition team of more than 150 personnel across North America and India, utilizing ITIL program management principles and regularly facilitated leadership stakeholder meetings to ensure a smooth transition.				
Skills Utilized and Experience Attained	Skills Utilized: Miguel managed the end-to-end execution of HEAPlus transition activities including the development of the detailed transition plan, knowledge transfer sessions, job shadowing, operational readiness assessment. Experience Attained: Miguel managed the transition of the maintenance and operations for the State of Arizona's integrated eligibility system (HEAPlus), a large and complex IT system, which serves over 3,900 state workers and over 1.9 million Arizonans.				
Project Title	Chesapeake Energy Corporation AO/IO Transition				
Position Title	Transition Manager				
Begin Date	06/2020	End Date	09/2020	# of Months	4 months

INFRASTRUCTURE TRANSITION MANAGER

Scope and Description of Responsibility	Scope: Miguel successfully led the AO/IO transition with a global team of 100 personnel across North America and India for the Chesapeake Energy Corporation, a multitower transition over four months. Responsibility: Miguel led a transition team utilizing ITIL program management principles in support of the transition of 300 non-SAP applications. He was also responsible for due diligence and joint transition planning.				
Skills Utilized and Experience Attained	Skills Utilized: Miguel used his skills in transition management, program management, and transformation to manage the transition of the multitower Chesapeake Energy Corporation transition (AO/IO). Experience Attained: Miguel led the transition within four months with no production disruption with teams working remotely in Canada, the U.S., and India.				
Project Title	Exelon ePeople Transition				
Position Title	Transition Manager				
Begin Date	02/2018	End Date	07/2018	# of Months	6 months
Scope and Description of Responsibility	Scope: Miguel managed the successful transition for the ePeople Transition project for an Oracle HCM (Human Capital Management) cloud solution involving multiple modules such as payroll, finance, and reporting and the set-up of infrastructure and tools across multiple geographic locations. Responsibility: Miguel led a global transition team of more than 200 personnel utilizing Information Technology Infrastructure Library (ITIL) program management principles. Miguel trained personnel on tools and processes and conducted analysis of risks and issues associated with the transition and managed regular checkpoints with Exelon team members and leadership.				
Skills Utilized and Experience Attained	Skills Utilized: Miguel used his skills in program management, Agile delivery methods, and communication to lead the transition in a highly complex operating environment. Experience Attained: Miguel managed the end-to-end execution of the transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of cutover activities.				
Education (add rows as needed)					
Years	Course of Study	School			
06/1998 – 03/2004	B.S., Electronics and Communications Engineering	University of Science and Technology of Southern Philippines			
Professional Certifications or Designations (add rows as needed)					
Certification or Designation	Organization	Dates			
ITIL v3 Foundation	EXIN	February 2011			
SAFe 5.1 Agilist	Scaled Agile, Inc	August 2021			

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE	
Minimum Qualification I-S15	A minimum of 18 months of experience within the past ten (10) years, performing operational transition activities on Projects involving large and complex IT systems.
Project #1	Contact #1
Company Name: Huntsman	Contact Name: [REDACTED]
Project Name: IT Managed Services (Project Imagine)	Company Name: Huntsman
Time Period: September 1, 2022 – February 28, 2023	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Transition Manager	
<p><i>Description of relevant experience:</i></p> <p>The IT Managed Services (Project Imagine) project meets the definition of “large and complex IT system,” based on the following criteria defined in the RFP:</p> <ol style="list-style-type: none"> 1. Integrates with at least two applications, one of which is a COTS: The transition of Huntsman’s IT Managed Services involved the support of all applications and underlying technology, including integration with SAP HANA, a COTS enterprise resource planning (ERP) platform, and an IBM Planning Analytics Tool for business performance management, and Accenture proprietary applications, including myWizard. 2. Interfaces with at least five external systems, at least one of which is real-time: Huntsman’s IT services interface with several external systems, including warehouse interfaces, banking interfaces, vendor interfaces, customer interfaces, government interfaces, and carrier interfaces, which operate in real-time. 3. Is accessed by at least 1,000 users at multiple locations: The solution is accessed by over 9,000 users across more than 70 production facilities in 30 countries. 4. Has a contract value of at least \$10 million: The solution contract value is \$110 million. 5. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms: The solution features multi-tiered processing, including a user-facing front end. It provides portal access to business users to facilitate key business processes such as reporting, costing run analysis, variance and result analysis, master data maintenance, adjustment, and revaluation. <p>As the Transition Manager, Miguel’s responsibilities included:</p> <ul style="list-style-type: none"> Managed operational transition activities for the IT Managed Services Project, a large and complex IT project in the resources industry, which transitioned from in-house and incumbent to Accenture Managed the end-to-end execution of transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of transition execution activities 	

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- **Successfully completed the transition on time and on budget**
 - **Led a global transition team of over 500 personnel in North America, APAC, EMEA (Accenture, Huntsman, Incumbent combined), utilizing ITIL, and SAFe program management principles**
 - Developed, delivered, maintained and executed a Transition-In plan in coordination with Huntsman that served as a master document for seamless transition
 - Worked alongside Huntsman team and incumbent to identify gaps in standard operating procedures and to provide best practices to fill those gaps
 - Performed gap analysis between existing documents and industry best practices to identify areas for change in Huntsman plans including process gap assessments on existing service management processes and incorporated Accenture best practices
 - Developed working plans for Huntsman based on the Transition-In Work Plan and prepared reports for Huntsman containing direct outputs from the Transition-In Work Plan
 - Scheduled meetings to do walk-through of deliverables and answered any questions to expedite deliverable approvals, led to quicker review turnaround and deliverable approvals and on-time submission
 - Developed, delivered, maintained, and executed a Transition-In Work Schedule with Huntsman and updated as needed until transition completion
 - Scheduled, tracked, documented, recorded, and shared agendas and meeting minutes for daily, weekly, and monthly transition meetings
 - Developed, delivered, and maintained an integrated master schedule/work plan for the full project scope, which included transition plans for infrastructure, applications, security, and automation
 - Created a comprehensive risk management and service continuity plan to comply with attrition impacts, business criticality and Huntsman's zero outage transition requirements
 - Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
 - Facilitated leadership stakeholder meetings with Huntsman, Accenture, and third party vendor executives
 - Managed due diligence, joint transition planning, and transition execution activities
 - Managed set-up and testing of the service desk L1 support across multiple regions including the U.S., Europe, Middle East, and Africa (EMEA), and Asia-Pacific (APAC)
 - Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
- Collaboration:**
- Worked collaboratively with Huntsman's existing IT services to understand client-specific operating processes and requirements to accomplish a smooth transition of all IT Managed Services' infrastructure components, including with the incumbent contractor to align on the roles and responsibilities, activities, and schedule for transitioning services
 - Collaborated with the Huntsman's transition manager to implement and manage a comprehensive project transition office and related communications

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- Worked closely with the Huntsman's transition manager to plan, manage, execute, and close out transition activities and support alignment across transition teams
- Led daily, weekly, and monthly meetings with Huntsman executives and internal and external stakeholders to discuss the progress of transition activities

Project #2	Contact #2
Company Name: McCormick	Contact Name: [REDACTED]
Project Name: McCormick Transition	Company Name: McCormick
Time Period: October 1, 2021 – March 31, 2022	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Transition Manager	
<p><i>Description of relevant experience:</i></p> <p>The McCormick Transition project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:</p> <ol style="list-style-type: none"> 1. Integrates with at least two applications, one of which is a COTS: The McCormick Transition involved the support of all applications and underlying technology, including the integration with SAP HANA, a COTS enterprise resource planning (ERP) platform, Denodo, which is a data virtualization platform for data service creation and delivery, and Accenture proprietary applications, including myWizard. 2. Interfaces with at least five external systems, at least one of which is real-time: McCormick's IT services interface with several external systems, including EUSHEETS supplied by Selerant, which is used to manage complex declarations on external documentations, which operates in real-time. Other external systems include CAS TPM, CCure, Hamilton Grant, Longstars, and Invar. 3. Is accessed by at least 1,000 users at multiple locations: The solution is accessed by over 20,000 users across multiple geographic locations including U.S., APAC, and EMEA. 4. Has a contract value of at least \$10 million: The solution contract value is \$30 million. 5. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms: The solution features multi-tiered processing, including a user-facing front end optimized for multiple user interface platforms. The applications support and enable functions within each specific market, including planning, manufacturing and direct procurement, distribution, and logistics, selling and go-to-market, business intelligence and reporting, corporate functions, and research and development (R&D). <p>As the Transition Manager, Miguel's responsibilities included:</p> <ul style="list-style-type: none"> • Managed operational transition activities on McCormick Transition, a large and complex IT project in the products industry from client in-house and the Accenture System Integration (SI) team to Accenture 	

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- **Managed the end-to-end execution of the transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of the transition execution activities**
- **Successfully completed the transition on time and on budget**
- **Led a global transition team of over 200 personnel across the U.S., APAC, and EMEA (Accenture, McCormick, incumbent combined), utilizing ITIL and SAFe program management principles**
- Managed the rapid service transition to mitigate client resource attrition with capacity staffing enabled and onboarded into operations within one month of Transition start
- Developed, delivered, maintained and executed Transition-In Work Plan in coordination with McCormick that served as a master document
- Performed gap analysis between existing documents and industry best practices to identify areas for change in McCormick plans
- Developed working plans for McCormick based on the Transition-In Work Plan and prepared reports for McCormick containing direct outputs from the Transition-In Work Plan
- Developed, delivered, maintained, and executed a Transition-In Work Schedule with McCormick and updated as needed until transition completion
- Scheduled, tracked, documented, recorded, and shared agendas and meeting minutes for weekly and monthly transition meetings
- Developed, delivered, and maintains an integrated master schedule/work plan for the full project scope, which included transition plans for applications and automation
- Created a comprehensive risk management and service continuity plan and managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
- Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
- Facilitated leadership stakeholder meetings, managed issues, and risks
- Managed due diligence, joint transition planning, and transition execution activities
- Developed, delivered, and maintains an integrated master schedule/work plan for the full project scope, which included transition plans for applications, and automation
- Created a comprehensive risk management and service continuity plan to ensure smooth execution of transition activities

Collaboration:

- Worked collaboratively with McCormick's existing IT services team to accomplish a smooth transition of all McCormick's components, including with the incumbent contractor to align on the roles and responsibilities, activities, and schedule for transitioning services.
- Collaborated with McCormick's transition manager to implement and manage a comprehensive project transition office and organizational change management team to manage transition activities and related communications and change management activities
- Worked closely with McCormick's transition manager to plan, manage, execute, and close out transition activities and support alignment across transition teams

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- Led daily, weekly, and monthly meetings with McCormick's executives and internal and external stakeholders to discuss transition activity progress

Project #3	Contact #3
Company Name: State of Arizona	Contact Name: [REDACTED]
Project Name: Health-e-Arizona Plus (HEAPlus) Maintenance & Operations (M&O)	Company Name: State of Arizona
Time Period: October 1, 2020 – June 30, 2021	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Transition Manager	
<p><i>Description of relevant experience:</i></p> <p>The State of Arizona project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:</p> <ol style="list-style-type: none"> 1. Integrates with at least two applications, one of which is a COTS: The Health-e-Arizona Plus (HEAPlus) solution integrates with multiple applications including COTS applications, such as Kofax for document/PDF transfer management, and Accenture proprietary applications including myWizard. 2. Interfaces with at least five external systems, at least one of which is real-time: The Health-e-Arizona Plus solution interfaces to a variety of external systems to provide web service and batch integration. These external systems with real-time interface include federal hub, state data integrations, and external private services like the Asset Verification System, Social Security, Medicaid program lookups, United States Postal Service (USPS) for address verification, and the Department of Motor Vehicles (DMV) for residency verification. 3. Is accessed by at least 1,000 users at multiple locations: The end-to-end solution that Accenture supported for the state of Arizona, serves over 3,900 internal state workers. 4. Has a contract value of at least \$10 million: The solution contract value is \$121 million. 5. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms: The Health-e-Arizona Plus solution includes a user-facing, multi-tiered, web-based portal application and accompanying mobile application that supports Android and Apple iOS platforms. HEAplus provides portals for consumers, eligibility workers, and community assistants and supports eligibility determinations and ongoing case management for State programs such as Medicaid, Children's Health Insurance Program (CHIP), Medicare Savings Program (MSP), Arizona Long-Term Care System (ALTCs), Supplemental Nutrition Assistance Programs (SNAP), and Temporary Assistance for Needy Families (TANF). <p>As the Transition Manager, Miguel's responsibilities included:</p>	

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- **Managed operational transition-in activities on the Health-e-Arizona Plus (HEAPlus) Maintenance & Operations (M&O) project, a large and complex IT system, to deliver a successful transition of infrastructure, applications, security, and IT services from incumbent to Accenture**
- **Successfully managed transition with no technical or functional documentation and with no access to code base, database, or environment on time and on budget**
- **Led a global transition team of more than 150 personnel across the North America and India, using ITIL program management principles**
- Managed the end-to-end execution of the transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of the cutover activities
- Managed the operational readiness testing (ORT) of HEAPlus in the Microsoft Azure cloud environment in preparation for service commencement
- Developed, delivered, maintained and executed Transition-In Master Plan in coordination with the State of Arizona that served as a master document by which other transition documents were referred which included transition plans for infrastructure, applications, security, and automation
- Performed gap analysis between existing documents and industry best practices to identify areas for change in State plans without access to existing code base, database, or Azure environments
- Led the creation of documentation of system design and technical components for the State
- Developed working plans for the State based on the Transition-In Work Plan and prepared reports for the State containing direct outputs from the Transition-In Work Plan
- Developed, delivered, maintained, and executed a Transition-In Work Schedule with the State of Arizona and updated as needed until transition completion
- Scheduled, tracked, documented, recorded, and shared agendas and meeting minutes for weekly and monthly transition meetings
- Facilitated leadership stakeholder meetings, managed issues, and risks
- Managed due diligence, joint transition planning, and transition execution activities
- Managed set-up and testing of the service desk for community assistors
- Created a comprehensive risk management and service continuity plan to ensure smooth execution of transition activities
- Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition

Collaboration:

- Worked collaboratively with the State of Arizona's existing IT services team to accomplish a smooth transition of all HEAPlus infrastructure components, including with the incumbent contractor to align on the roles and responsibilities, activities, and schedule for transitioning services
- Collaborated with the State of Arizona's transition manager to implement and manage a comprehensive project transition office to manage transition activities and related communications

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- Worked closely with the State of Arizona's transition manager to plan, manage, execute, and close out transition activities and support alignment across transition teams
- Led daily, weekly, and monthly meetings with the State of Arizona's executives including internal and external stakeholders to discuss the progress of transition activities

Project #4	Contact #4
Company Name: Chesapeake Energy Corporation	Contact Name: [REDACTED]
Project Name: AO/IO Chesapeake Transition	Company Name: Chesapeake Energy Corporation
Time Period: June 1, 2020 – September 30, 2020	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Transition Manager	
<p><i>Description of relevant experience:</i></p> <p>The AO/IO Chesapeake Transition project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:</p> <ol style="list-style-type: none"> 1. Integrates with at least two applications, one of which is a COTS: The transition of AO/IO services for Chesapeake involved the support of all applications and underlying technology, including integration with SAP ECC, a COTS enterprise resource planning (ERP) platform, and other applications such as Concur, Concur Expense, including homegrown applications such as CHKShot and Treasury AMC (access management control). 2. Interfaces with at least five external systems, at least one of which is real-time: Chesapeake's IT services interface with several external systems in real-time, including Bar Tender that is used to print thermal labels for core materials in the RTC warehouse. Other external systems include data visualizer, GeoDepth, global energy mapper, NeuraSection, Techlog. 3. Is accessed by at least 1,000 users at multiple locations: The solution is accessed by over 1,300 users across multiple facilities in the U.S. 4. Has a contract value of at least \$10 million: The solution contract value is \$40 million. 5. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms: The solution features multi-tiered processing, including a user-facing front end. It provides portal access to business users to facilitate key business processes such as reporting, costing run analysis, variance and result analysis, and master data maintenance. <p>As the Transition Manager, Miguel's responsibilities included:</p>	

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- **Managed operational transition activities on the AO/IO Chesapeake Transition project, a large and complex IT project in the resources industry from incumbent to Accenture**
 - **Managed the end-to-end execution of the transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of the cutover activities**
 - **Successfully completed the transition on time**
 - Led a global transition team of over 100 personnel, using ITIL program management principles
 - Managed the rapid service transition to mitigate client resource attrition with capacity staffing enabled and onboarded into operations within one month of Transition start
 - Developed, delivered, maintained and executed Transition-In Master Plan in coordination with Chesapeake that served as a master document by which other transition documents were referred
 - Performed gap analysis between existing documents and industry best practices to identify areas for change in Chesapeake plans
 - Developed working plans for Chesapeake based on the Transition-In Work Plan and prepared reports for Chesapeake containing direct outputs from the Transition-In Work Plan
 - Developed, delivered, maintained, and executed a Transition-In Work Schedule with Chesapeake and updated as needed until transition completion
 - Scheduled, tracked, documented, recorded, and shared agendas and meeting minutes for weekly and monthly transition meetings
 - Developed, delivered, and maintains an integrated master schedule/work plan for the full project scope, which included transition plans for infrastructure, applications, and automation
 - Created a comprehensive risk management and service continuity plan
 - Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
 - Facilitated leadership stakeholder meetings, managed issues, and risks
 - Managed due diligence, joint transition planning, and transition execution activities
 - Created a comprehensive risk management and service continuity plan to ensure smooth execution of transition activities
 - Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
- Collaboration:**
- Worked collaboratively with the Chesapeake Energy Corporation's existing IT services team to accomplish a smooth transition of infrastructure components, including with the incumbent contractor to align on the roles and responsibilities, activities, and schedule for transitioning services
 - Collaborated with Chesapeake Energy Corporation's transition manager to implement and manage a comprehensive project transition office to manage transition activities and related communications
 - Worked closely with Chesapeake Energy Corporation's transition manager to plan, manage, execute, and close out transition activities and support alignment across transition teams

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- Led daily, weekly, and monthly meetings with Chesapeake Energy Corporation's executives including internal and external stakeholders to discuss the progress of transition activities

Project #5	Contact #5
Company Name: Exelon	Contact Name: [REDACTED]
Project Name: ePeople Transition	Company Name: Exelon
Time Period: February 1, 2018 – July 31, 2018	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]

Staff Role: Transition Manager

Description of relevant experience:

The ePeople Transition project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:

1. **Integrates with at least two applications, one of which is a COTS:** The transition of Oracle HCM Cloud solution (ePeople Transition) involved the support of payroll, benefits and compensation, payroll, and HR modules. The solution is also integrated with COTS application such as HP Service Management (HPSM), a ticketing tool.
2. **Interfaces with at least five external systems, at least one of which is real-time:** The Oracle HCM Cloud solution interfaces with several external systems in real-time, including BI publisher and OBIEE for reporting, eTime and Taleo for time and expense management, and Oracle Event Processing, an SOA interface.
3. **Is accessed by at least 1,000 users at multiple locations:** The solution is accessed by over 35,000 users across multiple facilities.
4. **Has a contract value of at least \$10 million:** The solution contract value is \$15 million.
5. **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The solution features multi-tiered processing, including a user-facing front end. It provides portal access to business users to facilitate key business processes such as reporting, costing run analysis, and master data maintenance.

As the Transition Manager, Miguel's responsibilities included:

- **Managed operational transition activities for the ePeople Transition Project, Oracle HCM Cloud, a large and complex IT system in the resources industry, which transitioned from in-house and Accenture Systems Integrations team to Accenture support team**
- **Managed the end-to-end execution of the transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of the cutover activities**
- **Successfully completed the transition on time and on budget**

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- **Led a global transition team of over 200 personnel in the U.S. and the Philippines (Accenture and Exelon combined), using ITIL program management principles**
 - Developed, delivered, maintained and executed Transition-In Master Plan in coordination with Exelon that served as a master document by which other transition documents were referred
 - Performed gap analysis between existing documents and industry best practices to identify areas for change in Exelon processes
 - Developed working plans for Exelon based on the Transition-In Work Plan and prepared reports for Exelon containing direct outputs from the Transition-In Work Plan
 - Developed, delivered, maintained, and executed a Transition-In Work Schedule with Exelon and updated as needed until transition completion
 - Scheduled, tracked, documented, recorded, and shared agendas and meeting minutes for weekly and monthly transition meetings
 - Developed, delivered, and maintained an integrated master schedule/work plan for the full project scope, which included transition plans for infrastructure tools, applications, and processes
 - Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
 - Facilitated leadership stakeholder meetings
 - Managed joint transition planning, and transition execution activities
 - Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
- Collaboration:**
- Worked collaboratively with Exelon's existing IT services to accomplish a smooth transition of all ePeople Transition components to align on the roles and responsibilities, activities, and schedule for transitioning services
 - Collaborated with the Exelon's transition manager to implement and manage a comprehensive project transition office and related communications
 - Worked closely with the Exelon's transition manager to plan, manage, execute, and close out transition activities and support alignment across transition teams
 - Led daily, weekly, and monthly meetings with Exelon executives and internal and external stakeholders to discuss the progress of transition activities

Total Duration of all Projects cited to meet the MQ:		2 years, 5 months
Minimum Qualification 1-S16	Experience within the past ten (10) years, managing the successful transition of large and complex IT systems from one (1) company or contract to another on at least two (2) separate Projects. The Transition Manager's experience will have been for a minimum duration of three (3) months for each Project.	
Project #1		Contact #1
Company Name: Huntsman		Contact Name: [REDACTED]

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

Project Name: IT Managed Services	Company Name: Huntsman
Time Period: September 1, 2022 – February 28, 2023	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]

Staff Role: Transition Manager

Description of relevant experience:

The IT Managed Services (Project Imagine) project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:

- 1. Integrates with at least two applications, one of which is a COTS:** The transition of IT Managed Services for Huntsman involved the support of all applications and underlying technology, including integration with SAP HANA, a COTS enterprise resource planning (ERP) platform, and IBM planning analytics tool for business performance management, and Accenture proprietary applications, including myWizard.
- 2. Interfaces with at least five external systems, at least one of which is real-time:** Huntsman's IT services interface with several external systems, including warehouse interfaces, banking interfaces, vendor interfaces, customer interfaces, government interfaces, and carrier interfaces, which operates in real-time.
- 3. Is accessed by at least 1,000 users at multiple locations:** The solution is accessed by over 9,000 associates across 70 plus production facilities in 30 countries.
- 4. Has a contract value of at least \$10 million:** The solution contract value is \$110 million.
- 5. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The solution features multi-tiered processing, including a user-facing front end. It provides portal access to business users to facilitate key business processes such as reporting, costing run analysis, variance and result analysis, master data maintenance, adjustment, and revaluation.

As the Transition Manager, Miguel's responsibilities included:

- **Managed operational transition activities for the IT Managed Services Project, a large and complex IT system in the resources industry which transitioned from in-house and incumbent to Accenture**
- **Managed the end-to-end execution of the transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of transition execution activities**
- **Successfully completed the transition on time and on budget**
- **Led a global transition team of over 500 personnel (Accenture, Huntsman, Incumbent combined), utilizing ITIL, and SAFe program management principles**
- **Developed, delivered, maintained and executed a Transition-In plan in coordination with Huntsman that served as a master document for seamless transition**

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- Worked alongside Huntsman team and incumbent to identify gaps in standard operating procedures and to provide best practices to fill those gaps
- Performed gap analysis between existing documents and industry best practices to identify areas for change in Huntsman plans including process gap assessments on existing service management processes and incorporated Accenture best practices
- Developed working plans for Huntsman based on the Transition-In Work Plan and prepared reports for Huntsman containing direct outputs from the Transition-In Work Plan
- Scheduled meetings to do walk-through of deliverables and answered any questions to expedite deliverable approvals, led to quicker review turnaround and deliverable approvals and on-time submission
- Developed, delivered, maintained, and executed a Transition-In Work Schedule with Huntsman and updated as needed until transition completion
- Scheduled, tracked, documented, recorded, and shared agendas and meeting minutes for daily, weekly, and monthly transition meetings
- Developed, delivered, and maintained an integrated master schedule/work plan for the full project scope, which included transition plans for infrastructure, applications, security, and automation
- Created a comprehensive risk management and service continuity plan to comply with attrition impacts, business criticality and Huntsman's zero outage transition requirements
- Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
- Facilitated leadership stakeholder meetings with Huntsman, Accenture, and third party vendor executives
- Managed due diligence, joint transition planning, and transition execution activities
- Managed set-up and testing of the service desk L1 support across multiple regions including the U.S., Europe, Middle East, and Africa (EMEA), and Asia-Pacific (APAC)
- Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition

Collaboration:

- Worked collaboratively with Huntsman's existing IT services to understand client-specific operating processes and requirements to accomplish a smooth transition of all IT Managed Services' infrastructure components, including with the incumbent contractor to align on the roles and responsibilities, activities, and schedule for transitioning services
- Collaborated with the Huntsman's transition manager to implement and manage a comprehensive project transition office and related communications
- Worked closely with the Huntsman's transition manager to plan, manage, execute, and close out transition activities and support alignment across transition teams
- Led daily, weekly, and monthly meetings with Huntsman executives and internal and external stakeholders to discuss the progress of transition activities

Project #2

Contact #2

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

Company Name: McCormick	Contact Name: [REDACTED]
Project Name: McCormick Transition	Company Name: McCormick
Time Period: October 1, 2021 – March 31, 2022	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Transition Manager	

Description of relevant experience:

The McCormick Transition project meets the definition of “large and complex IT system,” based on the following criteria defined in the RFP:

- 1. Integrates with at least two applications, one of which is a COTS:** The transition for McCormick involved the support of all applications and underlying technology, including the integration with SAP HANA, a COTS enterprise resource planning (ERP) platform, and Denodo, which is a data virtualization platform for data service creation and delivery, and Accenture proprietary applications, including myWizard.
- 2. Interfaces with at least five external systems, at least one of which is real-time:** McCormick's IT services interface with several external systems, including EUSHEETS supplied by Selerant, which is used to manage dangerous declarations on external documentations, which operates real-time. Other external systems include CAS TPM, CCure, Hamilton Grant, Longstars, and Invar.
- 3. Is accessed by at least 1,000 users at multiple locations:** The solution is accessed by over 20,000 users across multiple geographic locations including US, APAC, and EMEA.
- 4. Has a contract value of at least \$10 million:** The solution contract value is \$30 million.
- 5. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The solution features multi-tiered processing, including a user-facing front end. The applications support and enable functions within each specific market, including planning, manufacturing and direct procurement, distribution and logistics, selling and go-to-market, business intelligence and reporting, corporate functions, and R&D.

As the Transition Manager, Miguel's responsibilities included:

- Managed operational transition activities on the McCormick Transition, a large and complex IT system in the products industry from client in-house and the Accenture System Integration team to Accenture
- Managed the end-to-end execution of the transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of the cutover activities
- Successfully completed the transition on time and on budget
- Led a global transition team of over 200 personnel (Accenture, McCormick, Incumbent combined), utilizing ITIL, and SAFe program management principles

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- Managed the rapid service transition to mitigate client resource attrition with capacity staffing enabled and onboarded into operations within one month of Transition start
- Developed, delivered, maintained and executed Transition-In Master Plan in coordination with McCormick that served as a master document by which other transition documents were referred
- Performed gap analysis between existing documents and industry best practices to identify areas for change in McCormick plans
- Developed working plans for McCormick based on the Transition-In Work Plan and prepared reports for McCormick containing direct outputs from the Transition-In Work Plan
- Developed, delivered, maintained, and executed a Transition-In Work Schedule with McCormick and updated as needed until transition completion
- Scheduled, tracked, documented, recorded, and shared agendas and meeting minutes for weekly and monthly transition meetings
- Developed, delivered, and maintains an integrated master schedule/work plan for the full project scope, which included transition plans for infrastructure, applications, security, and automation
- Created a comprehensive risk management and service continuity plan
- Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
- Facilitated leadership stakeholder meetings, managed issues, and risks
- Managed due diligence, joint transition planning, and transition execution activities
- Developed, delivered, and maintains an integrated master schedule/work plan for the full project scope, which included transition plans for applications, and automation
- Created a comprehensive risk management and service continuity plan to ensure smooth execution of transition activities
- Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition

Collaboration:

- Worked collaboratively with McCormick's existing IT services to accomplish a smooth transition of all McCormick's components, including with the incumbent contractor to align on the roles and responsibilities, activities, and schedule for transitioning services.
- Collaborated with McCormick's transition manager to implement and manage a comprehensive project transition office and organizational change management team to manage transition activities and related communications and change management activities
- Worked closely with McCormick's transition manager to plan, manage, execute, and close out transition activities and support alignment across transition teams
- Led daily, weekly, and monthly meetings with McCormick's executives and internal and external stakeholders to discuss transition activity progress

Project #3

Contact #3

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

Company Name: State of Arizona	Contact Name: [REDACTED]
Project Name: Health-e-Arizona Plus (HEAPlus) Maintenance & Operations (M&O)	Company Name: State of Arizona
Time Period: October 1, 2020 – June 30, 2021	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Transition Manager	
<p><i>Description of relevant experience:</i></p> <p>The State of Arizona project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:</p> <ol style="list-style-type: none"> 1. Integrates with at least two applications, one of which is a COTS: The Health-e-Arizona Plus (HEAPlus) solution integrates with multiple applications including COTS applications, such as Kofax for document/PDF transfer management, and Accenture proprietary applications, including myWizard. 2. Interfaces with at least five external systems, at least one of which is real-time: The Health-e-Arizona Plus solution interfaces to a variety of external systems to provide web service and batch integration. These external systems with real-time interface include federal hub, state data integrations, and external private services like the Asset Verification System, Social Security, Medicaid program lookups, United States Postal Service (USPS) for address verification, and the Department of Motor Vehicles (DMV) for residency verification. 3. Is accessed by at least 1,000 users at multiple locations: The end-to-end solution that Accenture supported for the state of Arizona, serves over 3,900 internal state workers. 4. Has a contract value of at least \$10 million: The solution contract value is \$121 million. 5. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms: The Health-e-Arizona Plus solution includes a user-facing, multi-tiered, web-based portal application and accompanying mobile application that supports Android and Apple iOS platforms. HEAplus provides portals for consumers, eligibility workers, and community assistors and supports eligibility determinations and ongoing case management for State programs such as Medicaid, Children's Health Insurance Program (CHIP), Medicare Savings Program (MSP), Arizona Long-Term Care System (ALTCs), Supplemental Nutrition Assistance Programs (SNAP), and Temporary Assistance for Needy Families (TANF). <p>As the Transition Manager, Miguel's responsibilities included:</p> <ul style="list-style-type: none"> Managed all infrastructure transition-in activities on the Health-e-Arizona Plus (HEAPlus) Maintenance & Operations (M&O) project, a large and complex IT system, to deliver a successful transition of infrastructure, applications, security, and IT services from incumbent to Accenture Successfully managed transition with no technical or functional documentation and with no access to code base, database, or environment on time and on budget Led a global transition team of more than 150 personnel across the North America and India, using ITIL program management principles 	

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- Managed the end-to-end execution of the transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of the cutover activities
- Managed the operational readiness testing (ORT) of HEAPlus in the Microsoft Azure cloud environment in preparation for service commencement
- Developed, delivered, maintained and executed Transition-In Master Plan in coordination with the State of Arizona that served as a master document by which other transition documents were referred which included transition plans for infrastructure, applications, security, and automation
- Performed gap analysis between existing documents and industry best practices to identify areas for change in State plans without access to existing code base, database, or Azure environments
- Led the creation of documentation of system design and technical components for the State
- Developed working plans for the State based on the Transition-In Work Plan and prepared reports for the State containing direct outputs from the Transition-In Work Plan
- Developed, delivered, maintained, and executed a Transition-In Work Schedule with the State of Arizona and updated as needed until transition completion
- Scheduled, tracked, documented, recorded, and shared agendas and meeting minutes for weekly and monthly transition meetings
- Facilitated leadership stakeholder meetings, managed issues, and risks
- Managed due diligence, joint transition planning, and transition execution activities
- Managed set-up and testing of the service desk for community assistors
- Created a comprehensive risk management and service continuity plan to ensure smooth execution of transition activities
- Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition

Collaboration:

- Worked collaboratively with the State of Arizona's existing IT services to accomplish a smooth transition of all HEAPlus infrastructure components, including with the incumbent contractor to align on the roles and responsibilities, activities, and schedule for transitioning services
- Collaborated with the State of Arizona's transition manager to implement and manage a comprehensive project transition office to manage transition activities and related communications
- Worked closely with the State of Arizona's transition manager to plan, manage, execute, and close out transition activities and support alignment across transition teams
- Led daily, weekly, and monthly meetings with the State of Arizona's executives including internal and external stakeholders to discuss the progress of transition activities

Project #4

Contact #4

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

Company Name: Chesapeake Energy Corporation	Contact Name: [REDACTED]
Project Name: AO/IO Chesapeake Transition	Company Name: Chesapeake Energy Corporation
Time Period: June 1, 2020 – September 30, 2020	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Transition Manager	
<p><i>Description of relevant experience:</i></p> <p>The AO/IO Chesapeake Transition project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:</p> <ol style="list-style-type: none"> 1. Integrates with at least two applications, one of which is a COTS: The transition of AO/IO services for Chesapeake involved the support of all applications and underlying technology, including integration with SAP ECC, a COTS enterprise resource planning (ERP) platform, and other applications such as Concur, Concur Expense, including homegrown applications such as CHKShot and Treasury AMC (access management control). 2. Interfaces with at least five external systems, at least one of which is real-time: Chesapeake's IT services interface with several external systems in real-time, including Bar Tender that is used to print thermal labels for core materials in the RTC warehouse. Other external systems include data visualizer, GeoDepth, global energy mapper, NeuraSection, Techlog. 3. Is accessed by at least 1,000 users at multiple locations: The solution is accessed by over 1,300 users across multiple facilities in the US. 4. Has a contract value of at least \$10 million: The solution contract value is \$40 million. 5. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms: The solution features multi-tiered processing, including a user-facing front end. It provides portal access to business users to facilitate key business processes such as reporting, costing run analysis, variance and result analysis, and master data maintenance. <p>As the Transition Manager, Miguel's responsibilities included:</p> <ul style="list-style-type: none"> • Managed operational transition activities on the AO/IO Chesapeake Transition project, a large and complex IT system in the resources industry from incumbent to Accenture • Managed the end-to-end execution of the transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of the cutover activities • Successfully completed the transition on time and on budget • Led a global transition team of over 100 personnel (Accenture and incumbent combined), using ITIL program management principles 	

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- Developed, delivered, maintained and executed Transition-In Master Plan in coordination with Chesapeake that served as a master document by which other transition documents were referred
- Performed gap analysis between existing documents and industry best practices to identify areas for change in Chesapeake plans
- Developed working plans for Chesapeake based on the Transition-In Work Plan and prepared reports for Chesapeake containing direct outputs from the Transition-In Work Plan
- Developed, delivered, maintained, and executed a Transition-In Work Schedule with Chesapeake and updated as needed until transition completion
- Scheduled, tracked, documented, recorded, and shared agendas and meeting minutes for weekly and monthly transition meetings
- Developed, delivered, and maintained an integrated master schedule/work plan for the full project scope, which included transition plans for infrastructure, applications, and automation
- Created a comprehensive risk management and service continuity plan
- Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
- Facilitated leadership stakeholder meetings, managed issues, and risks
- Managed due diligence, joint transition planning, and transition execution activities
- Created a comprehensive risk management and service continuity plan to ensure smooth execution of transition activities
- Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition

Collaboration:

- Worked collaboratively with the Chesapeake Energy Corporation's existing IT services to accomplish a smooth transition of infrastructure components, including with the incumbent contractor to align on the roles and responsibilities, activities, and schedule for transitioning services
- Assisted Chesapeake Energy Corporation's team in understanding transition-in activities, timelines, and impacts
- Collaborated with Chesapeake Energy Corporation's transition manager to implement and manage a comprehensive project transition office to manage transition activities and related communications
- Worked closely with Chesapeake Energy Corporation's transition manager to plan, manage, execute, and close out transition activities and support alignment across transition teams
- Led daily, weekly, and monthly meetings with Chesapeake Energy Corporation's executives including internal and external stakeholders to discuss the progress of transition activities

Project #5	Contact #5
Company Name: Exelon	Contact Name: [REDACTED]
Project Name: ePeople Transition	Company Name: Exelon
Time Period: February 1, 2018 – July 31, 2018	Phone Number: [REDACTED]

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

Percentage of Time: 100%

Email: [REDACTED]

Staff Role: Transition Manager

Description of relevant experience:

The ePeople Transition project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:

- 1. Integrates with at least two applications, one of which is a COTS:** The transition of Oracle HCM Cloud solution (ePeople Transition) involved the support of payroll, benefits and compensation, payroll, and HR modules. The solution is also integrated with COTS application such as HP Service Management (HPSM), a ticketing tool.
- 2. Interfaces with at least five external systems, at least one of which is real-time:** The Oracle HCM Cloud solution interfaces with several external systems in real-time, including BI publisher and OBIEE for reporting, eTime and Taleo for time and expense management, and Oracle Event Processing, an SOA interface.
- 3. Is accessed by at least 1,000 users at multiple locations:** The solution is accessed by over 35,000 users across multiple facilities.
- 4. Has a contract value of at least \$10 million:** The solution contract value is \$15 million.
- 5. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The solution features multi-tiered processing, including a user-facing front end. It provides portal access to business users to facilitate key business processes such as reporting, costing run analysis, and master data maintenance.

As the Transition Manager, Miguel's responsibilities included:

- **Managed operational transition activities for the ePeople Transition Project, Oracle HCM Cloud, a large and complex IT system in the resources industry, which transitioned from in-house and Accenture Systems Integrations team to Accenture support team**
- **Managed the end-to-end execution of the transition activities including the development of the detailed transition plan, execution of knowledge transfer sessions, job shadowing, operational readiness assessment, and oversight of the cutover activities**
- **Successfully completed the transition on time and on budget**
- **Led a global transition team of over 200 personnel in the U.S. and the Philippines (Accenture and Exelon combined), using ITIL program management principles**
- Developed, delivered, maintained and executed Transition-In Master Plan in coordination with Exelon that served as a master document by which other transition documents were referred
- Performed gap analysis between existing documents and industry best practices to identify areas for change in Exelon processes
- Developed working plans for Exelon based on the Transition-In Work Plan and prepared reports for Exelon containing direct outputs from the Transition-In Work Plan
- Developed, delivered, maintained, and executed a Transition-In Work Schedule with Exelon and updated as needed until transition completion

PART 2 – INFRASTRUCTURE TRANSITION MANAGER MINIMUM QUALIFICATIONS TABLE

- Scheduled, tracked, documented, recorded, and shared agendas and meeting minutes for weekly and monthly transition meetings
- Developed, delivered, and maintained an integrated master schedule/work plan for the full project scope, which included transition plans for infrastructure tools, applications, and processes
- Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition
- Facilitated leadership stakeholder meetings
- Managed joint transition planning, and transition execution activities
- Managed project risks and developed mitigation plans to minimize potential impact to end users and business operations during transition

Collaboration:

- Worked collaboratively with Exelon's existing IT services to accomplish a smooth transition of all ePeople Transition components to align on the roles and responsibilities, activities, and schedule for transitioning services
- Collaborated with the Exelon's transition manager to implement and manage a comprehensive project transition office and related communications
- Worked closely with the Exelon's transition manager to plan, manage, execute, and close out transition activities and support alignment across transition teams
- Led daily, weekly, and monthly meetings with Exelon executives and internal and external stakeholders to discuss the progress of transition activities

Total Duration of all Projects cited to meet the MQ:

2 years, 5 months



This is to certify that
De Ramas, Miguel Jr. Orozco

Has achieved the
**ITIL® Foundation Certificate
in IT Service Management**

Effective from
1 February 2011

Certificate number
4119547.892233

Candidate Number
4119547

Peter Hepworth, CEO, AXELOS

drs. Bernd W.E. Taselaar, CEO, EXIN

The validity of this certificate can be checked on www.exin.com/certificate-authentication
This certificate remains the property of the issuing Examination Institute and shall be returned immediately upon request.



AXELOS, the AXELOS logo, the AXELOS swirl logo, ITIL, PRINCE2, PRINCE2 AGILE, MSP, MoR, P3M3, P3O, MoP and MoV are registered trade marks of AXELOS Limited. RESILIA is a trade mark of AXELOS Limited.

SCALED AGILE FRAMEWORK® (SAFe®)



SCALED AGILE

This certificate verifies

Miguel de Ramas

has successfully met the requirements of a

Certified SAFe 5 Agilist

VALID UNTIL: MAY 31, 2024

CERTIFICATE ID: 37641357-5717

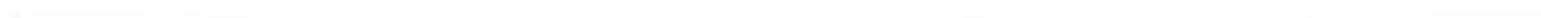
A handwritten signature in black ink.

Dean Leffingwell
Chief Methodologist, SAFe®
Co-founder Scaled Agile, Inc.

A handwritten signature in black ink.

Chris James
Chief Executive Officer
Scaled Agile, Inc.

The logo consists of three blue diagonal lines followed by the word "SAFe" in bold. To the right, it says "PROVIDED BY SCALED AGILE".
Scaled Agile Framework® and SAFe® are trademarks of Scaled Agile, Inc.



1.6 INFRASTRUCTURE SECURITY MANAGER STAFF QUALIFICATIONS

INFRASTRUCTURE SECURITY MANAGER			
PART 1 – RÉSUMÉ			
Contractor	Accenture LLP		
Candidate Name	Alexander (Alex) Hsiung		
Position in the Company	Security Senior Manager	Length of Time in Position	1 year
Project Position & Responsibilities	Infrastructure Security Manager Project responsibilities will be as defined in RFP section 12.1.3.6.6.		
Skills & Qualifications for Project Position	<p>Skills: Alex delivers security services and provides delivery oversight for infrastructure security solutions. He helps align systems, tools, strategies, processes, and documentation with compliance frameworks and security best practices. He provides advisory oversight and delivery leadership for cybersecurity solutions supporting Amazon Web Services (AWS) hosted infrastructure, identity and access management (IAM), application security and penetration testing, security monitoring, threat analysis, and IT security compliance.</p> <p>Qualifications: Alex has managed security solutions for large complex IT environments. He is a subject matter advisor (SMA) for security, privacy, and regulatory standards, including NIST 800-53, GLBA, SOC 1, SOC 2, ISO 27001, FFIEC CAT, PCI DSS, NY DFS, and HIPAA. Alex has more than 10 years of experience as a security professional and more than four years of experience as a manager. He provides oversight of service delivery activities and collaborates with application development teams, technical architects, and security policy experts to assess, define and implement an integrated framework of solution security architecture (MQ I-S1: Exceeds). He has served as a lead for the past four years, developing, implementing, improving, and monitoring industry standard security strategies, solutions, and processes on projects involving large and complex IT systems, including AWS cloud environments (MQ I-S2: Exceeds). Alex has four years of experience applying Information Security principles, methods, and techniques in the development of Project security Deliverables on projects involving large and complex IT systems (MQ I-S3: Exceeds). He has four years of experience assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) to identify appropriate security controls to protect Personally Identifiable Information (PII), Protected Health Information (PHI), and/or Federal Tax Information (FTI) data (MQ I-S4: Exceeds). Alex has four years of experience with systems that comply with the National Institute of Standards and Technology (NIST) 800-53 moderate baseline (MQ I-S25: Exceeds). Alex holds an (ISC)² Certified Information Systems Security Professional (CISSP) certification and will maintain it for the duration of the contract. He also holds professional certifications with the International Association of Privacy Professionals (IAPP), including the Certified Information Privacy Professional / United States (CIPP/US) (MQ I-S26: Exceeds).</p>		
Relevant Experience (Add additional tables as needed)			
Project Title	Silvergate Bank		
Position Title	Security Technology Delivery Lead		

INFRASTRUCTURE SECURITY MANAGER					
Begin Date	February 2022	End Date	May 2023	# of Months	11 Months (through December 2022)
Scope and Description of Responsibility	Scope: Alex led a shared security team to perform a security due diligence assessment of the assets and the operational run and hardening of the acquired assets. He helped with the design and build of AWS infrastructure using Terraform. Responsibility: Alex managed the overall security strategy of the acquired assets. He conducted security assessments, network and endpoint vulnerability scans, threat intelligence reports, and audits to identify potential weaknesses in the environment and worked with technical engineering teams and security teams to drive remediation efforts.				
Skills Utilized and Experience Attained	Skills Utilized: Alex used his skills and experience managing large and complex IT environments to oversee the security due diligence assessment, identify gaps, provide recommendations and operational support, and lead the integration of applications and systems into Silvergate's environment. Experience Attained: Alex attained first-hand experience with a complex blockchain-based IT solution. As the security technology lead, he answered all security questions, assisted with investigation and remediation processes, and informed the Chief Information Security Officer (CISO) of any potential security incidents.				
Project Title	Diem Association				
Position Title	Security Due Diligence Lead				
Begin Date	November 2021	End Date	January 2022	# of Months	3 months
Scope and Description of Responsibility	Scope: Alex led the security due diligence efforts to review a blockchain-based solution and identify potential technological red flags in the context of an acquisition. Responsibility: Alex was responsible for defining the security assessment plan and leading interviews. He led a high-velocity security due diligence assessment in order to identify potential red flags and areas of concern that required communication with the buyer. Alex provided detailed findings identified and a recommendation to proceed with the purchase.				
Skills Utilized and Experience Attained	Skills Utilized: Alex used his technical security background to quickly execute a four-week assessment through walkthrough screenshare sessions, and rationalizing the risk of publicly available source code repositories. Experience Attained: Alex gained experience performing a security due diligence assessment against a complex, decentralized blockchain solution. He reviewed the IT systems, tools, and applications developed by Facebook. Alex collaborated across teams to understand how the system was designed with security principles from the ground up.				
Project Title	Farmers Insurance Group				
Position Title	Security Delivery Lead				
Begin Date	July 2021	End Date	October 2021	# of Months	3.5 months
Scope and Description of Responsibility	Scope: Alex reviewed, assessed, designed, built, and remediated Farmers' cybersecurity and GRC capabilities to align with NY DFS and NIST CSF baseline maturity requirements. He identified gaps against baseline requirements, recommended areas to remediate, and built a new risk assessment, risk treatment process and risk register. Responsibility: Alex defined the project plan, timeline, scope, and deliverables in coordination with stakeholders and oversaw delivery				

INFRASTRUCTURE SECURITY MANAGER					
	of the engagement. He provided oversight during walkthrough sessions with stakeholders to drive remediation discussions and furnishing deliverables.				
Skills Utilized and Experience Attained	Skills Utilized: Alex used his technical security and compliance background to assess and review Farmers' information security practices. He delivered a gap assessment and helped to design and build Farmers' risk assessment process. Experience Attained: Alex attained experience in overall service delivery and project management of the engagement. He navigated a complex IT environment and ensured that deliverables were provided to Farmers' expectations.				
Project Title	Microsoft				
Position Title	Security Delivery Manager				
Begin Date	November 2018	End Date	June 2021	# of Months	31.8 months
Scope and Description of Responsibility	Scope: Alex conducted the certification assessments of Microsoft's Azure cloud hosting services against security and system standards. Responsibility: Alex was responsible for the overall service delivery of the project. He defined the project plan, timeline, scope, and deliverables. He provided the infosec certification assessment, findings summary reports, and updated certificates.				
Skills Utilized and Experience Attained	Skills Utilized: Alex used his security and compliance background to assess and review Microsoft's infosec practices pertaining to the Microsoft Azure environment against key compliance frameworks and regulatory requirements. Experience Attained: Alex gained experience driving a multi-framework security engagement for a complex IT environment while providing security insights and achieving project milestones and timelines.				
Education (add rows as needed)					
Years	Course of Study			School	
01/2010 – 12/2012	B.S., Business Administration			University of Southern California	
Professional Certifications or Designations (add rows as needed)					
Certification or Designation		Organization		Dates	
Certified Information Systems Security Professional (CISSP)		International Information System Security Certification Consortium (ISC) ²		March 7, 2018 – March 31, 2024, Credential: 654089	
Certified Information Privacy Professional / United States (CIPP/US)		International Association of Privacy Professionals (IAPP)		June 21, 2017 – June 30, 2023* <i>*Note: Alex will renew his certification by submitting the necessary continuing professional education (CPE) credits.</i>	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
Minimum Qualification I-S21	A minimum of three (3) years of experience as a Security Lead directly responsible for collaborating with application development teams, technical architects, and security policy experts to define and/or implement an integrated framework of solution security architecture.
Project #1	Contact #1
Company Name: Silvergate Bank	Contact Name: [REDACTED]
Project Name: Project Mañana	Company Name: Silvergate Bank
Time Period: February 1, 2022 – May 19, 2023 (ongoing)	Phone Number: [REDACTED]
Percentage of Time: February 1, 2022 – March 31, 2023: 100% April 1, 2023 – May 19, 2023 (ongoing): 50%	Email: [REDACTED]
Staff Role: Security Tech Lead	
<p><i>Description of relevant experience:</i></p> <p>As the Security Tech Lead, Alex's accomplishments and responsibilities included:</p> <p>Collaboration</p> <ul style="list-style-type: none"> • Collaborating with application development teams, technical architects, GRC policy expert team members, CISO and Deputy CISO, Legal and Privacy, to define and implement an integrated framework of security solution architecture that comprised the information security policies and procedures, and system configurations to promote confidentiality, integrity, and availability of the acquired Diem blockchain-based stablecoin technology assets and data • Through collaborative walkthrough discussions and assessments with application development team members and technical architects, generated a backlog of program enhancements. Coordinated daily touchpoints with key stakeholders to advance project work items to completion and reduce the backlog of priority items for remediation and enhancement. The processes included developing and implementing a Security Monitoring solution for the Blockchain technology that included integrating the AWS Testnet, Premainnet, and Mainnet environments with Qualys for endpoint scanning and integrating alerts with PagerDuty to ensure that the team was aware of security vulnerabilities identified in real-time. • Through collaboration with the CISO and broader Security Team, introduced a CSPM (Prisma Cloud from Palo Alto Networks) to perform a scan of the acquired Diem Association technology assets and identified more than 3,500 security findings (including high, medium, and low) within the combined cloud environments (which included AWS and Azure components) and developed a plan to prioritize the remediation efforts • Coordinated with Cloud Infrastructure, IT, Networking, and Security team members to remediate more than 3,000 AWS security findings, leveraging Terraform's open-source solution to apply remediations using infrastructure as code to quickly tear down and rebuild workloads where possible and improved the scalability of golden Amazon Machine Images (AMIs) 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- Worked with the application development, technical architects, and other functional teams to drive the root cause analysis and remediation of incidents that were identified across the technology assets because of security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments
- Assisted the application development and IT teams with the discovery and remediation of a significant security finding that allowed certain GitHub users to merge their own source code changes into the production branch using containerized code from Docker.
- Identified information security (IS) weaknesses or potential gaps in the current environment and collaborated with the security team as well as internal Accenture teams to document the work tasks and rationalize the prioritization in order to remediate the identified gaps and align with standard best practices
- Coordinated and collaborated with IT, networking, and security stakeholders to manage the identity and access management of Silvergate's software-as-a-service (SaaS) applications and vendors, including AWS and Azure for cloud hosting services, Okta for single sign-on (SSO) and user administration, GitHub for source code management, Qualys for endpoint vulnerability scanning, 1Password for secrets management, PagerDuty for security alerting, Slack for instant messaging and alerting, Docker for software container management, and the usage of Entrust's managed hardware security module (HSM) capabilities to ensure that the application architecture design, ongoing development, and implementation were operating according to security best practices

Solution development

- Evaluated new/emerging security products and technologies and made recommendations for adoption to Silvergate executives, such as the CrowdStrike solution for Cloud Security Posture Management (CSPM), Tenable for vulnerability management, HashiCorp's Terraform for Business license for infrastructure as code

Reporting

- Communicated weekly security updates for Silvergate executives, reporting on any newly identified security vulnerabilities within the cloud environment (which included AWS), security remediation progress across the application and IT environment supporting the stablecoin assets, and overall security strategy roadmap progress
- Monitored the threat landscape using AWS' native Security Hub tooling, paired with CrowdStrike Falcon for CSPM which was integrated with PagerDuty to ensure that real-time alerts were captured by our Security Team and prioritized for investigation, any identified security vulnerabilities were communicated to the CISO and security organization for awareness and additional resources were introduced as necessary to remediate and address the issues identified
- Prepared key security deliverables using collaborative input from Security, IT, Networking, and GRC teams deliverables, including the Disaster Recovery Plan, Security Incident Response Management plan and process, Technical Design Documents and Operational Manuals and Runbooks for security tools (i.e. AWS Security Hub, GitHub, CrowdStrike, Terraform), and Security Architecture Diagrams

Compliance

- Collaborated with members across the organization, including application security, cloud infrastructure, technical architects, networking, IT, security, and GRC teams to ensure information security services followed applicable standards and regulatory requirements (such as applicable NIST 800-53 controls and CIS Benchmarks) and was in accordance with the project's approved System Security Plan

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- Collaborated with project team members supporting activities across application development, system architecture, cloud infrastructure, and security to conduct ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Silvergate-specific security training materials upon project onboarding/roll-on
- Collaborated with project team members supporting activities across application development, system architecture, cloud infrastructure, and security to implement, maintain, and enforce stringent security and privacy requirements across the technology stack at the direction of the CISO. This included these security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:
 - Federal Information Processing Standard Publication 199
 - FFIEC CAT Baseline Requirements
 - HIPAA regulatory standards
 - NIST 800-53: Security and Privacy Controls for Information Systems Organizations

Project #2	Contact #2
Company Name: Farmers Insurance Group	Contact Name: [REDACTED]
Project Name: Security Team Risk Assessment and Regulatory Alignment	Company Name: Farmers Insurance Group
Time Period: July 5, 2021 – October 29, 2021	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Delivery Lead	
<p>Description of relevant experience:</p> <p>As the Security Delivery Lead, Alex's accomplishments and responsibilities included:</p> <p>Collaboration</p> <ul style="list-style-type: none"> • Collaborated with application development teams, application security teams, threat, and vulnerability management teams, cloud security teams, technical architects, GRC policy expert team members, CISO and Deputy CISO, Legal and Privacy, to define and implement an integrated framework of security solution architecture that comprised the information security policies and procedures, and system configurations to improve the confidentiality, integrity, and availability of Farmers Insurance Groups' cybersecurity team systems and supporting documentation • Collaborated with application security, software development, and GRC teams to identify gaps in the current DevSecOps policies and processes and align stakeholders on target future-state enhancements, including ensuring that a file integrity monitoring (FIM) tool was 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

utilized to reduce the risk that changes could be deployed across systems without ensuring segregation of duties between change requester and approvers

- Collaborated with incident response, threat, and vulnerability management, and GRC teams to identify gaps in the current incident response processes and align stakeholders on target future-state enhancements. Confirmed that chain of custody requirements and providing adequate notice to regulatory bodies was followed in the event that security incidents were identified
- Collaborated with GRC team members and the CISO to identify gaps in the current risk assessment and risk treatment process, noting that a cybersecurity and IT-specific risk assessment process was not yet in place. The discussions led to the design, development, and completion of an initial cyber risk assessment and risk treatment process, along with a risk register to drive subsequent updates across the cybersecurity organization at Farmers
- Through collaborative walkthrough discussions across the Farmers security team (including technical architects, application development teams, etc.) identified more than 40 information security weaknesses or potential gaps in the current environment and collaborated with the security team to bring information security operations up to standards

Solution development

- Developed a prioritized cybersecurity strategy roadmap focusing on ten (10) key initiatives for Farmers to align existing technologies and capabilities with future state aspirational goals, largely driven by upcoming regulatory compliance requirements

Reporting

- Communicated weekly project updates to Farmers CISO and direct reports.
- Reported on any new security gaps identified in the walkthrough discussions with the overall Farmers' cybersecurity team (i.e. cloud security, application security, incident response, vulnerability and threat management, identity and access management, and software development teams) and GRC team, cloud environment (which included AWS)
- Communicated the ongoing recommended security remediation roadmap across the application and IT environment supporting Farmers and the overall security strategy roadmap progress
- Worked with the team to furnish deliverables that detailed the outcomes of walkthrough discussions with the overall Farmers' cybersecurity team. Deliverables included an assessment of the overall maturity of the cybersecurity program, using NIST Cyber Security Framework(CSF) as a benchmark, recommended remediations for prioritization rationalized against low-hanging fruit and high-effort strategic initiatives

Compliance

- Confirmed delivery of information security services followed applicable standards and regulatory requirements (such as NIST 800-53 controls and NY DFS regulatory requirements) and was in accordance with the project's approved System Security Plan
- Performed security awareness training for newly onboarded Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures upon project onboarding/roll-on
- At the direction of the Farmers Security Team, implemented, maintained, and enforced stringent security and privacy requirements across the Accenture team, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
<ul style="list-style-type: none"> – Federal Information Processing Standard Publication 199 – FFIEC CAT Baseline Requirements – HIPAA regulatory standards – NIST 800-53: Security and Privacy Controls for Information Systems Organizations 	
Project #3	Contact #3
Company Name: <i>Microsoft</i>	Contact Name: [REDACTED]
Project Name: Microsoft Azure Security Compliance	Company Name: Microsoft
Time Period: November 5, 2018 – June 25, 2021	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Delivery Manager	
<p><i>Description of relevant experience:</i></p> <p>As the Security Delivery Manager, Alex's accomplishments and responsibilities included:</p> <p>Collaboration</p> <ul style="list-style-type: none"> • Collaborated with application development teams, identity and access management, network security architects, third-party risk management, GRC, incident response, encryption, IT asset management, human resources security, and technical architects to define and implement an integrated framework of security solution architecture that aligned with ISO 27001, ISO 27701, ISO 9001, ISO 20000-1, and ISO 22301 • Collaborated with the application development, technical, and GRC teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments <p>Solution development</p> <ul style="list-style-type: none"> • Assessed and reviewed the design elements of a comprehensive security program that aligned to standards from the National Institute of Standards and Technology (NIST) 800-37 Risk Management Framework and 800-53 System Security Plan controls, as well as the requirements set forth in ISO 27001, ISO 27701, ISO 9001, ISO 20000-1, and ISO 22301 for an information security management system, privacy information management system, quality management system, service management system, and business continuity management system for the Microsoft Azure suite of cloud hosting products • Conducted recurring information security risk assessment and privacy impact assessments on a quarterly basis surrounding the Microsoft suite of cloud hosting products to align with requirements set forth in Clauses 6.2, 6.3, 8.2, and 8.3 of the ISO 27001 standard, as well as the ISO 27701 standard • Validated security controls and processes via recurring security control reviews in accordance with the ISO 27001, ISO 27701, ISO 9001, ISO 20000-1, and ISO 22301 standards, and reviewed results of reviews and opportunities for improvement with senior Azure security leadership 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
<ul style="list-style-type: none"> Reviewed and tracked security remediation progress identified during assessments and audits using the Microsoft Azure DevOps project management tool in accordance with Microsoft's Plan of Action and Milestones (POA&M) process Assessed the provisioning and secure management processes which cover nearly 1 billion users, and approximately 25,000 internal users 	
Reporting <ul style="list-style-type: none"> Planned, organized, and led project assessment planning sessions, project kickoff meetings, weekly statuses, and closing meetings with senior Microsoft Azure security and GRC leadership which entailed discussing the project progress, deliverables status, and overall findings of the assessments against the ISO 27001, ISO 27701, ISO 9001, ISO 20000-1 and ISO 22301 consolidated assessment Drafted and furnished project deliverables which included internal and external-facing audit assessment reports and narratives of the processes observed in-scope for the assessment, as well as a summary of the findings and issuance of the certificate(s) noting conformance to the requirements set forth in the ISO standards. 	
Compliance <ul style="list-style-type: none"> Adhered to security compliance and privacy requirement standards, including the NIST 800-37 Risk Management Framework, NIST 800-53 System Security Plan controls, and the requirements set forth in ISO 19011 which details the guidelines and requirements for auditing and assessing management systems Reviewed and maintained security measures during the course of the engagement as agreed to with Microsoft Azure's senior security leadership team, and recommended actions for improvement based on the findings identified 	
Total Duration of all Projects cited to meet the MQ:	
3 years, 10.3 months (through December 2022)	
Minimum Qualification I-S22	A minimum of three (3) years of lead experience within the past ten (10) years developing, implementing, improving and monitoring industry standard Security strategies, solutions, and processes on Projects involving large and complex IT systems and/or AWS cloud environment.
Project #1	Contact #1
Company Name: Silvergate Bank	Contact Name: [REDACTED]
Project Name: Project Manana	Company Name: [REDACTED]
Time Period: February 1, 2022 – May 19, 2023 (ongoing)	Phone Number: [REDACTED]
Percentage of Time: February 1, 2022 – March 31, 2023: 100% April 1, 2023 – May 19, 2023 (ongoing): 50%	Email: [REDACTED]
Staff Role: Security Tech Lead	
Description of relevant experience:	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

The Silvergate Bank project meets both the definition of a "large and complex IT system," as well as an AWS cloud environment based on the following criteria defined in the RFP:

- **Integrates with at least two applications, one of which is a COTS:** The Silvergate blockchain solution integrated with multiple applications (i.e. Okta, AWS, Logstash, PagerDuty, Slack, Atlassian, etc.), a large portion of which were COTS applications using available application programming interfaces (APIs). Access to the AWS environment was managed via SSO through Okta (COTS) where data from the AWS cloud hosting services was being scraped by the Logstash (COTS) enterprise monitoring tool and was being fed into PagerDuty (COTS) for alerting, which would also integrate with Slack (COTS) and Atlassian (COTS) for actioning and ticketing to resolve issues identified.
- **Interfaces with at least five external systems, at least one of which is real-time:** The Silvergate blockchain solution was designed with a public-facing ledger component referred to as the Diem Explorer, this solution provided a real-time view of transactions being posted to the Internet. The Diem Explorer was connected to a distributed network of externally-hosted validators who had permissions to approve transactions on the blockchain. The consensus module operated on a Byzantine Fault Tolerance which requires that at least 67% of the validators operate in consensus to approve transactions; this is represented by $f < (n - 1) / 3$, where n represents the number of authorized validators on the network, and f equates to the number of faulty or malicious validator nodes that can be tolerated. As a function of the risk accepted by the bank, a minimum of two (2) faulty or malicious nodes was acceptable, and as a result, 7 external validator nodes were required. These nodes were hosted by several external partner entities on the network, which included Blockdaemon and Bison Trails. Whenever a blockchain transaction was to occur, five (5) out of seven (7) validators on the network would need to submit the same transaction values which would then be posted to the Diem Explorer for external awareness. Additionally, COTS applications interfaced with the blockchain to provide endpoint security monitoring (Qualys), CSPM (CrowdStrike), real-time alerting (Slack and PagerDuty), and source code management (GitHub). **In summary, the Silvergate blockchain solution interfaced with a real-time Diem Explorer, seven (7) external validator nodes, and a variety of COTS applications (Qualys, CrowdStrike, Slack, PagerDuty, and GitHub) for a minimum total of 13 interconnected systems providing real-time information to the blockchain environment.**
- **Is accessed by at least 1,000 users at multiple locations:** The Diem Association blockchain solution (acquired by Silvergate) was a publicly available open-sourced solution on GitHub and the repositories were accessed and contributed to by more than 1,800 users globally.
- **Has a contract value of at least \$10 million:** Our team's overall due diligence, operational support, and enhancements contract values totaled more than \$18 million.
- **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The Silvergate blockchain solution featured a customized front end (Diem Explorer) which was accessible via web browser and mobile devices (specifically iOS for Secure Enclave) to provide transparency into the transactions being posted to the blockchain. This graphical user interface (GUI) was fed information via the controlled application logic housed within Diem's GitHub repositories that manage the transaction rulesets for which all the external validators must abide by when submitting transactions; a minimum of 67% of the validators must be in agreement on any given transaction before posting to the blockchain which would, in turn, be represented on the Diem Explorer. Each validator hosts their own data tier back-end, for Silvergate, the data tier back-end was stored within AWS' Simple Storage Service (S3) for backup

As the Security Tech Lead, Alex's accomplishments and responsibilities included:

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

Solution development and implementation

- **Developed, implemented, improved, and monitored the AWS Testnet, Premainnet, and Mainnet environments, and associated integrations with Okta, Logstash, PagerDuty, Slack, Atlassian, and a network of seven (7) externally hosted validators which comprised Silvergate's blockchain solution utilizing industry-standard security strategies, solutions, and processes**
- Served as the incident response manager when potential security incidents were identified across the technology assets, with the application development, technical architects, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments
- Assisted with the discovery and remediation of a significant security finding that allowed certain GitHub users to merge their own source code changes into the production branch using containerized code from Docker.
- Identified information security (IS) weaknesses or potential gaps in the current environment and collaborated with the security team as well as internal Accenture teams to document the work tasks and rationalize the prioritization in order to remediate the identified gaps and align to standard best practices
- Evaluated new/emerging security products and technologies and made recommendations for adoption to Silvergate executives, such as the CrowdStrike solution for CSPM, Tenable for vulnerability management, HashiCorp's Terraform for Business license for infrastructure as code

Improving and monitoring solutions

- Through collaboration with the CISO and broader Security Team, introduced a CSPM (Prisma Cloud from Palo Alto Networks) to perform a scan of the acquired Diem Association technology assets and identified more than 3,500 security findings (including high, medium, and low) within the combined cloud environments (which included AWS and Azure components) and developed a plan to prioritize the remediation efforts
- Coordinated with Cloud Infrastructure, IT, Networking, and Security team members to remediate more than 3,000 AWS security findings, leveraging Terraform's open-source solution to apply remediations using infrastructure as code to quickly tear down and rebuild workloads where possible and improved the scalability of golden Amazon Machine Images (AMIs)
- Through walkthrough discussions with application development team members and technical architects, a backlog of program enhancements was generated and coordinated daily touchpoints with key stakeholders to advance project work items through to completion and reduce the backlog of priority items for remediation and enhancement. The processes touched on included developing and implementing a Security Monitoring solution for the Blockchain technology that included integrating the AWS Testnet, Premainnet, and Mainnet environments with Qualys for endpoint scanning and integrating alerts with PagerDuty to ensure that the team was aware of security vulnerabilities identified in real-time.
- Managed the identity and access management of Silvergate's software-as-a-service (SaaS) applications and vendors, including AWS and Azure for cloud hosting services, Okta for single sign-on (SSO) and user administration, GitHub for source code management, Qualys for endpoint vulnerability scanning, 1Password for secrets management, PagerDuty for security alerting, Slack for instant messaging and alerting, Docker for software container management, and the usage of Entrust's managed hardware security module (HSM) capabilities to

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

ensure that the application architecture design, ongoing development, and implementation were operating according to security best practices

Reporting

- Communicated weekly security updates for Silvergate executives, reporting on any newly identified security vulnerabilities within the cloud environment (which included AWS), security remediation progress across the application and IT environment supporting the blockchain assets, and overall security strategy roadmap progress
- Monitored the threat landscape using AWS' native Security Hub tooling, paired with CrowdStrike Falcon for CSPM which was integrated with PagerDuty to ensure that real-time alerts were captured by our Security Team and prioritized for investigation, any identified security vulnerabilities were communicated to the CISO and security organization for awareness and additional resources were introduced as necessary to remediate and address the issues identified
- Responded timely to security events/incidents and provided notification of incidents to the CISO and Client Security Team within an hour of identifying security incidents
- Oversaw the preparation of key security deliverables, including the Disaster Recovery Plan, Security Incident Response Management plan and process, Technical Design Documents and Operational Manuals and Runbooks for security tools (i.e. AWS Security Hub, GitHub, CrowdStrike, Terraform), and Security Architecture Diagrams

Compliance

- Ensured that delivery of information security services followed applicable standards and regulatory requirements (such as applicable NIST 800-53 controls and CIS Benchmarks) and were in accordance with the project's approved System Security Plan
- Conducted ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Silvergate-specific security training materials upon project onboarding/roll-on
- Created, updated, and managed the project's disaster recovery plans and business continuity plans
- At the direction of the CISO, Implemented, maintained, and enforced stringent security and privacy requirements across the technology stack, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:
 - Federal Information Processing Standard Publication 199
 - FFIEC CAT Baseline Requirements
 - HIPAA regulatory standards
 - NIST 800-53: Security and Privacy Controls for Information Systems Organizations

Project #2	Contact #2
Company Name: <i>Diem Association</i>	Contact Name: [REDACTED]
Project Name: Security Due Diligence Assessment	Company Name: Diem
Time Period: November 2, 2021 – January 28, 2022	Phone Number: [REDACTED]

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Due Diligence Lead	
<p><i>Description of relevant experience:</i></p> <p>The Diem Association Security Due Diligence Assessment Project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:</p> <ul style="list-style-type: none"> Integrates with at least two applications, one of which is a COTS: The Diem Association blockchain solution integrated with multiple application i.e. Okta, AWS, Logstash, PagerDuty, Slack, Atlassian, etc.), a large portion of which were COTS applications using available application programming interfaces (APIs). Access to the AWS environment was managed via SSO through Okta (COTS) where data from the AWS cloud hosting services was being scraped by the Logstash (COTS) enterprise monitoring tool and was being fed into PagerDuty (COTS) for alerting, which would also integrate with Slack (COTS) and Atlassian (COTS) for actioning and ticketing to resolve issues identified. Interfaces with at least five external systems, at least one of which is real-time: The Diem Association blockchain solution was designed with a public-facing ledger component referred to as the Diem Explorer, this solution provided a real-time view of transactions being posted to the Internet. The Diem Explorer was connected to a distributed network of externally-hosted validators who were permissioned to approve transactions on the blockchain. The consensus module operated on a Byzantine Fault Tolerance which requires that at least 67% of the validators operate in consensus to approve transactions; this is represented by $f < (n - 1) / 3$, where n represents the number of authorized validators on the network, and f equates to the number of faulty or malicious validator nodes that can be tolerated. As a function of the risk accepted by the bank, a minimum of two (2) faulty or malicious nodes was acceptable, and as a result, 7 external validator nodes were required. These nodes were hosted by several external partner entities on the network, which included Shopify, Lyft, Uber, Blockdaemon and Bison Trails. Whenever a blockchain transaction were to occur, five (5) out of seven (7) validators on the network would need to submit the same transaction values which would then be posted to the Diem Explorer for external awareness. Additionally, COTS applications interfaced with the blockchain to provide endpoint security monitoring (Qualys), CSPM (CrowdStrike), real-time alerting (Slack and PagerDuty), and source code management (GitHub). In summary, the Silvergate blockchain solution interfaced with a real-time Diem Explorer, seven (7) external validator nodes, and a variety of COTS applications (Qualys, CrowdStrike, Slack, PagerDuty, and GitHub) for a minimum total of 13 interconnected systems providing real-time information to the blockchain environment. Is accessed by at least 1,000 users at multiple locations: The Diem Association blockchain solution was a publicly available open-sourced solution on GitHub and the repositories were accessed and contributed to by more than 1,800 users globally. Has a contract value of at least \$10 million: Our team's overall due diligence, operational support, and enhancements contract values totaled more than \$18 million. Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms: The Diem Association blockchain solution featured a customized front end (Diem Explorer) which was accessible via web browser and mobile devices (specifically iOS for Secure Enclave) to provide transparency into the transactions being posted to the blockchain. This graphical 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

user interface (GUI) was fed information via the controlled the application logic housed within Diem's GitHub repositories that manage the transaction rulesets for which all the external validators must abide by when submitting transactions; a minimum of 67% of the validators must be in agreement on any given transaction before posting to the blockchain which would, in turn, be represented on the Diem Explorer. Each validator hosts their own data tier back-end, for Silvergate, the data tier back-end was stored within AWS' Simple Storage Service (S3) for backup

As the Security Due Diligence Lead, Alex's accomplishments and responsibilities include:

Solution development and implementation

- **Developed and implemented a plan to improve the AWS Testnet, Premainnet and Mainnet environments, and associated integrations with Okta, Logstash, PagerDuty, Slack, Atlassian, and a network of seven (7) externally hosted validators which comprised the Diem Association's blockchain solution according to industry-standard security strategies, solutions, and processes**
- Collaborated with application development teams, technical architects, GRC policy expert team members, CISO and Deputy CISO, Legal and Privacy, to define and implement an integrated framework of security solution architecture that comprised the information security policies and procedures, and system configurations to promote confidentiality, integrity, and availability of the acquired Diem blockchain-based technology assets and data

Improving and monitoring solution

- Through walkthrough discussions with application development team members and technical architects, a backlog of program enhancements was generated and coordinated daily touchpoints with key stakeholders to advance project work items through to completion and reduce the backlog of priority items for remediation and enhancement. The processes touched on included developing and implementing a Security Monitoring solution for the Blockchain technology that included integrating the AWS Testnet, Premainnet, and Mainnet environments with Qualys for endpoint scanning and integrating alerts with PagerDuty to ensure that the team was aware of security vulnerabilities identified in real-time
- Identified information security (IS) weaknesses or potential gaps in the current environment and collaborated with the security team as well as internal Accenture teams to document the work tasks and rationalize the prioritization in order to remediate the identified gaps and align to standard best practices

Reporting

- Communicated weekly security findings updates for Accenture team and Diem team consumption, reporting on any newly identified security vulnerabilities within the cloud environment (which included AWS), security remediation progress across the application and IT environment supporting the blockchain assets, and overall security strategy roadmap progress
- Monitored the threat landscape using AWS' native Security Hub tooling, paired with CrowdStrike Falcon for CSPM which was integrated with PagerDuty to ensure that real-time alerts were captured by our Security Team and prioritized for investigation, any identified security vulnerabilities were communicated to the CISO and security organization for awareness and additional resources were introduced as necessary to remediate and address the issues identified

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- Responded timely to security events/incidents and provided notification of incidents to the CISO and Client Security Team within an hour of identifying security incidents

Compliance

- Ensured that delivery of information security services followed applicable standards and regulatory requirements (such as applicable NIST 800-53 controls and CIS Benchmarks) and were in accordance with the project's approved System Security Plan
- Conducted ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Silvergate-specific security training materials upon project onboarding/roll-on
- Created, updated, and managed the project's disaster recovery plans and business continuity plans
- At the direction of the CISO, Implemented, maintained, and enforced stringent security and privacy requirements across the technology stack, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:
 - Federal Information Processing Standard Publication 199
 - FFIEC CAT Baseline Requirements
 - HIPAA regulatory standards
 - NIST 800-53: Security and Privacy Controls for Information Systems Organizations

Project #3	Contact #3
Company Name: Farmers Insurance Group	Contact Name: [REDACTED]
Project Name: Security Team Risk Assessment and Regulatory Alignment	Company Name: Farmers Insurance Group
Time Period: July 5, 2021 – October 29, 2021	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Delivery Lead	

Description of relevant experience:

The Farmers Insurance Group project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:

- **Integrates with at least two applications, one of which is a COTS:** The primary system in-scope included the Farmers Insurance Group's customer insurance portal which was supported by an in-house hosted on-prem Mainframe-based infrastructure layer with integrations to several COTS solutions for front-end authentication (SailPoint), security monitoring (Splunk), endpoint scanning (VMware), and workforce management ticketing solutions (ServiceNow). **In summary, the customer insurance portal interfaced with at least four (4) COTS applications (SailPoint, Splunk, VMware, and ServiceNow).**

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- **Interfaces with at least five external systems, at least one of which is real-time:** The Farmers Insurance Group's **customer portal solution** provides real-time policy information to customers which interfaces with the **50 State-wide Departments of Motor Vehicles / Registries of Motor Vehicles' registration databases** to query and corroborate State-managed database tables with registered vehicle identification numbers (VINs), and major auto repair shops with whom Farmers has partnerships with to obtain **real-time updates** and information regarding claims statuses. Integrations between web applications are utilized to connect information submitted to the **claims adjuster portal to more than 100+ repair shop owners** to input information with claims adjusters into the portal which is then transferred to the customer portal solution for customers to obtain real-time updates of their claims status. **In summary, the customer insurance portal interfaces with at least 50+ external State-managed systems (i.e. dmv.ny.gov, dmv.ca.gov, www.mass.gov, etc.), and 100+ partner repair shops to submit updates on claim statuses which is integrated with the Farmers customer portal.**
- **Is accessed by at least 1,000 users at multiple locations:** Farmers Insurance Group has more than 19 million policyholders across the United States.
- **Has a contract value of at least \$10 million:** The total contract value for services provided to Farmers Insurance Group was approximately \$32 million.
- **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The Farmers Insurance Group customer portal solution included a customer-facing user interface experience built on React JavaScript libraries that was optimized for a mobile and desktop experience. The solution included an application and data layer along with a rules engine and implemented micro-services to access various services across the solution. The data tier back-end was supported by Oracle databases for storage

As the Security Delivery Lead, Alex's accomplishments and responsibilities included:

Solution development and implementation

- **Led the development, implementation, improvement, and ongoing monitoring of industry-standard security strategies, solutions, and processes using COTS applications, such as Oracle, SailPoint, Splunk, VMware, and ServiceNow to align with key industry-standard regulatory requirements and compliance frameworks**
- Developed a prioritized cybersecurity strategy roadmap focusing on ten (10) key initiatives for Farmers to align existing technologies and capabilities with future state aspirational goals, largely driven by upcoming regulatory compliance requirements
- Collaborated with application security, software development, and GRC teams to identify gaps in the current DevSecOps policies & processes and align stakeholders on target future-state enhancements, including ensuring that a file integrity monitoring (FIM) tool was utilized to reduce the risk that changes could be deployed across systems without ensuring segregation of duties between change requester and approvers
- Collaborated with incident response, threat and vulnerability management, and GRC teams to identify gaps in the current incident response processes and align stakeholders on target future-state enhancements, including ensuring that chain of custody requirements and providing adequate notice to regulatory bodies was followed in the event that security incidents were identified
- Collaborated with GRC team members and the CISO to identify gaps in the current risk assessment and risk treatment process, noting that a cybersecurity and IT-specific risk assessment process was not yet in place; the results of the discussions led to the design, development

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

and completion of an initial cyber risk assessment and risk treatment process, along with a risk register to drive subsequent updates across the cybersecurity organization at Farmers

- Developed a cybersecurity strategy roadmap for Farmers to align existing technologies and capabilities with future target-state aspirational goals, largely driven by upcoming regulatory compliance requirements

Improving and monitoring solution

- Collaborated with application development teams, application security teams, threat and vulnerability management teams, cloud security teams, technical architects, GRC policy expert team members, CISO and Deputy CISO, Legal and Privacy, to define and implement an integrated framework of security solution architecture that comprised the information security policies and procedures, and system configurations to improve the confidentiality, integrity, and availability of Farmers Insurance Groups' cybersecurity team systems and supporting documentation
- Through collaborative walkthrough discussions across the Farmers security team (including application system owners overseeing COTS software, technical architects, application development teams, etc.) identified more than 40 information security weaknesses or potential gaps in the current environment and collaborated with the security team to bring information security operations up to standards

Reporting

- Communicated weekly project updates to Farmers CISO and direct reports.
- Reported on any new security gaps identified in the walkthrough discussions with the overall Farmers' cybersecurity team (i.e. cloud security, application security, incident response, vulnerability and threat management, identity and access management, and software development teams) and GRC team, cloud environment (which included AWS)
- Communicated the ongoing recommended security remediation roadmap across the application and IT environment supporting Farmers and the overall security strategy roadmap progress
- Furnished deliverables that detailed the outcomes of walkthrough discussions with the overall Farmers' cybersecurity team. Deliverables included an assessment of the overall maturity of the cybersecurity program, using NIST CSF as a benchmark, recommended remediations for prioritization rationalized against low-hanging fruit and high-effort strategic initiatives

Compliance

- Confirmed delivery of information security services followed applicable standards and regulatory requirements (such as NIST 800-53 controls and NY DFS regulatory requirements) and was in accordance with the project's approved System Security Plan
- Performed security awareness training for newly onboarded Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures upon project onboarding/roll-on
- At the direction of the Farmers Security Team, implemented, maintained, and enforced stringent security and privacy requirements across the Accenture team, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:
 - Federal Information Processing Standard Publication 199
 - FFIEC CAT Baseline Requirements

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
<ul style="list-style-type: none"> – HIPAA regulatory standards – NIST 800-53: Security and Privacy Controls for Information Systems Organizations 	
Project #4	Contact #4
Company Name: Microsoft	Contact Name: [REDACTED]
Project Name: Microsoft Azure Security Compliance	Company Name: Microsoft
Time Period: November 5, 2018 – June 25, 2021	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Delivery Manager	
<p><i>Description of relevant experience:</i></p> <p>The Microsoft Azure Security Compliance project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:</p> <ul style="list-style-type: none"> • Integrates with at least two applications, one of which is a COTS: The Microsoft Azure environment integrates with a multitude of COTS applications, with a significant majority developed by Microsoft, which comprised of Windows Servers for Operating systems and IT infrastructure, Azure Active Directory for user management and policy configuration, Microsoft 365 for productivity suite integrations with Mail and Teams, SQL Server databases for information storage, Azure DevOps for task and ticketing management, and Microsoft Defender for security / vulnerability scanning as examples • Interfaces with at least five external systems, at least one of which is real-time: The Microsoft Azure environment has external interfaces with a variety of technology service providers, including Palo Alto Networks for firewall solutions, Alation for data governance, Databricks for data lake optimization, Privacera for data security, and Tableau for business intelligence (BI) and visualization as examples. • Is accessed by at least 1,000 users at multiple locations: The Microsoft Azure cloud hosting solution has approximately 722 million active users who access the environment from a variety of global locations. • Has a contract value of at least \$10 million: The total contract value was approximately \$12 million. • Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms: The Microsoft Azure cloud solution included a customer-facing user Azure Portal presentation layer which was accessible via web application browser and mobile app. The Azure portal provided the GUI that allowed for central management of the Azure services, alternatively, a Command-Line Interface (CLI) could be utilized to manage Azure resources using scripts to automate tasks without using the GUI layer. The Application Layer was supported by services such as Azure App Service, Azure Logic Apps and Azure Batch which allowed for developers to build and deploy applications leveraging Azure's infrastructure and services. The data processing layer was responsible for handling data storage, management and processing, which were serviced by Azure Storage, Azure Cosmos DB, and Azure SQL Database. To enable integration with other Azure services and external systems, an integration layer was supported by Azure Service Bus, Azure Event Grid, and Azure API Management to allow for event-driven architectures, messaging, and integrations with on-prem systems and external 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

services. The security and management layer was supported by Azure Security Center and Microsoft Defender to ensure the security, monitoring, governance, and compliance of the Azure resources. The infrastructure layer was comprised of the physical data centers, servers, storage, networking infrastructure, and virtualization technologies that support the operation of Azure's services.

As the Security Delivery Manager, Alex's accomplishments and responsibilities included:

Solution development and implementation

- **Led the assessment and development of ongoing implementation enhancements and areas for improvement resulting from industry-standard security strategies, frameworks, solutions, and processes using COTS applications, Microsoft 365 and Azure DevOps, to align with key industry-standard regulatory requirements and compliance frameworks**
- Collaborated with application development teams, identity and access management, network security architects, third-party risk management, GRC, incident response, encryption, IT asset management, human resources security, and technical architects to **define and implement an integrated framework of security solution architecture that aligned with ISO 27001, ISO 27701, ISO 9001, ISO 20000-1, and ISO 22301**
- **Validated security controls and processes via recurring security control reviews in accordance with the ISO 27001, ISO 27701, ISO 9001, ISO 20000-1, and ISO 22301 standards, and reviewed results of reviews and opportunities for improvement with senior Azure security leadership**
- Reviewed and tracked security remediation progress identified during assessments and audits using the Microsoft Azure DevOps project management tool in accordance with Microsoft's Plan of Action and Milestones (POA&M) process
- Assessed the provisioning and secure management processes which covers nearly 1 billion users, and approximately 25,000 internal users

Improving and monitoring solution

- Conducted recurring information security risk assessment and privacy impact assessments on a quarterly basis surrounding the Microsoft suite of cloud hosting products to align with requirements set forth in Clauses 6.2, 6.3, 8.2, and 8.3 of the ISO 27001 standard, as well as the ISO 27701 standard

Reporting

- Planned, organized, and led project assessment planning sessions, kickoff meetings, weekly statuses, and closing meetings with senior Microsoft Azure security and GRC leadership which entailed discussing the project progress, deliverables status, and overall findings of the assessments against the ISO 27001, ISO 27701, ISO 9001, ISO 20000-1 and ISO 22301 consolidated assessment
- Drafted and furnished project deliverables which included internal and external-facing audit assessment reports and narratives of the processes observed in-scope for the assessment, as well as a summary of the findings and issuance of the certificate(s) noting conformance to the requirements set forth in the ISO standards.

Compliance

- Adhered to security compliance and privacy requirement standards, including the NIST 800-37 Risk Management Framework, NIST 800-53 System Security Plan controls, and the requirements set forth in ISO 19011 which details the guidelines and requirements for auditing and assessing management systems

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
<ul style="list-style-type: none"> Reviewed and maintained security measures during the course of the engagement as agreed to with Microsoft Azure's senior security leadership team, and recommended actions for improvement based on the findings identified Collaborated with the application development, technical, and GRC teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments Implemented, maintained, and enforced stringent security and privacy requirements across the technology stack, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data: <ul style="list-style-type: none"> Federal Information Processing Standard Publication 199 ISO 27001 Information Security Management System Standard ISO 27701 Privacy Information Management System Standard ISO 9001 Quality Management System Standard ISO 20000-1 Service Management System Standard ISO 22301 Business Continuity Management System Standard HIPAA regulatory standards NIST 800-53: Security and Privacy Controls for Information Systems Organizations 	
Total Duration of all Projects cited to meet the MQ:	4 years, 1.3 months (through December 2022)
Minimum Qualification I-S23	A minimum of three (3) years of experience within the past ten (10) years applying Information Security principles, methods, and techniques in the development of Project security Deliverables on Projects involving large and complex IT systems.
Project #1	Contact #1
Company Name: Silvergate Bank	Contact Name: [REDACTED]
Project Name: Project Manana	Company Name: Silvergate Bank
Time Period: February 1, 2022 – May 19, 2023 (ongoing)	Phone Number: [REDACTED]
Percentage of Time: February 1, 2022 – March 31, 2023: 100% April 1, 2023 – May 19, 2023 (ongoing): 50%	Email: [REDACTED]
Staff Role: Security Tech Lead	
Description of relevant experience:	
The Silvergate Bank project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- **Integrates with at least two applications, one of which is a COTS:** The Silvergate blockchain solution integrated with multiple applications (i.e. Okta, AWS, Logstash, PagerDuty, Slack, Atlassian, etc.), a large portion of which were COTS applications using available application programming interfaces (APIs). Access to the AWS environment was managed via SSO through Okta (COTS) where data from the AWS cloud hosting services was being scraped by the Logstash (COTS) enterprise monitoring tool and was being fed into PagerDuty (COTS) for alerting, which would also integrate with Slack (COTS) and Atlassian (COTS) for actioning and ticketing to resolve issues identified.
- **Interfaces with at least five external systems, at least one of which is real-time:** The Silvergate blockchain solution was designed with a public-facing ledger component referred to as the Diem Explorer, this solution provided a real-time view of transactions being posted to the Internet. The Diem Explorer was connected to a distributed network of externally-hosted validators who had permission to approve transactions on the blockchain. The consensus module operated on a Byzantine Fault Tolerance which requires that at least 67% of the validators operate in consensus to approve transactions; this is represented by $f < (n - 1) / 3$, where n represents the number of authorized validators on the network, and f equates to the number of faulty or malicious validator nodes that can be tolerated. As a function of the risk accepted by the bank, a minimum of two (2) faulty or malicious nodes was acceptable, and as a result, 7 external validator nodes were required. These nodes were hosted by several external partner entities on the network, which included Blockdaemon and Bison Trails. Whenever a blockchain transaction was to occur, five (5) out of seven (7) validators on the network would need to submit the same transaction values which would then be posted to the Diem Explorer for external awareness. Additionally, COTS applications interfaced with the blockchain to provide endpoint security monitoring (Qualys), CSPM (CrowdStrike), real-time alerting (Slack and PagerDuty), and source code management (GitHub). **In summary, the Silvergate blockchain solution interfaced with a real-time Diem Explorer, seven (7) external validator nodes, and a variety of COTS applications (Qualys, CrowdStrike, Slack, PagerDuty, and GitHub) for a minimum total of 13 interconnected systems providing real-time information to the blockchain environment.**
- **Is accessed by at least 1,000 users at multiple locations:** The Diem Association blockchain solution (acquired by Silvergate) was a publicly available open-sourced solution on GitHub and the repositories were accessed and contributed to by more than 1,800 users globally.
- **Has a contract value of at least \$10 million:** Our team's overall due diligence, operational support, and enhancements contract values totaled more than \$18 million.
- **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The Silvergate blockchain solution featured a customized front end (Diem Explorer) which was accessible via web browser and mobile devices (specifically iOS for Secure Enclave) to provide transparency into the transactions being posted to the blockchain. This graphical user interface (GUI) was fed information via the controlled application logic housed within Diem's GitHub repositories that manage the transaction rulesets for which all the external validators must abide by when submitting transactions; a minimum of 67% of the validators must be in agreement on any given transaction before posting to the blockchain which would, in turn, be represented on the Diem Explorer. Each validator hosts their own data tier back-end, for Silvergate, the data tier back-end was stored within AWS' Simple Storage Service (S3) for backup

As the Security Tech Lead, Alex's accomplishments and responsibilities include:

Applying Information Security principles, methods, and techniques to furnish project security deliverables and solutions

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- **Applied information security principles, methods, and techniques and led the development, management and execution of project security deliverables which included: Silvergate's rebuild of the acquired Diem technology assets into a greenfield AWS environment, designed with project-specific security controls and procedures, Disaster Recovery Plan, Security Incident Response Management plan and process, Technical Design Documents and Operational Manuals and Runbooks for security tools (i.e. AWS Security Hub, GitHub, CrowdStrike), and Security Architecture Diagrams**
- Through walkthrough discussions with application development team members and technical architects, a backlog of program enhancements was generated and coordinated daily touchpoints with key stakeholders to advance project work items through to completion and reduce the backlog of priority items for remediation and enhancement. The processes touched on included developing and implementing a Security Monitoring solution for the Blockchain technology that included integrating the AWS Testnet, Premainnet, and Mainnet environments with Qualys for endpoint scanning and integrating alerts with PagerDuty to ensure that the team was aware of security vulnerabilities identified in real-time. **Developed the Runbook Procedures to assist with security monitoring activities for the Bank, including consideration for cross-functional team communication channels, monitoring schedules, and examples of what to do for illustrative incident types.**
- Through walkthrough discussions with application development team members and technical architects, a backlog of program enhancements was generated and coordinated daily touchpoints with key stakeholders to advance project work items through to completion and reduce the backlog of priority items for remediation and enhancement. The processes touched on included developing and implementing a Security Monitoring solution for the Blockchain technology that included integrating the AWS Testnet, Premainnet, and Mainnet environments with Qualys for endpoint scanning and integrating alerts with PagerDuty to ensure that the team was aware of security vulnerabilities identified in real-time. **Developed the Runbook Procedures to assist with security monitoring activities for the Bank, including consideration for cross-functional team communication channels, monitoring schedules, and examples of what to do for illustrative incident types.**
- Assisted with the discovery and remediation of a significant security finding that allowed certain GitHub users to merge their own source code changes into the production branch using containerized code from Docker. **Delivered updated Runbooks detailing appropriate software development lifecycle procedures that included considerations around segregation of duties, mandatory security testing, and peer review.**
- Through collaboration with the CISO and broader Security Team, introduced a CSPM (Prisma Cloud from Palo Alto Networks) to perform a scan of the acquired Diem Association technology assets and identified more than 3,500 security findings (including high, medium, and low) within the combined cloud environments (which included AWS and Azure components) and **delivered a report prioritizing remediation efforts**
- Coordinated with Cloud Infrastructure, IT, Networking, and Security team members to remediate more than 3,000 AWS security findings, leveraging Terraform's open-source solution to apply remediations using infrastructure as code to quickly tear down and rebuild workloads where possible and improved the scalability of golden Amazon Machine Images (AMIs). **Delivered a report detailing the remediation activities completed and recommendations for the next steps to improve ongoing security enhancements.**

Reporting

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- Communicated weekly security updates for Silvergate executives, reporting on any newly identified security vulnerabilities within the cloud environment (which included AWS), security remediation progress across the application and IT environment supporting the blockchain assets, and overall security strategy roadmap progress
- Monitored the threat landscape using AWS' native Security Hub tooling, paired with CrowdStrike Falcon for CSPM which was integrated with PagerDuty to ensure that real-time alerts were captured by our Security Team and prioritized for investigation, any identified security vulnerabilities were communicated to the CISO and security organization for awareness and additional resources were introduced as necessary to remediate and address the issues identified
- Responded timely to security events/incidents and provided notification of incidents to the CISO and Client Security Team within an hour of identifying security incidents
- Oversaw the preparation of key security deliverables, including the AWS Security Remediations Report, Disaster Recovery Plan, Security Incident Response Management plan and process, Technical Design Documents and Operational Manuals and Runbooks for security tools (i.e. AWS Security Hub, GitHub, CrowdStrike, Terraform), and Security Architecture Diagrams

Compliance

- Created, updated, and managed the project's disaster recovery plans and business continuity plans in accordance with NIST 800-53 controls
- At the direction of the CISO, Implemented, maintained, and enforced stringent security and privacy requirements across the technology stack, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:
 - Federal Information Processing Standard Publication 199
 - FFIEC CAT Baseline Requirements
 - HIPAA regulatory standards
 - NIST 800-53: Security and Privacy Controls for Information Systems Organizations

Project #2**Contact #2**

Company Name: Farmers Insurance Group

Contact Name: [REDACTED]

Project Name: Security Team Risk Assessment and Regulatory Alignment

Company Name: Farmers Insurance Group

Time Period: July 5, 2021 – October 29, 2021

Phone Number: [REDACTED]

Percentage of Time: 100%

Email: [REDACTED]

Staff Role: Security Delivery Lead

Description of relevant experience:

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

The Farmers Insurance Group project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:

- **Integrates with at least two applications, one of which is a COTS:** The primary system in-scope included the Farmers Insurance Group's customer insurance portal which was supported by an in-house hosted on-prem Mainframe-based infrastructure layer with integrations to several COTS solutions for front-end authentication (SailPoint), security monitoring (Splunk), endpoint scanning (VMware), and workforce management ticketing solutions (ServiceNow). **In summary, the customer insurance portal interfaced with at least four (4) COTS applications (SailPoint, Splunk, VMware, and ServiceNow).**
- **Interfaces with at least five external systems, at least one of which is real-time:** The Farmers Insurance Group's customer portal solution provides real-time policy information to customers which interfaces with the **50 State-wide Departments of Motor Vehicles / Registries of Motor Vehicles' registration databases** to query and corroborate State-managed database tables with registered vehicle identification numbers (VINs), and major auto repair shops with whom Farmers has partnerships with to obtain real-time updates and information regarding claims statuses. Integrations between web applications are utilized to connect information submitted to the **claims adjuster portal to more than 100+ repair shop owners** to input information with claims adjusters into the portal which is then transferred to the customer portal solution for customers to obtain real-time updates of their claims status. **In summary, the customer insurance portal interfaces with at least 50+ external State-managed systems (i.e. dmv.ny.gov, dmv.ca.gov, www.mass.gov, etc.), and 100+ partner repair shops to submit updates on claim statuses which is integrated with the Farmers customer portal.**
- **Is accessed by at least 1,000 users at multiple locations:** Farmers Insurance Group has more than 19 million policyholders across the United States.
- **Has a contract value of at least \$10 million:** The total contract value for services provided to Farmers Insurance Group was approximately \$32 million.
- **Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms:** The Farmers Insurance Group customer portal solution included a customer-facing user interface experience built on React JavaScript libraries that was optimized for a mobile and desktop experience. The solution included an application and data layer along with a rules engine and implemented micro-services to access various services across the solution. The data tier back-end was supported by Oracle databases for storage

As the Security Delivery Lead, Alex's accomplishments and responsibilities included:

Applying Information Security principles, methods, and techniques to furnish project security deliverables and solutions

- **Applied information security principles, methods, and techniques and led the development of project security deliverables, including the Farmers' enterprise-wide cyber risk assessment and risk treatment methodology, cyber risk register, as well as a gap assessment and remediation roadmap developed against the Farmers cybersecurity team's ability to align with customer-facing regulatory requirements such as NY DFS and the NIST CSF.**

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- Developed a prioritized cybersecurity strategy roadmap report focusing on ten (10) key initiatives for Farmers, informed by the more than 40 security findings identified during the collaborative walkthrough sessions, to align existing technologies and capabilities with future state aspirational goals, largely driven by upcoming regulatory compliance requirements
- Collaborated with application security, software development, and GRC teams to identify gaps in the current DevSecOps policies & processes and align stakeholders on target future-state enhancements, including ensuring that a file integrity monitoring (FIM) tool was utilized to reduce the risk that changes could be deployed across systems without ensuring segregation of duties between change requester and approvers
- Collaborated with incident response, threat and vulnerability management, and GRC teams to identify gaps in the current incident response processes and align stakeholders on target future-state enhancements, including ensuring that chain of custody requirements and providing adequate notice to regulatory bodies was followed in the event that security incidents were identified
- Collaborated with GRC team members and the CISO to identify gaps in the current risk assessment and risk treatment process, noting that a cybersecurity and IT-specific risk assessment process was not yet in place; the results of the discussions led to the design, development and completion of an initial cyber risk assessment and risk treatment process, along with a risk register to drive subsequent updates across the cybersecurity organization at Farmers
- Developed a cybersecurity strategy roadmap for Farmers to align existing technologies and capabilities with future target-state aspirational goals, largely driven by upcoming regulatory compliance requirements

Reporting

- Communicated weekly project updates to Farmers CISO and direct reports.
- Reported on any new security gaps identified in the walkthrough discussions with the overall Farmers' cybersecurity team (i.e. cloud security, application security, incident response, vulnerability and threat management, identity and access management, and software development teams) and GRC team, cloud environment (which included AWS)
- Communicated the ongoing recommended security remediation roadmap across the application and IT environment supporting Farmers and the overall security strategy roadmap progress
- Furnished deliverables that detailed the outcomes of walkthrough discussions with the overall Farmers' cybersecurity team. Deliverables included an assessment of the overall maturity of the cybersecurity program, using NIST CSF as a benchmark, recommended remediations for prioritization rationalized against low-hanging fruit and high-effort strategic initiatives

Compliance

- Confirmed delivery of information security services followed applicable standards and regulatory requirements (such as NIST 800-53 controls and NY DFS regulatory requirements) and was in accordance with the project's approved System Security Plan
- At the direction of the Farmers Security Team, implemented, maintained, and enforced stringent security and privacy requirements across the Accenture team, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:
 - Federal Information Processing Standard Publication 199

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
<ul style="list-style-type: none"> – FFIEC CAT Baseline Requirements – HIPAA regulatory standards – NIST 800-53: Security and Privacy Controls for Information Systems Organizations 	
Project #3	Contact #3
Company Name: Microsoft	Contact Name: [REDACTED]
Project Name: Microsoft Azure Security Compliance	Company Name: Microsoft
Time Period: November 5, 2018 – June 25, 2021	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Delivery Manager	
<p><i>Description of relevant experience:</i></p> <p>The Microsoft Azure Security Compliance project meets the definition of "large and complex IT system," based on the following criteria defined in the RFP:</p> <ul style="list-style-type: none"> • Integrates with at least two applications, one of which is a COTS: The Microsoft Azure environment integrates with a multitude of COTS applications, with a significant majority developed by Microsoft, which comprised of Windows Servers for Operating systems and IT infrastructure, Azure Active Directory for user management and policy configuration, Microsoft 365 for productivity suite integrations with Mail and Teams, SQL Server databases for information storage, Azure DevOps for task and ticketing management, and Microsoft Defender for security / vulnerability scanning as examples • Interfaces with at least five external systems, at least one of which is real-time: The Microsoft Azure environment has external interfaces with a variety of technology service providers, including Palo Alto Networks for firewall solutions, Alation for data governance, Databricks for data lake optimization, Privacera for data security, and Tableau for business intelligence (BI) and visualization as examples. • Is accessed by at least 1,000 users at multiple locations: The Microsoft Azure cloud hosting solution has approximately 722 million active users who access the environment from a variety of global locations. • Has a contract value of at least \$10 million: The total contract value was approximately \$12 million. • Includes multi-tiered processing, including a customer or user-facing front-end optimized for multiple user interface platforms: The Microsoft Azure cloud solution included a customer-facing user Azure Portal presentation layer which was accessible via web application browser and mobile app. The Azure portal provided the GUI that allowed for central management of the Azure services, alternatively, a Command-Line Interface (CLI) could be utilized to manage Azure resources using scripts to automate tasks without using the GUI layer. The Application Layer was supported by services such as Azure App Service, Azure Logic Apps and Azure Batch which allowed for developers to build and deploy applications leveraging Azure's infrastructure and services. The data processing layer was responsible for handling 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

data storage, management and processing, which were serviced by Azure Storage, Azure Cosmos DB, and Azure SQL Database. To enable integration with other Azure services and external systems, an integration layer was supported by Azure Service Bus, Azure Event Grid, and Azure API Management to allow for event-driven architectures, messaging, and integrations with on-prem systems and external services. The security and management layer was supported by Azure Security Center and Microsoft Defender to ensure the security, monitoring, governance, and compliance of the Azure resources. The infrastructure layer was comprised of the physical data centers, servers, storage, networking infrastructure, and virtualization technologies that support the operation of Azure's services.

As the Security Delivery Manager, Alex's accomplishments and responsibilities included:

Applying Information Security principles, methods, and techniques to furnish project security deliverables and solutions

- **Applied information security principles, methods, and techniques and led the development of project security deliverables, including the execution of security assessments against Microsoft Azure's ISO 27001 (information security), ISO 27701 (privacy information), ISO 9001 (quality), ISO 20000-1 (service management) and ISO 22301 (business continuity), management systems, which included the review and assessment of Microsoft's risk assessment and risk treatment process, privacy impact assessment and treatment process, service level agreement (SLA) framework, and business continuity and disaster recovery plans, all of which were updated on a quarterly basis**
- Collaborated with application development teams, identity and access management, network security architects, third-party risk management, GRC, incident response, encryption, IT asset management, human resources security, and technical architects to define and implement an integrated framework of security solution architecture that aligned with ISO 27001, ISO 27701, ISO 9001, ISO 20000-1, and ISO 22301
- Assessed and reviewed the design elements of a comprehensive security program that aligned to standards from the National Institute of Standards and Technology (NIST) 800-37 Risk Management Framework and 800-53 System Security Plan controls, as well as the requirements set forth in ISO 27001, ISO 27701, ISO 9001, ISO 20000-1, and ISO 22301 for an information security management system, privacy information management system, quality management system, service management system, and business continuity management system for the Microsoft Azure suite of cloud hosting products
- Conducted recurring information security risk assessment and privacy impact assessments on a quarterly basis surrounding the Microsoft suite of cloud hosting products to align with requirements set forth in Clauses 6.2, 6.3, 8.2, and 8.3 of the ISO 27001 standard, as well as the ISO 27701 standard
- Validated security controls and processes via recurring security control reviews in accordance with the ISO 27001, ISO 27701, ISO 9001, ISO 20000-1, and ISO 22301 standards, and reviewed results of reviews and opportunities for improvement with senior Azure security leadership
- Reviewed and tracked security remediation progress identified during assessments and audits using the Microsoft Azure DevOps project management tool in accordance with Microsoft's Plan of Action and Milestones (POA&M) process
- Assessed the user access provisioning / deprovisioning and secure access management processes which cover nearly 1 billion users, and approximately 25,000 internal users

Reporting

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
<ul style="list-style-type: none"> Planned, organized, and led project assessment planning sessions, kickoff meetings, weekly statuses, and closing meetings with senior Microsoft Azure security and GRC leadership which entailed discussing the project progress, deliverables status, and overall findings of the assessments against the ISO 27001, ISO 27701, ISO 9001, ISO 20000-1 and ISO 22301 consolidated assessment Drafted and furnished project deliverables which included internal and external-facing audit assessment reports and narratives of the processes observed in-scope for the assessment, as well as a summary of the findings and issuance of the certificate(s) noting conformance to the requirements set forth in the ISO standards. <p>Compliance</p> <ul style="list-style-type: none"> Adhered to security compliance and privacy requirement standards, including the NIST 800-37 Risk Management Framework, NIST 800-53 System Security Plan controls, and the requirements set forth in ISO 19011 which details the guidelines and requirements for auditing and assessing management systems during the process of furnishing project security deliverables 	
Total Duration of all Projects cited to meet the MQ:	3 years, 10.3 months (through December 2022)
Minimum Qualification I-S24	A minimum of three (3) years of experience assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) to identify appropriate security controls to protect Personally Identifiable Information (PII), Protected Health Information (PHI) and/or Federal Tax Information (FTI) data.
Project #1	Contact #1
Company Name: Silvergate Bank	Contact Name: [REDACTED]
Project Name: Project Manana	Company Name: Silvergate Bank
Time Period: February 1, 2022 – May 19, 2023 (ongoing)	Phone Number: [REDACTED]
Percentage of Time: February 1, 2022 – March 31, 2023: 100% April 1, 2023 – May 19, 2023 (ongoing): 50%	Email: [REDACTED]
Staff Role: Security Tech Lead	
Description of relevant experience:	
<p>As the Security Tech Lead, Alex's accomplishments and responsibilities include:</p> <p>Assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199)</p> <ul style="list-style-type: none"> Assessed system data sensitivity using industry-standard security categorizations (i.e. public, restricted, confidential, highly confidential designations) while identifying and implementing the following security controls to protect PII and PHI to align with regulatory compliance 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

requirements such as NIST 800-111 Guide to Storage Encryption Technologies for End User Devices (11/2007), NIST 800-88 Guidelines for Media Sanitation (12/2014), NIST 800-71 Recommendation for Key Establishment Using Symmetric Block Ciphers (06/2018), NIST 800-39 Managing Information Security Risk (03/2011), NIST 800-30 Risk Management Guide for Information Technology Systems (09/2012), NIST 800-63-3 Electronic Authentication Guideline, Federal Information Processing Standard (FIPS) Publication 199 Standards for Security Categorization of Federal Information and Information Systems (02/2004), Information Privacy Act (Civil Code section 1798 et seq.), Public Records Act (California Gov. Code Section 6250 et seq.), HIPAA regulatory standards, NIST 800-53: Security and Privacy Controls for Information Systems Organizations:

- Applying access controls such as strong, complex passwords across the application suite (i.e. Okta, Atlassian, PagerDuty, CrowdStrike, Qualys, Slack, etc.); multi-factor biometric authentication driven through Okta and requiring mobile application push code to access the application suite; terminating user access for individuals rolled off from the project or no longer working at the Bank; and performing monthly access reviews to ensure user access permissions were appropriate and commensurate with job functions
- Applying encryption solutions on all in-scope systems that could potentially store PII or PHI, including ensuring server-side encryption was applied to all AWS S3 buckets that could potentially store PII or PHI, applying Transport Layer Security (TLS) 1.2 or greater on all sensitive web application servers, and ensuring all user workstations were applying disk encryption (monitored via Qualys)
- Ensuring that data retention schedules were adhered to in compliance with the Bank's information security policies which aligned with NIST 800-88 by ensuring that AWS S3 buckets that potentially stored PII or PHI were configured to dispose of such information in accordance with the retention schedule as defined in the Bank's data classification policy and restricting the use of universal storage buses (USBs) at all times across all user workstations (monitored via Qualys)
- At the direction of the CISO, Implemented, maintained, and enforced stringent security and privacy requirements across the technology stack, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:
 - Federal Information Processing Standard Publication 199
 - FFIEC CAT Baseline Requirements
 - HIPAA regulatory standards
 - NIST 800-53: Security and Privacy Controls for Information Systems Organizations

Reporting

- **Monitored the threat landscape using AWS' native Security Hub tooling, paired with CrowdStrike Falcon for CSPM which was integrated with PagerDuty to detect potential incidents where PII or PHI may be exposed** and ensured that real-time alerts were captured by our Security Team and prioritized for investigation, any identified security vulnerabilities were communicated to the CISO and security organization for awareness and additional resources were introduced as necessary to remediate and address the issues identified
- Responded timely to security events/incidents and provided notification of incidents to the CISO and Client Security Team within an hour of identifying security incidents

Compliance

- Ensured that delivery of information security services followed applicable standards and regulatory requirements (such as applicable NIST 800-53 controls and CIS Benchmarks) and was in accordance with the project's approved System Security Plan

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- Conducted ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Silvergate-specific security training materials upon project onboarding/roll-on
- Created, updated, and managed the project's disaster recovery plans and business continuity plans

Project #2	Contact #2
Company Name: Diem Association	Contact Name: [REDACTED]
Project Name: Security Due Diligence Assessment	Company Name: Diem
Time Period: November 2, 2021 – January 28, 2022	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Due Diligence Lead	
Description of relevant experience:	
<p>As the Security Due Diligence Lead, Alex's accomplishments and responsibilities include:</p> <p>Assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) and solution development</p> <ul style="list-style-type: none"> • Assessing whether or not system data sensitivity processes and controls were in place, using security categorizations while identifying and ensuring that the following security controls were implemented to protect sensitive information, trade secrets, PII, and PHI in accordance with regulatory compliance requirements set forth in ISO 27001:2013 – Information Security Management System, ISO 27701:2019 – Privacy Information Management System, NIST 800-111 Guide to Storage Encryption Technologies for End User Devices (11/2007), NIST 800-88 Guidelines for Media Sanitation (12/2014), NIST 800-71 Recommendation for Key Establishment Using Symmetric Block Ciphers (06/2018), NIST 800-39 Managing Information Security Risk (03/2011), NIST 800-30 Risk Management Guide for Information Technology Systems (09/2012), NIST 800-63-3 Electronic Authentication Guideline, Federal Information Processing Standard (FIPS) Publication 199 Standards for Security Categorization of Federal Information and Information Systems (02/2004), Information Privacy Act (Civil Code section 1798 et seq.), Public Records Act (California Gov. Code Section 6250 et seq.), HIPAA regulatory standards, NIST 800-53: Security and Privacy Controls for Information Systems Organizations: <ul style="list-style-type: none"> – Determined whether or not the following access controls were in place: strong, complex passwords across the application suite (i.e. Okta, Atlassian, PagerDuty, CrowdStrike, Qualys, Slack, etc.); multi-factor biometric authentication driven through Okta and requiring mobile application push code to access the application suite; timely revocation of access; and periodic user access reviews to ensure user access permissions were appropriate and commensurate with job functions – Determined whether or not encryption solutions were applied on all in-scope systems that could potentially store sensitive information, trade secrets, PII, or PHI, including ensuring that server-side encryption was applied to all AWS S3 buckets that could potentially store PII 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

or PHI, applying Transport Layer Security (TLS) 1.2 or greater on all sensitive web application servers, and ensuring all user workstations were applying disk encryption (monitored via Qualys)

- Assessed data disposal and retention risk by determining whether or not data retention schedules were adhered to in compliance with the information security policies, by ensuring that AWS S3 buckets that potentially stored PII or PHI were configured to dispose of such information in accordance with the retention schedule as defined in the data classification policy and restricting the use of universal storage buses (USBs) at all times across all user workstations (monitored via Qualys)
- **At the direction of the CISO, Implemented, maintained, and enforced stringent security and privacy requirements across the technology stack, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:**
 - Federal Information Processing Standard Publication 199
 - FFIEC CAT Baseline Requirements
 - HIPAA regulatory standards
 - NIST 800-53: Security and Privacy Controls for Information Systems Organizations
- **Collaborated with application development teams, technical architects, GRC policy expert team members, CISO and Deputy CISO, Legal and Privacy, to define and implement an integrated framework of security solution architecture that comprised the information security policies and procedures, and system configurations to promote confidentiality, integrity, and availability of the acquired Diem blockchain-based technology assets and data**

Reporting

- Reported on identified instances where risks or concerns around the exposure of PII and PHI data existed within the technology stack and helped to identify solutions to remediate and address the root cause of the exposure, including ensuring that publicly exposed S3 buckets be configured to restricted to necessary users only

Compliance

- Ensured that delivery of information security services followed applicable standards and regulatory requirements (such as applicable NIST 800-53 controls and CIS Benchmarks) and were in accordance with the project's approved System Security Plan
- Conducted ongoing security awareness efforts for Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures, including the completion of the required Silvergate-specific security training materials upon project onboarding/roll-on
- Created, updated, and managed the project's disaster recovery plans and business continuity plans

Project #3

Contact #3

Company Name: Farmers Insurance Group

Contact Name: [REDACTED]

Project Name: Security Team Risk Assessment and Regulatory Alignment

Company Name: Farmers Insurance Group

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
Time Period: July 5, 2021 – October 29, 2021	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Delivery Lead	
<p><i>Description of relevant experience:</i></p> <p>As the Security Delivery Lead, Alex's accomplishments and responsibilities included:</p> <p>Assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) and solution development</p> <ul style="list-style-type: none"> Assessing whether or not system data sensitivity processes and controls were in place, using security categorizations while identifying and ensuring that the following security controls were implemented to protect sensitive information, trade secrets, PII, and PHI in accordance with regulatory compliance requirements set forth in ISO 27001:2013 – Information Security Management System, ISO 27701:2019 – Privacy Information Management System, NIST 800-111 Guide to Storage Encryption Technologies for End User Devices (11/2007), NIST 800-88 Guidelines for Media Sanitation (12/2014), NIST 800-71 Recommendation for Key Establishment Using Symmetric Block Ciphers (06/2018), NIST 800-39 Managing Information Security Risk (03/2011), NIST 800-30 Risk Management Guide for Information Technology Systems (09/2012), NIST 800-63-3 Electronic Authentication Guideline, Federal Information Processing Standard (FIPS) Publication 199 Standards for Security Categorization of Federal Information and Information Systems (02/2004), Information Privacy Act (Civil Code section 1798 et seq.), Public Records Act (California Gov. Code Section 6250 et seq.), HIPAA regulatory standards, NIST 800-53: Security and Privacy Controls for Information Systems Organizations: <ul style="list-style-type: none"> Determined whether or not the following access controls were in place: strong, complex passwords across the application suite (i.e. customer web portal, SailPoint, ServiceNow, etc.); multi-factor biometric authentication driven through SailPoint and requiring mobile application push code to access the application suite; timely revocation of access; and periodic user access reviews to ensure user access permissions were appropriate and commensurate with job functions Determined whether or not encryption solutions were applied on all in-scope systems that could potentially store sensitive information, trade secrets, PII or PHI, including ensuring that Oracle database servers applied server-side encryption to all databases that could potentially store PII or PHI, applying Transport Layer Security (TLS) 1.2 or greater on all sensitive web application servers, and ensuring all user workstations were applying disk encryption Assessed data disposal and retention risk by determining whether or not data retention schedules were adhered to in compliance with the information security policies, by ensuring that Oracle database servers that potentially stored PII or PHI were configured to dispose of such information in accordance with the retention schedule as defined in the data classification policy and restricting the use of universal storage buses (USBs) at all times across all user workstations Implemented a risk assessment and risk treatment process that resulted in the review of all known system types as identified within the ServiceNow configuration management database (CMDB) to codify and organize IT assets into risk categories based on the types of information processed, including whether PII or PHI data is ingested. The process assisted with informing the requisite level of controls to 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

be applied to protect these system categories and inform security management on appropriate steps to take in order to accept or treat the risks identified. The resultant risk register is updated on a continuous basis by Farmer's GRC team

- At the direction of the Farmers Security Team, implemented, maintained, and enforced stringent security and privacy requirements across the Accenture team, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:
 - Federal Information Processing Standard Publication 199
 - FFIEC CAT Baseline Requirements
 - HIPAA regulatory standards
 - NIST 800-53: Security and Privacy Controls for Information Systems Organizations
- Through collaborative walkthrough discussions across the Farmers security team (including application system owners overseeing COTS software, technical architects, application development teams, etc.) **identified more than 40 information security weaknesses or potential gaps, including potential risks around the handling and retention of data stores housing PII or PHI**
- **Developed a prioritized cybersecurity strategy roadmap focusing on ten (10) key initiatives for Farmers to address key findings around the handling and retention of PII and PHI**, to align existing technologies and capabilities with future state aspirational goals, largely driven by upcoming regulatory compliance requirements

Reporting

- Reported on any new security gaps identified in the walkthrough discussions with the overall Farmers' cybersecurity team (i.e. cloud security, application security, incident response, vulnerability and threat management, identity and access management, and software development teams) and GRC team, cloud environment (which included AWS)
- Communicated the ongoing recommended security remediation roadmap across the application and IT environment supporting Farmers and the overall security strategy roadmap progress
- Furnished deliverables that detailed the outcomes of walkthrough discussions with the overall Farmers' cybersecurity team. Deliverables included an assessment of the overall maturity of the cybersecurity program, using NIST CSF as a benchmark, recommended remediations for prioritization rationalized against low-hanging fruit and high-effort strategic initiatives

Compliance

- Confirmed delivery of information security services followed applicable standards and regulatory requirements (such as NIST 800-53 controls and NY DFS regulatory requirements) and was in accordance with the project's approved System Security Plan
- Performed security awareness training for newly onboarded Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures upon project onboarding/roll-on

Project #4

Company Name: Microsoft

Contact #4

Contact Name: [REDACTED]

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
Project Name: Microsoft Azure Security Compliance	Company Name: Microsoft
Time Period: November 5, 2018 – June 25, 2021	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Delivery Manager	
<p>As the Security Delivery Manager, Alex’s accomplishments and responsibilities included:</p> <p>Assessing system data sensitivity using security categorizations (e.g., FIPS Publication 199) and solution development</p> <ul style="list-style-type: none"> Assessing whether or not system data sensitivity processes and controls were in place, using security categorizations while identifying and ensuring that the following security controls were implemented to protect sensitive information, trade secrets, PII, and PHI in accordance with regulatory compliance requirements set forth in ISO 27001:2013 – Information Security Management System, ISO 27701:2019 – Privacy Information Management System, NIST 800-111 Guide to Storage Encryption Technologies for End User Devices (11/2007), NIST 800-88 Guidelines for Media Sanitation (12/2014), NIST 800-71 Recommendation for Key Establishment Using Symmetric Block Ciphers (06/2018), NIST 800-39 Managing Information Security Risk (03/2011), NIST 800-30 Risk Management Guide for Information Technology Systems (09/2012), NIST 800-63-3 Electronic Authentication Guideline, Federal Information Processing Standard (FIPS) Publication 199 Standards for Security Categorization of Federal Information and Information Systems (02/2004), Information Privacy Act (Civil Code section 1798 et seq.), Public Records Act (California Gov. Code Section 6250 et seq.), HIPAA regulatory standards, NIST 800-53: Security and Privacy Controls for Information Systems Organizations: <ul style="list-style-type: none"> Determined whether or not the following access controls were in place: strong, complex passwords across the application suite (i.e. Azure web portal, Microsoft 365, Azure DevOps, etc.); multi-factor biometric authentication driven through Azure Active Directory and requiring mobile application push code to access the application suite; timely revocation of access; and periodic user access reviews to ensure user access permissions were appropriate and commensurate with job functions Determined whether or not encryption solutions were applied on all in-scope systems that could potentially store sensitive information, trade secrets, PII, or PHI, including ensuring that Azure servers applied server-side encryption to all infrastructure that could potentially store PII or PHI, applying Transport Layer Security (TLS) 1.2 or greater on all sensitive web application servers, and ensuring all user workstations were applying disk encryption Assessed data disposal and retention risk by determining whether or not data retention schedules were adhered to in compliance with the information security policies, by ensuring that Azure servers that potentially stored PII or PHI were configured to dispose of such information in accordance with the retention schedule as defined in the data classification policy and restricting the use of universal storage buses (USBs) at all times across all user workstations Reviewed the risk assessment and risk treatment process across the IT assets (servers, databases, endpoints) that support the Azure cloud hosting services to determine whether the risk assessment process took into account information processed, including whether PII 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

or PHI data was ingested. Reviewed the process to determine whether or not the requisite level of controls were applied to protect these system categories to treat the risks identified.

- **Led the assessment and development of ongoing implementation enhancements and areas for improvement resulting from industry-standard security strategies, frameworks, solutions, and processes using COTS applications, Microsoft 365 and Azure DevOps, to align with key industry-standard regulatory requirements and compliance frameworks**
- Implemented, maintained, and enforced stringent security and privacy requirements across the technology stack, including the following security and compliance standards, regulations, policies, and frameworks **to protect PII and PHI data:**
 - Federal Information Processing Standard Publication 199
 - ISO 27001 Information Security Management System Standard
 - ISO 27701 Privacy Information Management System Standard
 - ISO 9001 Quality Management System Standard
 - ISO 20000-1 Service Management System Standard
 - ISO 22301 Business Continuity Management System Standard
 - HIPAA regulatory standards
 - NIST 800-53: Security and Privacy Controls for Information Systems Organizations

Reporting

- Planned, organized, and led project assessment planning sessions, kickoff meetings, weekly statuses, and closing meetings with senior Microsoft Azure security and GRC leadership which entailed discussing the project progress, deliverables status, and overall findings of the assessments against the ISO 27001, ISO 27701, ISO 9001, ISO 20000-1 and ISO 22301 consolidated assessment
- Drafted and furnished project deliverables which included internal and external-facing audit assessment reports and narratives of the processes observed in-scope for the assessment, as well as a summary of the findings and issuance of the certificate(s) noting conformance to the requirements set forth in the ISO standards.

Compliance

- Adhered to security compliance and privacy requirement standards, including the NIST 800-37 Risk Management Framework, NIST 800-53 System Security Plan controls, and the requirements set forth in ISO 19011 which details the guidelines and requirements for auditing and assessing management systems
- Reviewed and maintained security measures during the course of the engagement as agreed to with Microsoft Azure's senior security leadership team, and recommended actions for improvement based on the findings identified
- Collaborated with the application development, technical, and GRC teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments

Total Duration of all Projects cited to meet the MQ:

4 years, 1.3 months (through December 2022)

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
Minimum Qualification I-S25	A minimum of three (3) years of experience with systems that comply with the National Institute of Standards and Technology (NIST) 800-53 moderate baseline.
Project #1	Contact #1
Company Name: Silvergate Bank	Contact Name: [REDACTED]
Project Name: Project Manana	Company Name: Silvergate Bank
Time Period: February 1, 2022 – May 19, 2023 (ongoing)	Phone Number: [REDACTED]
Percentage of Time: February 1, 2022 – March 31, 2023: 100% April 1, 2023 – May 19, 2023 (ongoing): 50%	Email: [REDACTED]
Staff Role: Security Tech Lead	
<p><i>Description of relevant experience:</i></p> <p>As the Security Tech Lead, Alex's accomplishments and responsibilities included:</p> <p>Systems that comply with NIST 800-53 moderate baseline</p> <ul style="list-style-type: none"> • Worked with the Silvergate Bank Diem blockchain system, which complied with NIST 800-53 moderate baseline as a result of the regulatory climate and scrutiny pertaining to the Financial Services industry and being a federally chartered bank; the risk environment necessitated a moderate baseline minimum with a suite of more than 325 NIST-aligned controls. • Through collaboration with the CISO and broader Security Team, introduced a CSPM (Prisma Cloud from Palo Alto Networks) to perform a scan of the acquired Diem Association technology assets and identified more than 3,500 security findings (including high, medium, and low) within the combined cloud environments (which included AWS and Azure components) and developed a plan to prioritize the remediation efforts, portions of the assessment criteria included findings that aligned with NIST 800 security principles and the NIST CSF (identify). • Coordinated with Cloud Infrastructure, IT, Networking, and Security team members to remediate more than 3,000 AWS security findings, leveraging Terraform's open-source solution to apply remediations using infrastructure as code to quickly tear down and rebuild workloads where possible and improved the scalability of golden Amazon Machine Images (AMIs) – NIST CSF Protect, Respond and Recover • Applied information security principles, methods, and techniques and led the development, management and execution of project security deliverables, which included: Silvergate's rebuild of the acquired Diem technology assets into a greenfield AWS environment, designed with project-specific security controls and procedures, Disaster Recovery Plan, Security Incident Response Management plan and process, Technical Design Documents and Operational Manuals and Runbooks for security tools (i.e. AWS Security Hub, GitHub, CrowdStrike), and Security Architecture Diagrams – NIST CSF Protect 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- Served as the incident response manager when potential security incidents were identified across the technology assets, with the application development, technical architects, and other functional teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments – **NIST CSF Respond and Recover**
- Assisted with the discovery and remediation of a significant security finding that allowed certain GitHub users to merge their own source code changes into the production branch using containerized code from Docker – **NIST CSF Detect**
- Identified information security (IS) weaknesses or potential gaps in the current environment and collaborated with the client security team as well as internal Accenture teams to document the work tasks and rationalize the prioritization in order to remediate the identified gaps and align to standard best practices – **NIST CSF Detect**
- Managed the identity and access management of Silvergate's software-as-a-service (SaaS) applications and vendors, including AWS and Azure for cloud hosting services, Okta for single sign-on (SSO) and user administration, GitHub for source code management, Qualys for endpoint vulnerability scanning, 1Password for secrets management, PagerDuty for security alerting, Slack for instant messaging and alerting, Docker for software container management, and the usage of Entrust's managed hardware security module (HSM) capabilities on behalf of the client to ensure that the application architecture design, ongoing development, and implementation were operating according to security best practices – **NIST CSF Protect**

Reporting

- Monitored the threat landscape using AWS' native Security Hub tooling, paired with CrowdStrike Falcon for CSPM which was integrated with PagerDuty to ensure that real-time alerts were captured by our Security Team and prioritized for investigation, any identified security vulnerabilities were communicated to the CISO and security organization for awareness and additional resources were introduced as necessary to remediate and address the issues identified
- Responded timely to security events/incidents and provided notification of incidents to the CISO and Client Security Team within an hour of identifying security incidents
- Oversaw the preparation of key security deliverables, including the Disaster Recovery Plan, Security Incident Response Management plan and process, Technical Design Documents and Operational Manuals and Runbooks for security tools (i.e. AWS Security Hub, GitHub, CrowdStrike, Terraform), and Security Architecture Diagrams

Compliance

- Ensured that delivery of information security services followed applicable standards and regulatory requirements (such as applicable NIST 800-53 controls and CIS Benchmarks) and were in accordance with the project's approved System Security Plan
- Created, updated, and managed the project's disaster recovery plans and business continuity plans in accordance with NIST 800-53 controls and CIS benchmarks
- At the direction of the CISO, Implemented, maintained, and enforced stringent security and privacy requirements across the technology stack, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:
 - Federal Information Processing Standard Publication 199
 - FFIEC CAT Baseline Requirements

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
<ul style="list-style-type: none"> – HIPAA regulatory standards – NIST 800-53: Security and Privacy Controls for Information Systems Organizations 	
Project #2	Contact #2
Company Name: Diem Association	Contact Name: [REDACTED]
Project Name: Security Due Diligence Assessment	Company Name: Diem
Time Period: November 2, 2021 – January 28, 2022	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Due Diligence Lead	
<p><i>Description of relevant experience:</i></p> <p>As the Security Due Diligence Lead, Alex's accomplishments and responsibilities included:</p> <p>Systems that comply with NIST 800-53 moderate baseline</p> <ul style="list-style-type: none"> • Worked with the Diem Association blockchain solution, which complied with NIST 800-53 moderate baseline as a result of the regulatory climate and scrutiny stemming from the Federal government and in preparation for issuing a solution that aligned value with fiat currency (US Dollars); the risk environment necessitated a moderate baseline minimum with a suite of more than 325 NIST-aligned controls. • Managed the transition of technological assets and ensured that appropriate access controls (provisioning, deprovisioning, user access reviews, multi-factor authentication) were applied during the transition phase, including SaaS applications and vendors, such as AWS and Azure for cloud hosting services, Okta for single sign-on (SSO) and user administration, GitHub for source code management, Qualys for endpoint vulnerability scanning, 1Password for secrets management, PagerDuty for security alerting, Slack for instant messaging and alerting, Docker for software container management, and the usage of Entrust's managed hardware security module (HSM) capabilities on behalf of the client to ensure that the application architecture design, ongoing development, and implementation were operating according to security best practices – NIST CSF Identify Protect <p>Reporting</p> <ul style="list-style-type: none"> • Maintained the IS strategy (forward-looking roadmap), aligning services to the strategy • Monitored the threat landscape using cloud access service broker (CASB) and native AWS security monitoring functionality, and made timely adjustments and/or recommendations to reduce risk – NIST CSF Respond and Recover <p>Compliance</p> <ul style="list-style-type: none"> • Ensured that delivery of information security services followed applicable standards and regulatory requirements (such as applicable NIST 800-53 controls and CIS Benchmarks) and were in accordance with the project's approved System Security Plan 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE	
<ul style="list-style-type: none"> Created, updated, and managed the project's disaster recovery plans and business continuity plans in accordance with NIST 800-53 controls and CIS benchmarks 	
Project #3	Contact #3
Company Name: Farmers Insurance Group	Contact Name: [REDACTED]
Project Name: Security Team Risk Assessment and Regulatory Alignment	Company Name: Farmers Insurance Group
Time Period: July 5, 2021 – October 29, 2021	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Delivery Lead	
<p><i>Description of relevant experience:</i></p> <p>As the Security Delivery Lead, Alex's accomplishments and responsibilities included:</p> <p>Systems that comply with NIST 800-53 moderate baseline</p> <ul style="list-style-type: none"> Worked with the Farmers Insurance Group customer portal system, which complies with NIST 800-53 moderate baseline as a result of the regulatory climate and scrutiny stemming from being a financial services firm in the United States; the risk environment necessitated a moderate baseline minimum with a suite of more than 325 NIST-aligned controls. Through collaborative walkthrough discussions across the Farmers security team (including application system owners overseeing COTS software, technical architects, application development teams, etc.) identified more than 40 information security weaknesses or potential gaps in the current environment as it relates to the NIST 800-53 standard and collaborated with the security team to bring information security operations up to standards – NIST CSF Identify and Protect Developed a prioritized cybersecurity strategy roadmap focusing on ten (10) key initiatives for Farmers to align existing technologies and capabilities with future state aspirational goals, largely driven by upcoming regulatory compliance requirements, including compliance with NIST 800-53 – NIST CSF Identify Applied information security principles, methods, and techniques and led the development of project security deliverables, including the Farmers' enterprise-wide cyber risk assessment and risk treatment methodology, cyber risk register, as well as a gap assessment and remediation roadmap developed against the Farmers cybersecurity team's ability to align with customer-facing regulatory requirements such as NY DFS and the NIST CSF. – NIST CSF Protect Collaborated with application development teams, application security teams, threat and vulnerability management teams, cloud security teams, technical architects, GRC policy expert team members, CISO and Deputy CISO, Legal and Privacy, to define and implement an integrated framework of security solution architecture that comprised the information security policies and procedures, and 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

system configurations to improve the confidentiality, integrity, and availability of Farmers Insurance Groups' cybersecurity team systems and supporting documentation – **NIST CSF Protect**

- Collaborated with application security, software development, and GRC teams to identify gaps in the current DevSecOps policies & processes and align stakeholders on target future-state enhancements, including ensuring that a file integrity monitoring (FIM) tool was utilized to reduce the risk that changes could be deployed across systems without ensuring segregation of duties between change requester and approvers– **NIST CSF Identify**
- Collaborated with incident response, threat and vulnerability management, and GRC teams to identify gaps in the current incident response processes and align stakeholders on target future-state enhancements, including ensuring that chain of custody requirements and providing adequate notice to regulatory bodies was followed in the event that security incidents were identified – **NIST CSF Identify, Protect and Respond**
- Collaborated with GRC team members and the CISO to identify gaps in the current risk assessment and risk treatment process, noting that a cybersecurity and IT-specific risk assessment process was not yet in place; the results of the discussions led to the design, development and completion of an initial cyber risk assessment and risk treatment process, along with a risk register to drive subsequent updates across the cybersecurity organization at Farmers – **NIST CSF Identify**
- Identified information security weaknesses or potential gaps in the current environment and collaborates with the client security team to bring information security operations up to standards – **NIST CSF Identify**

Reporting

- Communicated weekly project updates to Farmers CISO and direct reports.
- Reported on any new security gaps identified in the walkthrough discussions with the overall Farmers' cybersecurity team (i.e. cloud security, application security, incident response, vulnerability and threat management, identity and access management, and software development teams) and GRC team, cloud environment (which included AWS)
- Communicated the ongoing recommended security remediation roadmap across the application and IT environment supporting Farmers and the overall security strategy roadmap progress
- Furnished deliverables that detailed the outcomes of walkthrough discussions with the overall Farmers' cybersecurity team. Deliverables included an assessment of the overall maturity of the cybersecurity program, using NIST CSF as a benchmark, recommended remediations for prioritization rationalized against low-hanging fruit and high-effort strategic initiatives

Compliance

- Confirmed delivery of information security services followed applicable standards and regulatory requirements (such as NIST 800-53 controls and NY DFS regulatory requirements) and was in accordance with the project's approved System Security Plan
- Performed security awareness training for newly onboarded Accenture team members to confirm understanding and compliance with relevant IS obligations, customer security policies, supporting documentation, and procedures upon project onboarding/roll-on
- At the direction of the Farmers Security Team, implemented, maintained, and enforced stringent security and privacy requirements across the Accenture team, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- Federal Information Processing Standard Publication 199
- FFIEC CAT Baseline Requirements
- HIPAA regulatory standards
- NIST 800-53: Security and Privacy Controls for Information Systems Organizations

Project #4	Contact #4
Company Name: Microsoft	Contact Name: [REDACTED]
Project Name: Microsoft Azure Security Compliance	Company Name: Microsoft
Time Period: November 5, 2018 – June 25, 2021	Phone Number: [REDACTED]
Percentage of Time: 100%	Email: [REDACTED]
Staff Role: Security Delivery Manager	
Description of relevant experience:	
<p>As the Security Delivery Manager, Alex's accomplishments and responsibilities included:</p> <p>Systems that comply with NIST 800-53 moderate baseline</p> <ul style="list-style-type: none"> • Worked with the Microsoft Azure cloud service, which complies with NIST 800-53 moderate baseline as a result of providing government cloud instances to the public sector and Federal Government contractors; the risk environment necessitated a moderate baseline minimum with a suite of more than 325 NIST-aligned controls. • Collaborated with application development teams, identity and access management, network security architects, third party risk management, GRC, incident response, encryption, IT asset management, human resources security, and technical architects to define and implement an integrated framework of security solution architecture that aligned with ISO 27001, ISO 27701, ISO 9001, ISO 20000-1, and ISO 22301 – NIST CSF Identify and Protect • Assessed and reviewed the design elements of a comprehensive security program that aligned to standards from the National Institute of Standards and Technology (NIST) 800-37 Risk Management Framework and 800-53 System Security Plan controls, as well as the requirements set forth in ISO 27001, ISO 27701, ISO 9001, ISO 20000-1, and ISO 22301 for an information security management system, privacy information management system, quality management system, service management system, and business continuity management system for the Microsoft Azure suite of cloud hosting products – NIST CSF Identify, Protect, Detect, Respond, and Recover • Conducted recurring information security risk assessment and privacy impact assessments on a quarterly basis surrounding the Microsoft suite of cloud hosting products to align with requirements set forth in Clauses 6.2, 6.3, 8.2 and 8.3 of the ISO 27001 standard, as well as the ISO 27701 standard – NIST CSF Identify and Protect 	

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE

- Validated security controls and processes via recurring security control reviews in accordance with the ISO 27001, ISO 27701, ISO 9001, ISO 20000-1, and ISO 22301 standards, and reviewed results of reviews and opportunities for improvement with senior Azure security leadership – **NIST CSF Identify, Protect, Detect, Respond, and Recover**
- Reviewed and tracked security remediation progress identified during assessments and audits using the Microsoft Azure DevOps project management tool in accordance with Microsoft's Plan of Action and Milestones (POA&M) process – **NIST CSF Recover**
- Assessed the provisioning and secure management processes which covers nearly 1 billion users, and approximately 25,000 internal users – **NIST CSF Identify and Protect**

Reporting

- Planned, organized, and led project assessment planning sessions, kickoff meetings, weekly statuses, and closing meetings with senior Microsoft Azure security and GRC leadership which entailed discussing the project progress, deliverables status, and overall findings of the assessments against the ISO 27001, ISO 27701, ISO 9001, ISO 20000-1 and ISO 22301 consolidated assessment
- Drafted and furnished project deliverables which included internal and external-facing audit assessment reports and narratives of the processes observed in-scope for the assessment, as well as a summary of the findings and issuance of the certificate(s) noting conformance to the requirements set forth in the ISO standards.

Compliance

- Adhered to security compliance and privacy requirement standards, including the NIST 800-37 Risk Management Framework, NIST 800-53 System Security Plan controls, and the requirements set forth in ISO 19011 which details the guidelines and requirements for auditing and assessing management systems
- Reviewed and maintained security measures during the course of the engagement as agreed to with Microsoft Azure's senior security leadership team, and recommended actions for improvement based on the findings identified
- Collaborated with the application development, technical, and GRC teams to drive the root cause analysis and remediation of results from security incidents, penetration tests, vulnerability scans, internal/external audits, and other assessments
- Implemented, maintained, and enforced stringent security and privacy requirements across the technology stack, including the following security and compliance standards, regulations, policies, and frameworks to protect PII and PHI data:
 - Federal Information Processing Standard Publication 199
 - ISO 27001 Information Security Management System Standard
 - ISO 27701 Privacy Information Management System Standard
 - ISO 9001 Quality Management System Standard
 - ISO 20000-1 Service Management System Standard
 - ISO 22301 Business Continuity Management System Standard
 - HIPAA regulatory standards
 - NIST 800-53: Security and Privacy Controls for Information Systems Organizations

PART 2 – INFRASTRUCTURE SECURITY MANAGER MINIMUM QUALIFICATIONS TABLE				
Total Duration of all Projects cited to meet the MQ:			4 years, 1.3 months (through December 2022)	
Minimum Qualification I-S26	Hold and maintain for the duration of the contract an (ISC)2® Certified Information Systems Security Professional (CISSP) certification, or ISACA Certified Information Security Manager (CISM).			
Certification / Degree Title	Certification Number	Original Grant Date	Expiration Date	Online Validation Link; if not available, attach a copy to the offer
(ISC)² Certified Information Systems Security Professional (CISSP)	654089	April 1, 2021 Certified Since 2018	March 31, 2024	www.isc2.org/verify
IAPP Certified Information Privacy Professional/United States (CIPP/US)	000303620I	July 1, 2021	June 30, 2023	https://iapp.org/certify/lookup/

International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Alex Hsiung

the credential of

Certified Information Systems Security Professional

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.



Yiannis Pavlosoglou - Chairperson



James Packer - Secretary



654089

Certification Number

Apr 1, 2021 - Mar 31, 2024

Certification Cycle

Certified Since: 2018

(ISC)²

Verify Member is in good standing at: www.isc2.org/verify

Printed On: 5/18/2023

The Chairperson and Directors of the

International Association of Privacy Professionals

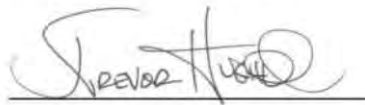
*decree that in recognition of the successful demonstration of the requisite
knowledge of information privacy with advanced concentration in U.S. private-sector laws, standards and practices, we do
confer upon:*

Alexander Hsiung

the designation of

Certified Information Privacy Professional/United States (CIPP/US)

*With all rights, privileges and distinction thereunto appertaining.
In witness hereof we have caused this certificate to be signed by the
duly authorized officers of the Association.*



President and CEO, IAPP



Chairperson



0003036201

Certificate Number

July 1, 2021

Effective Date

June 30, 2023

Expiration Date

1.7 INFRASTRUCTURE OPERATIONS SERVICE DESK LEAD STAFF QUALIFICATIONS

INFRASTRUCTURE OPERATIONS SERVICE DESK LEAD			
PART 1 – RÉSUMÉ			
Contractor	Accenture LLP		
Candidate Name	Jamala Rule		
Position in the Company	Service Desk Associate Manager	Length of Time in Position	7.5 Years
Project Position & Responsibilities	<p>Infrastructure Operations Service Desk Lead</p> <p>Jamala meets all the requirements as defined in RFP section 12.1.3.6.7.</p>		
Skills & Qualifications for Project Position	<p>Skills: Jamala specializes in high quality customer service and management of service desk ticketing processes. Her skills include effectively managing activities in support of service desk and coordinating with Tier 1, 2 and 3 application and technical teams to resolve tickets and correct all incidents. She provides high quality service with consistent and clear responses to tickets, incorporating best practices and leveraging technology to enhance and improve service desk ticket handling. She makes recommendations for improvements to the service desk to enhance service delivery, optimize costs, and maintain knowledge repositories.</p> <p>Jamala builds productive working relationships with stakeholders and keeps them informed of service desk activities. She has experience managing Tier 1 and Tier 2 non-production and production environments and handling escalation to Tier 3. She conducts reviews and leads updates to process documentation as well as maintaining and enhancing the knowledge repositories used by service desk team members. She has trained, coached and mentored service desk specialists.</p> <p>She collaborates with Tier 3 application development and technical teams to ensure each team follows best practices for ticket handling, including, but not limited to, meeting SLA requirements, updating aging tickets, and providing clear and appropriate responses to tickets. She is a hands-on manager, known for an ability to work with disparate teams and coordinates with other contractors on projects to resolve issues. She has extensive experience in user training and has worked with diverse groups to develop and provide training, mentor and share information in a format that users can understand, regardless of their technical skill level.</p> <p>She has extensive experience coordinating ticket escalation and resolution. She has worked with the ServiceNow application since 2019 and experience in transitioning service desks from other ITSM applications to ServiceNow.</p> <p>Qualifications: Jamala's service desk operations experience includes serving as Tier 3 Lead, Incident Manager and the Accenture Service Desk Lead for both the C-IV and CalSAWS Project for the past 7.5 years. She currently serves as Incident Manager and manages the CalSAWS ServiceNow instance processes. She has two years experience with ServiceNow, starting with ServiceNow training in 2019, ServiceNow implementation in 2020 and go live of the ServiceNow application in 2021. She also has significant experience developing and providing software training. She</p>		

INFRASTRUCTURE OPERATIONS SERVICE DESK LEAD

has 3.5 years of experience leading a service desk **(MQ I-S27: Exceeds)**, working in help desk environments that serve more than 2,500 end users **(MQ I-S28: Exceeds)**, and experience with the ServiceNow platform and tools **(MQ I-S29: Exceeds)**. Jamala is certified in ITIL v4 Foundation **(MQ I-S30: Meets)**.

Relevant Experience (Add additional tables as needed)

Project Title	California State Automated Welfare System (CalSAWS)				
Position Title	Incident Manager/Accenture Service Desk Lead				
Begin Date	9/27/2021	End Date	Ongoing	# of Months	15 months
Scope and Description of Responsibility	<p>Scope: As the Incident Manager/Accenture Service Desk Lead on the CalSAWS project, Jamala oversees Tier 3 reported issues and manages service desk support for the California counties CalSAWS users. She also works with Tier 1 and Tier 2 service desk agents to smooth operation and ensure ticket resolution.</p> <p>Responsibility: Jamala oversees Tier 3 operations and develops and coordinates training for the CalSAWS help desk and county staff. She reviews and updates Tier 2 and Tier 3 process documentation, and manages urgent issues, ticket escalations, incident and problem ticket handling and reporting trends. She coordinates and facilitates meetings between county and project staff and helps identify training needs to maintain and exceed required SLAs and prompt ticket resolution.</p>				
Skills Utilized and Experience Attained	<p>Skills Utilized: Jamala uses her knowledge of CalSAWS functionality and processes, along with her skills in training, ticket handling, and ServiceNow reporting in her role on the CalSAWS project.</p> <p>Experience Attained: Jamala played a pivotal role in planning, developing, and testing the roll out of ServiceNow for the CalSAWS application. This experience, coupled with her knowledge of CalSAWS gained from the C-IV project and work with participating county personnel, allowed her to help develop over 900 incident categories in ServiceNow to implement the automated incident routing inherent in the application. This work also facilitated the improvement in service levels that the project experienced on the project. This background provided the necessary experience with ServiceNow and the CalSAWS internal processes required to prepare and facilitate the more than 100 training sessions with county and project staff that occurred during the roll out of the ServiceNow application. She gained experience in assigning, triaging and responding to escalations and following up on tickets. This contributed to achieving and maintaining the monthly help desk Diagnosis SLA compliance.</p>				
Project Title	CalSAWS Consortium IV (C-IV)				
Position Title	Tier 3 Lead/Accenture Service Desk Lead				
Begin Date	10/1/2014	End Date	9/26/2021	# of Months	84 months

INFRASTRUCTURE OPERATIONS SERVICE DESK LEAD

Scope and Description of Responsibility	Scope: As the Tier 3 Lead/Accenture Service Desk Lead on the C-IV Project, Jamala managed and supported the C-IV help desk and Level 3 teams triaging and resolving reported issues and change orders for 39 California counties, in addition to managing county concerns and escalations and providing training to staff as needed. Responsibility: Jamala provided guidance to the Tier 2 C-IV help desk for ticket handling best practices in addition to coordinating training for 30+ help desk staff. She managed and triaged over 300 tickets weekly and monitored and reported on ticket trends and widespread system issues. She also coordinated responses for county concerns/escalations and facilitated application functional meetings between county and project staff.	
Skills Utilized and Experience Attained	Skills Utilized: Jamala brought her service desk experience, gained as a Tier 3 service desk analyst, and her training skills, which contributed to educating and informing help desk and project staff on the Computer Associates (CA) Service Desk tool, ticket trends, and best practices for ticket handling. Experience Attained: Triaging over 300 tickets weekly and monitoring trends for several years allowed Jamala to learn the C-IV application, which assisted with triage and resolving issues in a timely manner. She also attained knowledge of county internal processes and C-IV help desk internal processes. She gained experience working with the various teams, prepared and presented training sessions and demonstrated leadership abilities in collaborating and working with SAWS management.	
Education (add rows as needed)		
Years	Course of Study	School
08/2001 – 05/2006	Bachelor of Science, Engineering	Clark Atlanta University
Professional Certifications or Designations (add rows as needed)		
Certification or Designation	Organization	Dates
ITIL v4 Foundation	PeopleCert	May 26, 2023

PART 2 – INFRASTRUCTURE OPERATIONS SERVICE DESK LEAD MINIMUM QUALIFICATIONS TABLE

Minimum Qualification I-S27	A minimum of two (2) years of lead experience within the past five (5) years working in a service desk/help desk.		
Project #1		Contact #1	
Company Name: CalSAWS Consortium		Contact Name: [REDACTED]	
Project Name: CalSAWS		Company Name: CalSAWS Consortium	
Time Period: September 27, 2021 – ongoing 100%		Phone Number: [REDACTED]	
Time Period: January 2, 2020 – September 26, 2021 – 50%		Email: [REDACTED]	
Percentage of Time: see above		Contact #2	
		Contact Name: [REDACTED]	
		Company Name: CalSAWS Consortium	
		Phone Number: [REDACTED]	
		Email: [REDACTED]	
Staff Role: Incident Manager/Accenture Service Desk Lead			
Description of relevant experience:			
<p>As an Incident Manager/Service Desk Lead, Jamala's responsibilities include:</p> <ul style="list-style-type: none">• Led the development and execution of a plan to increase the help desk Diagnosis SLA compliance metric to meet minimum requirement of 98%<ul style="list-style-type: none">– Within six months of the 39 C-IV counties' cutover to the CalSAWS system(September 27,2021 – March 2022), increased the help desk Diagnosis SLA compliance from 81.4% to 98.2%, and have maintained that level exceeding the minimum compliance of 98%• Lead and coordinate training sessions for Tier 2 CalSAWS help desk in effort to increase agents' knowledge of the CalSAWS application<ul style="list-style-type: none">– Created and implemented tracking of learning management system (LMS) courses completed by service desk agents– Identify training requirements and lead weekly training on ServiceNow functionality as required– Coordinated and led recurring training sessions with the Tier 3 online application development team– Provide guidance on ticket resolution to 38 subcontractor Tier 2 help desk staff• Review and provide feedback on Tier 2 CalSAWS help desk process documentation, including the call back process and training documentation for new staff• Oversee requests, incidents and problems reported to the Service Desk• Worked closely with the subcontractor managing Tier 1 to provide feedback on escalation, documentation and scripts used• Update ServiceNow Knowledge Base repository			

PART 2 – INFRASTRUCTURE OPERATIONS SERVICE DESK LEAD MINIMUM QUALIFICATIONS TABLE

- Perform major incident management (MIM) by creating problem records, performing ticket analysis, and contacting county help desk staff to join troubleshooting bridge and/or to confirm resolution of the reported issue
- Solicit and analyze observed ticket trends from Tier 2 and Tier 3 staff
- Work with Tier 1, 2 and 3 teams to evaluate gaps in existing training material and provide updates when needed
- Works with other contractor staff BenefitsCal-related tickets.
- Review ticket status with teams and gather updates to ensure meeting of SLA targets
- Manage incidents, problems, and service requests by sending daily reports to project teams for:
 - Aging tickets
 - Incidents approaching SLA breach
 - Unresolved incidents linked to resolved problems
 - Unresolved problems linked to Jira items that are in production or have been rejected
 - KPIs and trends
 - Training and procedure refresh as needed
- Provide guidance, information, issue escalation and updating documentation and scripts for Tier 1 handled by a subcontractor.
- Organize and facilitate the Tier 2/Tier 3 weekly connect meetings, which cover:
 - ServiceNow tips and tricks
 - Provide guidance and best practices for ticket handling
 - Discuss County/CalSAWS Consortium concerns and feedback
 - Current monthly help desk Diagnosis compliance SLA percentage month-to-date
 - Review of tickets assigned to each team that are approaching SLA breach
 - Upcoming training, systems upgrades, etc.
 - Current ticket trends and demonstrations from Tier 3 on CalSAWS functionality
 - Provide problem analysis to determine causes

Project #2	Contact #1
Company Name: CalSAWS Consortium	Contact Name: [REDACTED]
Project Name: C-IV	Company Name: CalSAWS Consortium
Time Period: January 2, 2018 – September 26, 2021	Phone Number: [REDACTED]
Percentage of Time: 50%	Email: [REDACTED]
	Contact #2
	Contact Name: [REDACTED]

PART 2 – INFRASTRUCTURE OPERATIONS SERVICE DESK LEAD MINIMUM QUALIFICATIONS TABLE

		Company Name: CalSAWS Consortium
		Phone Number: [REDACTED]
		Email: [REDACTED]
Staff Role: Tier 3 Lead/Accenture Service Desk Lead		
Description of relevant experience:		
<p>As Tier 3 Lead/Accenture Service Desk Lead, Jamala's responsibilities included:</p> <ul style="list-style-type: none"> • Managed the Tier 3 application support and change order queue for 39 counties and triaged/reassigned tickets to the appropriate application development and technical teams • Managed Tier 1 and Tier 2 C-IV help desk with creating and updating process documentation, including a "frequently asked questions" (FAQ) document for implementation of the Affordable Care Act (ACA) and ticket troubleshooting steps • Analyzed, identified, and reported on KPIs and ticket trends to project leads and CalSAWS Consortium management • Coordinated efforts to report widespread C-IV system issues—including establishing parent/problem tickets, linking related tickets to the parent/problem ticket, and drafting and distributing communication of the issue to county staff • Coordinated training sessions for the CalSAWS service desk to increase their knowledge of C-IV system • Coordinated onboarding of new C-IV help desk staff for San Bernardino induction training to support C-IV system knowledge • Managed, mature and maintained the service desk knowledge repository • Managed the phone/ticket escalation process and coordinated responses between county and project staff 		
Total Duration of all Projects cited to meet the MQ:		4 years (through Dec. 2022)
Minimum Qualification I-S28	A minimum of two (2) years of experience within the past five (5) years working in a help desk environment serving over 2,500 end users.	
Project #1		Contact #1
Company Name: CalSAWS Consortium		Contact Name: [REDACTED]
Project Name: CalSAWS		Company Name: CalSAWS Consortium
Time Period: September 27, 2021 – ongoing 100%		Phone Number: [REDACTED]
Time Period: January 2, 2020 – September 26, 2021 – 50%		Email: [REDACTED]
		Contact #2
		Contact Name: [REDACTED]
		Company Name: CalSAWS Consortium

PART 2 – INFRASTRUCTURE OPERATIONS SERVICE DESK LEAD MINIMUM QUALIFICATIONS TABLE

	Phone Number: [REDACTED]
	Email: [REDACTED]
Staff Role: Incident Manager/Accenture Service Desk Lead	
Description of relevant experience:	
<p>As Incident Manager/Service Desk Lead, Jamala's responsibilities include:</p> <ul style="list-style-type: none"> • Lead the Accenture CalSAWS help desk, which serves 18,500 daily end users and up to 41,500 users in total. • Visit county sites to discuss ticket concerns and execute process improvement initiatives for conversion efforts and ticket handling <ul style="list-style-type: none"> – Conducted follow-up meetings and received positive feedback from counties indicating improvements with ticket handling • Research and follow up on county and CalSAWS Consortium escalations regarding ticket concerns and requests for updates • Coordinate and facilitate weekly ticket troubleshooting sessions between county help desk and project staff, which provides quicker resolution turnaround time • Coordinate and facilitate the help desk operations meeting for 48 counties, which covers ServiceNow ticket handling best practices, CalSAWS functionality, ticket trends, and training material for ticket trends • Document, audit and regularly improve processes used by the Service Desk • Oversee requests, incidents and problems reported to the Service Desk • Facilitate the monthly trends meeting with CalSAWS Consortium staff, which covers upcoming enhancements, help desk ticket metrics, and an analysis of ticket trends 	
Project #2	Contact #1
Company Name: CalSAWS Consortium	Contact Name: [REDACTED]
Project Name: C-IV Help Desk	Company Name: CalSAWS Consortium
Time Period: January 2, 2018 – September 26, 2021	Phone Number: [REDACTED]
Percentage of Time: 50%	Email: [REDACTED]
	Contact #2
	Contact Name: [REDACTED]
	Company Name: CalSAWS Consortium
	Phone Number: [REDACTED]
	Email: [REDACTED]
Staff Role: Tier 3 Lead/Accenture Service Desk Lead	
Description of relevant experience:	

PART 2 – INFRASTRUCTURE OPERATIONS SERVICE DESK LEAD MINIMUM QUALIFICATIONS TABLE

As Tier 3 Lead/Accenture Service Desk Lead, Jamala's responsibilities included:

- **Led the Accenture C-IV help desk, which served 18,000 total end users**
- Managed the Tier 3 application support queue for 39 counties and triaged/reassigned tickets to the appropriate application development and technical teams
- Analyzed, identified, and reported on KPIs and ticket trends for Tiers 1, 2 and 3 to project leads and CalSAWS Consortium management
- Coordinated efforts to report widespread C-IV system issues—including establishing parent/problem tickets, linking related tickets to the parent/problem ticket, and drafting and distributing communication of the issue to county staff
- Coordinated training sessions for the CalSAWS service desk to increase their knowledge of C-IV system
- Coordinated inclusion of new C-IV help desk staff at San Bernardino induction training to support understanding of C-IV system
- Coordinated and facilitated C-IV functional learning sessions with C-IV county help desk staff, which covered C-IV system functionality and ticket handling best practices
- Facilitated the quarterly help desk committee meeting with the CalSAWS Consortium help desk manager, covering change order updates
- Managed and maintained the service desk knowledge repository
- Managed the ticket escalation process and coordinated responses between county and project staff

Total Duration of all Projects cited to meet the MQ:		4 years (through December 2022)
Minimum Qualification I-S29	A minimum of two (2) years of experience within the past five (5) years with the ServiceNow platform and tools.	
Project #1		Contact #1
Company Name: CalSAWS Consortium		Contact Name: [REDACTED]
Project Name: CalSAWS		Company Name: CalSAWS Consortium
Time Period: Sept 27, 2021 – ongoing – 100%		Phone Number: [REDACTED]
Time Period: January 2, 2020 – Sept.26 2021 – 50%		Email: [REDACTED]
Percentage of Time: see above		
		Contact #2
		Contact Name: [REDACTED]
		Company Name: CalSAWS Consortium
		Phone Number: [REDACTED]
		Email: [REDACTED]
Staff Role: Incident Manager/Accenture Service Desk Lead		

PART 2 – INFRASTRUCTURE OPERATIONS SERVICE DESK LEAD MINIMUM QUALIFICATIONS TABLE

Description of relevant experience:

As the Incident Manager/Accenture Service Desk Lead, Jamala's responsibilities include:

- **Participated in the establishment and build-out of CalSAWS ServiceNow processes**
 - Performed planning, development, and testing of case, incident, problem, and service request forms and processes in ServiceNow
 - Analyzed, provided recommendations, and developed fields needed from Computer Associates Service Desk Manager to CalSAWS ServiceNow
 - Analyzed and developed CalSAWS ServiceNow category hierarchy and automatic routing rules for over 900 categories
- **Organized, prepared, and facilitated training and support sessions for CalSAWS ServiceNow processes and functionality**
 - Trained more than 700 county help desk staff on ServiceNow functionality
 - Conducted 115 CalSAWS training and support sessions on ServiceNow for previous LRS, C-IV, and CalWIN counties
- Represented C-IV and county staff and actively participated in ServiceNow requirements gathering, design discussions, training and field mapping for transition to ServiceNow from CA Service Desk starting in January 2020 with the CalSAWS Consortium and other third party contractors
- Completed training in ServiceNow functionality in 2019 in preparation for the evaluation of and subsequent implementation of the ServiceNow platform for CalSAWS.
- Manage and maintain the CalSAWS ServiceNow Knowledge Bases
 - Created 30 knowledge base articles that cover CalSAWS ServiceNow processes and functionality

Total Duration of all Projects cited to meet the MQ:

2 years 1 month

Minimum Qualification I-S30	Hold and maintain for the duration of the contract an ITIL certification.			
Certification / Degree Title	Certification Number	Original Grant Date	Expiration Date	Online Validation Link; if not available, attach a copy to the offer
ITIL Foundation Certification in IT Service Management	GR671522933JR	5/26/2023	5/25/2026	Copy of certification included at the end of this section (Section 1.7).

This is to certify that

Jamala Glena Rule

Has achieved the

**ITIL[®] Foundation Certificate in
IT Service Management**

Effective from **26 May 2023**

Renew by **26 May 2026**

Certificate number **GR671522933JR**

Candidate number **9980079398582199**



Byron Nicolaides
Chairman and Group CEO, PeopleCert

ITIL 4 Edition

Printed on 30 May 2023

This certificate remains the property of the issuing Examination Institute and shall be returned immediately upon request.