**3.1 Insert the network architecture**

**Azure VM Architectural Diagram:**

Diagram

Description automatically generated

The below components are Azure inbuilt with architecture which is used in architecture

**Azure NSG, VNET, Public IP, Network Interface, Routing, Point to Site VPN, and firewalls**

The interconnections with external networks are made by any of the following as per the requirements

Azure networking supports the following secure remote access scenarios:

* Connect individual workstations to a virtual network

The point-to-site VPN connection enables you to set up a private and secure connection between the user and the virtual network. When the VPN connection is established, the user can RDP or SSH over the VPN link into any virtual machine on the virtual network.

* Connect your on-premises network to a virtual network with a VPN

A site-to-site VPN connects an entire network (such as your on-premises network) to a virtual network. Site-to-site VPNs to a virtual network use the highly secure IPsec tunnel mode VPN protocol.

* Connect your on-premises network to a virtual network with a dedicated WAN link

Azure provides you the ability to use a dedicated WAN link that you can use to connect your on-premises network to a virtual network. Azure ExpressRoute, Express route direct, and Express route global reach enable this

**3.2 Indicate the hardware used,**

**3.3 Indicate the software used**

**Below tables specified the standard hardware and software used in our application-**

**Application Server:**

|  |  |
| --- | --- |
| **Component** | **Minimum** |
| Access | Remote desktop or Web-ex or TeamViewer Sessions details before the scheduled time. |
| Server | Window Server 2016 R2 Enterprise or Above |
| Processor | 3.7 gigahertz (GHz) |
| RAM | 56 Gigabyte (GB) |
| Disk | NTFS file system–formatted partition with a minimum of 3 GB of free space |
| Display | 1366 × 768 |
| Network | 56 kilobits per second (Kbps) connection between client computers and server |
| IIS | IIS server 10 |
| IIS Folders | Read and write access of the folder C:\inetpub\wwwroot\ |
| Framework | Dot net framework 2, 3.5, 4, 4.5, & 4.7.2 |
| ASP.NET Core SDK | 3.1 & 5.0.301 |
| ASP.NET Core Runtime | 3.1 & 5.0.7 |
| Windows Server Hosting | 3.1.3 & 5.0.7 |
| ImageMagick-7.0.2-Q16 | To be installed on the Application server. Provide read and write access to everyone on the installed folder. |
| Phantomjs-1.9.2-windows | To be copied on an application server with reading and write access to everyone on the copied folder. |

**Dashboard Server:**

|  |  |
| --- | --- |
| **Component** | **Minimum** |
| Access | Remote desktop or Web-ex or TeamViewer Sessions details before the scheduled time. |
| Server | Window Server 2016 R2 or above |
| Processor | 3.7 gigahertz (GHz) |
| RAM | 56 Gigabyte (GB) |
| Disk | NTFS file system–formatted partition with a minimum of 3 GB of free space |
| Display | 1366 × 768 |
| Network | 56 kilobits per second (Kbps) connection between client computers and server |
| IIS | IIS server 10 |
| IIS Folders | Read and write access of the folder C:\inetpub\wwwroot\ |
| Framework | Dot net framework 2, 3.5, 4, 4.5, & 4.7.2 |
| ASP.NET Core SDK | 3.1 & 5.0.301 |
| ASP.NET Core Runtime | 3.1 & 5.0.7 |
| Windows Server Hosting | 3.1.3 & 5.0.7 |

**Database Server:**

|  |  |
| --- | --- |
| **Component** | **Minimum** |
| Access | Remote desktop or Web-ex or TeamViewer Sessions details before the scheduled time. |
| Server | Window Server 2016 R2 or above |
| Processor | 3.7 gigahertz (GHz) |
| RAM | 64 Gigabyte (GB) |
| Disk | NTFS file system–formatted partition with a minimum of 3 GB of free space |
| External data Drive | Separate Data and LOG drives (512 Gib or More each) |
| Display | 1366 × 768 |
| Network | 56 kilobits per second (Kbps) connection between client computers and server |
| SQL Server subscription | SQL 2016 SP2 Standard or above |

**3.4 What is the Maturity Level of RM.1 Risk Management?**

Comments: Need to check with GG Sir/Ravi Sir

**3.10 What is the Maturity level of GA.5 Access Management Control?**

We have the possibility to set the user timeout using configuration. If the user is inactive exceeding that time, the application logoff whenever the next operation will be performed.

If the user tries out 3 wrong passwords, the user gets locked in a certain time.

We have abandoned the user session once he logged off from the system.

As soon as the user logins to the system a new session ID is generated and is kept in the browser for the identification of user requests.

Authentication credentials don’t pre-filled.

 For security management, we have the Form-Based Authentication, 2-factor authentication and we also have the Single Sign-on for managing the security through the user Active Directory.

**3.11 What is the Maturity Level of THE GA.6 Control Minimization of the processing of personal data?**

We have an inbuild authorization system that validates the users and gives authorization based on the access defined for that particular data.

We have the authorization process which processes only the authorized data.

We have a defined set of User Roles for the policy that actively take part in User Authorization to avoid any unauthorized access.

**3.12 What is the Maturity level of the GA.7 Control Minimization of the processing of personal data?**

We have an isolated environment for the testing, development, and production and we make sure of the security of the user data across the environments.

We have inbuild procedures and Microsoft Identity Principle which we are using for the security management for Authorize access.

**3.13 What is the Maturity level of GA.8 System Administrators Control?**

Yes, we have a certified System Administrator.

Yes, we have a process for verification of System Administrator work annually.

Below are some verification Checklists verifying the system administrator works annually.

1. Activities and Audit logs are verified for the activities done over servers.

2. Verify disaster recovery plans work

## 3. Check server health and performance- Audit and analysed the health reports of the servers that were generated and stored in monitoring logs.

## 4. Update licensing/ certification agreements

## 5. Perform patch and change management verification

**3.14 What is the Maturity level of GA.9 System Administrators?**

Comments: Need to check with GG Sir/Ravi Sir

**3.21 What is the Maturity Level of SRS Control.1 Network and Systems Security?**

Yes, the vulnerability assessment, a penetration test is done, and a report is generated and accordingly, proper actions are taken to resolve issues priority-wise

Yes, the formalized process is defined as vulnerability assessment, penetration test is done before any version to the customer is released.

It’s carried out before release/periodically.

* indicate whether a Penetration Test is carried out annually on the exposed transnational services

Comments: Need to check with GG Sir/Ravi Sir

yes, verifications are done by qualified third parties with networks and infrastructures.

* indicate the specifications (e.g. presence of written procedures, name of suppliers carrying out VA/PT, periodicity and method of action, etc.)

Comments: Need to check Name of suppliers with GG Sir/Ravi Sir

**3.22 What is the Maturity Level of SRS Control.2 Network and Systems Security?**

 Yes, security patches and fixes for known system vulnerabilities, are released by manufacturers, promptly tested, and implemented by Vendor while minimizing vulnerability exposure time

Yes, software upgrades priorities and installation times are predefined. Most of the upgrades and installation are done over the weekend on pre-informed and approved time duration with the customer and Team.

Yes, Logs of patches are kept for the systems.

Yes, we have internal legislation and an appointed team to support and carried out the activity.

**3.23 What is the Maturity Level of SRS Control.3 Network and Systems Security?**

Comments: Need to check with GG Sir/Ravi Sir

**3.24 What is the Maturity Level of SRS Control.4 Network and Systems Security?**

Yes, we have well planned and secured backup policy of our server’s data over Azure.

Below are the details and architecture of data and security.

**Azure Server Architecture for Backup vault**

Diagram

Description automatically generated

**Features Recovery services vault provides:**

Azure Backup creates recovery points that are stored in geo-redundant recovery vaults. When you restore from a recovery point, you can restore the whole VM or just specific files.

Diagram

Description automatically generated

**Backup Strategy:**

|  |  |
| --- | --- |
| **BACKUP STRATEGY**  **FOR SYSTEM** |  |
| Application Server | Daily complete Backup every 24 Hours |
| SQL Server Databases | Every 15 minutes Log Backups of SQL Server Databases |
| Retention Period | 180 Days for server and 35 Days for SQL log backups |

**3.26 What is the Maturity Level of SRS Control.6 Network and Systems Security?**

The content is grouped by the **security controls** defined by the Azure Security Benchmark and the related guidance applicable to Azure Virtual Network.

Microsoft Defender for Cloud continuously analyzes the security state of Azure resources for network security best practices. When Defender for Cloud identifies potential security vulnerabilities, it creates recommendations that guide us through the process of configuring the needed controls to harden and protect our resources.

Defined and implemented standard security configurations for network resources with Azure Policy and review the built-in network policy definitions for implementing network security groups.

Have enabled distributed denial of service (DDoS) Standard protection on our Azure Virtual Network to guard against DDoS attacks

Have enabled Azure Monitor for access to our audit and activity logs which includes event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. Logging and monitoring have been continuously done.

Azure Point to Site VPN is configured only through the VPN authorized user can access the system.

**3.27 What is the Maturity Level of SRS Control.7 Network and Systems Security?**

Yes, external access to systems and applications that process customer ownership data take place through Strong Authentication with at least one double authentication factor.

For security management, we have the Form-Based Authentication, 2-factor authentication and we also have the Single Sign-on for managing the security through the user Active Directory.

We have MFA in which users can do the login by OTP that is generated through API which is then sent to the Email ID and on designated Authenticator APP (PO Authenticator) for the user, and after authenticating through both places’ applications can be accessed by users.

**3.28 What is the Maturity Level of SRS Control.8 Network and Systems Security?**

Yes, the network is appropriately segregated in such a way as to guarantee adequate protection to critical systems that process the data owned by the Customer

On Azure, we have the below set of segmentation that protected the networks.

Graphical user interface, text

Description automatically generated

We have separated environment with the separate virtual networks for Prod and Dev environments with firewalls to maintain stateful traffic of production and nonproduction traffic

## We have the below architecture of Multiple Virtual Networks with peering in between them

Diagram

Description automatically generated

**3.29 What is the Maturity Level of SRS Control.9 Network and Systems Security?**

We are using only TLS 1.2 protocols for our servers with using best practices cipher suites enabled only which enhances the security all TLS/SSL protocols below this are completely disabled.

Also on all our application links, we have enabled HTTPS only with a secure site SSL certificate. Certificates we are using from one of the most trusted and advanced security features enabled CA providers is DigiCert.

We are using Zero compromise certificates that offer complete, pro-grade security beyond encryption. It's a Secure Site plus a lot more:

* Priority Support & Validation
* Certificate Transparency (CT)
* Log Monitoring
* Vulnerability Assessment & Blocklist Check
* Vulnerability assessment

**3.30 What is the Maturity Level of SRS.10 Network and Systems Security?**

### On Azure, we are using managed disks which implied encryption

### Platform-managed keys

### By default, managed disks use platform-managed encryption keys. All managed disks, snapshots, images, and data written to existing managed disks are automatically encrypted at rest with platform-managed keys.

Data in Azure-managed disks is encrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant.

## For more security, we are using Double encryption at rest

For High security-sensitive, it is an additional layer of encryption using a different encryption algorithm/mode at the infrastructure layer using platform-managed encryption keys. This new layer is applied to persisted OS and data disks, snapshots, and images, all of which are encrypted at rest with double encryption.

**3.31 What is the Maturity level of BCM.1 Business Continuity Management?**

**And**

**3.32 What is the Maturity level of BCM.2 Business Continuity Management?**

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

The principal objective of the disaster recovery program is to develop, test, and document a well-structured and easily understood Failover test that will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations.

When disaster strikes, business suffers. A goal of business planning is to mitigate disruption of product and services delivery to the greatest degree possible when disruption due to disaster occurs. Business continuity is the overarching concern.

Project Objects encourages to proactively execute an IT Disaster Recovery plan and periodically test the plan. We have standard policies and planned tests for technology disaster recovery.

An IT disaster recovery plan is the lynchpin of an overall business continuity strategy. And the purpose of business continuity is to maintain a minimum level of service while restoring the organization to business as usual.

**Overview on our Disaster Recovery and Backup Solution**

## **About Site Recovery for servers**

Azure Recovery Services contributes to our BCDR strategy:

* **Site Recovery service**: Site Recovery ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at our primary site, we can failover to a secondary location, and access apps from there. After the primary location is running again, we can fail back to it.
* **Backup service**: The Azure Backup service keeps our data safe and recoverable.

Site Recovery can manage replication for:

* Azure VMs replicating between Azure regions.

## **What does site Recovery Provide us?**

|  |  |
| --- | --- |
| **Azure VM replication** | we set up disaster recovery of Azure VMs from a primary region (west Europe) to a secondary region (North Europe). |
| **RTO and RPO targets** | Keep recovery time objectives (RTO) and recovery point objectives (RPO) within organizational limits. Site Recovery provides us continuous replication for Azure VMs and replication frequency as low as 30 seconds. |

**Azure Server Architecture for Failover Site**

Graphical user interface, application

Description automatically generated

**ASR Replication structure for servers over Azure**

Diagram

Description automatically generated

**3.34 What is the CS.2 Cloud Security Control Maturity Level (if applicable)?**

**3.35 What is the CS.3 Cloud Security Control Maturity Level (if applicable)?**

**3.36 What is the Maturity level of CS.4 Cloud Security Control (if applicable)?**

**3.37 What is the CS.5 Cloud Security Control Maturity Level (if applicable)?**

**Comments: For the above 4 points, we need to discuss with Ravi sir/GG Sir**