Service Desk Scope & Metrics

Key Activity Drivers	
Percentage	**Activity**
56%	Applications & Data (Exchange, Messaging, Finance, SAP, SFDC, O365)
26%	Accounts & Access (O365, Messaging, Service-Now, SaaS apps)
18%	Salesforce.com (Business operations, CloudPC, Apollo, Data Center)

Expected SLAs		
Severity	**Response**	**Resolution**
• P1	15 minutes	8 hours
• P2	1 hour	24 hours
• P3	6 hours	36 hours
• P4	8 hours	48 hours

Daily Average Workload Drivers	Percentage of team activity	To note: Response times are driven by SLA
• P1	1%	
• P2	51%	
• P3	37%	
• P4	11%	

Below datapoints are specific to SLA types when handled by the agents. Ticketing SLAs must still be followed in lieu of below.

Service Level Agreements	Performance Target	Jun	Jul	Aug	Sep	Oct	Nov
Call ASA (Average Speed of Answer)	90% in 120 seconds	96.20%	92.90%	94.00%	96.40%	96.80%	98.40%
Call Abandonment Rate	< 10% in 60 seconds	0.80%	0.80%	1.30%	1.50%	0.60%	1.10%

KPIs	Performance Target						
Web ticket Response Time	90% in 90 minutes	98.00%	97.90%	98.30%	96.30%	96.40%	96.80%
Chat Response SLA	90% in 120 secs	97.40%	96.00%	96.80%	98.00%	97.80%	98.10%
Chat Abandonment Rate	< 10% in 60 seconds	2.60%	0.20%	2.00%	1.80%	1.20%	0.90%
Customer Satisfaction	92% MAN factors	100.00%	99.30%	100.00%	100.00%	100.00%	100.00%
FCR% (First Contact Resolution)	90%	99.60%	99.50%	99.00%	98.90%	99.30%	99.70%
FLR (First Level Resolution)	50%	56.90%	56.00%	58.30%	53.30%	52.60%	58.90%
Resolution of Incidents (P2)	90% in 4 hours	97.10%	97.80%	97.40%	94.60%	100.00%	95.80%
Resolution of Incidents (P3)	90% in 8 hours	95.40%	97.00%	98.30%	92.50%	94.10%	93.90%
Resolution of Incidents (P4)	90% in 8 hours	99.10%	98.90%	98.50%	98.20%	97.50%	96.60%
Time to Resolve Requests (P3)	95% in 1 day	99.60%	99.60%	100.00%	99.70%	99.40%	99.50%
Time to Resolve Requests (P4)	95% in 2 days	100.00%	100.00%	100.00%	99.90%	100.00%	100.00%
Quality Audit Score (Call / Chat / Ticket)	90%	90.80%	96.80%	94.40%	94.50%	95.60%	92.90%

KPIs	Performance Target	Jun	Jul	Aug	Sept	Oct	Nov
Chat Volume	-	911	1149	1063	944	885	888
Abandoned Chats	-	24	83	21	17	11	8
Chat Average Wait Time	90 seconds	18	28	20	22	26	15
Chat Average Handle Time	865 seconds	606	614	637	643	629	595
Call Average Handle Time	10 minutes	9:21	8:59	9:18	10:16	10:28	9:36
Misrouted Tickets	< / = 2 per month	0	0	0	0	0	0
L2 feedback	< / = 8 per month	0	0	0	0	0	2
Attrition	-	0.00%	0.00%	0.00%	6.30%	0.00%	0.00%

Service Desk Key Skills

Skills required/certifications
Applications/Platforms Resolve basic ("Level 1") technical issues:
·   O365 applications (all including PowerBI and Visio)
·   Active Directory/Azure AD
·   Zoom client
·   SharePoint
·   Print Server
·   Microsoft Authenticator
·   Duo
·   SaaS installations
·   Mobility Platform

Basic Responsibilities
·   Password resets and user account setups.
·   VPN, Multifactor applications account admin and access troubleshooting.
·   Troubleshooting of basic computer issues.
·   Troubleshooting of O365 issues.
·   Access requests from users for application, database, security group, and shared drives.
·   Software installations/uninstallation for end users.
·   Assign any technical issues requiring on-site support (Level 2, 3 and/or appropriate Service Support teams)
·   Create / publish knowledge articles for Service Desk in Autodesk knowledge management system.

· Strong command of written and spoken English.

Incident Manage Scope & Metrics

Incident Management currently consists of a Cloud Services Operations Center (CSOC) and an Enterprise Operations Center (EOC)

Two separate teams performing similar functions.   The Scope and Metrics are listed below.

**Cloud Services
Operations Center
(CSOC)**
CSOC provides the following services for Autodesk Cloud Products and Services:

Autodesk cloud services support - Level 1 support of autodesk cloud services administration and maintenance

S**cope**: 24x7x365 Coverage for the following:

Current Level 1 Support Services
Monitoring and Event Management – Monitoring significant state changes for cloud services typically in the form of alerts or notifications which require action or possibly Incidents to be created. Full support of all industry standard monitoring tools and metrics. Monitoring will be addressed under the general categories of 1) performance 2) service 3) capacity

Incident Management – Management of the incident lifecycle with the primary goal of returning an IT Service to operational state for users as quickly as possible. Includes running basic first responder triage and break fix processes and procedures. Acting as Major incident Commander for customer impacting service disruptions

Service Request Management – Management of the request lifecycle with the primary goal of executing a known documented procedure not related to an incident.

Documentation/Run Book Management – Document, publish, and maintain documentation and procedures associated with key service components. Review and update quarterly or as necessary with client. Includes creation of all documentation appropriate to support or assist in delivery of Services herein

o Update and maintain documentation and procedures associated with key service components.
o Administer edits and updates for all relevant Process and Run Book documentation, using an agreed revision review process, for all Autodesk approved changes.
o Manage the document the refresh process to ensure all documentation is regularly updated, and any documents that are not being used are retired per Autodesk process.
o Includes creation of all documentation appropriate to support or assist in delivery of Services herein.
o Publish new or updated SOP/Run Book documentation upon approval from Autodesk.
o Where a gap in the Run Book is identified as the reason why first touch resolution was not possible, supplier shall be responsible for identifying the missing information, clarifying and updating the Run Book in order to improve the SLO for first touch resolution.

Current Level 2 Support Services

Enhanced Incident Troubleshooting and Resolution Services
o L2 incident troubleshooting and resolution support of all AWS Cloud environment services and Autodesk services that have been on-boarded to the CloudOps SOC support team. Utilize the AWS console and available tools to administer, troubleshoot, and resolve cloud environment and service issues.
o Follow AWS Standardized or Autodesk Standardized troubleshooting and resolution approaches per Run Book.
o Reduce invalid alerts by providing tuning to Cloudwatch, Cloudtrail and other tools provided by Autodesk to ensure non-actionable alerts are reduced.
o Provide reports on Alert metrics and reductions including overall efficiencies gained. (e.g. HeatMaps, Metric Alerts mapped to primary concerns within Autodesk Cloud environment)
o Provide necessary Incident and technical information input to the Autodesk Incident to Improvement (I2I)
process

Monitoring Administration Services:

oAdminister edits and updates for all relevant monitoring administration documentation, using an agreed revision review process, for all Autodesk approved changes.
 o Add and remove managed nodes/hosts/end-points in the environment
 o Work with Autodesk SME's and staff to understand and define the standard alert and monitor set for each device or end-point type
 o Make recommendations for tuning of non-Actionable Alerts in order to reduce them. If approved by Autodesk, Supplier will manage implementation of any tuning monitoring configurations.
 o Administer changes and refinements in defined alerts – thresholds, settings, configuration entries
 o Keep the services configurations current and tuned to minimize false alerts.
 o Configure new standard host checks or service checks into the environment
 o Administer notification settings, globally, per user, per team, per host, per end-point, etc.
 o Administer monitoring configuration changes
 o Coordinate with Autodesk SME's for threshold changes through Autodesk change control
 o Observe all current Autodesk cloud infrastructure change management practices and ensure any necessary changes are implemented into Supplier processes.
 o Administer monitoring suppression as needed as directed by Autodesk
 o Provide Analysis and Reporting based on off-the-shelf capabilities of tool(s) in scope
oRun and administer standard reports on monitoring performance
 o Perform regular reviews of alerts for trends and patterns

Expected Incident (INC) SLA			
	SLA (Minutes)	SLA (Minutes/Hours)	SLA (Minutes/Hours)

		Mean time to respond (Mttr) Time to respond to an Incidentreceived directly from monitoring into Autodesk's ServiceNowsystem. SLA is aggregated monthly and is unmet if falls under 92%	Mean time to communicate (Mttc) Average time elapsedbetween the time an Incident is created within the ServiceNow system, and when the initial Service Bulletin is issued.This SLA will be considered unmet if aggregate metric falls below 92% per month	Mean time to communicate to customers (Mttc) Average time elapsedbetween the time an Incident is created ServiceNow system, and when the initial Outage notification i autodesk health dashboard.This SLA will be considered unmet metric falls below 92% per month
			Initial Communication	
·	Sev 0 (urgent)	5 minutes	20 minutes	15 minutes
·	Sev 1 (critital)	10 minutes	20 minutes	15 minutes
·	Sev 2 (major)	15 minutes	20 minutes	15 minutes
·	Sev 3 (normal)	20 minutes	N/A	N/A
·	Sev4 (Low)	35 minutes	N/A	N/A
			Ongoing Communication	Ongoing Communication
			Sev 0 30 Minutes	Sev 0 30 Minutes
			Sev 1 60 Minutes	Sev 1 60 Minutes
			Sev 2 4 Hours	Sev 2 4 Hours
			Sev 3 N/A	Sev 3 N/A
			Sev 4 N/A	Sev 4 N/A

Service Request (SR) SLA	
	SLA (Minutes)
	SR Mean time to respond Average time in business hours to acknowledge a pre-defined documented service request received directly into Autodesk's

	ServiceNow. Measured from the time the service request is entered into Service Now
Normal	12 hours
Low	24 hours

Resolution Service Level Objectives ("SLOs")		
Metrics	**Description**	**SLO**
First touch Resolution Rate	Count of all incidents resolved by Supplier with no escalation divided by total count of all incidents. If metric falls below this target level, Supplier will provide to Autodesk a detailed report listing out issues related to falling below this target and an improvement plan to reach this target.	Current target % 25% -

	Tools	Ticketing system /Contact Channels
Zoom	New Relic	Phone
ServiceNow	DataDog	Email
Jira	Dynatrace	Chat (Slack)
Confluence	Sensu	Monitoring alerts
Slack	AWS furnished tools	
Divvycloud	Autodesk proprietary tools and automations	

Key Metrics

Key Activities (Feb 1, 2022 - Jan 31, 2023)	Types of cases	
80%	ServiceNOW Incidents (non custoer impacting)	
16%	Requests & ruboook reviews	
4%	High Sev Incidents +MCIR (customer impacting)	MCIR=Major Customer Incident response

Incident Management Metrics (Feb 1, 2022 - Jan 31, 2023)		
Daily Average Workload Drivers	**Percentage of team activity**	**To note: Response times are driven by SLA**
· Sev 0	0.10%	100% SLA compliance
· Sev 1	0.50%	100% SLA compliance
· Sev2	2%	100% SLA compliance
· Sev 3	97.30%	98% SLA compliance
· Sev 4	0.1% %	100% SLA compliance

Service Request Management	
Normal	336 service onboarding Jiras
Low	

Annual Volumes	
Type	**Volume**
Incidents	7125

Current Enterprise Operation Center Activities (EOC)

The Enterprise Operations Centre (EOC) is the central point of escalation for all Major Incidents for the Enterprise Systems and Experience (ESE) Team (ESE =Autodesk

EOC Scope –
S**cope**: 24x7x365 Coverage for the following:

Current EOC/SOC activities:

Initial Triage of incidents

a. Eye On Glass Activities (examples as in current environment but not limited to the list mentioned thereof.)
b. Alert monitoring
c. Verifying false positives
d. Catch and dispatch
e. Escalation as appropriate
f. Identify Support Group or POC for undefined, ownerless issues

Incident Management (Major Incident Management & P1):

a. Coordinating with service teams for MI resolution at the earliest
b. Drive MI to closure
c. Communicate to stakeholders and impacted users within defined SLA
d. Responsible to Identify the related MI tickets and attach related incidents to parent ticket.
e. Post, update and validate Service Health Dashboard notifications.
f. Maintain Critical Applications List along with respective owners & escalations details on regular basis
g. Maintain Facilities Contact List
h. Follow up with Incident Manager/Support Team to complete post Major Incident data in respective tools (ServiceNow) within a stipulated timeline.
i. Draft MI timeline, Track Major Incident learnings and publish to management.
j. Compliance to MI closure checklist (Example ensure Monitoring Alerts tickets details are captured)
k. Maintain Major Incident Management documents (FAQ, Do's and Don'ts and Knowledge Articles)
l. Distribution List maintenance
m. Ensure Appropriate Escalation matrix is followed for MI, P1 & Vendor related issues.
n. Drive Weekly major Incident management (CAB) Governance - Internal Governance / Executive Leadership Governance
o.Provide bridge support and coordinate with other support groups, engineers, or SMEs
p. Report Services Health Dashboard on Monthly basis to management.
q. Track and report on Major Incidents weekly and monthly
r. Trend Analysis of MI's and reporting
s. Report on DES EDC Incident Management SLA achievement on Weekly basis
t. Report on DES Teams Aged Tickets and P1/P2/P3/P4 SLAs on a Monthly basis
u. Monitoring recalibration coordination for Incident CI clean-up
v. Monitor Major Incident-related Power BI dashboards to ensure data is synced monthly with ServiceNow
w. Identify process improvement for major incidents

Problem Management:

a. Coordinate and ensure Cause Analysis (CA), Root Cause Analysis (RCA), Future Avoidance (FA) are conducted as per defined SLO/ SLA.
b. Regularly track FA Implementation and escalate as appropriate
c. Track and report on Problem Tickets weekly and monthly.
d. Identify & suggest continuous Process Improvements for MI & PM areas.

EMR Activities
a. Post announcements and send communications to impacted users
b. Attend EMR Walkthrough and review scope
c. Track potential EMR related issues and connect with possible Major Incident events

Planned Network and Power Maintenance activities
a. Coordinate and track activities with all stakeholders
b. Communicate to impacted users

Non-Major Incident and other Maintenance Communications
a. Draft, send for review and release communications
b. Draft, post and send for review banners in Autodesk One page

SSL Certificate Management
a. Approval
b. Basic troubleshooting and user assistance

Tool sustenance
a. Ensure tools and supported services are running
b. Monitor policies and procedures

Major Customer Incident Response (MCIR)
a. Provide bridge support and coordinate with other support groups, engineers, or SMEs
b. ServiceNow Ticket flagging and validation of Business Service for MCIR

		Major Incidents	
SLAs/KPIs	**Details**	**Description**	Target
SLA	Response time to Events	Time from receiving first event to the action taken (Clear, Acknowledge, Open Incident) based on Priority	<15 Minutes
SLA	Major Incident Initiation & Notification Time	Time from Major Incident declaration to time Major Incident Alert was sent	<10 Minutes
KPI	Bridge Request Response Time	Time from Major Incident Declaration	<2 Minutes
SLA	Data Gathering Completion	Time from MI Alert sent to completion of Data Gathering from Incident Managers.	<15 Minutes
KPI	Service Bulletin Release	Time from Major Incident Declaration to time Service Bulletin was sent	<20 Minutes
KPI	FIR	Creating FIR for the MI's	Within 4 hours of MI closure

KPI	Major Incident Performance Feedback	Survey sent to Service Owners after each Major Incident	Must MEET or EXCEED expectations
SLA	Voice of customer	Quarterly Survey and Individual MI Survey to the Service Managers, Owners & users	Must MEET or EXCEED expectations
KPI	CSI	Analysis & Process Improvement	2/quarter
SLA	Governance Meetings with Auto Desk	Regular Governance Meeting with Leadership Team of Autodesk	Fortnightly / Monthly / Quarterly
SLA	New Hire Training	Ensure New Joinee KT + Training by Senior EOC Team members	Completed within one month of onboarding

Time to Resolve Requests - 72 Hours	
EOC-Incident-P2-Response (20 mins)	
EOC-Incident-P3-Response (45 mins)	
EOC-Incident-P1-Response (10 mins)	

Incident+ Task (Overall Ticket) "Low Volume")			
SLA/KPI	**Description**	**Target**	**Benchmark**
			One MIMTD
Response Time	Response to ticket	30 minutes	98%
Resolution Time	Ticket Resolution	60 minutes	95%
FLR	First level resolution (In scope)	85%	

Methods of communication

MS Outlook Emails / Slack / MS Teams / EverBridge

Current Tools Environment –	
• Service Health Dashboard – Service availability dashboard	• Wiki – Knowledge Base
• ServiceNow – Ticketing Tool	• Jira – Service Planning
• Digicert/Venafi – SSL Certificate	• Pager Duty - Major Incident alert
• Site Status – Network Devices Monitoring Tool	• Everbridge - Major Incident alert
• Catchpoint – Monitoring	• Slack – Major Incident messaging tool
• Dynatrace – Monitoring	• Zoom/MS Teams – Messaging Tool
• BigPanda – Monitoring	• Chatter – Messaging tool for EMR
• Grafana – Monitoring	• OneDrive
• DPE Site Status - Monitoring	• AlertBot – Slack Bot for Major Incident communication
• Serenity - Report Dashboard	• BT Conferencing – Conferencing Tool
• Power BI - Report Dashboard	

Key Metrics

Key Activities (Types of cases and the percentage)	
12%	Planned Power Maintenance
17%	Network outage in specific countries/GEO (not MI)
All	Incidents (including major)

56 out of 452 planned power maintenance were coordinated by EOC

77 out of 452 network outage were coordinated by EOC

15 - Major Incidents managed by EOC (All Major Incidents are managed by EOC)

2087 - Incidents assigned to EOC and later reassigned by EOC to the specific resolver groups/assignment groups. This data is for the period of Feb'22 – Jan'23
452 - Requests coordinated by EOC – Communication (Focused, Network, Infosys Banner, EMR Communication), Bridge Request, Power Maintenance and Certificate R
5079 - Eye on Glass (EOG) – RITM's created by EOC to capture the effort of the Follow up's performed by EOC through ServiceNow along with Monitoring.

EOC Annual Volumes Incidents and Requests (Feb'22 – Jan'23)	
Type	**Volume**
Incidents	2087
RITM (Eyes on Glass EOG)	5079
Major Incidents	15

SLAs/KPIs	Details	Major Incident Description	Target
SLA	Response time to Events	Time from receiving first event to the action taken (Clear, Acknowledge, Open Incident) based on Priority	<15 minutes
SLA	Major Incident Initiation & Notification Time	Time from **Major Incident declaration** to time Major Incident Alert was sent	<10 minutes
KPI	Bridge Request Response Time	Time from Major Incident Declaration	< 2 Mins

SLA	Data Gathering Completion	Time from MI Alert sent to completion of Data Gathering from Incident Managers.	<15 Mins
KPI	Service Bulletin Release	Time from Major Incident Declaration to time Service Bulletin was sent	<20 Mins
KPI	FIR	Creating FIR for the MI's	Within 4 hours of MI Closure
KPI	Major Incident Performance Feedback	Survey sent to Service Owners after each Major Incident	Must MEET or EXCEED expectations
SLA	Voice of customer	Quarterly Survey and Individual MI Survey to the Service Managers, Owners & users	Must MEET or EXCEED expectations
KPI	CSI	Analysis & Process Improvement	2/ Quarter

SLA	Governance Meetings with Auto Desk	Regular Governance Meeting with Leadership Team of Autodesk	Fortnightly / Monthly / Quarterly
SLA	New Hire Training	Ensure New Joinee KT + Training by Senior EOC Team members	Completed within one month of onboarding

Incident+ Task (Overall Ticket) "Low Volume hence overall measurement)

SLAs/KPIs	Description	Target	Benchmark
			One MI-MTD
Response Time	Response to ticket	30 Minutes	98%
Resolution Time	Ticket Resolution	60 Minutes	95%
FLR	First level resolution (In scope)	85%	

Incident Management Key Skills

CSOC current skillsets required:
AWS certification
Minimum of three years of system administration experience in production cloud/(Software/Platform/Software) as a service environments
Strong communication, customer service and interpersonal skills *written and spoken English
Cloud and on-prem knowledge to perform lower-level engineering tasks

Skills to include:
Resource tuning and optimization
Troubleshooting and operational maintenance of larger-scale cloud deployments
Incident management and root cause analysis for high severity incidents/outages
Ability to synthesize incident facts into customer relevant updates
Familiarity with sys admin tools In Windows and Linux
Understanding of Infrastructure as Code concepts
Production experience with cloud platforms and technologies
Comprehension of Code Revision Control
Technical knowledge of network technologies and protocols
Proficiency writing scripts in Python, Bash, Powershell
Certifications: One or more of the following: GCP, AWS, Azure, or IBM Cloud, CompTIA A+, Network+, Security+, or similar network certification (CCNA, PCNSA, etc)
Managerial experience for people managers

Other skills requirements
FedRamp High resources - requirement for US Persons starting in 2025

Applications/Platform Proficiency
AWS
Microsoft Suite
Observbility tools - Splunk, datadog, newrelic, catchpoint..etc

EOC current skill sets required
Very Good Communication Skills (written & Spoken English)
EOC Lead / Incident Co-ordinator - 10 plus years of experience / ITIL Certification

Incident Co-ordinator - Minimum 5 Plus experience in Incident Management, Major Incident Management & Problem Management
Should have very good understanding of overall ITIL Service Management
ITIL Certification / Should have experience working with Global Customers
Should have basic or good understanding of IT Technical terminologies
Managerial experience for people managers

Applications/Platform Proficiency
Microsoft Suite
AWS