

Updraft's Cloud Hosting & Managed Services

An overview of our comprehensive
platform for security, resilience,
performance and support



Executive Summary

This presentation defines how the Updraft SaaS solution is deployed, managed, and supported on either OCI or AWS cloud.

Governed by clearly defined terms and conditions, the Updraft SaaS offering ensures a stable, secure, and efficient operational environment throughout the service lifecycle.

This outline summarises the following elements of the Updraft SaaS solution and cloud managed services:

- Security frameworks

- Hosting elements

- In-house support capabilities

- Backup and DR strategies

- Scalability & capacity practices

- Client reporting mechanisms

- End-of-service provisions

- Managed Services Catalogue



Professional Software Solutions

Secure Software Development Lifecycle (SSDLC)

- All code changes are subject to peer reviews and automated scanning for potential security issues prior to release.
- Strict segregation between development, staging, and production environments to reduce the risk of cross-contamination and unauthorized changes.

Data Protection & Encryption

- All stored data is encrypted using cloud-native Key Management Services (OCI Vault or AWS KMS). TLS/SSL-encrypted endpoints safeguard data in transit
- Robust key rotation policies, secure generation, and storage of cryptographic keys to comply with data protection mandates.

Vulnerability Management

- Monthly or quarterly updates for operating systems, databases, and applications. Critical patches are applied with accelerated SLAs.
- Scheduled internal/external penetration tests to identify vulnerabilities early, followed by remediation and improvement of security controls.

Threat Detection & Incident Response

- Native security services (OCI Cloud Guard / AWS GuardDuty) continuously scan for unusual activities and policy deviations, alerting security teams for rapid response.
 - Cloud-based firewalls, WAFs, and DDoS protection (OCI WAF, AWS Shield) help detect and automatically mitigate malicious traffic.
-

Regulatory & Compliance Alignment

- OCI and AWS adhere to industry standards such as SOC 1/2/3, ISO 27001, GDPR, and HIPAA (where applicable).
- Detailed logs (via, Oracle Logging / AWS CloudTrail / System Logs) are retained for compliance audits, forensic analysis, and continuous improvement.

Continuous Improvement

- Annual reviews of security policies, incident response plans and risk registers ensure alignment with evolving threats and regulatory requirements.
 - Where required, additional controls or custom security measures can be implemented (IP whitelisting, on-premise connectivity, private endpoints) subject to T&Cs.
-



Deployment Options

- SaaS Cloud Offering:
 - A fully managed, cloud-based solution that delivers all the benefits of rapid deployment, automatic updates, and minimal overhead.
 - Customised hosting options and associated service terms are available.

Infrastructure

- Cloud Deployments leverage Virtual Private Cloud Networking, Compute, block and object storage.
- Core services Include Load Balancers, File Storage and Oracle DB services
- High availability is achieved using multi-AD Availability Domain architecture, combined with network redundancies and active health monitoring.

Performance & Monitoring

- Continuous monitoring of CPU, memory, IOPS, and network throughput via Logging, Cloud Native Monitoring and industry-leading tooling.
- Capacity Management leverages native seamless horizontal or vertical scaling of resources to ensure demand is always met.

Security & Compliance

- User permissions are controlled by Identity and Access Management (IAM) policies.
- Regulatory and data protection compliance is ensured by Web Application Firewalls (WAF) and data encryption (at rest and in transit)

Inhouse Offerings



Contact centre

A dedicated Service Desk provides immediate telephonic support.



Ticketing System

Ticketing tools (Jira Service Management) ensure efficient tracking, escalation, and resolution.



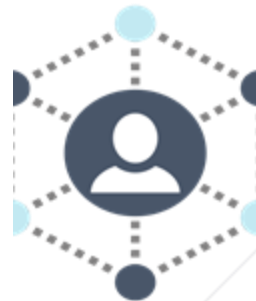
SLA and Reporting

Incident response times and SLAs defined per contractual agreements.



Custom Integration Services

Integrate with CRM, ERP, and HR systems via REST APIs.



Single Sign-On (SSO) & Identity Integration

Support for SSO protocols (SAML 2.0) to streamline user authentication.

Tailored solutions can be developed on a per-requirement basis, governed by mutually agreed T&Cs.

Backup & Recovery Procedures

Updraft's backup strategy leverages Oracle Data Guard to provide a robust, real-time replication of critical databases, minimizing data loss (low RPO) and enabling swift failover in the event of primary site outages. By continuously transferring redo logs from the primary to a standby database, Data Guard keeps the standby environment closely synchronized, ensuring that failover or switchover operations can occur with minimal downtime. Additionally, regular full and incremental backups are taken in conjunction with Data Guard, enabling point-in-time restores while preserving transactional integrity.

Data Backup

- Full backups performed weekly, with incremental backups daily.
- Cloud-native backup tools (OCI Backup Service, AWS Backup) ensure reliable data copies and encrypted storage.

Disaster Recovery (DR)

- Standby databases (Oracle Data Guard on OCI) maintain near-real-time synchronization with the primary database.
- Regular DR drills validate failover procedures, ensuring quick RTO and defined RPO.

Archive & Retention Policies

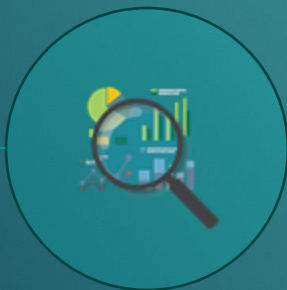
- Standard 30-day rolling backup window. Extended archiving available per project requirement.
- Secure vaulting ensures compliance with legal and regulatory data retention needs.

Scalability & Capacity



Horizontal & Vertical Scaling

- Horizontal scaling via additional OCI Compute instances or AWS EC2 instances behind load balancers.
- Vertical scaling by upgrading instance shapes (OCI) or instance types (AWS) as usage grows.



Capacity Planning

- Periodic load tests to verify system performance under projected peaks.



Resource Optimization

- Regular performance tuning of databases and applications.
- Automated recommendations guide cost-effective scaling decisions.

Capacity guidelines defined by contractual T&Cs, ensuring resource availability aligns with business growth.



SaaS Performance Dashboards (In-App)

- Real-time dashboards showing contract volumes, processing times, and SLA adherence.
- Users access usage metrics, contract lifecycle statuses, and compliance checks directly within the application UI.



Strategic Roadmap Sessions

- Regular stakeholder meetings align platform evolutions with client objectives.
- Performance metrics, new regulatory requirements, and user feedback inform future development cycles.



Support & Incident Reporting

- Monthly support summaries detail ticket volumes, resolution times, and common issues.
- Quarterly reviews offer roadmap insights, highlighting upcoming features, infrastructure upgrades, and integration enhancements.

End of Service Support and Processes



01

Data Export & Transition

On contract termination, clients receive a full export of all stored documents and associated interview data and metadata in a commonly accepted format (CSV, JSON).

Assistance provided for secure data transfer to client-managed storage or alternative platforms.

02

Post-Service Documentation & References

Final service summary report detailing performance, support history, and completed project deliverables.

Availability of consultancy services for smooth handover to internal teams, as per mutually agreed T&Cs.

03

Decommissioning Infrastructure

Formal deprovisioning of SaaS resources following a data retention grace period.

Secure deletion of all backup copies after client sign-off, ensuring no residual data.

04

Post-Service Check-in

The insights from this check-in feed directly into our continuous improvement process, ensuring we refine our offerings and maintain a strong relationship with the client for any future engagements.

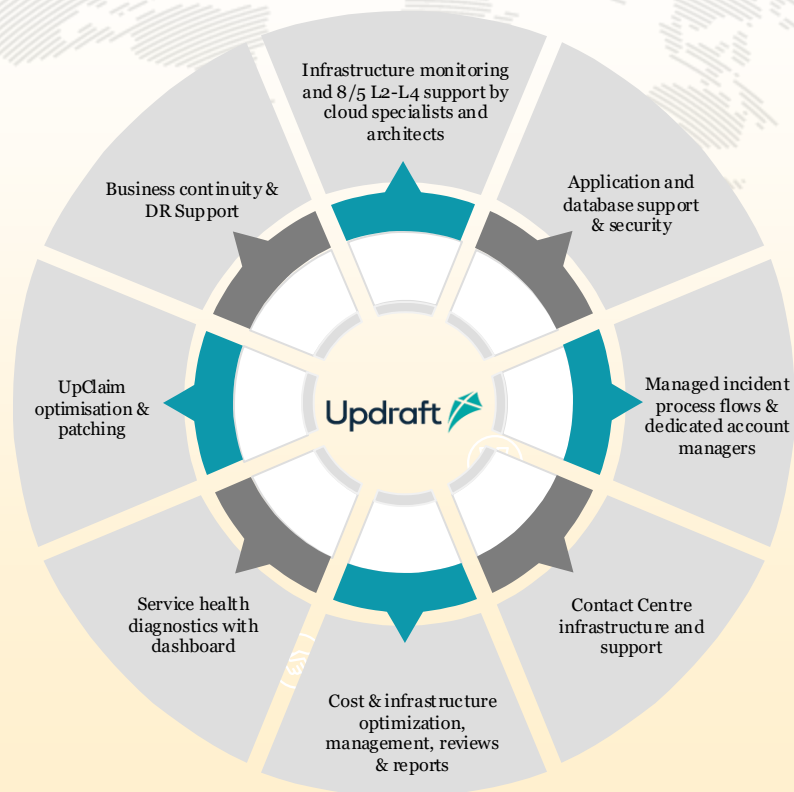


UpClaim

Detailed outline of the Cloud Managed Services included in the fully-hosted UpClaim solution.



Managed services summary:



Cost Optimization, OCI reviews, monitoring, ticketing

- Server Health Check Monitoring
- Managing Alert and Monitoring
- OCI Cost Optimization
- Handling Jira tickets for Reporting and Tracking
- DevOps & OCI enhancement & reviews
- SLA tracking and monthly reporting
- Other managed service work

Security and Network

- OCI and Database Security
- IAM and OS Access Management
- Data encryption and security certificates
- Backup and Restore
- DR Drill Half yearly
- OCI Network Management
- OCI DNS Management
- OS Patching and Hardening

Application and Database

- OCI DevOps, CI / CD pipelines & deploys
- Oracle production & pre-production database management, security, back-ups and deploys
- Application patches, releases and deploy pipelines, config., testing & stabilization
- Application, database & platform bug fixes
- DB tuning and maintenance
- Configure HA/DR
- Electronic signature infrastructure

Legal Contact Centre

- Contact centre infrastructure and applications support
- PBX management, config. & support
- Network security and management
- Telephony systems, support & resilience
- Firewall maintenance & support
- IVR and routing management
- Agent desktop support & provisioning
- Performance & call data reporting

Client Services

- Oracle invoice & payment management
- Dedicated incident & account managers
- OCI cost monitoring & dashboards
- Service health monitoring, alerts & fixes
- Half-yearly OCI and cost review with client
- 8/5 L2-4 support by cloud specialists and architects
- Incident tickets, playbooks & reporting

Legal process optimisation

- Patching & stabilisation for business-driven changes in claims workflows
- Case law or legislative database and configuration updates
- Operational management of legal solution enhancement
- Maintenance, back-up and support of legal databases and research resources

Managed Services Catalogue:

Cloud Infrastructure

Category	Service		
Server / VM Monitoring	Monitoring and management of each server's CPU, Memory, IOPS, Throughput and Disk utilization		
	Maintenance and support of continuous 'load balancing' virtual machine management of load, health status and redirection of traffic to backend VM pools in line with defined routing policies, load and availability		
	Track, test and support infrastructure health, incident and performance alerts		
	Maintain and monitor infrastructure issue tracking and performance dashboards, distribution channels and incident management processes		
	Active engagement with Oracle to address and resolve any hardware, performance, throughput, storage or resilience issues related to the OCI architecture		
	Implement and test solutions and OCI configuration changes necessary to resolve or mitigate issues related to Memory, IOPS, Throughput and Disk Utilization		
Backup	Monitor and support Oracle Data Guard components and config. for back-up, data replication, database sync. strategies and disaster recovery in Primary and secondary Fault Domain		
	Create, maintain, manage, and monitor the Oracle Data Guard integrated standby databases and replicated primary environment		
	Maintain and configure data rolling back-ups and approved data retention lifecycles		
	Implement, test and support business continuity and DR drills through required switches of the standby database and architecture to a primary production role (and vice versa) in the case of resilience or other risk issues		
	Conduct regular back-up and disaster recovery testing of the cloud infrastructure and the hosted Application elements		
Alert	Configure and monitor OCI metrics tools, dashboards and management consoles		
	Configure and monitor Oracle budget, CPU, storage and other alerts		
	Monitor and support notification or streamed alerts automatically triggered of OCI aggregated metrics and managed configurations / subscriptions		
Security	Provision and maintenance of multi-tiered OCI architecture security with adherence to industry best-practice WAF security enforcement, including the ongoing management, support and optimization of the following security components:		
	Web Application Firewall	Built-for-purpose web server	Least Privilege implementation
	Private subnets	Software IDS & firewall	Database ACLs
	Oracle vault and OCI compartment isolation	SSO integration via SAML2	Multi-layered logging
	Hardened VM OS	Cryptographic Nonce	Data in-rest and in-transit encryption
Network	Implementation and management of firewalls, VPN, private subnets, SSO integrations and associated privileges.		

Managed Services Catalogue:

Cloud Infrastructure

Category	Service
Access	Management, support and maintain user group, users, policy and Security Group Roles within SSO integration config and Application security group matrix
	Support and troubleshooting of user access related issues
	Monthly reporting on user access, activity and issues
	Monitor and manage the security roles and configuration
DR Drill	Implement and test regular DR drills to ensure seamless failover and support of failover fault domain and secondary architecture
	Manage, maintain and monitor full, incremental and scheduled data back-ups and resilience of secondary Fault Domain
Cost Optimization	Oracle and third party invoice analysis, management, payments and cost tracking
	Configure and monitor OCI cost optimization metrics tools, dashboards and management consoles
	Architecture Reviews every six months, with cost analysis and reporting, including any recommendations for further cost optimization
	Tracking and reporting on scalable cost elements, including Load Balancer bandwidth, VM instance pools, database storage and CPU
	Implementation and management of NFS file systems, block storage, object storage as required
	Scaling and optimisation of VM pools on numerous axes, including instances, CPU, memory, capacity type, disk speed, network and disk performance
DNS	Implementation and testing of cost-driven configuration changes
	Monitor existing DNS configurations
Other managed Services	Support existing team to troubleshoot DNS issues from Infra side
	Tiers 1-3 Support team training and stabilization in the initial stages after go-live
	Year 2 integration API support and testing for Guidewire's Release 2
	Handover and transition training as part of architecture transfer and transition in the final year of the contract period
	Conduct OCI well architected reviews every six months
	Cost, relationship and communications management for OCI required security certificates, licenses and third-party tools
	Provision new services as part of enhancement work of live environment
	Support Application Team during deployment or implementation activities
	Maintain proper logging for OCI architecture performance and resilience
OS patching	Knowledge sharing on OCI new services / features
	Manage and implement Enterprise Linux upgrades, patching, security hardening and tests
	Maintain regular patching plan and OS patching reports
	Troubleshoot OS patching related issues

Managed Services Catalogue:

Application Services

Category	Service
DevOps	Monitor and manage the CI/CD pipelines setup through OCI native services
	Monitor, log and manage any container environments setup through OCI native services
	Manage, implement and support patching, upgrades and releases within all environments, as well as any pipeline changes
	Manage the automated deployment of the environments
Application Server Support	Resolution of operational and infrastructure issues within the OCI environment
	Version upgrades, certificate installations, performance tunings and security patch update activity
	Any production incidents requiring immediate remediation
	Maintenance, support, upgrades and configuration changes for virtual machines, database, data encryption, hosting, firewall, email and mobile verification platforms necessary for Updraft's electronic signature modules
	User verification updates and access control and function permission management as per security group configurations
	Maintain and troubleshoot issues regarding integrations with Load Balancer, Web Server, Database, or third-party tools
	Support the application team on any issues related to platform during the deployment
	Support the application team from a platform point of view during DR drill
	Creation of any separate component in the Application/Middleware layer
	Reconfiguring the existing nodes after major issues, outages and re-establishing all the necessary integrations
	Reconfiguration due to change in design and deployment architecture
	Troubleshooting issues by analyzing application server logs
	Fixing security loopholes from a platform and infrastructure point of view that arise from a VAPT exercise
	Addressing any major change that is identified as a part of RCA of a Production incident
	Batch/infra monitoring and log analysis for high severity incident in order to perform the Application server level RCA
	Configuration optimization recommendations to scale up app server performance
	Any deployment or provisioning related process automation including creating or amending deployment scripts
	Analyzing trends of incidents and establishing patterns to help take pro-active corrective/preventive measures
	Installation, configuration and/or migration of new application server instance
	Fixing any defects or issues related to performance and security that is identified during performance testing and VAPT
	Architecture design enhancements and support of optimization initiatives

Managed Services Catalogue:

Application Services

Category	Service
Incident Management	Maintain Jira or equivalent issue tracker to manage and process tickets and Change Requests
	Document, update and maintain incident management processes, escalation structures and reporting. Compile and update project documentation related to Change Requests
Database Support	Management and support of scheduled and automated back-ups: 60 days of rolling backup, with weekly full and daily incremental back-ups
	Perform scheduled DR drills and monitoring to support seamless failover
	Monitoring and management of database storage and CPU, NFS file systems (with managed block and/or object storage)
	Major patch upgrade or service pack upgrade including post installation sanity and validation
	DB patch upgrade, DB refresh activity, ensure DB connectivity at all times
	Monitoring of backups (ensure full, differential and log-backups are working), DB process and checking of audit logs
	Troubleshoot DB Job failures, take Ad-Hoc backup if required
	Undertake data transfers and updates to pre-production environments as required
	User Group maintenance, tuning of DB / Application parameters as required
	Installation and configuration of new DB instance; Applying service packs to DB; Configure HA-DR solutions
	Setting up maintenance plans and SoPs for different DB maintenance activities
	Troubleshoot locking issues, including deadlocks, blocking, lock timeouts and fix them
	Handle database object deployment to Production environment; Work on performance tuning to continually improve DB performance
	Configure automated alerts and notifications due to change in SLAs or inclusion of new architectural components; Configure changes in DC-DR setup; Contribute in the RCA of incidents and Change tickets
	Setup maintenance plans for Backups, Database integrity check; Rebuild index and Update statistics
	Work on performance tuning issues like identifying missing index and creating them
	Responsible to review, recommend and implement physical and architectural changes in database due to change in capacity or tech stack. Writing custom code and store procs, views and triggers
OCI Services	Provide, maintain, upgrade and support the Oracle Cloud infrastructure, including all virtual machines, databases, environments, networking and architecture components set out in this presentation.
	Oracle invoice, payment and cost management
	Monitoring the OCI performance, resilience, security and optimization
	Managing the CICD pipeline, production releases and any changes in the existing pipelines

Managed Services Catalogue:

Business Process Services

Category	Service
Legal Call Centre Support	Hosting, maintenance, support, upgrades and configuration changes for virtual machines, database, PBX, email platforms, VoiP channels, firewall and DR environment
	Monitoring and management of VM / server CPU, Memory, data throughput and disk utilization
	Support for call recording storage, data volume threshold management, recording retrieval, back-ups and application of retention policies
	Network security and management, user privilege configuration and support
	Version upgrades, certificate installations, performance enhancement and security patch updates and licensing management for telephony platform, databases, VM's, security and remote access configurations
	Firewall maintenance & support
	Virtual PBX and IVR management, configuration and support, including diagnostics and remedial measures related to fibre connectivity, data speeds and VoiP line quality
	Track, test and support infrastructure health, incident and performance alerts and associated reporting
	Active engagement with Oracle to address and resolve any hardware, performance, throughput, storage or resilience issues related to the contact centre cloud architecture
	Implement, test and support business continuity and DR drills through required switches of the standby database, virtual PBX and architecture to a primary production role (and vice versa) to resolve resilience or other risk issues
Legal Optimization Support	Support and incident management for Agent desktop, connectivity, cloud infrastructure or network issues
	Database support and data retrieval for agent performance management, data retrieval, analytics and service reporting
	Manage, implement and support patching, upgrades and releases within all environments, arising from business-driven or legal development changes in claims workflows
	Hosting, back-up, maintenance and updates to case law and legislative databases and research resources, including data security and access updates, licensing and config.
	Monitoring and management of database storage, CPU, throughput and operational alerts
	Support, implement and stabilise legal database and application configuration updates and optimisation changes
	Operational management of legal solution enhancement; Change Request management, testing and deploy
	Management of user and administrator access and privileges within the legal databases, editing platform and configuration consoles
	Support, update and monitor online legal editing and configuration platform
	Legal data encryption, back-ups, disaster recovery and updates

Q & A

T. +27 (0)21 300 3800

E. info@updraftsoftware.com

W. www.updraftsoftware.com



COMPLETE CONTRACTING