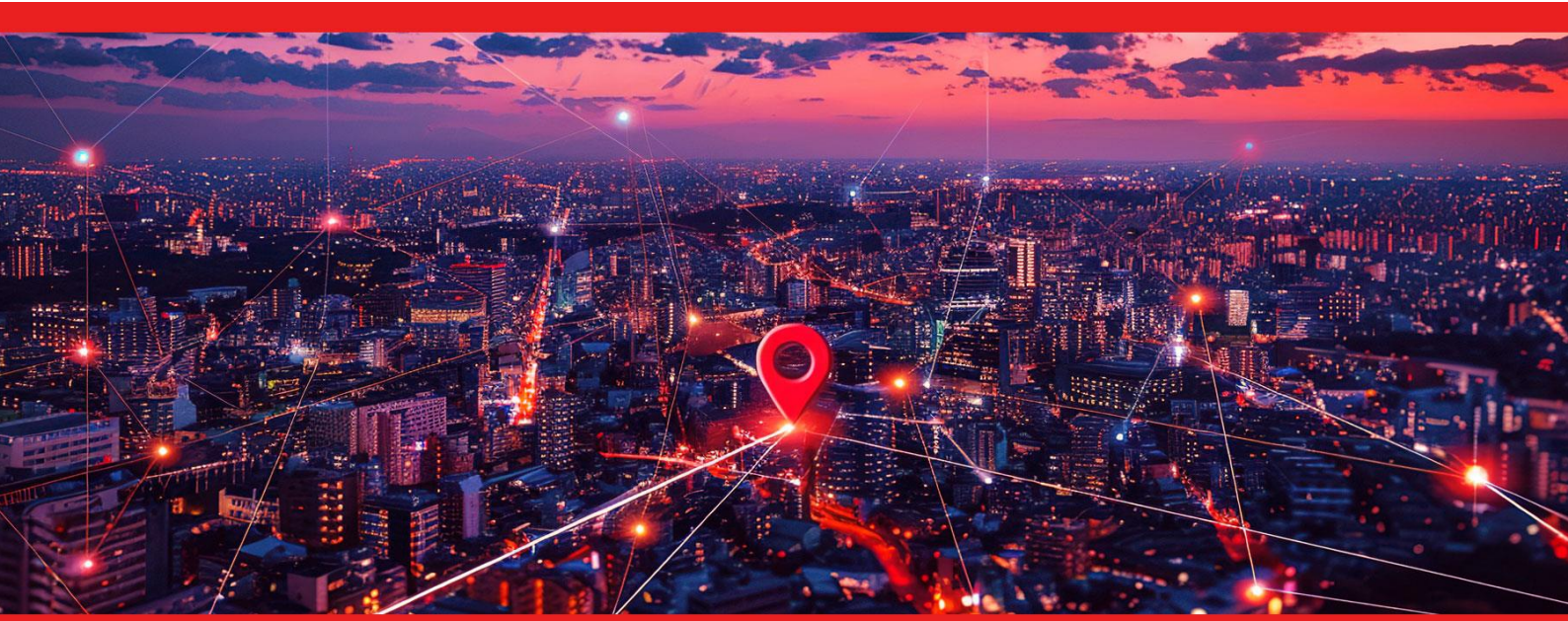# UC Manage

Service Description

IMS098 V1.1

Copyright

The information contained in this document is the property of Koris365, a trading name of Koris365 Central Limited, Koris365 South Limited, Koris365 North Limited and Koris365 Ireland Limited. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means; electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Koris365. Legal action will be taken against any infringement.

Confidentiality

All information contained in this document is provided as Commercial-in-Confidence. It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing. These obligations shall not apply to information which is published or becomes known legitimately and independently of either party.

Legal Entities

Koris365 is the trading name for the following legal entities:

Koris365 North	Koris365 Central	Koris365 South	Koris365 Ireland
Unit 15 Pavilion Business Park, Royds Hall Lane, Leeds, LS12 6AJ	8 Grovelands, Boundary Way, Hemel Hempstead, HP2 7TE	8 Grovelands, Boundary Way, Hemel Hempstead, HP2 7TE	Trinity House, Charleston Road, Ranelagh, Dublin 6, Ireland, D06 C8X4
Company Reg No: 02276852	Company Reg No: 06215347	Company Reg No: 07709017	Company Reg No: 727514
VAT No: 631921945	VAT No: 912862719	VAT No: 927332425	VAT No: IE04083398OH

IMS098 V1.1

Contents

1 Summary

1.1 Overview

UC Manage provides customers with the day-to-day systems administration of their UC infrastructure such as the creation of users, addition of devices, and routine configuration changes. UC Manage is not a standalone service, its purpose is to form a comprehensive managed solution when combined with UC Resolve.

1.2 Features

UC Manage provides:

- Management of UC infrastructure including:
  - Cisco Unified Communication Manager
  - Cisco Unified Presence
  - Cisco Unity Connection
  - Cisco Unified Contact Center Express
  - Cisco Expressway
  - Cisco Unified Attendant Console
  - Cisco UCS server
  - Cisco Cube
  - Skype for Business
  - Microsoft Teams
  - Ribbon SBC
  - EICC
  - QMS
  - Red Box Recorder
- Management of backups including:
  - Cisco Unified Communication Manager
  - Cisco Unity Connection
  - Cisco Unified Contact Center Express
  - Cisco Cube (customer must also have UC Monitor)
  - Skype for Business
  - Ribbon SBC
  - EICC
  - QMS
  - Red box Recorder
- Monthly service reporting
- Monthly exception reporting (customer must also have UC Monitor)
- Quarterly lifecycle reporting (customer must also have UC Monitor)

1.3 Suitable Customers

Any organisation with a UC infrastructure can benefit from UC Manage including:

- Organisations with limited, or no inhouse IT resource
- Organisations struggling to manage complex IT infrastructures
- Organisations looking for more support and guidance towards their IT roadmap
- Organisations not getting value from their existing management solution
- Organisations looking to remove the day-to-day burden of routine administrative tasks
- Organisations requiring management ownership and accountability

1.4 Pricing

UC Manage pricing is based on the number and type of devices, services, and users to be managed.

2 Detailed Service Description

2.1 Pre-requisites

To provide Manage, Koris365 will require the following:

- UC Resolve
- The customer must provide a comprehensive list of devices to be managed complemented with a good standard of documentation
- The supported system must be in a good operational state, with best-practice configuration and good vendor support status
- The customer must have out of band management cards configured (e.g., CIMC)
- The customer must provide relevant company detail such as quantity of users, locations, hours of work
- The customer must provide permanent remote access
- Koris365 must be provided with administrative accounts for the systems to be managed
- The customer will need to provide at least one named decision maker
- The customer must specify at least one person who is able to raise tickets (typically limited to IT personnel)

2.2 Onboarding Procedure

1. Koris365 will work with the customer to identify the technical documentation required
2. Customer provides Koris365 with technical documentation, including:
    a. Any applicable administrative accounts and systems access
    b. Network diagrams
    c. Configurations
    d. Application ID's
3. A full audit of the Customer's UC infrastructure may be compulsory depending on the level of information available. The audit is not included in MAC and will be an additional cost to the Customer.
4. Koris365 will work with the customer to complete the Services Onboarding form. The purpose of this document is to collect and support the gathering of necessary information to provision the service, including:
    a. Details of customer contacts, escalation paths, and site locations

IMS098 V1.1

b. Overview of the customers' environment at point of onboarding
c. Record the collection and the review of the technical documentation
d. High level health check of the customers' environment at point of onboarding
5. If required, Koris365 make recommendations to remedy any pre-existing faults or misconfigurations
6. If applicable, customer remediates any pre-existing faults or misconfigurations (Koris365 can provide professional services resource at additional cost if required)
7. Koris365 and customer agree on IT procedures e.g., new starters, leavers, permission changes
8. Koris365 customer documentation is updated.
9. Customer receives welcome pack including ticket logging instructions.

2.3 Deliverables
2.3.1 Cisco

Cisco Unified Communication Manager	Included
User Management	Configuration of: New user accounts, new user device profiles, user pins/passwords, name changes, device association, CTI application user association, deleting users
Dial Plan Management	Configuration of: New directory numbers, line device association, user device profile (UDP) association, external mask configuration, call forwarding, pickup group assignment, line group assignment, existing dial plan elements
Device Management	Configuration or addition of: Phones, analogue telephone adaptors (ATA), gateways, trunks, video endpoints
Route Plan Management	Configuration of: Line groups, hunt list, hunt pilot, pickup groups, translation patterns, transformation patterns, partitions, calling search spaces, route patterns, route groups, route lists
System Management	Configuration of: Region, location, device pools
License Management	Installing new licenses, generating licensing report
Backup Management	Adding backup device, scheduling backup jobs, managing backups (application level only)
Cisco Unified Presence	Included
User Management	Configuration of: User accounts, assigning users to presence
License Management	Installing new licenses, generating licensing report
Backup Management	Adding backup device, scheduling backup jobs, managing backups (application level only)

Cisco Unity Connection	Included
User Management	Configuration of: User accounts, sync and import users, resetting pin, name changes
Call Handler Management	Configuration of: Call Handler, transfer rules, caller inputs, greetings
Mailbox Management	Configuration of: Mailbox quota, message aging policies, message expiration, Unified Messaging
System Management	Configuration of: LDAP, SMTP, schedules, holiday schedules
License Management	Installing new licenses, generating licensing report
Backup Management	Adding backup device, scheduling backup jobs, managing backups (application level only)

Cisco Unified Contact Centre Express	Included
RmCm Management	Configuration of: Skills, resources, resource groups, supervisors, contact centre queue
Application Management	Configuration of: Triggers, applications, scripts, prompts
System Management	Configuration of: SSO, CUIC reporting, real-time reporting, historical reporting, user management, password management
License Management	Installing new licenses, generating licensing report
Backup Management	Adding backup device, scheduling backup jobs, managing backups (application level only)

Cisco Expressway	Included
General Management	Configuration of: Search rules, zones, transformations
System Management	Configuration of: DNS, NTP, NIC

Cisco Unified Attendant Console	Included
User Management	Configuration of: Queues, modes, schedules, agents
License Management	Installing new licenses, generating licensing report

Cisco UCS server	Included
Minor Configurations	Network Interface Controller (NIC) settings, time, storage adapters, log settings
Resource Management	Migrating Virtual Machines (VM) between hosts, changes to resource groups, Distributed Resource Scheduler (DRS) configuration changes, high availability (HA) admission control
Disk expansion	Using RAID utilities to increase size of a volume and expand datastores

Cisco Cube	Included
Dial Plan Management	Configuration of: Dial-peers, translation rules, translation profiles
SIP Management	Configuration of: Voice service VoIP, SIP trunk, server pools
Security Management	Configuration of: VoIP trust list, access list
System Management	Configuration of: Logging, user accounts, privileges, TACACS, AAA
License Management	Installing new licenses, generating licensing report
Backup Management	Adding and managing backup jobs

Cisco Webex Calling	Included
User Management	Configuration of: New users, dial plan, policies assignment/change, enable/disable voicemail, disabling users, enable/disable call recording, call groups
Dial Plan Management	Configuration of: DDIs, Dial plan, meetings, Meeting policies/settings, call park policies, conference bridges, Live event policies/settings, hunt groups
Route Plan Management	Configuration of: Voice routing policy, routing, Auto attendants, call queues, Holidays, Resource accounts, Direct routing, SBC, Caller ID policies, Emergency policies, Operators, calling policies

Cisco Webex Contact Centre	Included
User Management	Configuration of: User management, license, skill and team assignment
Customer Experience Management	Configuration of: Flows, entry points, queues and schedules, Desktop and user profiles, Tenant customisation
Digital Channel Management	Configuration of: Configuration of Engage & Connect, Digital flows and assets

2.3.2 Mitel

Mitel MiVoice Business	Included
User Management	Configuration of: Adding/deleting user accounts, user pins/passwords, name changes and key configuration
Call Routing	Configuration of: Digits dialled, call barring, route lists, call forwarding
Device Management	Configuration or addition of: Phones, ONS ports, analogue telephone adaptors (ATA), trunks
System Management	Configuration of: System usernames and passwords, SNMP, SMTP, alarms, zones, system options, IP addressing, networking, clustering, SDS, logs and certificates
Licence Management	Installing, allocating and deploying
Backup Management	Adding backup device, scheduling backup jobs, managing backups (application level only)

Mitel MiContact Centre Business	Included
User Management	Configuration of: Adding/deleting user accounts, ignite account details, employee/agent/queue changes, employee/agent/queue group changes, scheduled tasks, permissions
Application Management	Configuration of: Subroutines, workflows, prompts, outbound, scripts and multimedia
System Management	Configuration of: Reporting, password management, REST API, SQL
Licence Management	Installing and allocating
Backup Management	Managing backups (application level only)

Mitel MiVoice Border Gateway	Included
User Management	Configuration of: Adding/deleting user accounts, user pins/passwords and name changes
Application Management	Configuration of: Ports, web proxy, trunking, call recording
System Management	Configuration of: Usernames and passwords, SNMP, SMTP, alarms, IP addressing, routing, SDS, logging and certificates
License Management	Installing and allocating licences
Backup Management	Managing backups (application level only)

Mitel MiCollab	Included
User Management	Configuration of: Adding/deleting user accounts, user pins/passwords, name changes, feature changes, client deployment
Application Management	Configuration of: Ports, web proxy, trunking, call recording, hostnames
System Management	Configuration of: Usernames and passwords, SNMP, SMTP, alarms, IP addressing, routing, SDS, logging and certificates
License Management	Installing and allocating licences
Backup Management	Managing backups (application level only)

Mitel MiVoice Call Recorder	Included
User Management	Configuration of: Adding/deleting user accounts, name changes, quality management, permissions
Application Management	Configuration of: Ports, CTI, Web Services
System Management	Configuration of: Usernames and passwords, SNMP, SMTP, alarms, IP addressing, logging, housekeeping and certificates
License Management	Installing and allocating licences
Backup Management	Managing backups (application level only)

Mitel Interaction Recording	Included
User Management	Configuration of: Adding/deleting user accounts, name changes, quality management, permissions
Application Management	Configuration of: Ports, CTI, Web Services
System Management	Configuration of: Usernames and passwords, SNMP, SMTP, alarms, IP addressing, logging, scheduled tasks and certificates
License Management	Installing and allocating licences
Backup Management	Managing backups (application level only)

Mitel Open Integration Gateway	Included
User Management	Configuration of: Adding/deleting user accounts, name changes, permissions
Application Management	Configuration of: Features, CTI, application services and integration
System Management	Configuration of: Usernames and passwords, SNMP, SMTP, alarms, IP addressing, routing, logging, scheduled tasks and certificates
License Management	Installing and allocating licences
Backup Management	Managing backups (application level only)

2.3.3   8x8

8x8 UCaas	Included
User Management	Configuration of: Adding/deleting user accounts, phone numbers, user pins/passwords and name changes
Device Management	Configuration or addition of: Physical and softphones, analogue telephone adaptors (ATA)
System Management	Configuration of: Usernames and passwords, hunt/pickup groups, channels, auto attendant, sites, options, analytics, roles/permissions and meetings
License Management	Installing and allocation licences

8x8 CCaas	Included
User Management	Configuration of: Adding/deleting user accounts, phone numbers, user pins/passwords and name changes
System Management	Configuration of: Queues, channels, scripts, CRM, options, roles/permissions, campaigns, integration, transaction/status codes and wallboard
License Management	Installing and allocation licences

2.3.4   Microsoft

Skype for Business	Included
User Management	Configuration of: New users, dial plan policy, voice policy, IM and presence policy, deleting users
Dial Plan Management	Configuration of: DDIs, meetings, dial-in access number, conferencing policies, call park, existing dial plan elements
Route Plan Management	Configuration of: Voice policy, routing, response groups, queues, workflows, PSTN usage, trunks, existing route plan elements
System Management	Configuration of: CDR, archive policy, federation and external access, location policy, bandwidth policy, region, routing
License Management	Installing new licenses, generating licensing report
Backup Management	Adding and managing backup jobs

Teams	Included
User Management	Configuration of: New users, dial plan, policies assignment/change, enable/disable voicemail, disabling users, enable/disable call recording, call groups
Dial Plan Management	Configuration of: DDIs, Dial plan, meetings, Meeting policies/settings, call park policies, conference bridges, Live event policies/settings
Route Plan Management	Configuration of: Voice routing policy, routing, Auto attendants, call queues, Holidays, Resource accounts, Direct routing, SBC, Caller ID policies, Emergency policies, Operators, calling policies
Reports	Analytics and reports

Ribbon SBC	Included
Dial Plan Management	Configuration of: Transformation, caller ID blocking, call blocking, DDI assignment
Route Plan Management	Configuration of: Call routing table, signalling groups, sip profile, sip server table, codec, dtmf, channels
System Management	Configuration of: Logging, user accounts, privileges, Radius, AAA
License Management	Installing new licenses, generating licensing report
Backup Management	Adding and managing backup jobs

2.3.5   Enghouse

EICC	Included
Queueing Management	Configuration of: Queues, modes, schedules, agents, agent login classes, delivery patterns
Console Management	Configuration of: Operator queues, modes, schedules, operators, operator login classes, delivery patterns
Announcement Management	Configuration of: Auto attendant, progress, announcements, position
General Management	Configuration of: User accounts, phone entries, security classes, functions and objects, line entries, holiday schedules, company pin policy
Voice Messaging Management	Configuration of: Mailbox classes, mailboxes, profiles and distributions lists
License Management	Installing new licenses, generating licensing report
Backup Management	Adding and managing backup jobs

QMS	Included
Recording Management	Configuration of: Users, recording profile, managed users, security profile, recording criteria, flag profile
Evaluation Management	Configuration of: Scorecards, categories, evaluator permissions
Reporting Management	Configuration of:

	Standard call recording and agent evaluation reports
General Management	Configuration of: SMTP, Active Directory integration, security policy, audit, encryption, retention settings, recording format, time zone
Archive Management	Configuring and scheduling archives
License Management	Installing new licenses, generating licensing report
Backup Managemen0t	Adding and managing backup jobs

2.3.6 Red Box Recorder

Red Box Recorder	Included
Recording Management	Configuring and scheduling archives
General Management	Configuration of: SMTP, security policy, retention settings, recording format, Time zone
License Management	Installing new licenses, generating licensing report
Backup Management	Adding and managing backup jobs

2.3.7 Reporting

Reporting	Included
Service Report	Monthly reporting of: Ticket analysis, SLA compliance, client survey results
Exception Report (customer must also have UC Monitor)	Monthly reporting of: Major Incidents, security notifications, backup and replication validation, license utilisation, average snapshot of CPU, memory, and interface utilisation
Lifecycle Report (customer must also have UC Monitor)	Quarterly reporting of: Device end-of-life status in a red, amber, green format

IMS098 V1.1

2.4 Exclusions

- Remediation
- Koris365 will investigate license requirements during any installations and will make recommendations but are not responsible for compliance, Software Asset Management, or the provision of licenses
- This is not Backup as a Service (BaaS). Koris365 will advise on suitable backup infrastructure but it is the responsibility of the customer to invest appropriately in a solution that meets organisation Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), archiving, and resilience objectives
- Koris365 take no responsibility for failure of hardware or the loss of data stored
- Seeding of new backup, backup copy, and replica jobs, or the provision any temporary storage required
- Koris365 take no responsibility for the failure of magnetic tapes, UPS batteries, RAID cache batteries, or similar consumables resulting in a loss of data
- Disaster recovery planning and testing
- Deployment of any previously unconfigured sites, services, features, new infrastructure, or applications
- Training
- Development
- Certificate management and installation
- Recording of announcements
- Direct end user service requests (tickets must be raised by named representative who can authorise and provide the necessary information to fulfil the request)
- New users will not be added without a completed Koris365 New User Template
- This is not a security service
- This is not a compliance service. It is the responsibility of the customer to provide Koris365 with validated information adhering to company compliance policies.
- Third-party outages are beyond our control, Koris365 will advise of status updates as they become available
- Any activity that requires a site visit
- Management of bespoke applications, bespoke alterations, or third-party integrations
- Configurations that are not supported by the vendor or don't follow vendor best practice
- End of life operating systems, applications, and devices
- Patching, major version migrations or upgrades
- Koris365 will not implement changes that carry a high risk of organisation disruption without suitable contingency
- Limitations may apply to third-party vendors
- The provision of additional resources such as CPU, memory, disk, and IP addresses where sufficient spare capacity does not exist

3 Service Level Agreement (SLA)

3.1 Hours of Service

Service	Mon - Fri	Weekends	Bank holidays
Standard	08:00 – 18:00 Standard Hours	Excluded	Excluded
24/7	08:00 – 18:00 Standard Operation (P1-P4) 18:00 – 08:00 Out of Hours (P1 and P2 incidents only)	Included (P1 and P2 incidents only)	Included (P1 and P2 incidents only)

Service hours are based upon GMT/BST time zone

3.2 Response & Restoration Times

Priority Level	Response Time	Target Restoration Time
Priority 1	30 minutes	4 hours
Priority 2	1 hour	8 hours
Priority 3	1 hour	32 hours
Priority 4 / Service Requests	Next Business Day	48 hours

UC Manage tickets will predominantly be treated as a Service Request. A ticket may be treated as an incident if Koris365 are performing a task to prevent an imminent outage.

- Priority 1 and 2 tickets must be raised or followed up via a phone call to the service desk
- Response time is measured from the customer logging a ticket to the customer being contacted to start investigation
- Target restoration time is a specified point in time where Koris365 aim to resolve the Incident or Service Request, this will not necessarily be a permanent fix and may need additional work and planned downtime to resolve completely
- Restoration may take longer than target time due to circumstances outside of our control, for example, non-redundant systems, backup system limitations, site visits, third party SLAs and patching cycles
- Incidents may be resolved by the service desk, an on-site engineering support team, or a third party
- Where the incident is determined to be the responsibility of a third party Koris365 will ensure all incident details are passed to the third party without undue delay
- Target restoration times are based upon contracted hours. Tickets not classed as Priority 1 will not be worked on outside of manned hours

3.3 Service Level Measurement

The SLA clock will commence on successful logging of a ticket. Elapsed time is measured from the point the ticket is created to the Response Time. The SLA clock then continues until the Restoration time.

During investigation and troubleshooting of a ticket, the SLA Timer will be paused, i.e. the elapsed time is halted, in the following situations;

- Awaiting information, or actions from the customer where Koris365 cannot reasonably be expected to progress the ticket without this information/action
- If customer contact cannot be made after three consecutive attempts, over at least three working days, a final email containing a closure warning will be sent; if Koris365 still do not receive a response the ticket will be closed
- Awaiting information, or actions from a third party where Koris365 cannot reasonably be expected to progress the ticket without this information/action
- Where the problem is associated with a change to the supported system that has not been implemented by Koris365 (ticket will be closed)
- Where the problem is associated with items outside of the supported system (ticket will be closed)
- Where restoration involves time constraints outside of our control, for example, non-redundant systems, backup system limitations, and site visits
- Priority 3, 4, and service request tickets received outside of contracted manned hours

Once the information or action has been received by Koris365, the service timer will be reactivated again.

Priority 1 and 2 calls will be measured throughout the 24/7 period where a 24/7 contract has been purchased.

3.4 Service Desk Key Performance Indicators (KPI)

The Service Desk are committed to meeting response and resolution SLAs with a KPI of 95% or above. The Service Desk aim to achieve a KPI of 90% or above on a target average call wait time of 60 seconds or under.

3.5 Ticket Types

3.5.1 Service Requests (IMACD)

Standard service requests are requests for information, moves, additions, changes and deletions (IMACD). No system is at fault and applications are working as expected. This could also take the form of a request that does impact a user's ability to work such as a password reset, in which case these are generally resolved at first point of contact. Most service requests however do not impact the user's ability to work and therefore should be submitted in advance of being required, normally in written format and, where applicable, a standard template such as a new starter form.

Any more than five individual service requests at the same time, i.e. bulk service requests, will require scheduling.

Where a service request is expected to take more than 1 hour to complete then the request will be reviewed and possibly assigned as a separate project.

3.5.2 Incidents

An incident is defined as any event not part of the standard operation of a service which causes an interruption to, or a reduction in the quality of that service.

All incidents and service requests are recorded in the Koris365 ticketing system with a priority selected from the Priority Level Definition table. The priority determines the order in which the Service Desk work on these tickets.

The Incident Priority Code is derived by assessment of the incident's impact and urgency. The Priority code will be provided at the time of logging or by return email. The Priority Code may be re-assigned when the impact or urgency is deemed to have changed.

3.6 Priority Level Classification

The priority of an incident is defined by assessing both impact and urgency.

- Urgency is a measure of how quickly the system needs to be restored
- Impact is a measure of the potential damage caused by the incident

3.6.1 Incident Urgency

Category	Description
High	- Damage caused by incident increases rapidly - Work that cannot be completed is highly time sensitive
Medium	- Damage caused by incident increases steadily - Work that cannot be completed is moderately time sensitive
Low	- Damage caused by incident increases marginally - Work that cannot be completed is not time sensitive

3.6.2 Incident Impact

| Category	Description
High	- Many employees are affected and not able to do their job - Large financial impact - Damage to reputation of business is likely to be high - Many customers are affected
Medium	- A moderate number of employees are affected and not able to do their job - Low financial impact - Damage to reputation of business is likely to be moderate - A moderate number of customers are affected
Low	- A minimal number of employees are affected - Negligible financial impact - Damage to reputation of business is likely to be minimal - A minimal number of customers are affected

3.6.3 Incident Priority Matrix

|		Impact		
		High	Medium	Low
Urgency	High	P1	P2	P3
	Medium	P2	P3	P4
	Low	P3	P4	P4

Priority Level	Action
Priority 1 (P1)	Service desk provide prioritised, sustained effort using all necessary resources until service is restored
Priority 2 (P2)	Service Desk reprioritise resources from lower priority jobs where necessary to focus on restoring the services
Priority 3 (P3)	Service Desk reprioritise resources from lower priority jobs where necessary
Priority 4 (P4)	Service Desk provide a response using standard operating procedures

IMS098 V1.1

3.7 Ticket Handling & Escalation
3.7.1 P1 and P2 Ticket Flow

IMS098 V1.1
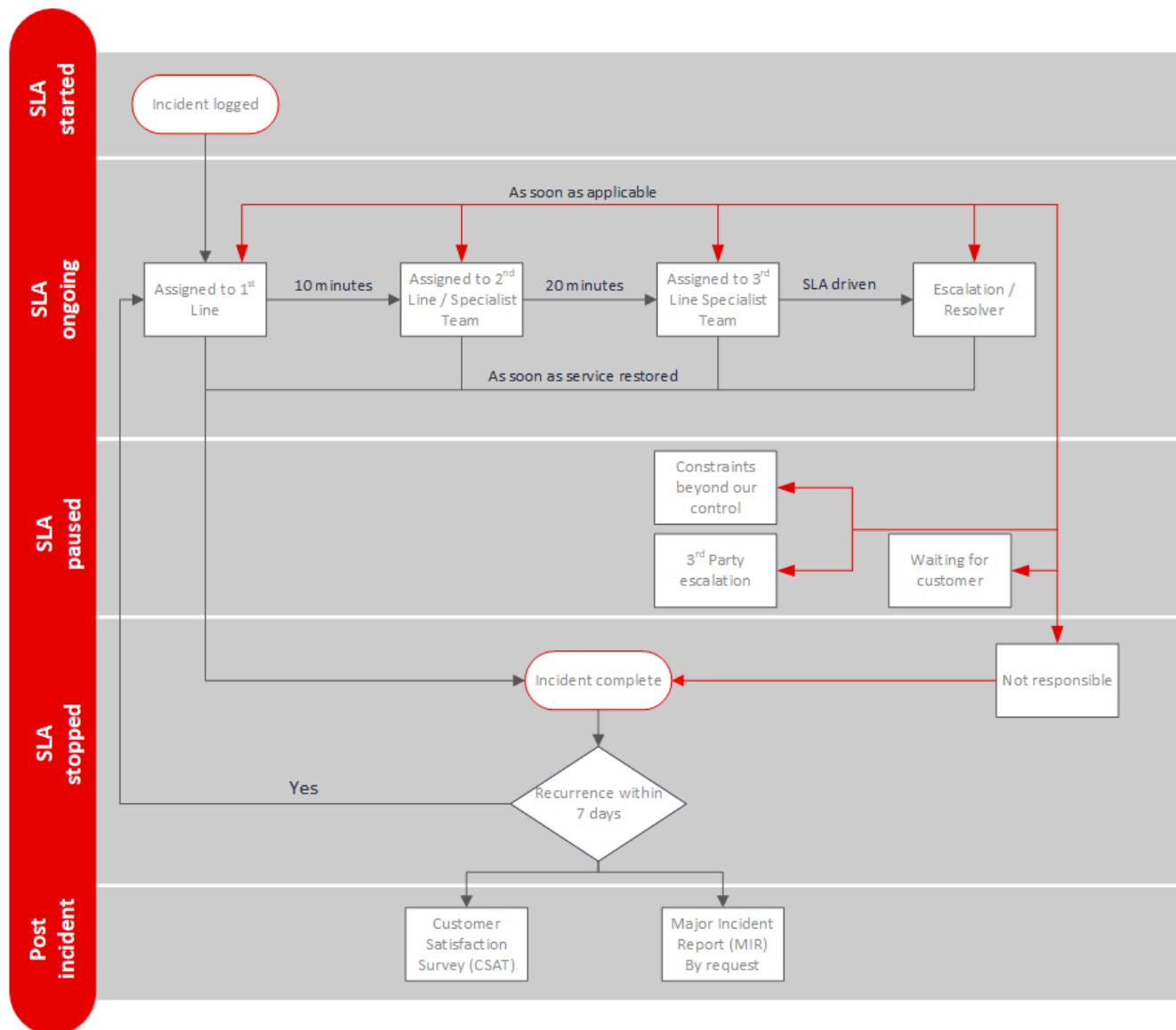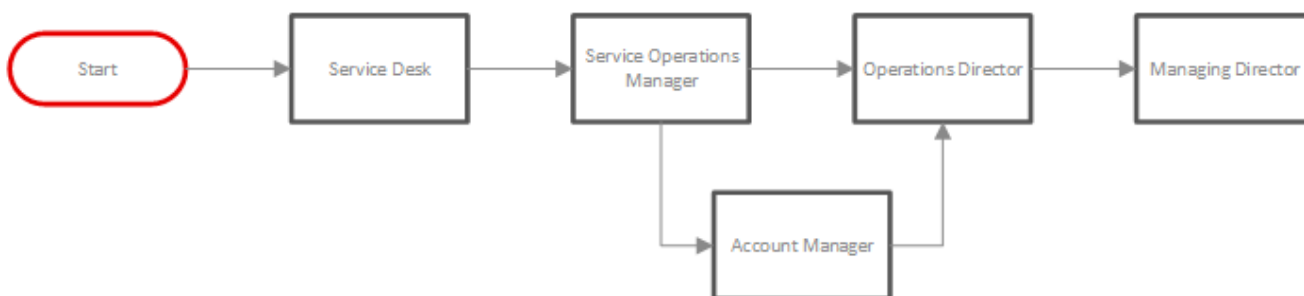
3.7.2 P3 and P4 Ticket Flow
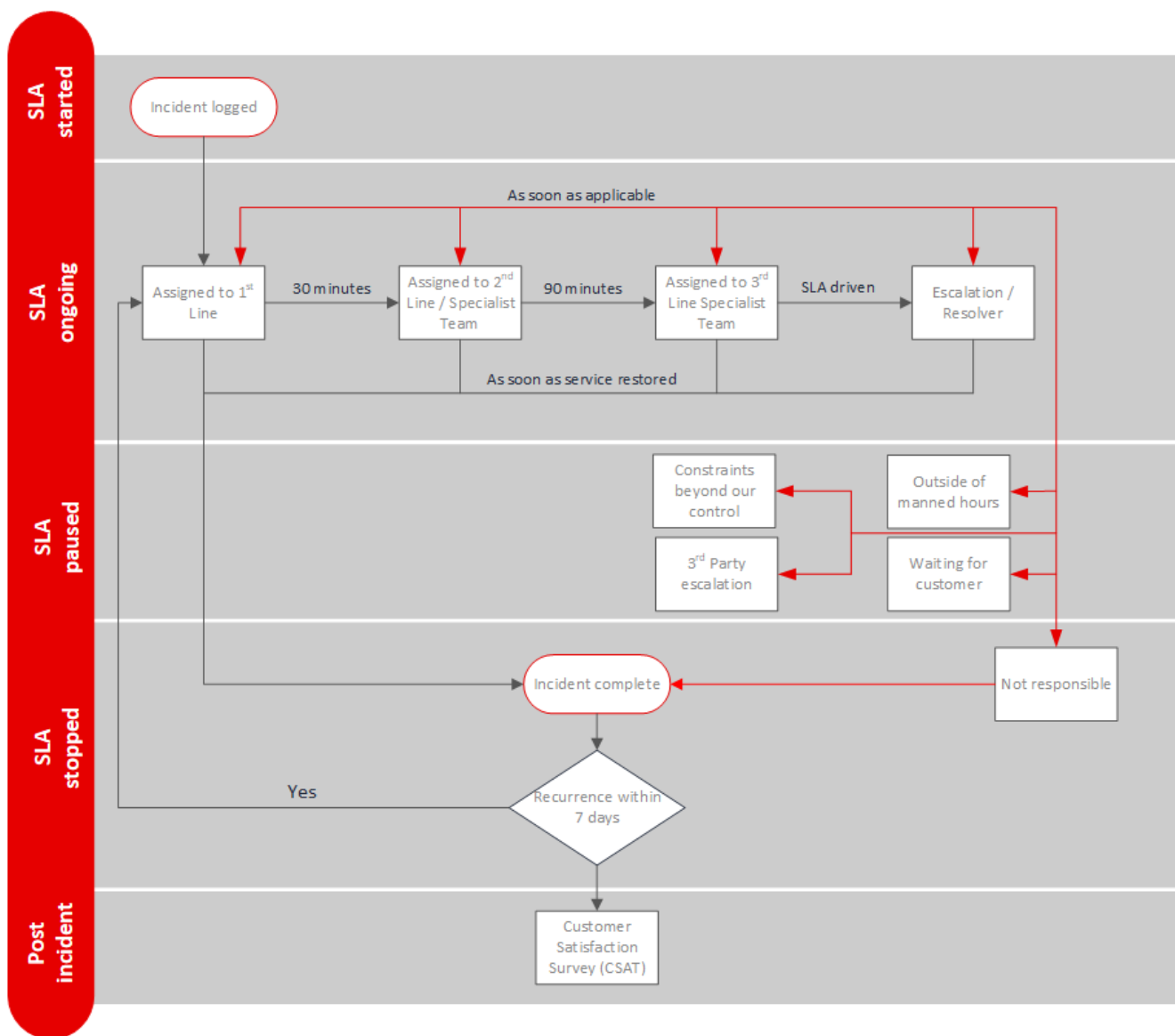
3.7.3 Customer Escalation

4 Offboarding Procedure

On the final day of contract Koris365 will:

- Provide any stored credentials to the customer
- Provide any existing supported systems documentation to the customer
- At the customer's request, engage with the incoming services provider to supply any existing supported systems documentation necessary for transition of the service
- Permanently disable remote access and monitoring
- Cease working on any outstanding tickets and provide an outstanding ticket summary
- Delete customer owned data stored within the Koris365 environment
- Deletion/redaction of customer user records
- Terminate service

The customer is expected to:

- Change passwords and disable accounts as necessary for security purposes
- Plan migration of data in advance of termination of service

Koris365 will not:

- Provide details of internal working practices
- Keep a copy of customer owned data stored within the Koris365 environment for future recovery purposes