



G-Cloud 14

Service Definition - Wipro Enterprise Digital Operations
Centre



Table Of Contents

Service Definitions.....	2
Key differentiators	3
Key Benefits	3
Service Description	4
Pricing Overview	4
Governance	4
Contact and Escalation.....	5
Supported Configuration	5
Supported Services	6
Service scope	6
User support.....	7
Onboarding and offboarding	8
Using the service.....	8
Scaling.....	9
Analytics.....	9
Resellers	10
Staff security	10
Asset protection	10
Data importing and exporting	11
Data-in-transit protection.....	11
Availability and resilience.....	11
Identity and authentication	12
Audit information for users.....	13
Standards and certifications	13
Security governance.....	14
Operational security	15
Public sector networks.....	17

Wipro intends to leverage its **Enterprise Digital Operation Centre** (EDOC) platform service is the universal marketplace of IT service consumption to provide a holistic and end-to-end fully integrated approach for customers to source, fulfill and operate IT across multiple IT supply sources (Datacenter, Private Cloud, Public Cloud and Public Containers) that is based upon the below solution tenants:

- Provide a single pane of glass for services aggregation and procurement.
- Leverage the Ready to Use EDOC platform to deliver services across multiple IT sources
- As infrastructure components would become programmable constituents of the larger estate, unified management will be achieved through Infrastructure abstraction and will become exempt from traditional technical dependencies
- Modular architecture with each datacenter environment individually controllable, expandable, and flexible
- Automated processes to drive agility and leaner time to market for next generation applications
- Transparent 360-degree view of the extended enterprise through cloud orchestration

Service Definitions

The aim of this EDOC Platform is to provide Enterprise IT managers, business decision makers, system operations staffs, application architects and application developers understand the functions of Cloud Management Platforms (CMPs). How they can be used to operate and manage applications and multiple cloud infrastructures including both on-premises and public cloud service providers.

EDOC helps customers in selecting a best-suited cloud service provider to their needs. While cloud brokerage and cloud management can be considered separate activities, the rise of hybrid IT architectures increases the importance of process harmonization and tools interoperability to meet evolving requirements.

The key features & functionalities that will be enabled for CUSTOMER over EDOC platform are:

- Unified and simplified management of platform to source, fulfill and operate production and non-production environments across multiple IT supply sources i.e. on-premise DC, hosted or Public Cloud hosted
- Unified service catalogues and service blueprints to request for cloud services, containers to be provisioned automatically through self-service portal and reduce time spent deployment design planning
- Faster deployment of services and improve service delivery quality by way of standardization and automation of processes
- Rapid Provisioning with templates and accelerators adhering to defined policies, guidelines and compliances
- Blueprints that bundle Compute, Storage, Network along with Enterprise policies for provisioning service with single click
- Governance framework in a single pane to ensure Security, Access controls, Compliance management, Operations for Day 2
- Upfront view of charges incurred for services, measured, and billed for consumed services with tighter control on provisioned services and ability to de-provision when not needed

- Monitor predictability in workloads and behavior through proactive performance management resulting in improved workload performance and optimal utilization of resources
- Monitoring business services as a “Service Tree” with components and dependency mapping coming from CMDB
- Optimization of day 0 and day 1 services delivered by cutting cycle times and increased levels of utilization
- Enforcement of security & compliance centrally thereby reducing the risk
- Reporting Utilization, Capacity for service improvements, Usage metering and costing details for financial management.

Key differentiators

Some of the key differentiators for EDOC are:

- Marketplace to compare, order and manage - cost and services across multiple clouds
- A visual designer that includes sync-and-discover capabilities to pull all assets (VMs) into a single, architectural view and management standard.
- Estimated bill of IT – determine scenarios based on cost and services provided
- Policy-based services catalog - Pre-configured AWS, Azure, Private Cloud, Oracle, Google and IBM cloud. Can be customized to include only the cloud services that an enterprise wants their employees to consume.
- Enable customers on Hybrid Cloud operations on Day-1
- Multi-tenant dual factor authentication for RBAC
- End to end Cloud Lifecycle Management through single pane of glass for Hybrid IT
- Integration of 3rd party tools via APIs
- Optimization of services across hybrid and multi-cloud providers

Key Benefits

- **Operations:** EDOC platform provides flexibility in selecting the right Tier of operations that ensure with provisioning, automation, monitoring, incidents, or patch management for matching the requirements within the environment. Technical experts on DC and cloud, who are deeply integrated alongside your existing operations team to provide excellent operational assistance
- **Security and Compliance:** EDOC platform with its governance and policies against repository of enterprise guidelines to meet operations and compliance standards. Through automated detection and remediation environments health is maintained.

- **Optimization:** EDOC enables financial and capacity optimization across hybrid cloud environments, any savings identified is notified and with policies defined will be automated to reduce cost without impacting operational services.
- **Innovate:** EDOC is enabled with integrated module of enterprise DevOps platform to help development teams to adopt application and innovation services at easy and quick. EDOC enables DevOps with pre-packed templates, blueprints, via repository bundled with cloud native services to fast track development activities.

Service Description

Wipro's Enterprise Digital Operations Center (EDOC) is built as a platform that provides hybrid cloud managed services for multiple customers (in a shared / dedicated) plug and play model. In addition, EDOC's automation and orchestration capabilities help choose the Cloud model for the right workload, helping to achieve elasticity, enhanced agility, and security, reduced operating costs, better uptime and augmented customer experience with list of services below:

List of services offered	
Monitoring across hybrid cloud	Incident / Change / Problem management
Event Management	Compliance Management
Patch Management	CSP Architect Support
OS upgrade	Golden Image management
Backup / Restore	Network management
Reporting and Dashboard	Managed DR and failover
Provisioning of services / stacks	Migration Capability
Optimization	Cloud Economics
Security Management	Infra as code
IT Service management	DevSecOps

Pricing Overview

Please see the G-Cloud 14 Pricing Document affiliated with this service in the Marketplace.

Governance

A designated Service Delivery Manager along with Service Quality Assurance member provide advisory and assistance across the managed service contract period. Team will ensure to have detailed understanding of services and technology architecture opted for the managed services across environments. SDM and SQA ensure all the best-practices recommendations throughout the development and operations processes are provided along with Technical architects and engineers. Key responsibilities include:

- Lead monthly governance and service review meetings between customers and ops teams.
- Provide details on Operations, security updates for managed environment and opportunities for automation.
- Recommend improvements across opted services (catalog, reports, dashboards etc)
- Update send notifications and help resolve billing and service reporting requests.
- Provide recommendations in the area of financial and capacity utilization and optimization.

Contact and Escalation

EDOC operations support works on customer requests during Business Hours as indicated below depending on the support matrix opted:

Service Windows:

Service Model	Service Window	Type of Support
Silver	8x5 / 16x5 / 24x7	Basic
Gold/Platinum	8x5/ 16x5 / 24x7	Advanced

Service Level Agreement

Priority	Incidents		Service Requests	
	Response(min)	Resolution(hrs)	Response(hrs)	Resolution(hrs)
P1	15*	4*	NA	NA
P2	30*	8*	NA	NA
P3	120	16	NA	NA
P4	240	32	32	48
	*P1 and P2 Incidents are serviced 24X7 (Elapsed hours). Others are serviced during Customer's business hours.			

Supported Configuration

- **Language:** Operations support is available in English.
- **Supported Operating Systems:**
 - Microsoft Windows Server 2019, 2016, 2012 R2
 - Red Hat Enterprise Linux (RHEL) 8.x, 7.x
 - Oracle Linux 7.5 and later minor versions
 - Ubuntu 18.04, 20.04, 21.10
 - CentOS 7.x
 - Amazon Linux 2
 - SUSE Linux Enterprise Server 15 SP0, SP1 and 12 SP4, SP5

Note:

- End of Support (EOS) operating systems have increased security risks.
- EDOC platform agents must be supported on these OS.
 - Agents may include but are not limited to: Monitoring, Backup, Automation, AD, Security.
- Extended support with the operating system vendor should be in place from the enterprise to receive updates
- EOS operating system follows the security controls as defined by enterprises and are monitored and notified for events
- EDOC team will provide recommendations to upgrade OS in the event of it is no longer able to support an EOS operating system

Supported Services

Wipro's Enterprise Digital Operations Center (EDOC) is focused on managing hybrid, multi-cloud environments. It helps customers manage public Cloud involving IaaS and PaaS services alongside the Cloud native services, DevOps, and micro services, Kubernetes, data etc. It helps customers to operate the cloud across public, private, and traditional environments.

- Datacenter services (Compute, Storage, Network)
- Public Clouds (native services include IaaS, PaaS, DBaaS, CaaS, serverless, DevOps)
- Integrations to cloud native services monitoring, optimize, automation, reporting to ensure single pane is provided to enterprise customers

Service scope

Software add-on or extension	Services will be extended to be consumed as a service. But can also be deployed as a standalone service
What software services is the service an extension to	Transformation of services into hybrid cloud. Discovery, Assessment, Migration, adoption of cloud native services across any CSP
Cloud deployment model	<ol style="list-style-type: none">1. Shared service2. Dedicated service3. Hybrid service
Service constraints	EDOC platform is highly scalable platform purpose built for x86 workloads. There will be planned updates and maintenance period, which will be informed 30 days in advance to client. Since the platform is highly available, we do not anticipate any service outage to client.

System requirements	EDOC platform is enabled to be accessed over any popular Browser, over a desktop, laptop, or mobile devices
---------------------	---

User support

Support method	Online ticketing, Email, Call
Support response times	Request Type Severity Classification Response Time Incident Management Priority Level 1 <30 Minutes Priority Level 2 <60 Minutes Priority Level 3 <120 Minutes Service Request Priority Level 1 <4 hours Priority Level 2 <10 hours Priority Level 3 <30 hours
User can manage status and priority of support tickets	Yes
Online ticketing support accessibility	WCAG 2.1 AA or EN 301 549
Phone support	Yes
Phone support availability	24 hours, 7 days a week
Web chat support	Yes
Web chat support availability	24 hours, 7 days a week
Web chat support accessibility standard	Communication access real-time translation (CART)
How the web chat support is accessible	We provide support using Microsoft Teams
Web chat accessibility testing	Tested for translation and support
Onsite support	Yes, available as per engagement and contract
Support levels	EDOC platform is provided in dedicated and shared models in which onsite/offshore combination of support for cloud services is provided for effective operational efficiency. We provide multiple support options to meet customer requirement. Support window options available are 24/7, 8x5, 16x5 and on call. There is at-least 15-25% cost variation in these support models. We also provide account manager to ensure constant touch point with customer for any escalation, new requirement as well as for overall engagement governance.

	<p>Support are provided via following mentioned channels:</p> <ul style="list-style-type: none"> • Service desk • Email • Phone • Live chat
Support available to third parties	Yes

Onboarding and offboarding

Getting started	<p>Customer hybrid cloud services will be onboarded to EDOC platform with simple to host proxy services. As part of transition, we can work with the customer for service assessment and feasibility checks and help to move them to Wipro EDOC platform.</p> <p>User documentation and user manual will be provided Post onboarding, we provide training which can be onsite or online depending upon the requirement and scope. Complete transition period is documented apart from routine day-to-day operation.</p>
Service documentation	Yes
Documentation formats	HTML / PDF
End-of-contract data extraction	<p>Wipro will help remove data and service information from the EDOC platform and provide the same in standard format.</p> <ul style="list-style-type: none"> - CSV - Database dump of current usage
End-of-contract process	<p>Wipro contractually commits to specific processes when a customer leaves a cloud service, or the contract expires. This includes</p> <ul style="list-style-type: none"> • Off-boarding customer service from platform • Deleting customer data from systems under platform • This process has a timeline to be agreed during contract

Using the service

Web browser interface	Yes
Supported browsers	All popular browsers
Application to install	No

Designed for use on mobile devices	Yes
Differences between the mobile and desktop service	All activities performed from the desktop are available on mobile.
Service interface	Yes
Description of service interface	Web Interface
Accessibility standards	WCAG 2.1 AA or CART on few of the modules
Description of accessibility	Chat, online captions, Transcriptions
API	Yes
What users can and can't do using the API	Service provisioning and automation Service consumption reports Service health, performance, utilization
API documentation	Yes
API documentation formats	HTML
API sandbox or test environment	Yes
Customisation available	Yes
Description of customisation	<ul style="list-style-type: none"> - Service Offerings and Blueprints can be customized for users - Reports and performance views - Consumption dashboards

Scaling

Independence of resources	EDOC platform is highly available and scalable. We always have the buffer capacity and leverages real time analytics to ensure there is no performance impact to end users in case of surge in demand from another customer.
---------------------------	--

Analytics

Service usage metrics	Yes
Metrics types	<p>Compute, Storage, Network, Operating system, Applications, Middleware, Databases, End user experience</p> <p>Public Cloud services IaaS, PaaS, CaaS, DBaaS, Cloud native services</p> <p>Monitoring the</p>

	availability performance capacity utilization network traffic services, patches, hotfixes, vulnerabilities Event management Tracking, alerting, correlate, AI based analytics, notification Run automation workflows to remediation issues Notify stakeholders on the events Perform root cause analysis
Reporting types	Real-time dashboards Regular reports Reports on request

Resellers

Supplier type	Managed service provider, not a reseller
---------------	--

Staff security

Staff security clearance	Other security clearance
Government security clearance	Up to Security Clearance (SC)

Asset protection

Knowledge of data storage and processing locations	Yes
Data storage and processing locations	<ul style="list-style-type: none"> United Kingdom European Economic Area (EEA) EU-US Privacy Shield agreement locations
User control over data storage and processing locations	Yes
Data sanitisation process	Yes

Data sanitisation type	Deleted data can't be directly accessed
Equipment disposal approach	A third-party destruction service

Data importing and exporting

Data export approach	Wipro EDOC provides secured authenticated access to users for data export which will be enabled within the enterprise network
Data export formats	CSV / Json
Data import formats	CSV / Json

Data-in-transit protection

Data protection between buyer and supplier networks	<ul style="list-style-type: none"> • TLS (version 1.2 or above) • IPsec or TLS VPN gateway • Legacy SSL and TLS (under version 1.2)
Data protection within supplier network	<ul style="list-style-type: none"> • TLS (version 1.2 or above) • IPsec or TLS VPN gateway • Legacy SSL and TLS (under version 1.2)

Availability and resilience

Guaranteed availability	<p>A standard set of Service Levels will be applied for the Service.</p> <ul style="list-style-type: none"> • Platform availability: 99.95%. • Single Datacentre 99.9% • Dual Datacentre 99.95%.
Approach to resilience	<p>EDOC platform is hosted in public clouds with no single point of failure to ensure no service outage due to single module or platform disturbance or component failure. All components within the platform such as compute, storage, databases, network to name few are redundant to ensure resiliency. Data is replicated across regions to ensure business continuity in case of disaster.</p>

Outage reporting	Each customer gets RBAC based dashboard to know the health of their environment. This dashboard is real time and provides detailed information of customer workloads, service consumption, utilization, service cost, vulnerabilities, compliance, and optimization recommendations.
------------------	--

Identity and authentication

User authentication needed	Yes
User authentication	<ul style="list-style-type: none"> • 2-factor authentication • Public key authentication (including by TLS client certificate) • Identity federation with existing provider • Username or password
Access restrictions in management interfaces and support channels	User access to IT infrastructure and applications is granted based on an individual's job responsibilities and business requirements which is described as Role Based Access Controls; on a "need to access" and "need-to-know" basis. Access restriction is role based and the authorization will be obtained as defined in the access control matrix.
Access restriction testing frequency	At least every 6 months
Management access authentication	<ul style="list-style-type: none"> • 2-factor authentication • Public key authentication (including by TLS client certificate) • Identity federation with existing provider • Username or password

Audit information for users

Wipro captures attributes of user activity as below:

- As a part of SOC1 and SOC2 audits done by 3rd party, the following are covered:
- RBAC policies
- Resource On/off board
- Data retention if required must be planned and on what tools/infra/applications

Access to user activity audit information	Stakeholders to receive audit information on a regular basis
How long user audit data is stored for	Between 6 months and 12 months
Access to supplier activity audit information	Stakeholders to receive audit information on a regular basis
How long supplier audit data is stored for	Between 6 months and 12 months
How long system logs are stored for	As per contractual agreements

Standards and certifications

- For tools, SOC1, SOC2 (type 2) and HIPPA
- For locations: SOC1, SOC2 (type 2), HIPPA and ISO 27000

ISO/IEC 27001 certification	Yes
Who accredited the ISO/IEC 27001	UKAS Management Systems
ISO/IEC 27001 accreditation date	10/9/2023
What the ISO/IEC 27001 doesn't cover	NA
ISO 28000:2007 certification	No
CSA STAR certification	Planned as below: PCI DSS and CSA are for Year 2022, CCM - 2023
PCI certification	Planned as below: PCI DSS and CSA are for Year 2022, CCM - 2023
Who accredited the PCI DSS certification	NA
PCI DSS accreditation date	NA
What the PCI DSS doesn't cover	NA
Other security certifications	Yes
Any other security certifications	<ul style="list-style-type: none">• FIPS 140-2 Compliant• Common Criteria Certified

	<ul style="list-style-type: none"> • ISO/IEC 27001:2013 • NIST SP 800 Series • PCI DSS V3.0
--	--

Security governance

Named board-level person responsible for service security	Yes
Security governance certified	Yes
Security governance standards	<ul style="list-style-type: none"> • SOC1 (SSAE-18), • SOC2 (type 2) • HIPPA
Information security policies and processes	<p>Wipro follows Open Web Application Security Project (OWASP) methodology to verify if the service/ platform/ application is exposed to the Top 10 OWASP vulnerabilities. Web Applications are tested for the presence of the OWASP Top 10 vulnerabilities:</p> <ul style="list-style-type: none"> ♣ Injection ♣ Cross-Site Scripting (XSS) ♣ Broken Authentication and Session Management ♣ Insecure Direct Object References ♣ Cross-Site Request Forgery (CSRF) ♣ Security Misconfiguration ♣ Insecure Cryptographic Storage ♣ Failure to restrict URL access ♣ Insufficient Transport Layer Protection ♣ Un-validated Redirects and Forwards <p>Wipro uses a combination of business impact and ease of exploitability in defining the severity of the vulnerabilities. Appropriate mitigation techniques are implemented to fix the vulnerabilities before the applications are promoted to the production environment. Final round of verification is done after the application goes live to ensure the security vulnerabilities do not resurface in production environment.</p>

Operational security

Configuration and change management standard	Conforms to a recognised standard, for example SOC1 (SSAE-18), SOC2 (type 2) and HIPPA
Configuration and change management approach	Wipro's configuration management process includes building a CMDB with required CI relationships mapped out. The process provides visibility on the interdependencies between the CIs as well as the lifecycle of these CIs. Data feed from a discovery tool is used to populate CMDB and then track CI components through lifetime for data accuracy. Any configuration change in the environment goes through a formal change management process that includes initiating RFC, going through CAB approvals, and executing with rollback plan in place. All changes are assessed for potential security impact. Corresponding CIs are updated post-successful completion of a configuration change.
Vulnerability management type	Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402
Vulnerability management approach	<ul style="list-style-type: none"> • It is mandatory to conduct VA scans for entire Wipro infra devices in a year. All Critical Enterprise infrastructure and devices in DMZ are scanned every month. On a yearly basis a Penetration Testing is performed by third party • Critical ,Important, Moderate & low patches are updated Within 2,3,5 & 10 days respectively from approval. • The information related to patches are obtained from authorized and genuine sources such as, but not limited to, Vendor

	mailing lists and websites, Security Alert announcements or bulletins like SANS & CERT and Virus advisories.
Protective monitoring type	Conforms to a recognised standard, for example CSA CCM v3.0 or SSAE-16 / ISAE 3402
Protective monitoring approach	<p>We have SIEM (Security Incident and Event Monitoring) tool in place which monitors all major network and select compute devices for any suspicious activity matching its comprehensive database of suspicious traffic patterns. Alerts get triggered and our 24x7 SIEM teams investigate into these alerts. They cut out the false positives and focus only on the suspicious cases. They then log a ticket and investigate further based on standard operating procedures.</p> <p>Wipro's Information Security Incident Management Policy/Process is published for centralized reporting, managing and escalating logical and physical security incidents/violations by Employees, Contractors, Trainees, and Clients working in Wipro premises.</p>
Incident management type	Conforms to a recognised standard, for example, CSA CCM v3.0 or ISO/IEC 27035:2011 or SSAE-16 / ISAE 3402
Incident management approach	<p>Wipro's incident management process includes incident identification, logging, categorisation and prioritisation, diagnosis, major incident review, updates/escalations, tracking, resolution/recovery, closure, and reporting. It uses strong event aggregation, correlation, and suppression to filter noise and treat common events. Users can either report incidents by reaching out to their service desk or through self-service portal made available to them. Alternatively, the common monitoring team will also raise an incident proactively based on qualified alerts received. Wipro uses ServiceNXT™ Smart View for single pane of glass reporting. The tool provides dashboard and</p>

	pulls out incident feeds from the ITSM to provide incident reports.
--	---

Public sector networks

Connection to public sector networks	Yes
Connected networks	<ul style="list-style-type: none"> • Public Services Network (PSN) • Police National Network (PNN) • NHS Network (N3) • Joint Academic Network (JANET) • Scottish Wide Area Network (SWAN)

Pricing

Price	£45 an instance a month
Discount for educational organisations	No
Free trial available	No



About Wipro Limited

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs. Leveraging our holistic portfolio of capabilities in consulting, design, engineering, and operations, we help clients realize their boldest ambitions and build future-ready, sustainable businesses. With 250,000 employees and business partners across more than 60 countries, we deliver on the promise of helping our clients, colleagues, and communities thrive in an ever-changing world.

