AIMS TECHNOLOGY OVERVIEW

2026

Technical Proposal

AIMS grant management products are supplied using Oracle Cloud Infrastructure (OCI) for hosting your solution. This allows us to meet the unique challenges faced by Grantmakers in each of their sectors, providing resilient and cost-effective technological solutions. It also allows us to host your AIMS solution, in whatever regions Oracle provide cloud infrastructure.

For AIMS, using OCI as our hosting cloud partner provides many benefits to our customers:

- secure, resilient global cloud infrastructure and services
- meet rapidly changing customer behaviours and expectations
- meet compliance challenges and provide in-country data storage
- accelerate digital transformation and data consolidation
- scalability to ensure optimal performance
- flexibility to better integrate with other web services
- faster deployment and faster maintenance
- faster network connections and greater bandwidth

Our standard OCI hosting set up and offer is described below.

AIMS technology

AIMS technology is divided between the back end and front end. The backend technology includes web frameworks, programming languages, servers, and operating systems. The frontend technology is the visual web interface, and application functionality.

AIMS is based on a web server written on C (Naviserver) using Oracle customer. C is widely used and the base of most of the computer systems. TCL is used as a higher-level scripting language that processes the users' requests – similar to other leading languages like Perl, Python for all back-end integrations.

1. AIMS Network

The network layout of the AIMS solution as it pertains to the AIMS program is described here. The solution will be hosted on OCI cloud infrastructure. AIMS is a three-tiered application with web, application and DB layer. Access to the AIMS hardware will be restricted to our Infrastructure and Security team and a number of our Software Engineers.

Each of the primary elements are on a cold stand-by (Mail Relay, Web/Application server and DB server. The servers run on Windows server and the DB is Oracle.

All memory and disks space proposals are based on information provided at the time of proposal. Both the database and Application servers will require an open relay to an SMTP mail server or Office365 to send out emails from AIMS and a Reverse proxy/load balance server to be placed in front of the Application servers to provide SSL encryption layer and load balancing across multiple Web servers. Other network protocols required SQL net, http, https, smtp, unc path.

2. Oracle Database Server

The Database Server runs on Windows server on a virtual environment or on a physical server. High Availability will be achieved using multiple Hardware components. The reverse proxy server provides SSL redirection, SSL termination, Isolates the Origin server and optimises content.

3. Load Balancer/Reverse Proxy

The reverse proxy server provides SSL redirection, SSL termination, Isolates the Origin server and optimises content.

- SSL redirection - If a customer request is detected on port 80 (HTTP) the request is redirected to port 443 (HTTPS)
- SSL Termination - The SSL termination option provides secure connections in reverse proxy mode between the customer and reverse proxy and optionally between reverse proxy and the origin server.
- Server Isolation - The origin server has no direct communication with customers since all traffic from the Internet passes through the reverse proxy first.
- Content optimisation - Content is compressed in order to speed up loading times.

4. Application Server

The AIMS Application Servers runs on Windows server on a virtual environment. High Availability will be achieved with multiple application server installation.

- A Reverse proxy will be placed in front of the Application server to provide SSL encryption layer/SSL termination.
- An open relay between the AIMS servers (DB and WEB) and the organisation's email server will be provided
- The Application servers and Database servers will be virtual
- AIMS will provide firewalls, proxy servers.

5. Mail Server

AIMS can provide an open relay to an SMTP mail relay server to send out emails from AIMS for both the Database and Application servers, but it is preferrable for the customer to use their own Office365 account with an open relay allowing smtp traffic from this environment.

6. System Performance

AIMS will be configured based on the information provided by the Customer, to meet their requirements. Additional Application servers can be added to the setup for higher performance. The database is designed to handle 1,000 forms submissions (applications, surveys) per hour at peak times.

7. System Availability

All hosting will be provided using OCI. We use a third-party tool to monitor and alert of any down time, System Security and Access Control

Service Availability does not include Scheduled Service Downtime, Unscheduled Service Downtime, Customer-caused or third party-caused outages or disruptions (except to the extent that such outages or disruptions are caused by those duly authorised third parties sub-contracted by the Supplier to perform the Managed Hosting Services), or outages or disruptions attributable in whole or in part to force majeure events.

8. Access Management

Access to AIMS is via a login screen which uses email address and password for identification and validation. Once a user is validated the appropriate Role is assigned giving access to AIMS functionality (see Levels of Account and Access to AIMS functionality below).

AIMS includes a number of configurable password policies which include the following:

- minimum password length
- account lockout after a configurable number of failures with a configurable lockout period
- Password history validation restricting reuse, etc.
- password lifetime in configurable number of days

The AIMS product uses cryptography to encrypt passwords that are stored in the database. The AIMS product uses SHA-1 cryptographic hash function to encrypt passwords.

9. Levels of Account and Access to AIMS Functionality

Security and Access management to the functionality within AIMS is controlled using Roles and Permissions. Role can be created with each Role assigned various Permissions to the functions with the Grant Schemes or Programmes (assuming they use separate Workflows). One or more User is then assigned to each Role.

A matrix of the various Roles and Permissions is maintained and controlled by System Administrators. Individual roles & responsibilities are critical to ensuring that business processes access rules are adhered to and appropriately controlled.

The system has the flexibility to allow System Administrators to define new roles as required, using the Roles Matrix. Using the Permissions Module, the administrator can then tick the “permissions” associated with the work that this new role may have access. This gives the organisation excellent flexibility and control to change processes and associated roles within the system through configuration.

Different roles can be set up within AIMS, which can be system wide or scheme specific. Users can then be associated with distinct roles. Access to functionality within the system, for example “add a payment”, is strictly controlled by a set of permissions that apply to each role.

10. Session Management

AIMS allocates sessions post user authentication. User sessions time out after a (configurable) period of inactivity, and the user is logged out. The AIMS product uses encrypted cookies to store the unique user ids and session ids.

11. Network, Firewall and Security

Data access security shall be provided by AIMS through managed firewall services with security using virtual Firewalls on OCI that delivers NGFW capabilities for organizations of all sizes, with the

flexibility to be deployed as a NGFW and/or VPN gateway. It enables broad protection and automated management for consistent enforcement and visibility across hybrid cloud infrastructures. The virtual Firewall scales from the smallest footprint in the industry to the highest capacity NGFW virtual appliance on OCI.

The service comprises of the following features:

- Supply and installation of a suitable Managed Security Appliance.
- Configured to an EAL4 (Evaluation Assurance Level) security standard.
- Optimised router configuration to meet Customer network requirements.

As well as a firewall there is also a Reverse Proxy server in front of the application for added security. The purpose of the Reverse Proxy is as follows:

- The reverse proxy server provides SSL redirection, SSL termination, Isolates the Origin server and optimises content.
- SSL redirection - If a customer request is detected on port 80 (HTTP) the request is redirected to port 443 (HTTPS)
- SSL Termination - The SSL termination option provides secure connections in reverse proxy mode between the customer and reverse proxy and optionally between reverse proxy and the origin server.
- Server Isolation - The origin server has no direct communication with customers since all traffic from the Internet passes through the reverse proxy first.
- Content optimisation - Content is compressed to speed up loading times.

Up to date anti-virus systems to scan all attachments being loaded into the system as well as OS scanning.

12. Network protocols & Port restrictions:

Network traffic will be controlled by security groups with protocol and port restrictions restricting any prohibited traffic. The infrastructure also undergoes a vulnerability assessment periodically to ensure the network is secure and any vulnerabilities are assessed, and the risks mitigated.

Oracle Cloud Infrastructure

AIMS has a longstanding partnership with Oracle to provide our customers with a robust and affordable solution.

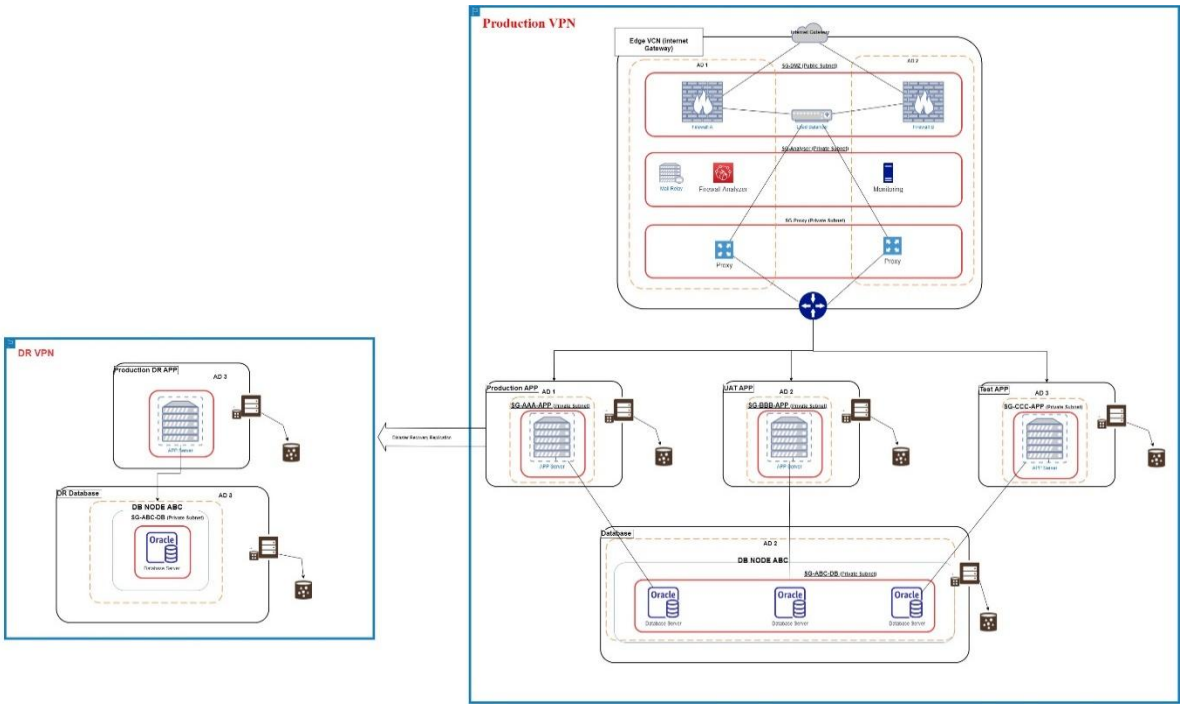
Oracle delivers a second-generation cloud. Oracle Cloud Infrastructure offers tools and architecture that help enterprises seamlessly move from on premise to the cloud, leveraging improved automation and built-in security to mitigate threats, ultimately supporting superior migration and economics.

Oracle Cloud Infrastructure is built for innovation. This includes industry-leading scalability and availability, integrated governance and control, and reliability backed by end-to-end SLAs. Oracle's cloud mission extends to supporting emerging technologies such as AI, machine learning (ML), the internet of Things (IoT), blockchain, and human interfaces.

Oracle's enterprise customers have progressed from experimenting with these technologies in a sandbox to implementing them for mission-critical applications, building new business models, and creating new business value. Oracle Cloud Infrastructure addresses key issues associated with first-generation cloud solutions, which were not developed to handle large financial systems, government workloads, or data-intensive applications. First-generation cloud solutions were built on decade-old technology in which performance, security, and migration options were afterthoughts. Oracle Cloud Infrastructure's next-gen architecture specifically meets the needs of today's enterprise by providing faster and more predictable performance, better pricing and security, and enhanced compatibility for enterprise workloads.

Oracle is the only provider that delivers IaaS, PaaS, and SaaS services as part of its second-generation cloud offering. And Oracle Autonomous Database services leverage the same high-speed network as other Oracle Cloud Infrastructure services—enabling you to deploy mission-critical applications rapidly in support of continuous innovation.

The below OCI diagram shows the AIMS network layout.



1. OCI Key benefits

1.1 Encryption at Rest

Oracle Database uses TDE transparently that encrypts data at rest in Oracle Databases. It stops unauthorized attempts from the operating system to access database data stored in files, without impacting how applications access the data using SQL. TDE can encrypt entire application tablespaces or specific sensitive columns. TDE is fully integrated with Oracle database. Encrypted data remains encrypted in the database, whether it is in tablespace storage files, temporary

tablespaces, undo tablespaces, or other files that Oracle Database relies on such as redo logs. Also, TDE can encrypt entire database backups (RMAN) and Data Pump exports.

1.2 Higher performance and availability

By using cloud computing resources together simultaneously, you reap greater performance gains than by having your own dedicated server hardware. Cloud computing increases input/output operations per second (IOPS). Oracle cloud delivers as much as 20X the IOPS of Amazon Web Services.

1.3 Maximized price/performance.

Oracle Cloud Infrastructure provides the best price/performance available in the market to date. Workloads deployed on Oracle Cloud Infrastructure often require fewer compute servers and block-storage volumes— lowering the cost of delivering optimized workload performance.

Oracle compute servers, such as Oracle Virtual Machines and bare metal, help businesses achieve significant cost savings of 25-65% compared to VMs from competitors such as AWS (as costs are going up this will minimize the impact to customer costs).

Oracle Databases run faster, and lower costs by up to 66% when compared to AWS— allowing you to achieve data- driven results more efficiently and affordably.

Additional features available:

Additional features available, such as Data Guard, Oracle RAC.

https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-ten-reasons.pdf

2. OCI Availability Service Level Agreements

2.1 OCI Compute Availability Service Level Agreement

With respect to a Cloud Service listed above for which the Availability Service Level Agreement under this subsection applies, Oracle will use commercially reasonable efforts to have each such Service available with a Monthly Uptime Percentage (as defined below) of at least 99.9% during any calendar month (the "Service Commitment"). In the event an applicable Cloud Service listed above does not meet its Service Commitment for the Availability Service Level Agreement under this subsection, you will be eligible to receive Service Credits for such Non-Compliant Service, with the Service Credit Percentage determined as follows:

Monthly Uptime Percentage for Regions with more than one Availability Domains	**Service Credit Percentage**
Less than 99.99% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

Monthly Uptime Percentage for Regions with one Availability Domain	**Service Credit Percentage**
Less than 99.95% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

Monthly Uptime Percentage for Single Instance	Service Credit Percentage
Less than 99.9%	100%

The following terms apply to the Availability Service Level Agreement for the applicable Cloud Services listed above:

- "Monthly Uptime Percentage" is calculated by subtracting from 100%, the percentage of minutes during the calendar month in which the applicable Cloud Service was Unavailable.
- "Unavailable" excludes circumstances resulting directly or indirectly from any Common Exclusion, and means any time when a problem with the applicable Cloud Service prevents external connectivity with:
    i. for regions with more than one Availability Domains, all instances of such Cloud Service that are deployed in more than one Availability Domain; or
    ii. for Regions with one Availability Domain, all instances of such Cloud Service that are deployed in more than one Fault Domain; or
    iii. for a single instance of such Cloud Service, each such instance.

2.2 Manageability Service Level Agreement

With respect to a Cloud Service listed above for which the Manageability Service Level Agreement under this subsection applies, Oracle will use commercially reasonable efforts to have each such Service available with a Monthly Uptime Percentage (as defined below) of at least 99.9% during any calendar month (the "Service Commitment"). In the event an applicable Cloud Service listed above does not meet its Service Commitment for the Manageability Service Level Agreement under this subsection, You will be eligible to receive Service Credits for such Non-Compliant Service, with the Service Credit Percentage determined as follows:

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.9% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

The following terms apply to the Manageability Service Level Agreement for the applicable Cloud Services listed above:

- "Control Plane API Error Rate" means, on a per Availability Domain basis, the percentage value corresponding to: (i) the total number of internal server errors returned by the applicable Cloud Service with an error status of "Internal Service Error" or "Service Unavailable" in a five-minute period during a calendar month divided by, (ii) the total number of Control Plane API requests made to such Cloud Service in such five-minute period. This excludes circumstances resulting directly or indirectly from any Common Exclusion.
- "Monthly Uptime Percentage" is calculated by subtracting from 100%, the average of the Control Plane API Error Rate for each five-minute period during the applicable calendar month.

2.3 Performance 1 Service Level Agreement

With respect to a Cloud Service listed above for which the Performance 1 Service Level Agreement under this subsection applies, Oracle will use commercially reasonable efforts to deliver the performance of the NVMe drives utilized in each such Cloud Service at a Monthly Performance Rate (as defined below) of at least 99.9% during any calendar month (the "Service Commitment"). In the event an applicable Cloud Service listed above does not meet its Service Commitment for the Performance 1 Service Level Agreement under this subsection, You will be eligible to receive Service Credits for such Non-Compliant Service, with the Service Credit Percentage determined as follows:

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.9% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

The following terms apply to the Performance 1 Service Level Agreement for the applicable Cloud Services listed above:

- “NVMe Performance Decay Rate” means the percentage value corresponding to: (i) the total number of hours in a calendar month during which the NVMe IOPS in the applicable Cloud Service is less than 90 percent of the minimum IOPS published by Oracle, divided by (ii) the total number of hours in such calendar month. This excludes circumstances resulting directly or indirectly from any Common Exclusion and any time while a backup or snapshot is being performed.
- “Monthly Performance Rate” is calculated by subtracting from 100%, the NVMe Performance Decay Rate for a calendar month of the applicable Cloud Service.

2.4 Performance 2 Service Level Agreement

With respect to a Cloud Service listed above for which the Performance 2 Service Level Agreement under this subsection applies, Oracle will use commercially reasonable efforts to deliver a Network Performance (as defined below) for each such Cloud Service at a Monthly Performance Rate (as defined below) of at least 99.9% during any calendar month (the "Service Commitment"). In the event an applicable Cloud Service listed above does not meet its Service Commitment for the Performance 2 Service Level Agreement under this subsection, You will be eligible to receive Service Credits for such Non-Compliant Service, with the Service Credit Percentage determined as follows:

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.9% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95.0%	25%
Less than 95.0%	100%

The following terms apples to the Performance 2 Service Level Agreement for the applicable Cloud Services listed above:

- “Monthly Performance Rate” is calculated by subtracting from 100%, the Network Performance Rate (as defined below) in the calendar month for the applicable Cloud Service.
- “Network Performance” is defined as the average rate of data transfer using 9KB packets over a 5-minute interval as measured between two bare-metal instances of the applicable

Cloud Service using VCN private IP addresses within an Availability Domain. This excludes circumstances resulting directly or indirectly from any Common Exclusion.

- "Network Performance Rate" means the percentage value corresponding to: (i) the total number of 5-minute intervals during a calendar month in which the Network Performance for the applicable Cloud Service is less than 90% of the Oracle-published network throughput per Oracle-provided compute instance shape, divided by (ii) the total number of 5-minute intervals in such calendar month.

Reference article:

https://www.oracle.com/ie/cloud/sla/