# **Offargu Migration to the Cloud Project**

MARCEL NJIGHE-TEZEH

CYBERSECURITY, WILMINGTON UNIVERSITY

## [SEC6040](https://wilmu.instructure.com/courses/43945): WEB AND DATA SECURITY

PROFESSOR [Michael](https://wilmu.instructure.com/courses/43945/users/14551) DaCrossa

JULY 08, 2022

**Organization Overview**

The organization I am using as the basis for this project is Offargu.com. Offargu.com is a marketplace company that offers its customers the ability to buy, sell, and get free classified products both online and locally through its iOS, Android, and web applications. OffargU is one of the startups in a very competitive digital e-commerce industry that provides consumer-to-consumer (C2C) and consumer-to-business (C2B) services.

**Introduction**

According to ahasayen.com, "cloud reference architecture serves as a collection of design guidance and design patterns to support a structured approach to deploying services and applications in the cloud." (Hasayen, 2021). Every data center migration has its justifications, such as the desire to become more cloud-native or to save money. What matters most is using an appropriate reference architecture to achieve an efficient data center migration to the cloud while successfully managing risk, maximizing the benefits, and creating a novel new design for internal users regardless of the organization's objectives.

**Business drivers**

The IT leadership team works closely with business partners to understand what they want to achieve with this migration. They want to:

* **address business growth.** Offargu is growing, so there's pressure on the company's on-premises systems and infrastructure.
* **limit risk.** The e-commerce application is critical for the Offargu business. The company wants to move the application to Azure with zero risk.
* **Extend.** Offargu doesn't want to modify the application, but it does want to ensure that the application is stable.

**Migration goals**

The Offargu cloud team has pinned down goals for this migration. It used these goals to determine the best migration method:

* They seek to reduce the cost of operations in the long run, increase efficiency and scalability, maximize their growth potential, and cut down on the number of staffers.
* Following the migration, the application should have the same performance capabilities in Azure as it does today in on-premise. The application will remain as critical in the cloud as it's been on-premises.
* Offargu doesn't want to change any application functionality. Only the application location will change.

**Current application**

* The application is tiered across two VMs (WEBVM and SQLVM).
* The VMs are located on the VMware ESXi host offargu1.0.offargu.com (version 6.5).
* The VMware environment is managed by vCenter Server 6.5 (vcenter.offargu.com.com) running on a VM.
* Offargu has an on-premises datacenter (offargu-datacenter) with an on-premises domain controller (offargu1).

**Architecture**

* Because the application is a production workload, the application VMs in Azure will reside in the production resource group OffarguRG.
* The application VMs will be migrated to the primary Azure region (East US 2) and placed in the production network (VNET-PROD-EUS2).
* The web front-end VM should reside in the front-end subnet (PROD-FE-EUS2) in the production network.
* The database VM should reside in the database subnet (PROD-DB-EUS2) of the production network.
* The on-premises VMs in the Offargu datacenter will be decommissioned after the migration is done.

Offargu will use SQL Server running on an Azure IaaS VM as it offers an optimal solution if Offargu needs to customize the operating system and the database or wants to use the SQL Server Azure Hybrid Benefits.

* **Zone-redundant:** A zone-redundant Application Gateway should route traffic to their VMs within the web tier.
* **Load balancer:** A zone-redundant load balancer should route traffic from the VMs in the web tier to the active SQL Server. In the event of a zone failure, the Application Gateway will route to VMs in other availability zones.

If the active SQL Server becomes unavailable, either due to a zone failure or local failure, a passive SQL Server becomes the active SQL Server. The zone-redundant load balancer detects the failover to the newly active SQL Server and routes traffic to it.

**Migration process**

Offargu will migrate the application front-end and database VMs to Azure VMs by using the agentless method in the Azure Migrate: Server Migration tool. Offargu should prepare and set up Azure components for Azure Migrate: Server Migration and prepare the on-premises VMware infrastructure.

**Azure infrastructure**

Offargu will sign a Microsoft Enterprise Agreement (EA) that details the pricing and entails an upfront monetary commitment to Azure. They will estimate what its yearly Azure spend will pay for the first year in full. After buying the subscription, Offargu will assign an IT system admin that will manage subscriptions, examine licensing, and explore Azure Hybrid benefits.

Offargu will extend its on-premises Active Directory into the cloud, rather than building a new separate system in Azure. Because Offargu isn't using Microsoft 365 yet, it will provision an Azure AD instance.

They will create an Azure AD directory, add a domain, set up on-premises and Azure groups and users, create resource groups, create matching security groups on-premises, and synchronize the two active directories (on-prem and cloud).

Offargu will design a network that allows traffic from the internet and from the corporate network by using a VPN to Azure.

The network architecture will have two boundaries: an untrusted front-end perimeter zone and a back-end trusted zone. And a firewall will have a network adapter in each zone, controlling access to trusted zones. Offargu will implement a class-A private network in Azure, and this will work because on-premises currently has a class-B private address.

**Considerations**

**Security: Offargu**has determined that specific VMs require encryption. Offargu will apply encryption to VMs with customer, confidential, or personal data using Microsoft Defender for Cloud, network security group (NSG), and Azure disk encryption.

**Availability:**Offargu's architecture will use resources spread across multiple zones to provide high availability for its e-commerce applications.

**Resiliency: Offargu will** use East US 2 (located in Virginia) as the primary region and the Central US (located in Iowa) as the secondary region.

Privacy: All Offargu enterprise data is not created equally, and these distinctions are important in a cloud environment. Offargu will classify data into SP levels and store them in different cloud databases.

**Legal and Regulatory Issues**

Given the idea of the cloud, there's always uncertainty over who is in control of the data stored in the cloud-by consumers. Cloud service providers like Microsoft Azure, AWS, IBM, Google, etc., are typically seen as the legal custodians or proprietors of the data, which makes it clear that the complexity brings several legal and regulatory issues in cloud computing.

**Privacy and security:** The Federal Trade Commission (FTC) mandates the adoption of comprehensive privacy and security policies that employ several techniques to safeguard customers' security and confidentiality. The FTC's primary tactic is to conduct enforcement actions to end law infringement and require businesses to make concrete efforts to correct illegal activity.

Based on Offargu's sensitivity and retention principles, Offargu will design a data management plan that tackles data sensitivity, data ownership, access control, data retention, and disposal requirements. Offargu will configure data access control lists based on the need to know of the user.

**Third-Party Access Issues**: Offargu will execute a business associate agreement (BAA) with its third-party supplier to ensure that its privacy and security policies are in compliance with US PII and HIPAA requirements. The twelve PCI-DSS data privacy and security requirements, such as encrypting cardholder data transmission, tracking and monitoring all networks, regularly testing systems and processes, etc., will be implemented and enforced. Because all third parties that use a public cloud use the same administrative interface, Offargu will implement multi-factor authentication for better security.

**How would you create and update a risk management program?**

The cloud governance team at Offargu would plan for the worst-case scenario and map every potential policy to the cloud. The MVP technique will be used by the team, who will utilize a risk register to document an initial starting point and set of assumptions. Every risk assumption will be assigned a risk ID, description, impact on migration efforts, identified by probability, impact, risk score, response type and strategy, and owner. The risk MVP will be used to support initial small-scale or test cloud deployments, then as a foundation for gradually detecting, updating, and remediating new risks when migration needs occur, or additional workloads are brought to the cloud environment. Offarrgu will use this technique to apply governance throughout the cloud migration process. Offargu will include the following as part of the initial risk assumptions:

* All assets are at risk of being deleted (through error, mistake, or maintenance).
* All assets are at risk of generating too much spending.
* All assets could be compromised by weak passwords or insecure settings.
* Any asset with open ports exposed to the internet is at risk of compromise.

**What policies or procedures are most likely needed?**

Availability of data is part of the triad of cybersecurity—Confidentiality, Integrity, and Availability. Offargu should be able to recover data in an event of data loss but should also be able to recover if they have lost data integrity, which may be the case after a security breach with unknown impacts on the system.

Offargu will establish and maintain a data recovery policy. This policy will address the scope of data recovery activities, recovery prioritization, and the security of backup data in this policy. They will review and update documentation annually or when significant enterprise changes occur that could impact this safeguard.

They will develop an access management policy. They will establish and follow a process, preferably automated, for granting access to enterprise assets upon the new hire, rights grant, or role change of a user and also maintain an inventory of the enterprise’s authentication and authorization systems, including those hosted on-site or in the cloud.

What are a couple of ways that risk could be minimized?

Users who do not have the appropriate security awareness training are considered a weak link in the security of an enterprise. These untrained users are easier to exploit than finding a flaw or vulnerability in the equipment that an enterprise uses to secure its network.

Offargu will establish and maintain a security awareness program. The purpose of this security awareness program will be to educate the workforce on how to interact with enterprise assets and data in a secure manner. Conduct training upon hire and, at a minimum, annually.

To further minimize risk, they will deploy centralized security event alerting across their assets for log correlation and analysis.

**CSA (Cloud Security Alliance) Cloud Data**

Offargu shall implement incident response best practices for providing security assurance within its cloud computing domain, as defined by CSA as "a practical and actionable roadmap for organizations seeking to adopt the cloud paradigm." (Security Guidance for Critical Areas, 2017).

**Incident Response (IR):** Offargu shall designate one key person, and at least one backup, who shall manage the enterprise's incident handling process. Establish contact information for parties that need to be informed of security incidents and review it annually or when significant enterprise changes occur that could impact this safeguard. Its key roles and responsibilities for incident response include staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Primary and secondary communication can include phone calls, emails, or letters.

**Cloud Data Storage Architectures**

According to Snowflake, "cloud data architectures contain the rules, models, and policies that define how data is collected, stored, used, and managed in the cloud within a business or an organization." (Cloud Data Architectures, n.d.) Offargu's data architectures manage the flow of data and how that data is processed and distributed across stakeholders and other applications for reporting, analytics, and other uses. Offargu's shall use relational databases for its diverse data types, from structured data (tables, CSV files) to semi-structured data (JSON, Avro, Parquet, etc.), all within a single, logically integrated solution. This architecture shall be implemented as follows:

* **Access method:** Offargu shall implement multiple Web service API methods because REST APIs are stateless, simple, and efficient to provide. It will implement APIs based on REST principles, which imply an object-based scheme developed on top of HTTP (using HTTP as a transport).
* **Performance:** Offargu shall use TCP network services for data movement through the global Internet.
* **Scalability:** The ability to scale storage needs (up and down) means improved costs for Offargu and increased complexity for the cloud storage provider. Its servers and storage shall be capable of resizing without impact to users, and scalability shall be provided not only for the storage itself (functionality scaling) but also the bandwidth to the storage (load scaling).
* **Availability:** To ensure that data is available when needed, Offargu will design and implement a business continuity or disaster recovery plan, a data backup policy, avoid single points of failure and develop redundancies.

**Data Security Strategies**

Offargu's digital assets include databases, files, accounts, etc., that are sensitive or critical to its operations. To determine the type of security required to protect its assets, Offargu will conduct an inventory assessment to discover any gaps and design security around the below strategies to close the gaps.

* **Security Awareness:** Offargu will provide users with frequent security awareness training to increase its overall security posture. The information provided by the security awareness training shall be relevant and provide insights into recent security incidents. Training shall also reiterate the necessity of using strong passwords, authentication best practices, spotting, and reporting phishing attacks, and how to identify, store, transfer, archive, and destroy sensitive data.
* **Data Encryption:** Offargu shall encrypt data on end-user devices containing sensitive data. Examples of implementations include Windows BitLocker, Apple FileVault, and Linux dm-crypt.
* Data Segmentation: Offargu shall segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.
* **Vulnerability Management:** Offargu will establish and maintain a documented vulnerability management process for enterprise assets. Its process will maintain a risk-based remediation strategy, automate patch management on a monthly basis, and vulnerability scans of internal enterprise assets.

**Data Discovery and classification controls**

Data discovery and classification adds capabilities for discovering, classifying, labeling, and reporting the sensitive data in Offargu's databases.

Offargu's data discovery and classification control shall be designed and implemented based on the following questions:

* What data does the enterprise store or handle?
* Who should have access to it?
* Where is it stored or accessed?
* When should it be deleted?
* Why does it need protection?

The goal of its data inventory and classification shall be to segment systems based on the types of data they handle and develop fine-grained user permissions to limit data exposure. This control shall address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements based on its sensitivity and retention standards.

Offargu shall use third-party tools to investigate, apply advanced analytics to data to detect informative patterns, identify needs, combine data from relevant sources, analyze the data, and share it with Offargu security for data classification and business operations.

**Protecting Privacy and PII (Personally Identifiable Information)**

Offargu shall at all times adhere to the Federal Trade Commission (FTC) requirements. These requirements mandate the adoption of comprehensive privacy and security policies that employ several techniques to safeguard customers' security and confidentiality. The FTC's primary tactic is to conduct enforcement actions to end law infringement and require businesses to make concrete efforts to correct illegal activity. As per Offargu's data discovery and classification controls, it shall configure data access control lists based on a user’s need to know. Apply data access control lists to local and remote file systems, databases, and applications to protect the below PII.

* Name, such as full name, maiden name, mother’s maiden name, or alias
* Personal identification number, such as social security number (SSN), passport number, driver‘s license number, taxpayer identification number, or financial account or credit card number
* Address information, such as street address or email address,
* Personal characteristics, including photographic images (especially of faces or other identifying characteristics), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry),

**Data Rights**

Offargu shall fully follow and implement the Federal Acquisition Regulations (FAR) prescribed policies, procedures, and clauses pertaining to data rights for civilian agencies and the Defense Federal Acquisition Regulations (DFARS) for DoD.

Offargu's technical data shall include any recorded information of a scientific or technical nature (e.g., product design or maintenance data, computer databases, and computer software documentation). “Computer software” includes executable code, source code, code listings, design details, processes, flow charts, and related material that would enable the software to be reproduced, recreated, or recompiled.

**Data Retention, Deletion, and Archiving Policies**

Offargu shall retain data according to the enterprise’s data management process. Data retention shall include both minimum and maximum timelines. The need to retain data for insight shall need to be counter-balanced by the desire to avoid a headline-grabbing data breach.

They shall ensure the disposal process and method are commensurate with the data sensitivity.

Offargu shall archive its data based on the overall data classification scheme for the enterprise. Enterprises may use labels such as “sensitive,” “confidential,” and “public” and then classify their data according to those labels. Review and update the classification scheme annually or when significant enterprise changes occur that could impact this safeguard.

**Auditability, Traceability, and Accountability of Data Events**

Offargu shall use audit logs to provide a rich source of data critical to preventing, detecting, understanding, and minimizing the impact of network or data compromise in a timely manner.

Offargu shall establish and maintain an audit log management process that defines the enterprise’s logging requirements. At a minimum:

1. Ensure that detailed, time-synchronized audit logs are collected across enterprise assets.
2. Ensure that logs are stored in a centralized location and retained for a minimum of 90 days.
3. Ensure audit log reviews are conducted on a weekly basis or more often to establish baselines and detect potential threats.
4. Ensure that logging destinations maintain adequate storage to comply with Offargu’s audit log management process.
5. Configure detailed audit logging for Offargu assets containing sensitive data. Include even source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.
6. Collect DNS query, URL request, command-line, and service provider audit logs on Offargu assets where appropriate and supported.

**Business Continuity and Cloud Disaster Recovery (BCDR) Strategy and Risk Analysis**

The Offargu BCDR aims to outline the strategy and needed actions for the cloud governance team to meet requirements for application and data resiliency, reliability, availability, and scalability. Through business function impact and risk analysis, Offargu will identify, define, and work with its cloud providers to implement controls in place to ensure key resources are available in case of disasters.

**Risk Analysis**

This analysis aims to identify assets within Offargu's cloud and predict the likelihood and consequences of disruption of business functions. The result is an understanding of the relevant assets, their associated business functions, and their importance to business continuity and disaster recovery design and development strategy. Offargu assets in the cloud at all times are exposed to risk in the following cloud areas:

|  |  |  |  |
| --- | --- | --- | --- |
| Risk dimension | Private internal | Private external | Public |
| Data security and regulatory | – Similar to traditional computing | Data leakage from a malicious insider  – Unauthorized data access by the service provider  – Lack of visibility into cloud operations and ability to monitor for compliance  – Dependence on a service provider to ensure adequate internal controls | Data leakage from a malicious insider  – Unauthorized data access by the service provider  – Data leakage across shared infrastructure  – Lack of flexibility for encryption, data control  – Lack of visibility into cloud operations and ability to monitor for compliance  – Dependence on a service provider to ensure adequate internal controls |
| Technology/Natural disaster | – Evolving technologies or flooded datacenter could require rearchitecture and/or retraining | – Evolving technologies could require rearchitected and/or retraining | – Limitations on customization of service offerings  – Compatibility with other cloud providers  – Limited choice or technology and related tools |
| Operational | – Service reliability and uptime | – Service reliability and uptime | – Lack of service-level customization – Control over quality – Control over application availability and disaster recovery |
| Vendor | – Similar to traditional computing | – Association and reliance on a service provider | – Association and reliance on a service provider |
| Financial | – Underestimating initial costs  – Continuing to carry capital expenditures of hardware and software | – Underestimating initial costs  – In some cases, continuing to carry capital expenditures of hardware and software  – Contract modification or cancellation fees  – Additional overhead of managing service provider(s) | – Contract modification or cancellation fees  – Runaway costs from poor planning and periodic monitoring  – Additional overhead of managing service provider(s) |

1. **Risk assumptions**

* Due to insecure APIs, failed encryption, accidental errors, and malware, there is an external attack.
* All assets are at risk of being deleted (through error, mistake, or maintenance) due to evolving technologies or natural disasters.
* All assets are at risk of generating too much spending.
* There exist compliance violations and contractual breaches that may lead to regulatory penalties.
* Assets could be compromised by weak passwords or insecure settings due to system misconfiguration.
* Any asset with open ports exposed to the internet is at risk of compromise.

**Business Impact Analysis**

Upon the above risk analysis, any event of the above nature, including CSP downtime, will negatively affect Offargu and its customers. Offargu's BCDR strategy focuses on its cloud resiliency, redundancy, and backup and restore to ensure its business-critical functions are recovered within established timelines. Key requirements to be included in this cloud BCDR strategy:

* Establishing RTOs and RPOs and ensuring resiliency through strategy, budgeting, planning, and vendor dependencies to support the RTOs and RPOs.
* Ensuring BC/DR considerations are part of the lifecycle process for the applications

**The Design of Offargu BCDR Strategy**

Offargu cloud resources are critical and significant as they provide IT resources to keep the e-commerce applications operational and functioning. This BCDR, supported by its IR security measures, will ensure availability and redundant systems to maintain little or no down time in the event of an incident. This strategy will adopt and implement multi-cloud deployment, backup and restore, cloud resiliency, incident response, and multiple cloud regions.

**Development**

1. **Multi-cloud adoption**: Offargu will run its major business functions in multi-clouds as a strategic means to have its static and ecommerce app content hosted in the second cloud. This will help during an outage by ensuring that the functioning traffic is re-directed to other static resources. Having more than one cloud vendor will ensure that its customers are less impacted in the event of a disaster. Offargu's second cloud service provider will serve as a disaster recovery site in case of outages.
2. **Backup: Offargu**backup and restore measures should aid in the prevention of data loss or corruption. Its backup and restore technique should necessitate the maintenance of a completely mirrored replica site, allowing for rapid switching between the live and backup sites. This measure will be used to alleviate the effects of a regional disaster by replicating data to other regions and will address a lack of redundancy for workloads deployed to a single availability zone.  These efforts will help resume Offargu's critical business functions after a cloud outage. Backup of data, applications, and other critical resources provides the basis for fast and adaptive disaster recovery.
3. **Using multiple cloud regions:**Offargu will use multiple cloud regions as chances are that an outage at the CSP will be limited to a single region. As such, Offargu will use the alternate region to reduce the impact of an outage.
4. **Cloud Resiliency:** Offargu will use the flexibility of cloud-based IT services to improve the efficiency and availability of its applications.

* **Testing and Monitoring**: It shall use an independent method to ensure that its equipment meets minimum behavioral requirements.
* **Replication**: The essential components of its cloud resources shall be replicated, using additional resources (hardware and software), ensuring that they are usable at any given time.

# **Incident Response:** Offargu must respond promptly, confidently, and accurately during a disaster. During a disaster, Offargu shall first solve the problem and then send out information to all individuals affected and what actions they can take to avoid further damage.

## ****Disaster Detection****

1. Offargu shall implement centralized security with vendor-defined event correlation alerts across its cloud assets for log correlation and analysis.
2. It shall deploy a host-based and network intrusion detection solution on its assets where appropriate and/or supported.
3. It shall perform traffic filtering between network segments where appropriate.
4. Offargu shall establish and maintain an Audit Log Management Process.
5. **Disaster Notification**

In the event of a disaster, employees, local and state officials, and third-party vendors shall receive an alert via email or text message letting them know what occurred and how they might have been affected.

## ****Testing****

Testing scenarios shall represent actual cases to train employees and third parties on how to react to and deal with security incidents and their processes. The tabletop exercises provide a safe environment to focus and train everyone to respond to a specific cyber incident or natural disaster. There are two different types of tabletop exercises.

* Technical Tabletop Exercise is for Offargu and the third-party technical security team. The exercise outputs help the team understand how to respond and refine IRP to better respond to cloud disasters.
* Executive Tabletop Exercise is for Offargus' executive-level employees. This tabletop exercise will walk through the decisions to support the IRP for man-made and technological incidents. The executive employees shall understand the various roles, processes, and internal and external communication approaches during a cloud security incident.

Testing of the IRP will occur on an annual basis unless significant software or infrastructure changes occur.

## ****Maintenance****

Maintenance includes the ongoing updating and revising of this living document to reflect ongoing changes to software, infrastructure, new or removal of functionality, changes in cloud providers, or the addition of new forensic testing tools ("MIT Business Continuity Plan," 1995; Snedaker & Rima, 2014). All changes need to adhere to the following change management process:

* Changes require testing to ensure they operate correctly.
* Changes to critical business processes require a review and approval from the Offargu's cloud infrastructure manager or CISO.
* Update the revision number.
* Update training and testing materials.
* Communicate the changes and perform training as required.
* Distribute the plan to the appropriate teams.

**Cloud Application Security**

Building security into its cloud applications is imperative for keeping non-public customer data private and ensuring that its applications are fast and responsive. Offargu's cloud security architecture design is crafted to address:

* Multitenant application isolation (containerization and virtualization)
* Identity and access management for applications (SSO, SAML, XML, and Federation)
* Web application protection (WAF, API, and cryptography)

As define by snyk, “Cloud security is the techniques and tools used to secure cloud infrastructure, applications, and data.” (Cloud Security - Essential to Your Cybersecurity | Snyk, 2022).

**Multitenant application isolation**

**VMs and Containers**

Offargu's cloud is designed with multitenancy in mind, allowing a single instance of its e-commerce application to serve numerous customers.

**Cloud Foundry:** Offargu's Azure Cloud architectural design makes use of Cloud Foundry features for application isolation. When offargu develops and deploys an application to Cloud Foundry: The Azure Cloud environment selects a suitable virtual server to which the application and its associated artifacts are sent. An application manager on each virtual server interfaces with the rest of the Azure Cloud architecture and manages the apps deployed to the virtual server. Containers are used on each virtual server to segregate and protect programs. The Azure Cloud installs the required framework and runtime for each application in each container. When a request arrives, Azure Cloud analyzes it, decides which application it is intended for, and then chooses an instance of that application to receive it.

**Kubernetes Service:** Offargu will employ the Kubernetes-based Azure Cloud Kubernetes Service to deliver built-in functionality for application isolation, risk analysis, and security protection. As a result of these efforts, Offargu will be able to safeguard its cluster architecture and network connection, isolate its computing resources, and assure security compliance across its infrastructure components and container deployments.

Offargu's containers will be deployed on cluster-specific worker nodes that provide compute, network, and storage isolation for Offargu customers.

**Identity and access management for applications**

Offargu's application team will determine an application's access and identity management requirements. The online or mobile application's authentication strategy must integrate and leverage APIs, including Azure cloud services (SSO, SAML, XML, and Federation), to authenticate its existing customers, business partners or suppliers, new customers, and internal employees and users.

* It will create and manage a database of authentication and authorization systems.
* Where MFA is implemented, Offargu will require all externally exposed or third-party apps to enforce it.
* Define and manage role-based access control by defining and documenting the access privileges required for each position within the company to carry out its assigned tasks properly.
* Where supported, Offargu will enable centralized access control for all enterprise assets via a directory service or SSO provider.
* Create a procedure for revoking access.

XML metadata will be transmitted between Offargu and the identity provider in order for SAML to operate between Azure AD and Offargu systems. The information must be used by these two systems to provide a valid authentication transaction between the two parties. To kickstart the trust process, Offargu's cloud team will leverage the SAML 2.0 well-defined, interoperable metadata format to bootstrap the trust process.

**Web application protection**

Distributed Denial of Service (DDoS) attacks are a major, common, and easy-to-execute threat to web applications. The Offargu cloud platform has built-in protection from DDoS attacks.

**WAF:**  This will serve as an application gateway feature that provides centralized security for Offargu web apps against typical attacks and vulnerabilities. Offargu must build web application firewalls based on OWASP core rule sets 3.0 or 2.2.9 rules.

For its e-commerce apps, the Authentication and Authorization module will perform numerous tasks:

* Users are authenticated using the given provider.
* Tokens may be validated, stored, and refreshed.
* Controls the authenticated session.
* Injects personal data into request headers.
* Tracing and logging.

**Cryptography:**  Offargu will encrypt sensitive data while it is in transit. Transport Layer Security (TLS) and Open Secure Shell are two examples of implementations (OpenSSH). Offargu will ensure that the encryption is correctly verified in addition to just encrypting data in transit. Remote systems should have proper DNS IDs and certificates issued by a trustworthy certification authority when using TLS.

It will encrypt sensitive data on servers, apps, and databases at rest. Offargu's minimal data protection policy requires storage-layer encryption, often known as "server-side encryption."

Cryptographically random keys will be produced and stored in memory as byte arrays. If a password is used, it must be turned into a key using an acceptable password base key derivation procedure.

**Offargu’s Cloud Security Operation**

Offargu's need for legal and regulatory evidence drives its cloud security operations. Offargu's cloud security operations (SecOps) function's primary goal is to identify, respond to, and recover from active cyberattacks on its assets. As Offargu's SecOps evolves, its security operations will reactively respond to cyberattacks discovered by tools and proactively hunt for attempts that elude reactive detection.

Offargu will design, implement, operate, manage, and support a physical and logical infrastructure for its cloud environment as part of its cloud operations environment strategy.

**Build and implement a physical and logical infrastructure for its cloud environment.**

**Hardware-specific security configuration:** For all assets in its data center, including end-user devices, portable and mobile, non-computing and IoT devices, and servers, Offargu will create and maintain a secure hardware configuration, secure change authority, secure build, and safe intimal configuration process. It will evaluate and update these documents on an annual basis or if there are substantial enterprise changes that may affect the present configurations.

**Installation and configuration of virtualization management tools:** Offargu's virtualization management tools will administer, monitor, and maintain virtualized computer resources. Offargu will only deploy technologies with monitoring and troubleshooting capabilities that create notifications and give insights to aid in problem resolution. Offargu's cloud environment requires the installation and configuration of these technologies to support a wide range of virtualization solutions from manufacturers such as VMware, Microsoft, Citrix, and Oracle. Offargu's solutions will manage virtual environments in the cloud, on-premises, and hybrid deployments.

**Virtual Hardware specific security configuration requirements:** Offargu will build VMs that employ the SecureBoot functionality, which assures that its VMs run cryptographically signed operating systems. SecureBoot restricts Offargu's VMs from booting in order to prevent the virus from propagating to the host machine. Offargu will limit VM users' access to activities in its Linux VMs by setting the libvirt daemons to use the polkit policy tools on their host system. Offargu will install the most recent WHQL-certified VirtIO drivers for its Windows VMs, utilize only VM firmware that supports UEFI boot, and install the edk2-OVMF package on its host systems.

**Operation Physical and logical infrastructure or cloud environment**

**Configure access control for local and remote access:** Offargu will establish and follow a process, preferably automated, for granting access to enterprise assets upon the new hire, rights grant, or role change of a user from a centralized access control system. This will entail maintaining Role-Based Access Control, revoking access processes, and implementing an MFA for remote network access.

**Secure network configuration.** Offargu will maintain network infrastructure by running the most recent stable release of software and utilizing presently available network-as-a-service (NaaS) solutions. Offargu's network design will solve concerns like as segmentation, least privilege, and availability. A centralized network authentication, authorization, and auditing (AAA) system will be designed and implemented by Offargu.

**Manage Physical and Logical Infrastructure for cloud environment**

Offargu patch management policy shall have a documented plan that describes:

1. How security patching will be completed in a timely manner
2. How vulnerabilities will be managed when end of support/end of life occurs (e.g., upgrade to a supported service, buy extended support, etc.)
3. It will validate the efficacy of all security patches prior to deployment.
4. Will provide patching status to the vulnerability management team in a timely manner.
5. Offargu will ensure that critical security patches are completed within 30 days of patch availability.

**Manage Physical and Logical Infrastructure for cloud environment.**

**Configuration and host and guest operating systems:** Offargu will define requirements for security configuration management, including ensuring business justification for software and systems and the use of available baseline configurations. Approved security baseline configurations shall be documented and implemented for Offargu standard platforms, to include:

Linux servers, Windows servers, Network devices/architecture, Virtual machines, Databases, and Workstations

Offargu will adhere to the baseline approved Technical Security Hardening Standards for system configurations. It will build and manage a centralized monitoring system to detect compliance issues against established system baseline configurations and will lead the effort in developing and updating system configuration standards annually.

**Implement Operational Controls and Standards**

**Incident management:** Offargu will develop and retain contact information for parties who require security incident notification. Internal personnel, third-party suppliers, law enforcement, cyber insurance providers, appropriate government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders may be contacted.

* + Shall deploy and configure automated incident handling mechanisms on Offargu systems.
  + Shall ensure security tools are implemented to effectively support Offargu business functions.
  + Shall take the appropriate corrective actions in the event a security tool is not operating as intended.
  + Shall monitor, analyze, and respond to security alerts in accordance with procedures.
  + Shall report suspicious activity to leadership in accordance with the Incident Response Plan.

**Conclusion**

Any cloud project needs a solid architecture to guarantee that the created cloud solution meets the requirements. Regardless of whether the solution uses a private, public, or hybrid. Offargu's design is a seamless user flow with an intuitive design that has a logical progression and offers value to its users while also servicing its customers with the right content.  Cloud computing raises several legal and regulatory issues that will require every organization to establish and maintain creative policies to meet legal and regulatory requirements and implement advanced capabilities to secure their perimeters.

For Offargu's cloud migration success, it shall follow the above holistic approach designed based on the principles and accepted guidelines of the eight cloud security categories and more to accomplish it goal. Offargu must focus their attention on addressing immediate threats to people, property, and business (Kelly, 2020). Forming a team and focusing on the emergency right away should be the first step. A level of preparedness prepares the Offargu for these events.

From all indications, the cloud undoubtedly offers tangible security benefits in addition to operational advantages. However, risks remain, and as Offargu shifts control of its infrastructure and data to the cloud, it is critical that it rethinks its application and infrastructure security efforts. The above are the measures, procedures, and tools that Offargu will use to address its cloud security needs. Offargu’s Systems, platforms, and applications shall be configured to meet minimum standards to capture sufficient details to support threat detection and cyber investigations and enable Offargu build and implement a physical and logical infrastructure for its cloud environment

References

Considerations & Elements in Oracle Cloud Architecture Design. (2021, April 6). IT Convergence. https://www.itconvergence.com/blog/considerations-for-designing-an-oracle-cloud-architecture/

Hasayen, A. (2021, September 1). Cloud Reference Architecture CRA P1 - Foundation. Ammar Hasayen. https://blog.ahasayen.com/cloud-reference-architecture-cra1/

Paun, G. (2017, July 18). Council Post: Migrating To The Cloud: UX Design And Why It’s Essential To A Smooth Transition. Forbes. https://www.forbes.com/sites/forbesagencycouncil/2017/07/18/migrating-to-the-cloud-ux-design-and-why-its-essential-to-a-smooth-transition/

Considerations & Elements in Oracle Cloud Architecture Design. (2021, April 6). IT Convergence. https://www.itconvergence.com/blog/considerations-for-designing-an-oracle-cloud-architecture/

Hasayen, A. (2021, September 1). Cloud Reference Architecture CRA P1 - Foundation. Ammar Hasayen. https://blog.ahasayen.com/cloud-reference-architecture-cra1/

Paun, G. (2017, July 18). Council Post: Migrating To The Cloud: UX Design And Why It’s Essential To A Smooth Transition. Forbes. https://www.forbes.com/sites/forbesagencycouncil/2017/07/18/migrating-to-the-cloud-ux-design-and-why-its-essential-to-a-smooth-transition/

Cloud Data Architectures. (n.d.). Snowflake. Retrieved July 21, 2022, from https://www.snowflake.com/trending/cloud-data-architectures

Security Guidance for Critical Areas of. (2017, July 7). Cloud Security Alliance. https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Privacy & Data Security. (2018). https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf

YOUNG, C. (2021, September 9). CIS Control 03: Data Protection - Protect and Identify to safeguard data. The State of Security. https://www.tripwire.com/state-of-security/controls/cis-control-3/

CIS (Center for Internet Security). (2021, June 15). Election Security Spotlight-Website Defacements. CIS. https://www.cisecurity.org/spotlight/cybersecurity-spotlight-website-defacements

CISA. (2009, November 4). Understanding Denial-of-Service Attacks. Cybersecurity and Infrastructure Security Agency CISA. https://us-cert.cisa.gov/ncas/tips/ST04-015

Goodison, S., Davis, R., & Jackson, B. (2015). Digital Evidence and the U.S. Criminal Justice System Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf

Chen, J. (2019, June 6). Making Containers More Isolated: An Overview of Sandboxed Container Technologies. Unit42. https://unit42.paloaltonetworks.com/making-containers-more-isolated-an-overview-of-sandboxed-container-technologies/

Levy, I. (2016, April 29). Virtual containers are replacing sandboxing as a technology option. Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/security-take-its-head-out-of-the/

Velimirovic, A. (2021, March 17). DevOps and Virtualization: Effect of VMs on Development. PhoenixNAP Blog. https://phoenixnap.com/blog/devops-virtualization

Cloud Security - Essential to Your Cybersecurity | Snyk. (2022, May 19). Snyk.io. https://snyk.io/series/cloud-security/

Access Control Models – UHWO Cyber Security. (n.d.). Westoahu.hawaii.edu. https://westoahu.hawaii.edu/cyber/best-practices/best-practices-weekly-summaries/access-control/

CIS Control 17: Incident Response Management. (2022, April 27). The State of Security. https://www.tripwire.com/state-of-security/controls/cis-control-17/

Cobb, M. (2021, April). What is physical security? - Definition from WhatIs.com. SearchSecurity. https://searchsecurity.techtarget.com/definition/physical-security

Geier, J. (2015). Designing and deploying 802.11 wireless networks : a practical guide to implementing 802.11n and 802.11ac wireless networks for enterprise-based applications (2nd ed.). Cisco Press, , Cop.

Hoelscher, P. (2018, September 13). WPA2: What is the difference between AES and TKIP? Comparitech. https://www.comparitech.com/blog/information-security/wpa2-aes-tkip/