***Our Assumptions and Considerations about AGW Water Works***

AGW Water Works is a critical public utility responsible for the full water lifecycle—from sourcing and purification to storage, distribution, and billing. Its digital ecosystem encompasses not only water-related logistics but also deeply integrated IT, cybersecurity, financial, compliance, and customer service domains. Given its public importance, operational scale, and regulatory responsibilities, modernizing its IT infrastructure is vital for enhanced service delivery, cost optimization, and sustainability.

AGW's operations span various interlinked domains:

* Water Resource Management: Purification kinds, volume targets, capacity, distribution pipelines, and routing all require real-time monitoring and optimization.
* User Systems: Employees, customers, and their interactions with water services and IT infrastructure.
* IT & Cybersecurity: Networking, IAM, software assets, security posture, disaster recovery, and threat intelligence are vital for resilience and compliance.
* Finance & Forecasting: Billing, payroll, CapEx, and predictive forecasting help maintain operational efficiency.
* Compliance & QC: Safety, regulatory, financial, and quality audits ensure transparency and accountability.

AGW's legacy systems are siloed, resource-heavy, and scattered across on-premise servers—leading to high OpEx, poor scalability, and elevated carbon emissions.

***Migration Strategy***

In this section, we will provide an overview of AGW’s migration approach, focusing on the key steps taken to transition from legacy systems to Azure-based solutions. Each resource category—such as shared databases, middleware dependencies, security systems, and others—will be analyzed individually, detailing the migration strategy employed for each. For every resource, we will highlight the chosen Azure tools, migration methods (Lift-and-Shift, Replatforming, Refactoring), and the timeline associated with the migration. Additionally, the benefits of these strategies will be discussed, including the reduction of operational costs, scalability improvements, and the overall efficiency gained through modernizing the infrastructure. You can expect a clear breakdown of the process involved in migrating AGW’s systems, providing a detailed roadmap of how legacy systems are transformed into scalable, secure, and cost-effective solutions on the Azure cloud platform.

**1. Shared Oracle Databases and Legacy Systems**

AGW’s IT infrastructure relies extensively on shared Oracle Database systems, which support a variety of both critical and non-critical business functions. These databases act as the backend for essential operations such as Water Distribution management, Storage Data tracking, Sensor and SCADA logs, Customer Billing Systems, and Payroll Processing. Over the years, these systems have grown complex due to accumulated application dependencies, rigid schemas, and centralized configurations that are difficult to decouple or modernize without impacting business continuity.

***Its significance:***  
These shared Oracle DBs are vital because they consolidate transactional, operational, and analytical data across key departments in AGW. By hosting multiple services on common database instances, AGW has historically reduced infrastructure costs and improved inter-system operability. However, the tight coupling has also introduced severe drawbacks—such as limited scalability, high vendor lock-in, increased maintenance overhead, and downtime risks due to shared failure domains. The inability to scale individual applications independently also hampers AGW’s agility and responsiveness to modern demands like real-time analytics or distributed microservices integration.

***Migration strategy:***To modernize this infrastructure, AGW has adopted a Lift-and-Shift approach using Azure Migrate and Azure Database Migration Assistant (DMA). This strategy involves assessing each Oracle instance for compatibility and performance metrics, then rehosting these databases to either Azure Database for Oracle or Azure SQL Managed Instance, depending on application compatibility. A key component of this migration includes decoupling monolithic services, enabling database-level isolation. This also involves integrating Azure Application Gateway and Load Balancer to intelligently route requests across replicated instances, thereby avoiding the risk of bottlenecks and allowing phased database migration while maintaining application uptime.

***Azure and other technologies used:***  
The migration leverages Azure Migrate for discovery, assessment, and orchestration, while Data Migration Assistant is used for schema and data transfer. AGW also deploys Azure Database for Oracle where high compatibility is required and uses Azure SQL Managed Instances for modernized applications. To ensure minimal downtime and improve load distribution, Azure Load Balancer and Azure Application Gateway are implemented. These technologies collectively modernize the legacy backend while ensuring HA (High Availability), scalability, and secure access via Azure Entra ID (formerly AAD) integration for authentication.

***Cost and savings:***  
By shifting away from on-premise Oracle licenses and shared server infrastructure, AGW anticipates a 40% reduction in licensing and support costs annually. Additional cost savings come from reduced physical server maintenance, data center cooling, and staffing needs. With Azure’s consumption-based pricing model and reserved instance offerings, further long-term operational expenditure (OPEX) optimizations are expected. Legacy systems often incur unpredictable maintenance costs, and modern cloud services eliminate such inefficiencies.

***Estimated time:***  
The migration of each critical database set is estimated to take around 4–6 weeks, which includes discovery, planning, testing, data transfer, cutover, and validation. Less critical databases may follow a trickle migration approach with ongoing synchronization and final switchovers scheduled during low-traffic periods.

***Benefits and carbon footprint improvement:***  
Migrating shared Oracle databases to Azure’s carbon-neutral data centers significantly reduces AGW's environmental impact. Azure’s global data centers operate using renewable energy sources, and their infrastructure is optimized for power and cooling efficiency. By offloading compute-intensive workloads from legacy, power-hungry hardware, AGW can lower carbon emissions, improve power usage effectiveness (PUE), and support corporate sustainability goals. In parallel, the modularization of the database layer increases system resilience, maintainability, and elasticity, enabling AGW to better align IT operations with its smart water management vision.

**2. Middleware Dependencies: Tomcat, Tibco, MQ Systems**

AGW's IT infrastructure includes several legacy middleware platforms, primarily Apache Tomcat for application hosting, IBM MQ for message queuing, and Tibco for event-driven data routing. These middleware components serve as the backbone for core applications such as legacy water quality monitoring dashboards, employee management and HR portals, and real-time sensor data ingestion pipelines. These systems have historically provided essential integration between services but have grown outdated, expensive to maintain, and inflexible in adapting to the company’s cloud-native goals.

***Its significance:***  
These middleware systems are critical because they manage application serving, inter-process communication, and data flow orchestration between diverse modules. For instance, Tomcat handles hundreds of concurrent web-based transactions, Tibco enables data routing between telemetry modules and monitoring dashboards, and IBM MQ supports reliable messaging between back-end systems. Together, they ensure data consistency, reliability, and asynchronous processing. However, the legacy setup involves hardware-bound deployments, limited horizontal scalability, manual provisioning, and minimal observability, making it challenging to respond to dynamic workloads or automate deployments.

***Migration strategy:***  
The modernization plan involves containerizing all Tomcat-based applications using Docker, and then deploying them onto Azure Kubernetes Service (AKS) for scalability and efficient orchestration. This enables AGW to standardize application packaging, streamline updates, and ensure isolated fault domains. For messaging and event routing, Tibco and IBM MQ are being gradually replaced with Azure-native messaging services such as Azure Service Bus, Event Grid, and Event Hubs, depending on the required messaging pattern (queue, publish-subscribe, or streaming). This transition eliminates legacy middleware licensing and reduces application coupling. A microservice-friendly communication backbone is thereby established, facilitating easier future development and integration.

***Azure and other technologies used:***  
The key technologies adopted in this migration include Docker for containerization, Azure Kubernetes Service (AKS) for orchestration, and Azure Container Registry to host and version Docker images. Azure-native alternatives like Service Bus, Event Grid, and Event Hubs take over event-driven communication responsibilities. Azure Monitor, Log Analytics, and Azure Application Insights are integrated for observability, while Azure DevOps pipelines manage CI/CD workflows, ensuring consistent, automated, and auditable deployments.

***Cost and savings:***  
Migrating from licensed on-premises middleware and hardware-bound queues to cloud-native PaaS solutions results in a substantial OPEX reduction of up to 50% per year. This is achieved by eliminating licensing fees, physical server maintenance, and manual operational costs. The automation of deployments using DevOps pipelines reduces personnel workload, while containerization improves resource utilization. Furthermore, adopting Azure messaging services on a pay-per-use basis allows for precise cost control aligned with workload patterns.

***Estimated time:***  
The estimated duration for migration is 6–8 weeks per middleware stack, which includes containerization of legacy Tomcat apps, deployment setup on AKS, integration with Azure messaging services, testing, and cutover. Legacy system dependencies are analyzed in the initial weeks, followed by iterative releases using Agile sprints to ensure minimal disruption.

***Benefits and carbon footprint improvement:***  
Transitioning to Azure PaaS messaging and container orchestration enables AGW to consolidate workloads, reduce server sprawl, and significantly lower energy consumption. By retiring on-prem hardware and legacy servers, AGW can achieve an estimated 35% drop in emissions, aligned with Microsoft Azure’s carbon-neutral operational model. Server consolidation also reduces e-waste, eliminates the need for continuous cooling systems, and improves sustainability. Moreover, containerization and microservices adoption future-proof the architecture, allowing AGW to innovate rapidly while maintaining environmental and financial efficiency.

**3. Networking and IAM Systems**

AGW currently operates with fragmented network infrastructure and lacks a centralized Identity and Access Management (IAM) system. The networking setup involves non-standardized hardware across regions and manual routing configurations, which lead to a fragile environment with increased maintenance overhead. In terms of identity and access, various departments follow disconnected access control practices, making it difficult to enforce uniform security standards or audit user privileges across the enterprise.

***Its significance:***  
A robust and unified network and IAM framework is vital for AGW’s secure and scalable operations. The lack of centralized IAM makes access provisioning time-consuming, creates inconsistency in permission levels, and increases the risk of unauthorized access. Similarly, non-standardized and hardware-dependent networking restricts AGW’s ability to adapt quickly to operational changes, introduce new digital services, or scale infrastructure in a secure and reliable manner. This directly impacts service availability, data governance, and cybersecurity posture across the enterprise.

***Migration strategy:***  
The proposed plan involves implementing a centralized identity governance system using Microsoft Entra ID (formerly Azure Active Directory), which will be synchronized with AGW's on-premise Active Directory. This will enable Single Sign-On (SSO), Multi-Factor Authentication (MFA), and role-based access control (RBAC) across all digital systems. Simultaneously, the legacy routing hardware is planned to be phased out and replaced with Azure-native networking components, including Azure Virtual Network (VNet), VPN Gateway, and Azure Firewall. These solutions will allow for policy-based routing, secure hybrid connectivity, and centralized traffic filtering.

***Azure and other technologies used:***  
The modernization effort will utilize Microsoft Entra ID for identity services, Azure AD Connect for directory synchronization, and Conditional Access Policies for enforcing security rules. On the networking side, Azure Virtual Network will establish logical network boundaries, while VPN Gateway will provide secure connections between on-prem and cloud environments. Azure Firewall, along with Network Security Groups (NSGs) and Application Security Groups (ASGs), will be configured to enforce granular security policies. Azure Bastion will be used to securely access virtual machines without exposing them to the public internet.

***Estimated time:***  
The rollout is expected to be completed within an estimated timeframe of 4 weeks, which includes identity directory synchronization, network topology configuration, policy definition, and phased cutover. A pilot phase is proposed for one regional site to validate the architecture and process before full-scale deployment.

***Cost and savings:***  
The proposed migration is projected to reduce administrative overhead by approximately 60%, particularly in areas like user onboarding, password resets, and access auditing. AGW will no longer need to maintain legacy IAM tools or physical networking gear, translating to lower hardware and support costs. Azure’s consumption-based pricing model offers better cost predictability, and centralized control eliminates the need for third-party security products or manual processes.

***Benefits and carbon footprint improvement:***  
This shift is expected to enhance network reliability, tighten security, and simplify identity audits, all while making the infrastructure scalable for future growth. Decommissioning energy-intensive hardware like legacy firewalls, routers, and access appliances will reduce network-related energy consumption, leading to an estimated 30% decrease in emissions. Additionally, adopting Azure's energy-efficient data centers will contribute to AGW’s sustainability goals, reducing its environmental footprint as part of its broader digital transformation.

**4. Sensor and IoT Infrastructure**

AGW’s sensor and IoT infrastructure is crucial for monitoring water sourcing, distribution, and quality control across various operations. The company utilizes a large-scale SCADA (Supervisory Control and Data Acquisition) and IoT infrastructure to collect and store data from thousands of sensors deployed in various locations. Currently, legacy systems manage this data on local servers, which results in data silos and limits the ability to perform advanced analytics or respond to real-time anomalies.

***Its significance:***  
This infrastructure plays a pivotal role in monitoring the status of water sources, ensuring compliance with safety regulations, and optimizing the water distribution network. The data collected from sensors provides valuable insights that can enhance operational efficiency, predict maintenance needs, and identify potential issues in water quality. However, the existing system has constraints that hinder AGW from unlocking the full potential of this data, such as poor scalability, limited analytics, and the inability to perform predictive maintenance.

***Migration strategy:***  
The migration plan proposes moving the existing sensor data and IoT infrastructure to Azure IoT Hub, enabling real-time data ingestion and better integration with cloud-based analytics services. Data will be archived long-term in Azure Data Lake, providing a centralized and scalable repository for historical and real-time data. To process the data, Azure Stream Analytics will be used for real-time data streams, and Azure Synapse Analytics will be leveraged for advanced analytics and business intelligence. These cloud services will allow AGW to perform predictive maintenance and quality assurance, unlocking actionable insights from the data.

***Azure and other technologies used:***  
Key Azure technologies will include Azure IoT Hub for IoT device management and data ingestion, Azure Stream Analytics for real-time event processing, and Azure Synapse Analytics for big data and advanced analytics. The data will be stored in Azure Data Lake for efficient long-term storage and accessibility. Additionally, Azure Monitor and Azure Security Center will be used for monitoring, security, and compliance management. These tools together form a robust ecosystem for managing and analyzing IoT data in a scalable, secure, and cost-efficient manner.

***Estimated time:***  
The migration of AGW’s sensor and IoT infrastructure to Azure is expected to take between 6 to 10 weeks, depending on the volume of data, the complexity of sensor integrations, and the migration of existing data into Azure Data Lake. A phased migration will ensure minimal disruption to ongoing operations.

***Cost and savings:***  
The migration is expected to generate savings in several areas. Moving to a cloud-based solution eliminates the need for on-prem physical server clusters, which reduces hardware maintenance and storage redundancy costs. It is anticipated that AGW can save up to 30% in operational costs related to server maintenance, energy consumption, and storage redundancy. Additionally, the adoption of Azure IoT Hub and Azure Synapse Analytics will reduce the time-to-insight and improve decision-making, thereby leading to cost efficiencies in day-to-day operations.

***Benefits and carbon footprint improvement:***  
The migration will significantly improve uptime, data accessibility, and decision-making by providing real-time insights and predictive maintenance capabilities. Moreover, the shift from physical servers to cloud-based infrastructure will result in energy consumption reductions, as Azure operates in carbon-neutral data centers. By consolidating compute workloads into Azure's green data centers, AGW is expected to reduce carbon emissions significantly. The estimated reduction in emissions from eliminating physical server clusters and transitioning to Azure's more efficient cloud infrastructure is projected to be substantial, contributing to the company's broader sustainability goals.

**5. Software and Asset Inventory Management**

AGW’s software and asset inventory management previously relied on manual and disjointed methods for tracking its various assets and software licenses. The lack of a centralized system, such as a Configuration Management Database (CMDB), made it difficult for AGW to manage software licenses, asset locations, and usage efficiently. This lack of visibility and control led to inefficiencies, including redundant purchases and overspending on software licenses. Key assets, including mobile devices, edge compute resources, workstations, and other IT hardware, were not tracked systematically, resulting in challenges in lifecycle management and compliance.

***Its significance:***  
Efficient asset and software inventory management is crucial for ensuring that AGW can maintain a clear view of its resources, avoid unnecessary expenditures, and ensure compliance with software licensing terms. Without a proper CMDB or asset tracking system, AGW faced risks related to non-compliance, potential software over-licensing, and wasted IT resources. By implementing a comprehensive asset management system, AGW can better understand its infrastructure, optimize resource usage, and ensure that software licenses are being fully utilized, while avoiding both shortages and excesses.

***Migration strategy:***  
The migration strategy involves implementing Azure Automation, Azure Log Analytics, and Azure Resource Graph to create a dynamic and integrated asset and software inventory system. Azure Automation is used to automate the discovery and lifecycle tracking of assets, while Log Analytics collects and aggregates data from various sources within AGW’s IT infrastructure. Azure Resource Graph allows AGW to query and visualize data about its resources in real time. By integrating this system with role-based access control (RBAC), AGW ensures that only authorized personnel have access to critical asset data, further enhancing security and compliance.

***Azure and other technologies used:***  
The key Azure technologies utilized for this transformation are Azure Automation, Azure Log Analytics, and Azure Resource Graph. These services work together to track asset lifecycle data, monitor software usage, and provide real-time visibility into the IT infrastructure. By automating the discovery and management of IT assets, AGW can also avoid the manual effort previously required for asset audits. Azure Policy and Azure Active Directory (AD) are also leveraged for enforcing compliance rules and managing access to asset and software information.

***Estimated time:***  
The transformation of AGW’s software and asset inventory management system is expected to take approximately 4 weeks. This timeframe accounts for the setup and configuration of the various Azure services, integration with AGW's existing IT systems, and the migration of asset and software data into the new system.

***Cost and savings:***  
By implementing this new inventory management system, AGW is projected to achieve savings of up to 25%. These savings stem from a reduction in redundant purchases, optimized software licensing, and more accurate tracking of asset usage. Additionally, the system provides a clear overview of assets throughout their lifecycle, helping AGW avoid purchasing unnecessary hardware and software and ensuring that software licenses are renewed only when necessary. The improvements in asset tracking and lifecycle management also reduce administrative overhead and the associated costs of manual audits.

***Benefits and carbon footprint improvement:***  
A smarter approach to asset lifecycle tracking and software inventory management not only leads to financial savings but also has a positive impact on sustainability. The reduction in redundant purchases and more efficient asset management minimizes e-waste, contributing to a 20% improvement in sustainability within AGW’s IT operations. By extending the useful life of hardware and minimizing excess purchases, AGW reduces its environmental impact, supporting its broader sustainability initiatives. Moreover, the efficient use of software licenses ensures that AGW is not over-purchasing, which reduces unnecessary consumption of digital resources and further contributes to its carbon footprint reduction goals.

**6. Storage and Backup Systems**

AGW’s IT infrastructure previously relied on isolated on-premises Storage Area Network (SAN) and Network-Attached Storage (NAS) systems for data storage and backup. These systems were limited in their disaster recovery capabilities and suffered from slow, manual backup processes. Data was stored in silos, leading to inefficiencies in data management, accessibility, and backup integrity. Furthermore, the on-prem systems were prone to single points of failure, and the manual processes increased the risk of data loss during critical recovery scenarios. These legacy storage solutions were expensive to maintain and operated with inefficient energy usage, contributing to AGW’s high operational costs.

***Its significance:***  
Storage and backup systems are essential for ensuring data availability, disaster recovery, and operational continuity. For AGW, these systems were vital for storing mission-critical data related to water distribution, quality monitoring, and operational logs. However, the on-prem SAN and NAS infrastructure was insufficient for meeting the company’s scalability and disaster recovery requirements. AGW’s reliance on manual backup routines also resulted in delays in restoring data, impacting business continuity and leading to longer downtimes in case of system failures. The significance of migrating to a more modern and efficient solution like Azure Blob Storage lies in its ability to provide faster backups, more reliable disaster recovery, and the potential for cost savings and energy efficiency.

***Migration strategy:***  
The migration strategy involved replacing AGW’s existing on-prem SAN and NAS systems with Azure Blob Storage, utilizing the Cool and Archive tiers for storing infrequently accessed and archival data. This transition is part of a broader cloud-first strategy to modernize the data storage and backup infrastructure. Azure Backup Vault was implemented to automate the backup process, enabling geo-redundant storage and versioning of production data. Legacy archival data was transferred using Azure Data Box in a big-bang approach, which facilitated the bulk transfer of large datasets to Azure without impacting operational systems. The migration involved careful planning to ensure minimal disruption to ongoing operations during the transition.

***Azure and other technologies used:***  
The migration leveraged Azure Blob Storage for scalable, cost-effective storage, with the use of Cool and Archive tiers to optimize costs based on the frequency of data access. Azure Backup Vault was used for automating the backup and restore process, offering reliable disaster recovery capabilities. The Azure Data Box was critical for transferring large amounts of archival data quickly and securely to Azure. These technologies ensured that AGW’s data was not only stored more efficiently but also backed up with automated policies to reduce human error and improve recovery time objectives (RTOs).

***Estimated time:***  
The estimated migration time varies depending on the type of data being transferred. For archival data, the migration using Azure Data Box is expected to take approximately 3 weeks. For live production systems, the migration is projected to take 6 to 8 weeks, which allows time for the setup of automated backup systems and migration of critical live data with minimal downtime.

***Cost and savings:***  
By migrating to Azure Blob Storage and using tiered storage options like Cool and Archive, AGW is expected to save 35-45% in storage costs compared to its previous on-premises SAN and NAS solutions. These savings are largely due to the pay-as-you-go pricing model of Azure Blob Storage, which eliminates the need for upfront capital investment in hardware. Furthermore, de-duplication and data compression techniques available in Azure help reduce storage costs further by eliminating redundant data. Additionally, the shift to automated backups reduces manual intervention and associated labor costs, improving overall operational efficiency.

***Benefits and carbon footprint improvement:***  
One of the key benefits of migrating to Azure Blob Storage is the significant reduction in energy consumption, with an estimated savings of up to 50%. This reduction is primarily due to the consolidation of storage resources into Azure’s green data centers, which are powered by renewable energy. The move to cloud storage eliminates the need for AGW to maintain power-hungry on-prem hardware and reduces the company’s overall energy usage, aligning with its sustainability goals. Furthermore, the automated backup process ensures that critical data is always available and recoverable, which enhances AGW’s disaster recovery capabilities and reduces the risk of data loss or downtime.

**7. Disaster Recovery and Regulatory Compliance**  
Previously, disaster recovery (DR) at AGW was a manual and inconsistent process across different departments. This lack of a centralized and automated strategy meant that critical business functions such as water distribution systems and sensor monitoring could be significantly impacted during system outages. Additionally, regulatory audit trails for data, such as compliance information for water quality, were stored in isolated formats across various departments, creating inefficiencies in tracking and auditing. Without a cohesive DR strategy or proper data governance, AGW faced challenges in meeting compliance requirements and ensuring business continuity during disruptions.

***Its significance:***  
Disaster recovery is crucial for AGW’s ability to maintain uninterrupted services, especially in scenarios like natural disasters, power outages, or data breaches. Given AGW’s critical role in water management, any extended downtime could have serious implications for public health and safety. Additionally, regulatory compliance is a key requirement for AGW, as the company must adhere to strict standards related to water safety, data retention, and auditability. Ensuring that disaster recovery and compliance measures are integrated into a cohesive system is critical for operational resilience and avoiding non-compliance penalties.

***Migration strategy:***  
To address these challenges, AGW leveraged Azure Site Recovery (ASR) for creating a comprehensive disaster recovery strategy. This involved failover to the cloud, where critical systems and data are replicated and backed up to Azure’s secure cloud environment. Additionally, automated recovery testing was implemented to ensure that recovery procedures could be executed quickly and effectively during an actual disaster scenario. For regulatory compliance, AGW adopted Microsoft Purview to manage and enforce data compliance, retention, and auditing policies across workloads. Azure Policy was also implemented to standardize compliance controls and data retention rules across all resources and services. The implementation of these tools enables a more streamlined and automated approach to disaster recovery and regulatory compliance, ensuring that AGW meets both operational and legal requirements.

***Azure and other technologies used:***  
The Azure Site Recovery (ASR) tool was the cornerstone of AGW's new disaster recovery strategy, ensuring replicated backups and failover capabilities. The system enables cloud-based failover, ensuring that if AGW’s on-prem systems fail, workloads can quickly shift to Azure. Microsoft Purview is used for data governance, including the enforcement of compliance, data retention, and auditing policies. Azure Policy allows AGW to enforce consistent policies across all workloads to ensure regulatory standards are met. These tools work together to provide automated, reliable disaster recovery and compliance enforcement, replacing manual, inconsistent processes.

***Estimated time:***  
The migration and implementation timeline for disaster recovery using Azure Site Recovery is estimated to take 4 to 5 weeks, depending on the complexity of the systems being replicated. For Microsoft Purview, the implementation is expected to take 3 weeks to integrate it into the existing IT environment, configure data governance policies, and automate compliance reporting.

***Cost and savings:***  
By adopting a cloud-based disaster recovery model using Azure, AGW will experience significant cost savings. The elimination of energy-intensive on-premises backup systems leads to lower operational expenses (OPEX), as AGW no longer needs to maintain costly physical infrastructure. Additionally, the automation of recovery testing and compliance monitoring significantly reduces manual effort and the need for dedicated compliance teams. This, in turn, leads to a more efficient use of resources, both in terms of personnel and hardware.

***Benefits and carbon footprint improvement:***  
The adoption of Azure Site Recovery and Microsoft Purview not only improves disaster recovery readiness and regulatory compliance but also has a positive impact on the company’s carbon footprint. With manual backup systems decommissioned and replaced by more energy-efficient cloud-based solutions, AGW can expect a significant reduction in energy consumption, leading to a lower carbon footprint. By utilizing Microsoft’s renewable energy-powered data centers, AGW is contributing to sustainability efforts while ensuring disaster recovery readiness and regulatory compliance. These changes collectively improve business continuity, reduce downtime, and enhance AGW’s ability to respond to emergencies with minimal impact.

**8. IT Security and Threat Management**  
AGW’s security framework was previously fragmented, relying on legacy antivirus software, manual patching processes, and disconnected threat intelligence. This lack of integration between different security tools meant that vulnerabilities were often missed or took longer to detect, leaving AGW exposed to potential security risks. Critical systems related to water quality management, sensor data, and billing systems were particularly vulnerable due to this lack of a unified security approach. Additionally, the absence of centralized logging and analysis hampered the effectiveness of security monitoring and response.

***Its significance:***  
Given AGW’s role in managing public water resources, maintaining robust cybersecurity is essential to ensure the integrity of systems and protect sensitive data from cyber threats. Security incidents could lead to severe disruptions in services, financial losses, and damage to AGW’s reputation. Moreover, protecting sensitive customer and operational data is not only a regulatory requirement but also crucial for maintaining public trust. Efficient threat detection and response are vital for securing the organization’s infrastructure and ensuring smooth and uninterrupted service.

***Migration strategy:***  
To address AGW’s fragmented security systems, the company transitioned to a unified and automated security solution by implementing Microsoft Defender for Cloud, Azure Sentinel (SIEM), and Microsoft Intune for endpoint detection and response (EDR) and vulnerability management. This migration centralizes threat intelligence, enabling real-time monitoring, detection, and automated response to security incidents. Microsoft Defender for Cloud provides continuous security assessments and threat protection across AGW’s cloud resources, while Azure Sentinel serves as a Security Information and Event Management (SIEM) system, consolidating logs and security alerts across systems for advanced analysis. Microsoft Intune enhances endpoint management, ensuring that all devices used within AGW’s infrastructure are compliant with security standards. Machine learning models built into these platforms help to identify potential threats and security breaches more quickly and accurately.

***Azure and other technologies used:***  
AGW adopted Microsoft Defender for Cloud for cloud security management, offering real-time threat detection and protection for workloads deployed across Azure. Azure Sentinel, a cloud-native SIEM tool, aggregates data from all security sources, enabling centralized log analysis and actionable insights. Microsoft Intune is utilized for managing and securing endpoints, ensuring that all devices accessing AGW’s systems adhere to security protocols. These tools are all integrated within Azure’s ecosystem, providing a seamless, unified approach to security. Additionally, machine learning models are employed to automate threat detection, helping to reduce manual intervention and enhance response times.

***Estimated time:***  
The migration to these security solutions is estimated to take 5 to 6 weeks. During this period, AGW will implement the tools, integrate them with existing systems, and optimize the configuration to ensure that security monitoring is both effective and scalable. The timeline includes the necessary steps for training, system integration, and validation of automated security processes.

***Cost and savings:***  
By transitioning to cloud-native security solutions, AGW reduces its reliance on physical security appliances, such as on-premises firewalls, intrusion detection systems, and antivirus servers, leading to substantial cost savings. The shift to Microsoft Defender for Cloud and Azure Sentinel eliminates the need for managing and maintaining separate legacy systems, which would otherwise require regular updates, licenses, and infrastructure support. The move to a centralized, automated security framework also decreases operational costs related to manual monitoring and patching efforts. The projected savings are further enhanced by the reduction in security incident response times, reducing the costs associated with breach containment and recovery.

***Benefits and carbon footprint improvement:***  
The adoption of cloud-native security solutions significantly reduces AGW’s physical hardware footprint by replacing on-premises security appliances with efficient, cloud-based systems. This consolidation not only lowers infrastructure costs but also reduces energy consumption. By using Microsoft’s renewable energy-powered data centers, AGW further reduces its carbon footprint associated with security operations. The centralized system improves threat detection and incident response times, providing AGW with the ability to proactively respond to cyber threats. The automated security processes also enhance operational efficiency and minimize manual intervention, improving overall security posture while making AGW’s infrastructure more sustainable and resilient.

**Summary Table of IT Infrastructure Modernization at AGW**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Resource/System** | **Significance** | **Azure Tech Used** | **Migration Strategy** | **Estimated Time** | **Cost Savings** | **Carbon Reduction** |
| Shared Oracle DBs | Core data handling (Billing, Sensor, Payroll) | Azure SQL MI, Data Migration Assistant | Lift & Shift + Load Balancer | 4–6 weeks | ~40% | High |
| Middleware (Tomcat, MQ, Tibco) | Application runtimes & messaging | AKS, Azure Service Bus, Event Grid | Containerize + Replatform | 6–8 weeks | ~50% | High |
| IAM and Networking | Access control & connectivity | Entra ID, Azure VNet, Azure Firewall | Sync + Policy Routing | 4 weeks | ~60% effort | Moderate |
| IoT/Sensor Systems | Real-time water operations data | Azure IoT Hub, Data Lake, Stream Analytics | Stream + Archive | 6–10 weeks | ~30% | High |
| Asset & Software Inventory | Track lifecycle and compliance | Azure Automation, Resource Graph | Discover + Integrate | 4 weeks | ~25% | Moderate |
| Storage & Backup | All data storage and archiving | Azure Blob, Backup Vault, Data Box | Tiered + Big Bang | 3–8 weeks | 35–45% | Very High |
| DR & Compliance | Operational resilience & audit | Site Recovery, Microsoft Purview | Replication + Automation | 4–5 weeks | Moderate | High |
| IT Security & Threat Intel | Breach detection and patching | Defender for Cloud, Azure Sentinel, Intune | Centralize + Automate | 5–6 weeks | Moderate | High |