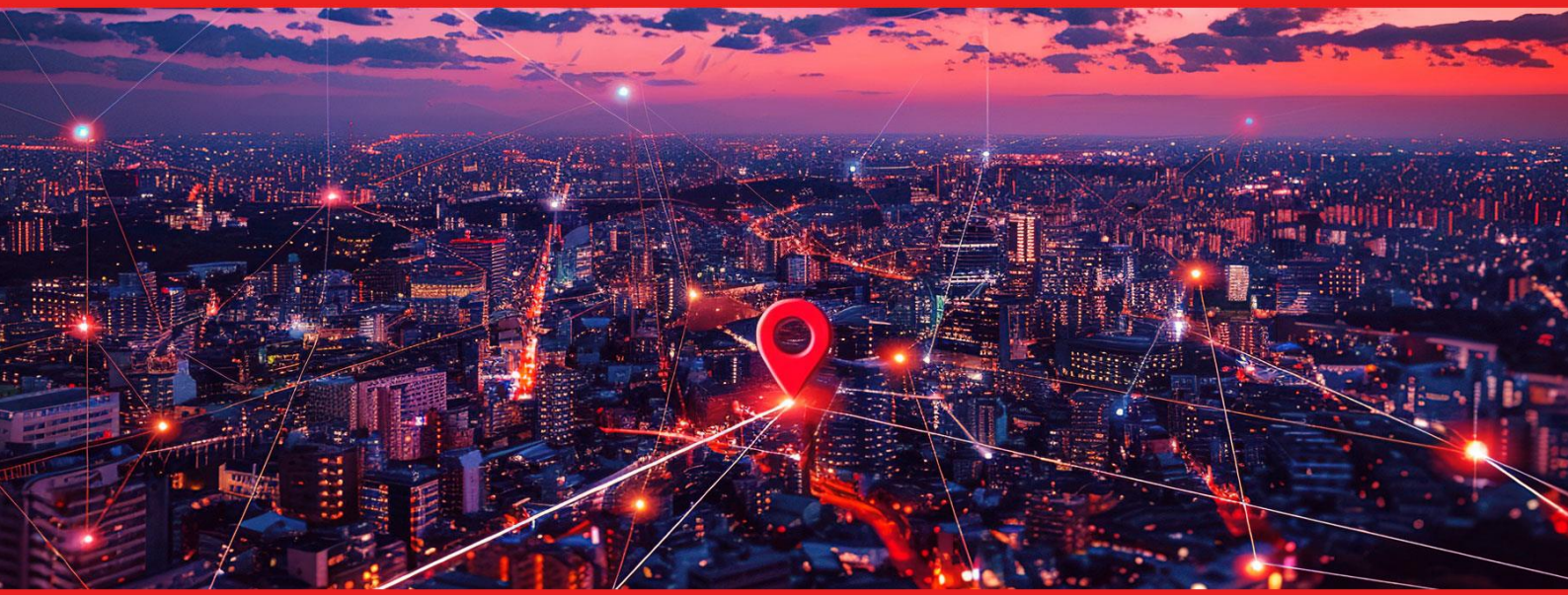
# Cloud and Infrastructure Resolve

## Service Description



Koris365 UK Limited
8 Grovelands, Boundary Way Hemel Hempstead, HP2 7TE
Reg No: 07709017 | VAT No: 927332425
Tel: 0345 505 5365 | Email: info@koris365.com

# Copyright



# 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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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.

# Contents

# 1 Summary

## 1.1 Overview

Cloud and Infrastructure Resolve provides a technical escalation point for a customer's IT department to aid in the troubleshooting and resolution of problems across the IT infrastructure, or in cases where a specific system requires very specialist expertise. Cloud and Infrastructure Resolve can also be combined with other Unify services to form part of a more comprehensive managed solution.

## 1.2 Features

Features available in the Cloud and Infrastructure Resolve service include:

- Resolving issues arising in a customers' IT infrastructure
- Liaising with third-party vendors for incidents related to contracted hardware and software
- Problem management
- Monthly service reporting

## 1.3 Suitable Customers

Any organisation with an IT infrastructure can benefit from Cloud and Infrastructure Resolve including:

- Organisations with limited IT resource
- Organisations looking for peace of mind that the expertise to deal with complex IT issues is available
- Organisations looking to deploy new solutions without the need to retrain
- Organisations looking to expand without the burden of IT recruitment

## 1.4 Pricing

Cloud and Infrastructure Resolve pricing is based on the number and type of devices.

# 2 Detailed Service Description

## 2.1 Pre-requisites

To provide the Cloud and Infrastructure Resolve service, Koris365 will require the following:

- The customer must provide a comprehensive list of devices to be supported and 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 provide relevant company detail such as quantity of users, locations, hours of work
- The customer must be prepared to facilitate remote access and provide credentials as necessary during support
- 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)
- The customer must provide a list of at least one technical person who can assist or take ownership when an issue, or part of, is out of scope

## 2.2 Onboarding

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. Configurations
3. Koris365 will work with the customer to complete the Unify 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
    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
4. If required, Koris365 make recommendations to remedy any pre-existing faults or misconfigurations
5. If applicable, customer remediates any pre-existing faults or misconfigurations (Koris365 can provide professional services resource at additional cost if required)
6. Koris365 and customer agree on IT procedures e.g. new starters, leavers, permission changes
7. Koris365 customer documentation is updated
8. Customer receives welcome pack including ticket logging instructions
9. Business as usual service commences

## 2.3 Deliverables

| Virtual Microsoft Windows Server | Included |
|---|---|
| Server configuration faults | Identifying issues caused by configuration for items such as virtual machine settings, boot order, various control panel items, and network settings |
| Operating System (OS) faults | Troubleshooting and implementing fixes or workarounds for general OS errors such as Blue Screen of Death (BSoD), instability, hanging, and other unexpected behaviours |
| Performance problems | Investigating and implementing or recommending solutions for performance issues such as memory or CPU spiking and slow applications |

| Physical Microsoft Windows Server | Included |
|---|---|
| Server configuration faults | Identifying issues caused by configuration for items such as BIOS settings, boot order, and various control panel items |
| Server hardware faults | Diagnosing hardware failures, liaising with hardware vendor where warranty exists |
| Operating System faults | Troubleshooting and implementing fixes or workarounds for general OS errors such as BSoD, instability, hanging, and other unexpected behaviours |
| Performance problems | Investigating and implementing or recommending solutions for performance issues such as memory or CPU spiking and slow applications |

| VMware ESXi Server | Included |
|---|---|
| Server hardware faults | Diagnosing hardware failures, liaising with hardware vendor where warranty exists |
| vCenter Server faults | Troubleshooting and implementing fixes or workarounds for vCenter issues such as the vCenter server crashing, services failing, boot errors, and other unexpected behaviours |
| ESXi Operating system faults | Troubleshooting and implementing fixes or workarounds for general OS errors such as purple screens, instability, hanging, and other unexpected behaviours |
| Performance problems | Investigating and implementing or recommending solutions for issues such as memory and CPU spiking, host and virtual machine performance, and resource contention issues |
| vSphere Configuration faults | Identifying issues caused by configuration for items such as ESXi host settings, network settings, vSphere cluster configurations, High Availability (HA), and Distributed Resource Scheduler (DRS) |

| On-Premises Exchange / Online | Included |
|---|---|
| Application faults | Troubleshooting and implementing fixes or workarounds for issues with the Exchange application such as services failing, management interface errors, and web app errors |
| Mail flow faults | Troubleshooting and implementing fixes or workarounds for issues with mail flow such as emails not sending or arriving, SMTP relaying, and hybrid mail flow issues |
| Connectivity faults | Troubleshooting and implementing fixes or workarounds for issues with client connectivity via Outlook, Outlook Web Access (OWA), ActiveSync, and cloud service issues |
| Database faults | Troubleshooting and implementing fixes or workarounds for database issues such as Database Availability Groups (DAG) replication and failover, dismounted databases, and mailbox move errors |

| Microsoft SharePoint | Included |
|---|---|
| Application faults | Troubleshooting and implementing fixes or workarounds for issues with the SharePoint application or Internet Information Services (IIS) |

| Microsoft SQL | Included |
|---|---|
| Application faults | Troubleshooting and implementing fixes or workarounds for issues with the SQL application or instance, maintenance plan failures, and liaising with 3rd party vendors |

| Microsoft Hyper-V | Included |
|---|---|
| Server configuration faults | Identifying issues caused by configuration for items such as virtual network settings, failover cluster settings, and general Hyper-V settings |
| Performance problems | Investigating and implementing or recommending solutions for issues such as memory and CPU spiking, host and virtual machine performance, and resource contention issues |

| Microsoft Remote Desktop Services (RDS) & Citrix | Included |
|---|---|
| Performance problems | Investigating and implementing or recommending solutions for issues such as memory and CPU, contention issues, and generally poor session performance |
| Connectivity/Login problems | Troubleshooting and implementing fixes or workarounds for server and network related user logon issues such as hanging logons, profile loading failures, and outright connection failures |

| Active Directory / Azure AD, DNS, DHCP | Included |
|---|---|
| Configuration faults | Identifying issues caused by configuration for items such as sites and services, replication config, Domain Name System (DNS) configuration, DHCP configuration, and Azure Active Directory (AD) Connect configuration issues |
| Service faults | Troubleshooting and implementing fixes or workarounds for Active Directory, Active Directory Federation Services (ADFS), Azure AD Connect, DNS, DHCP windows service failures |
| Replication faults | Troubleshooting and implementing fixes or workarounds for Active Directory replication, Azure AD Connect synchronisation failures |
| DNS resolution faults | Troubleshooting and implementing fixes or workarounds for DNS resolution issues and failures |
| DHCP faults | Troubleshooting and implementing fixes or workarounds for DHCP server issues such as failure to obtain leases, scopes filling up, and conflicts |

| Storage Area Network (SAN) | Included |
|---|---|
| Hardware faults | Diagnosing hardware failures, liaising with hardware vendor where warranty exists |
| Configuration faults | Identifying issues caused by configuration for items such as network settings, volume settings, and host settings |
| Performance problems | Investigating and implementing or recommending solutions for issues such as memory and CPU spiking, and disk performance |

| Network Attached Storage (NAS) | Included |
|---|---|
| Hardware faults | Diagnosing hardware failures, liaising with hardware vendor where warranty exists |
| Configuration faults | Identifying issues caused by configuration for items such as network settings, volume settings, and host settings |
| Performance problems | Investigating and implementing or recommending solutions for issues such as memory and CPU spiking, and disk performance |

| Veeam Backup | Included |
|---|---|
| Backup job warnings and failures | Troubleshooting and implementing fixes or workarounds for backup failures and warnings |
| Veeam application faults | Troubleshooting and implementing fixes or workarounds for issues with the Veeam application |

| Veeam Replication | Included |
|---|---|
| Replication job warnings and failures | Troubleshooting and implementing fixes or workarounds for replication failures and warnings |

| Acronis Backup | Included |
|---|---|
| Backup job warnings and failures | Troubleshooting and implementing fixes or workarounds for backup failures and warnings |
| Acronis application faults | Troubleshooting and implementing fixes or workarounds for issues with the Backup Exec application |

| Reporting | Included |
|---|---|
| Service Report | Monthly reporting of:<br>Ticket analysis, SLA compliance, client survey results |

## 2.4 Exclusions

- Any service outside of fault resolution
- Replacement parts or the addition of new hardware
- Liaising with third-party vendors for incidents related to hardware and software outside of the supported system
- Performance issues or failures caused by underspecified hardware resources
- Performance issues or failures caused by outdated operating systems, firmware, drivers, and application patch levels
- Remediating issues caused by customer or third-party changes (this will be considered chargeable)
- 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 of 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
- Koris365 take no responsibility for Backup failures resulting from the customer not changing tapes, exceeding the recommended tape lifespan, or due to poor tape drive maintenance
- Training
- Issues caused by the improper management of SSL certificates
- Support for end user, client devices, and third-party internet connections
- Third-party outages are beyond our control, Koris365 will advise of status updates as they become available
- Any activity that requires a site visit
- Troubleshooting of bespoke applications, bespoke alterations, or third-party integrations
- Troubleshooting configurations that are not supported by the vendor or don't follow vendor best practice
- End of life operating systems, applications, and devices
- Where a peer in a site-to-site VPN is owned and maintained by a third-party Koris365 will not be responsible for that device
- Patching, major version migrations or upgrades (this is considered a separate project and chargeable)
- Koris365 will not implement changes that carry a high risk of organisation disruption without suitable contingency
- Limitations may apply to third-party vendors
- Resolving issues with systems that are beyond economical repair e.g. the system would take longer to repair than to restore or rebuild
- Diagnosis of hardware faults of systems without appropriate vendor tools installed

# 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 (Out of standard hours) | P1 and P2 incidents only | P1 and P2 incidents only | 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 |

Cloud and Infrastructure Resolve tickets will always be treated as incidents. Service requests are not included in Cloud and Infrastructure Resolve, but available as part of Cloud and Infrastructure Manage.

- 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 or 2 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 and 4 tickets 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<br>• Work that cannot be completed is highly time sensitive |
| Medium | • Damage caused by incident increases steadily<br>• Work that cannot be completed is moderately time sensitive |
| Low | • Damage caused by incident increases marginally<br>• 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<br>• Large financial impact<br>• Damage to reputation of business is likely to be high<br>• Many customers are affected |
| Medium | • A moderate number of employees are affected and not able to do their job<br>• Low financial impact<br>• Damage to reputation of business is likely to be moderate<br>• A moderate number of customers are affected |
| Low | • A minimal number of employees are affected<br>• Negligible financial impact<br>• Damage to reputation of business is likely to be minimal<br>• A minimal number of customers are affected |

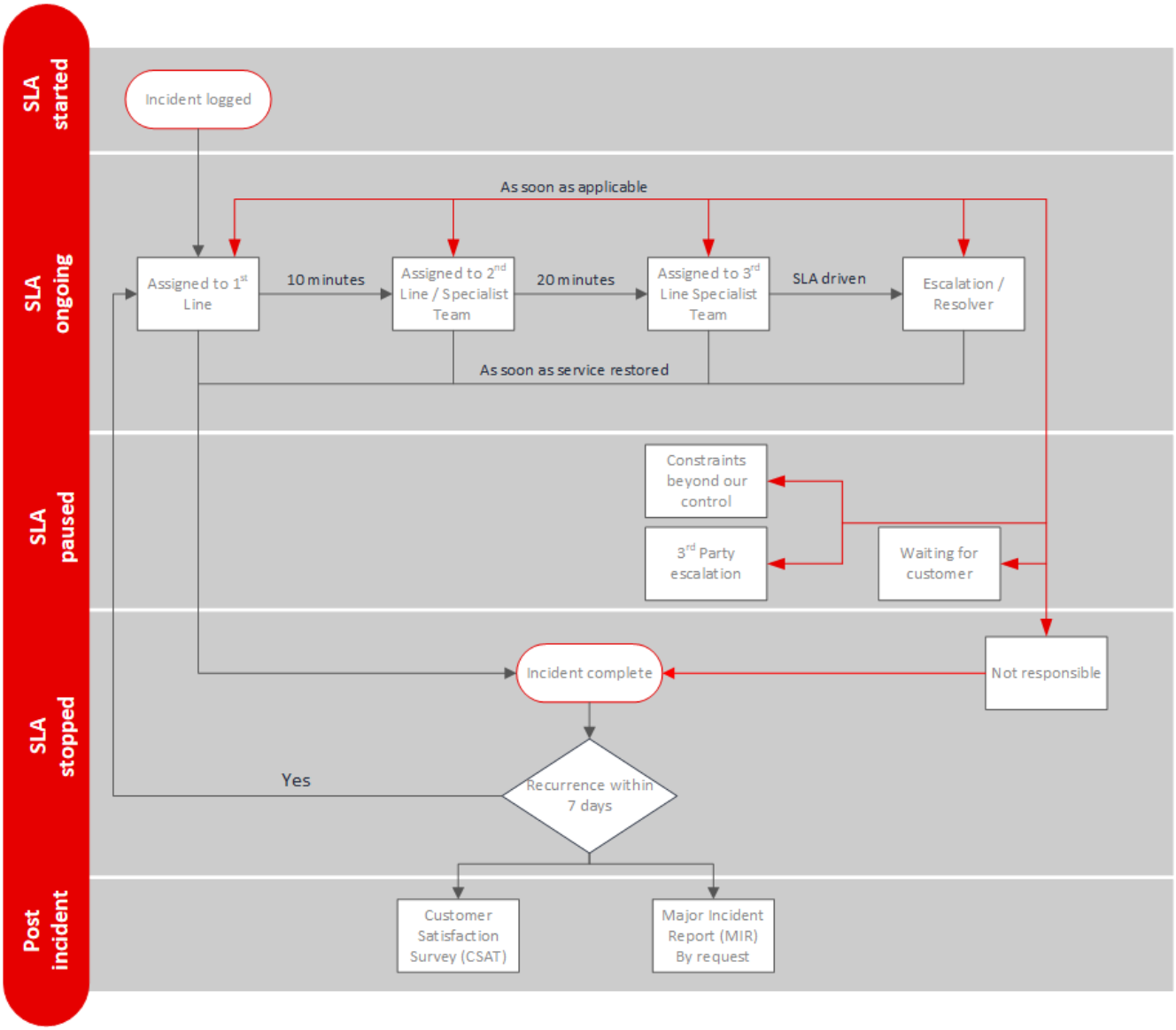
## 3.6.3 Incident Priority Matrix

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

| Priority Level | Action |
|---|---|
| Priority 1 (P1) | Servicedesk 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 |

## 3.7 Ticket Handling & Escalation Process

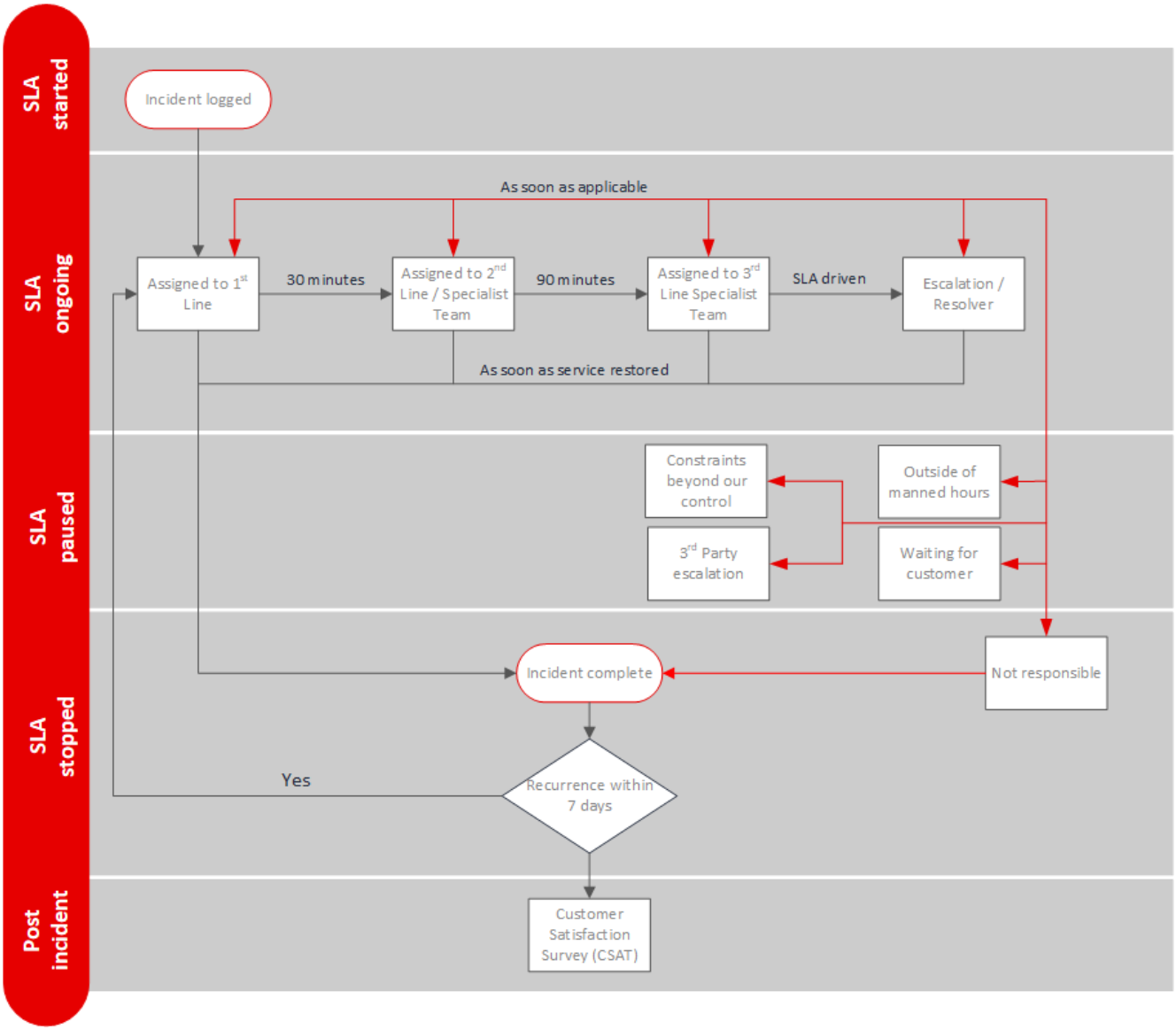
### 3.7.1 P1 and P2 Ticket Flow



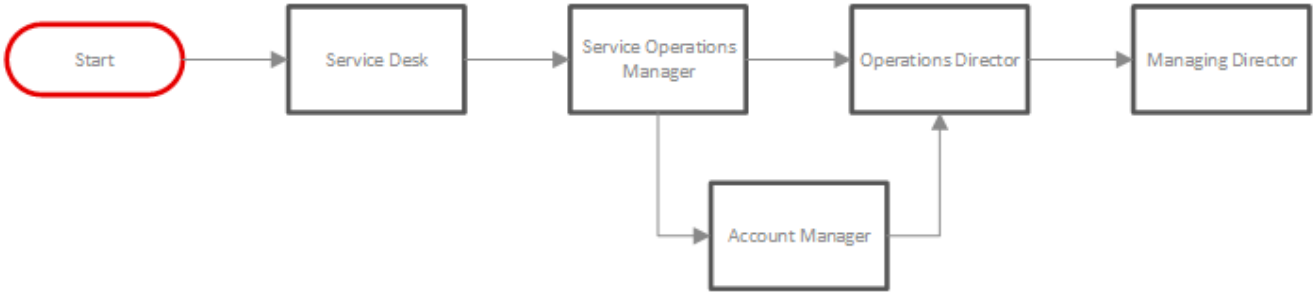



Koris365 UK Limited
8 Grovelands, Boundary Way Hemel Hempstead, HP2 7TE
Reg No: 07709017 | VAT No: 927332425
Tel: 0345 505 5365 | Email: info@koris365.com

## 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