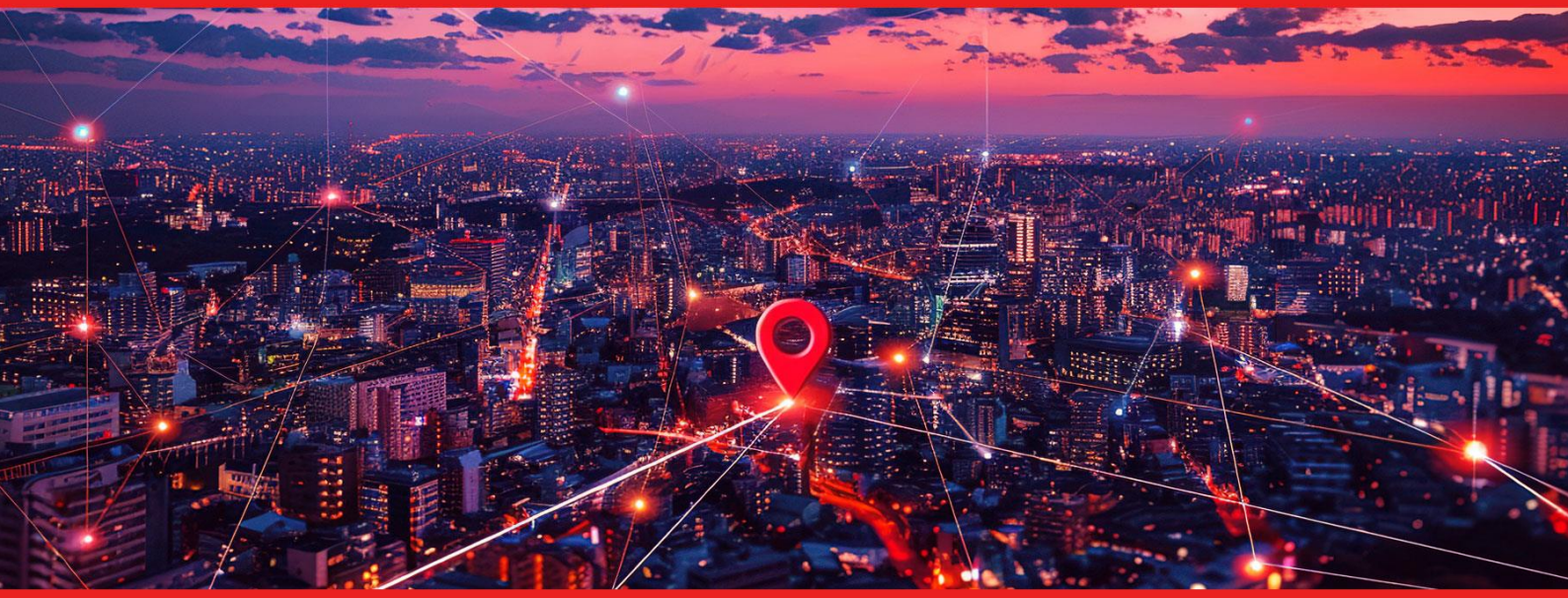
End User Compute

Service Description



Copyright

Confidentiality

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 VAT No: 631921945	Company Reg No: 06215347 VAT No: 912862719	Company Reg No: 07709017 VAT No: 927332425	Company Reg No: 727514 VAT No: IE04083398OH

Contents

1 Summary

1.1 Overview

End User Compute is a managed service that can be added to Cloud and Infrastructure Manage allowing end users to have a single point of contact for client related IT issues and requests. Koris365 can troubleshoot and resolve client issues directly rather than through a nominated IT contact.

1.2 Features

Features available in the End User Compute service include:

- Troubleshoot and resolve client-side IT issues
- Liaising with third-party vendors for desktop/laptop hardware and client-side software issues
- Direct end user ticket logging
- Monthly reporting including customer satisfaction results

1.3 Suitable Customers

Any organisation with a user base who require regular IT assistance can benefit from End User Compute including:

- Organisations with limited IT resource
- Organisations looking to free up IT resources to focus on IT projects and development
- Organisations looking to provide their user base with a single point of contact
- Organisations looking to expand without the burden of IT recruitment

1.4 Pricing

End User Compute pricing is based on the size of the user base to be supported.

2 Detailed Service Description

2.1 Pre-requisites

To provide the End User Compute service, Koris365 will require the following:

- An up-to-date client device and printer asset list
- An up-to-date list of client line of business applications
- An up-to-date list of third-party support contacts and relevant contract details
- 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 allow ad-hoc remote assistance sessions directly between Koris365 analysts and the end user
- The customer will need to provide at least one named decision maker
- 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 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. Asset and application lists
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

Remote end user support	Included
Troubleshooting desktop and laptop operating systems and hardware	Troubleshooting Microsoft client operating system errors, diagnosing desktop/laptop hardware faults and liaising with manufacturer to arrange repairs, basic advice on using features
Troubleshooting of client applications	Troubleshooting issues with Microsoft office applications, reasonable endeavours troubleshooting of third-party applications and escalating to software vendors as needed, providing basic advice using Microsoft applications, aiding with spam identification, administering message hygiene and web content filtering systems to block/unblock/release items as required
Troubleshooting printer errors	Troubleshooting printer errors, liaising with printer manufacturer or contracted third-party to arrange repairs
Password resets/account unlocks	Active Directory and Azure Active Directory password resets and account unlocks. Troubleshooting self-service portal errors.

2.4 Exclusions

- Replacement parts or the addition of new hardware
- 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
- End user training
- Support for end user's personal devices
- Support for third-party internet connections such as home internet and public hotspots
- 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
- Patching, major version migrations or upgrades (this is considered a separate project and chargeable)
- Client application or client device rollouts
- Imaging/reimaging/building/rebuilding client devices
- 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
- Management or supply of consumables
- Password resets/account unlocks outside of the supported system
- Password resets/unlock requests exceeding 5% of contracted user quantity per month, end user training and self-service tools will be recommended
- User behaviour leading to security breaches, end user training, password policy reviews, and multi factor authentication will be recommended
- Responsibility for verification of identity where no agreed process is in place
- Responsibility for authority for service requests where no agreed process is in place

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

End User Compute tickets can be treated as incidents or service requests. High priority incidents will generally be identified by the volume of end user tickets reporting similar issues. Issues that are identified to be server or network related will generally be classified as Cloud and Infrastructure Resolve tickets.

- 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
- Password resets/account unlocks are classified as a Service Request, however, if the user telephones the Service Desk, then the ticket will usually be dealt with immediately

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 outside of contracted manned hours

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

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

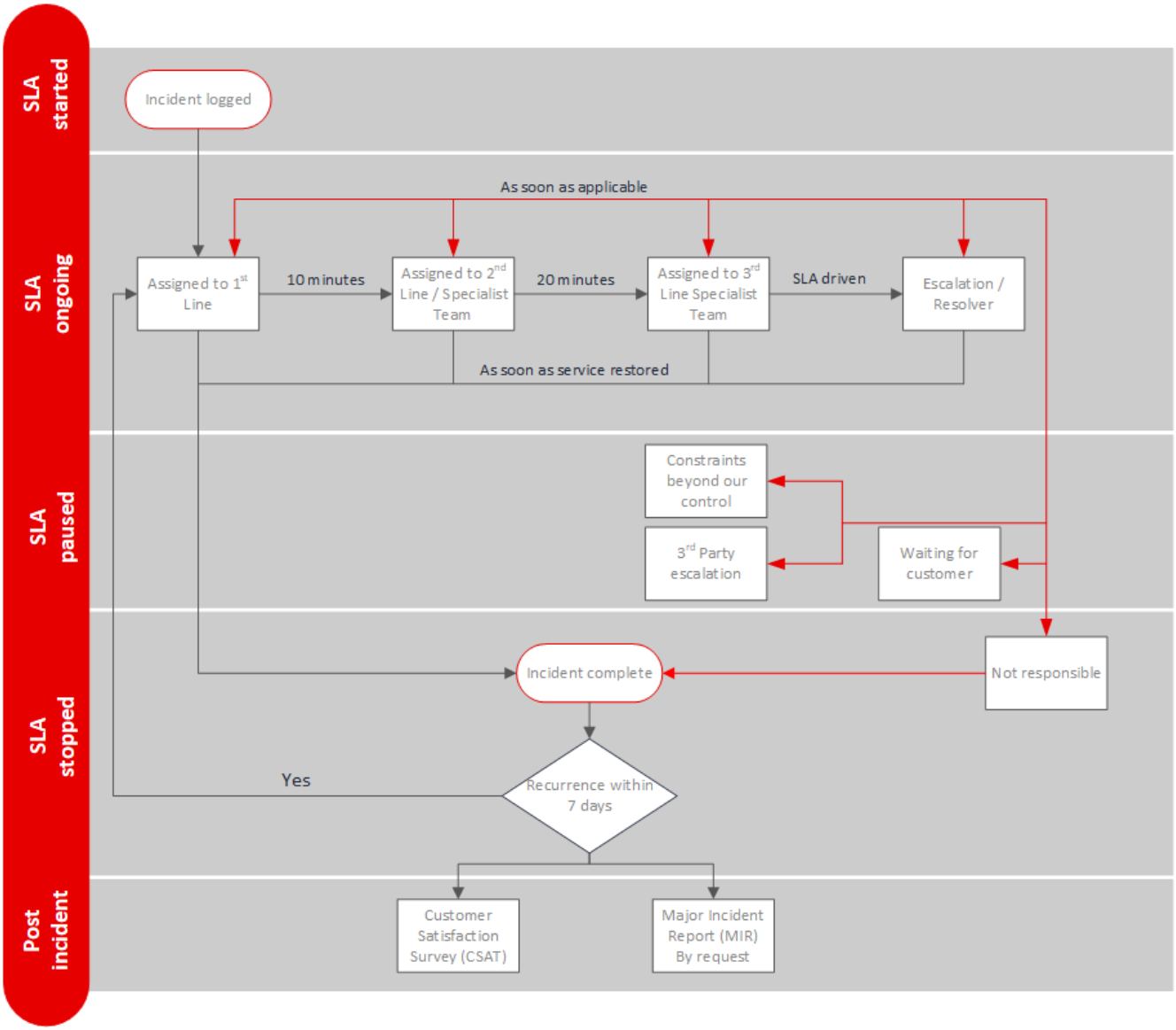
3.6.3 Incident Priority Matrix

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

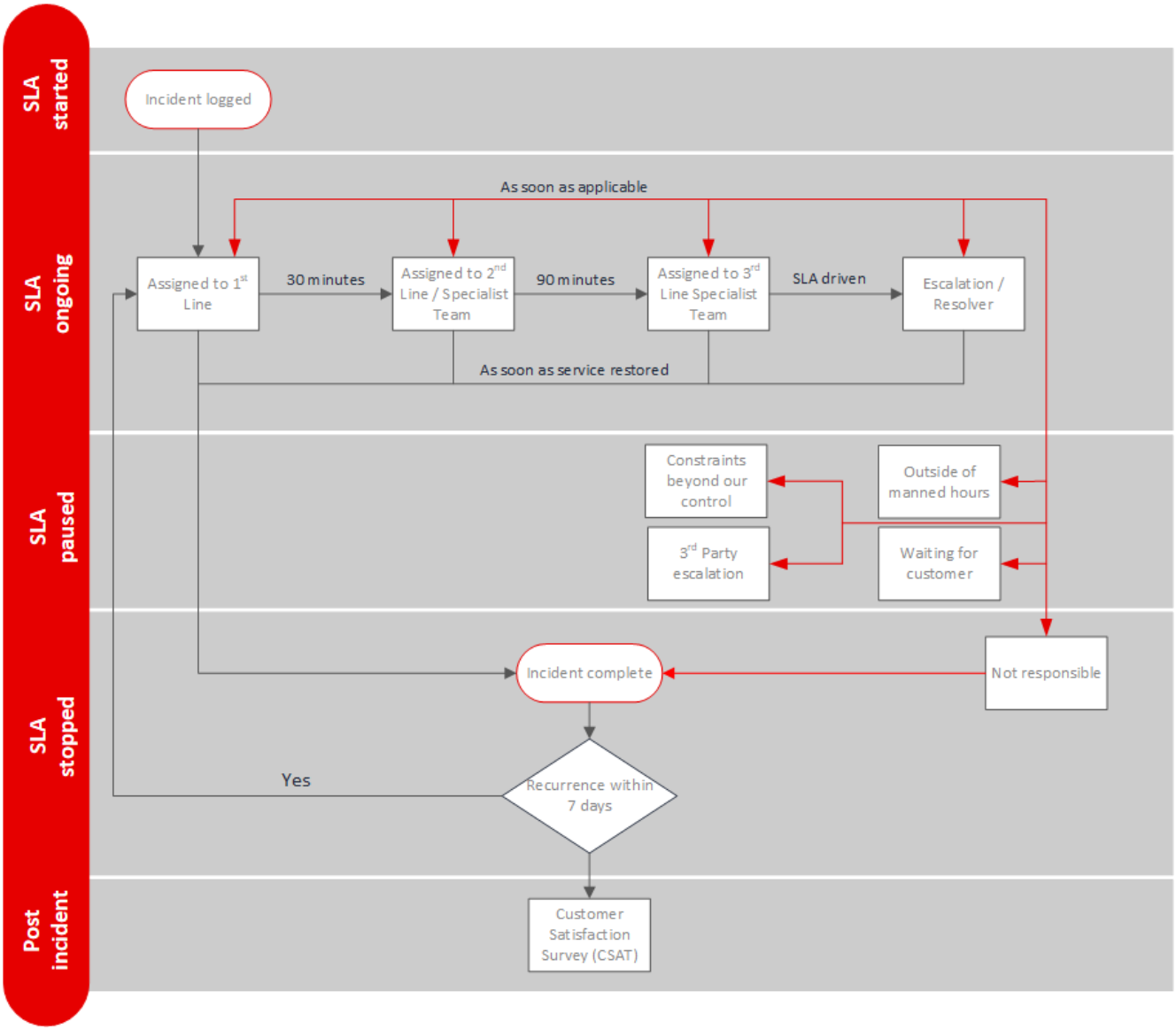
Priority Level	Action
Priority 1 (P1)	Servicedesk provide prioritised, sustained effort using all necessary resources until service is restored
Priority 2 (P2)	Service Desk reprioritise resources from lower priority jobs where necessary to focus on restoring the services
Priority 3 (P3)	Service Desk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

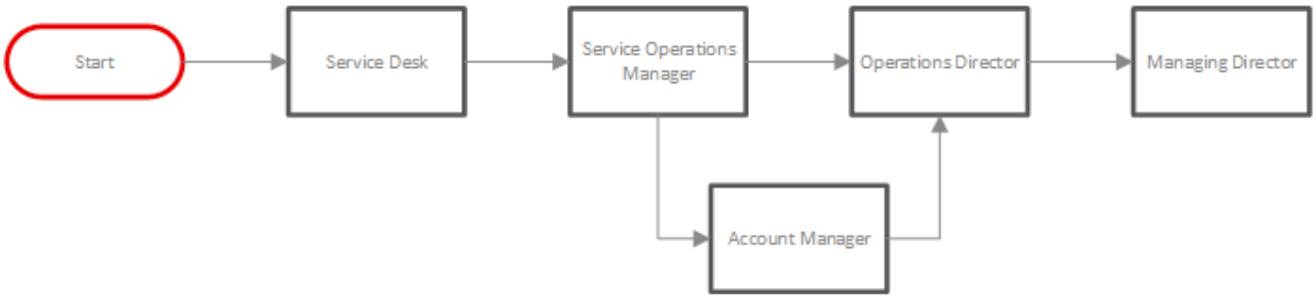
3.7.1 P1 and P2 Ticket Flow



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