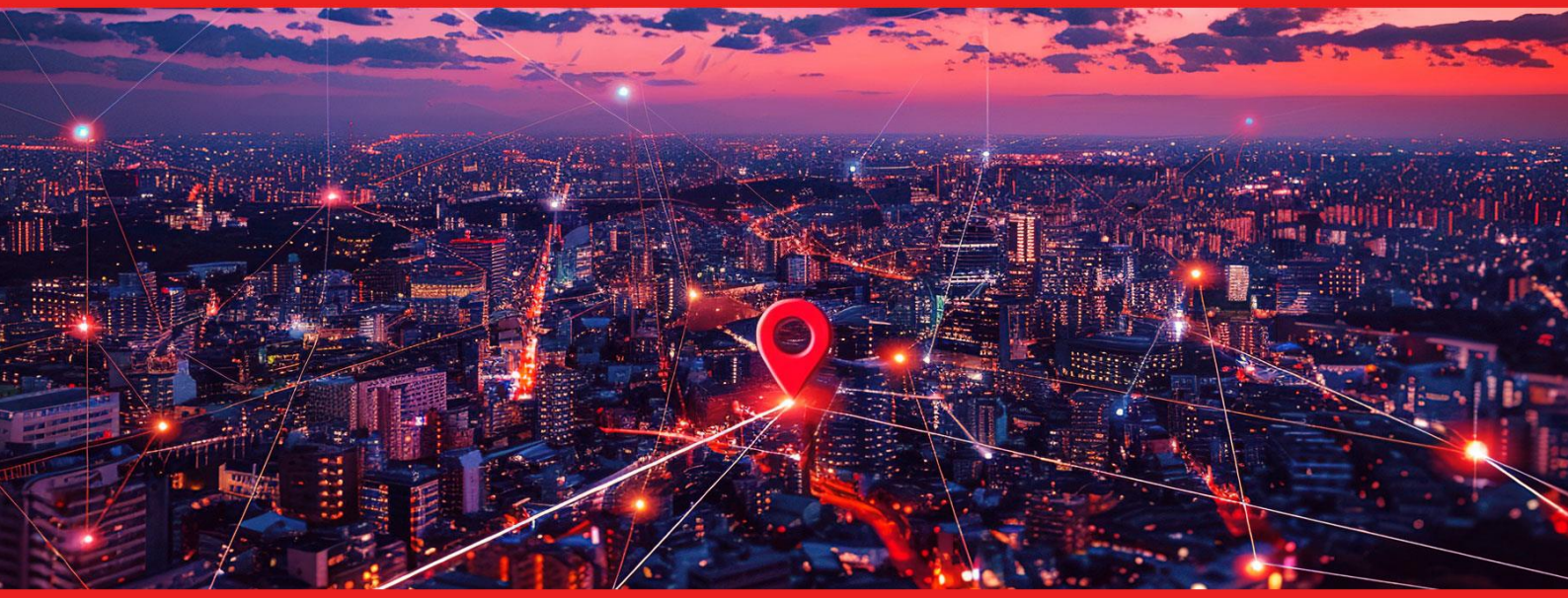
Cloud and Infrastructure Manage

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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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 Manage provides customers with the day-to-day systems administration of their IT infrastructure such as the creation of users, management of permissions, and routine configuration changes. Cloud and Infrastructure Manage is not a standalone service, its purpose is to form a comprehensive managed solution when combined with Cloud and Infrastructure Monitor and Cloud and Infrastructure Resolve.

1.2 Features

Features available in the Cloud and Infrastructure Manage service include:

- Management of server estates including physical, and virtualised environments
- Management of common Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Software as a Service (SaaS) solutions
- Management of server applications
- Management of storage
- Management of backups
- Technology roadmap planning
- Monthly service reporting

1.3 Suitable Customers

Any organisation with an IT infrastructure can benefit from Cloud and Infrastructure 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
- Organisations looking to expand without the burden of IT recruitment

1.4 Pricing

Cloud and Infrastructure Manage pricing is based on the number and type of devices combined with the size of the user base to be managed.

2 Detailed Service Description

2.1 Pre-requisites

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

- Cloud and Infrastructure Monitor and Cloud and Infrastructure Resolve
- The customer must provide a comprehensive list of devices to be managed complemented with a good standard of documentation
- The customer must provide relevant company detail such as quantity of users, locations, hours of work
- 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)
- 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
VM Setting Changes	CPU, Memory, Disk size
Minor Windows Configurations	Time, Regional settings, IP address, name, domain joining
Anti-Virus Installation	Installing anti-virus (AV) agents for existing AV solution
Client Application Installation	Installation of existing client applications

Physical Microsoft Windows Server	Included
Minor Windows Configurations	Time, Regional settings, IP address, name, domain joining
Disk expansion	Using RAID utilities and disk management to increase size of a volume
Anti-Virus Installation	Installing anti-virus agents for existing AV solution
Client Application Installation	Installation of existing client applications

VMware ESXi Server	Included
Minor ESXi 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

On-Premises Exchange / Online	Included
Transport Configurations	New connectors and changes to connectors, transport rules
SMTP Relay changes	Minor receive connector changes for SMTP relaying
User mailbox and distribution group management	Creating/deleting users' mailboxes (i.e. new starters/leavers), granting full access and send as permissions, calendar permissions (should encourage self-service), creating distribution groups and managing membership, setting forwards (should encourage self-service), quota changes
Message hygiene management (anti-spam)	Routine administration, releasing items from quarantine, blacklisting, whitelisting
Resource mailbox management	Creating and managing resource mailboxes e.g. room or equipment calendars

Database management	Creation/Removal, quota changes, logging changes, changes to existing Database Availability Groups (DAG)
Planned Cluster Failovers	Planned failover of DAG databases and client access
SSL Certificate Installation	Annual certificate renewal

Microsoft SharePoint	Included
Permission administration	Adding and removing user/group permissions for SharePoint libraries, folders, and files

Microsoft SQL	Included
Basic maintenance plan changes	Minor alterations to existing maintenance plans
Elective database backups/restores	Verifying backups, refresh demo/live databases

Microsoft Hyper-V	Included
Minor Windows Configurations	Time, Regional settings, IP address, name, domain joining
Disk expansion	Using RAID utilities and disk management to increase size of a volume
Anti-Virus Installation	Installing anti-virus agents for existing AV solution
Resource Management	Migrating VMs between hosts, changes to cluster configuration

Microsoft Remote Desktop Services (RDS) & Citrix	Included
Client Application Installation	Installation of existing client applications
Expanding farms	Cloning existing session host and adding to farm
RDS related Group Policy changes	Changes to RDS group policies such as farm settings, user lockdowns
Remote Desktop (RD) Gateway changes	Modifications to Resource Authorisation Policies (RAP) and Connection Authorisation Policies (CAP), changing user access
SSL Certificate Installation	Annual certificate renewal

Active Directory (AD) / Azure AD, DNS, DHCP	Included
Domain management	Minor changes to sites and services e.g. adding subnets, UPN suffixes, replication times, moving of FSMO roles. Removal of computer objects
User management	Starters/Leavers account creation and deletion
Group management	Creation/Deletion of security groups, membership changes
Organisational Unit (OU) management	Creation/Deletion of OU's and movement of objects
Group policy management	Modification of existing group policy, small additions to group policy
Azure AD Connect	Minor synchronisation changes

Active Directory Federation Services (ADFS)	Annual certificate renewal
DNS Management	Creation/deletion of static records, lookup zones, minor setting changes such as TTL, scavenging, forwarders. Public DNS records
Microsoft DHCP server management	Changes to existing scopes e.g. exclusions, reservations, lease length, scope options, conflict detection

Storage Area Network (SAN)	Included
Disk/LUN expansion	Using SAN Web User Interface (WUI) to increase the size of a volume
Host/Target/Permission changes	Adding/removing/changing iSCSI targets, CIFS or NFS Shares and permissions changes

Network Attached Storage (NAS)	Included
Disk/LUN expansion	Using NAS WUI to increase the size of a volume
Host/Target/Permission changes	Adding/removing/changing iSCSI targets, CIFS or NFS Shares and permissions changes

Veeam Backup	Included
Management of backup and backup copy jobs	Modifications to existing jobs, creation of jobs
Management of backup infrastructure	Minor changes including adding VMWare or Hyper-V hosts, adding or altering repositories, updating Veeam application
Elective Restores	Elective restores

Tape Backup	Included
Management of tape jobs	Managing tape catalogue, directing onsite staff on tape changes, advising on life span, drive cleaning, and optimising of jobs

Veeam Replication	Included
Management of replica jobs	Modifications to existing jobs, creation of jobs, managing offline replicas e.g. removing snapshots

Acronis Backup	Included
Management of backup jobs	Modifications to existing jobs, creation of jobs
Management of backup infrastructure	Minor changes including adding VMWare or Hyper-V hosts, adding or altering storage resources, installing agents
Elective Restores	Elective restores otherwise see "Cloud and Infrastructure Resolve" service

Reporting	Included
Service Report	Monthly reporting of: Ticket analysis, SLA compliance, client survey results

2.4 Exclusions

- 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
- Remediating issues caused by customer or third-party changes (this will be considered chargeable)
- 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
- 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
- Elective restores of more than one per quarter and exceeding a one hour restore time
- Disaster recovery planning and testing
- Deployment of any previously unconfigured services, features, new infrastructure, or applications
- Training
- Development
- Certificate management and installation (if not procured through Koris365)
- Issues caused by the improper management of SSL certificates
- Direct end user service requests (tickets must be raised by named representative who can authorise and provide the necessary information to fulfil the request)
- This is not a security service
- Third-party outages are beyond our control, Koris365 will advise of status updates as they become available
- Koris365 take no responsibility for false positives, malware, spam, or users disclosing their passwords
- 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
- 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
- Temporary guest wireless PSK provisioning, customer staff should carry out this task
- 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
- The provision of additional resources such as CPU, memory, disk, and IP addresses where sufficient spare capacity does not exist
- Customer is responsible for clearly communicating Firewall and Network changes; Koris365 is not responsible for any resulting weakening of security or direct/indirect impact on traffic forwarding

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 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 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, 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

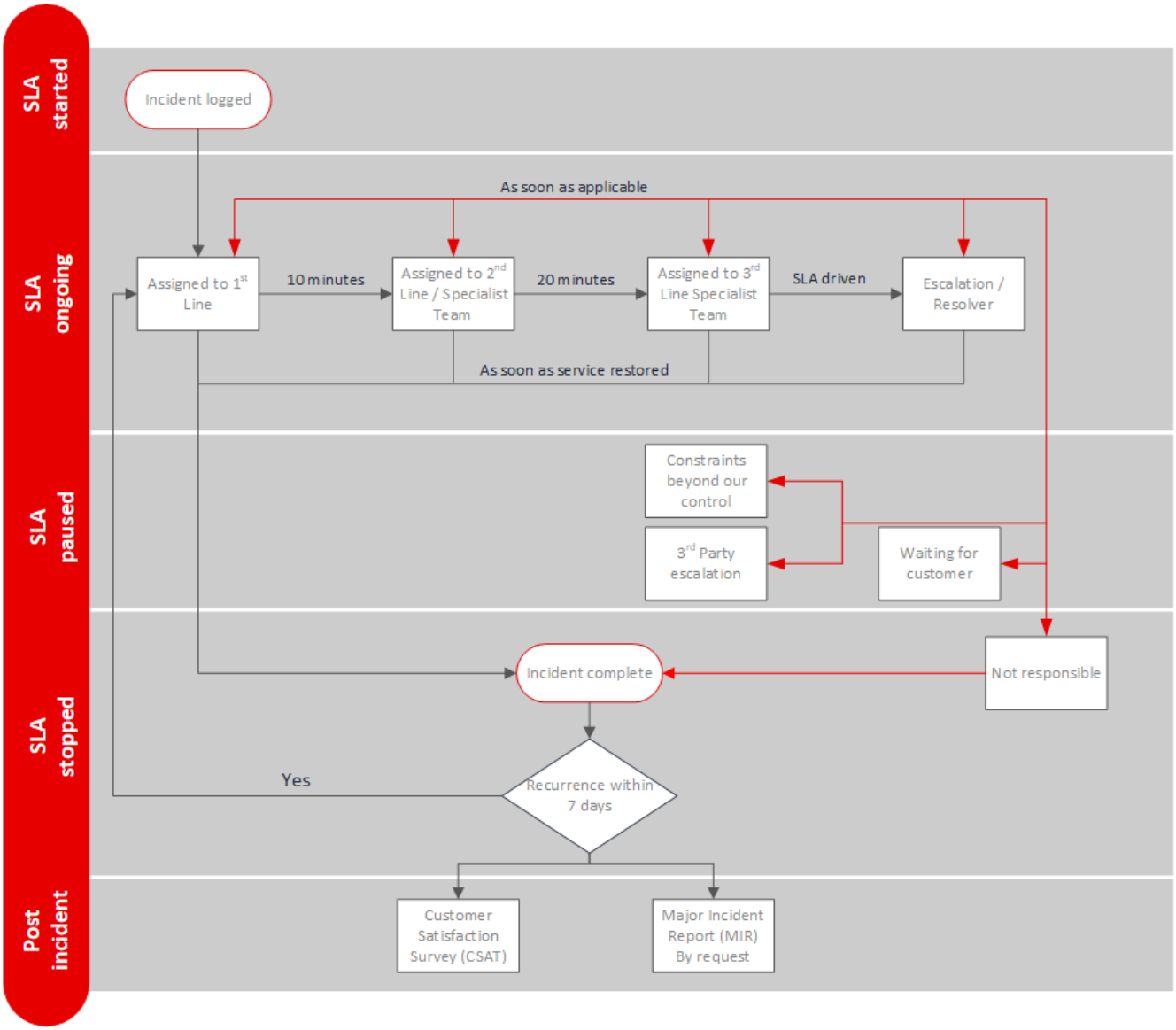
3.6.3 Incident Priority Matrix

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

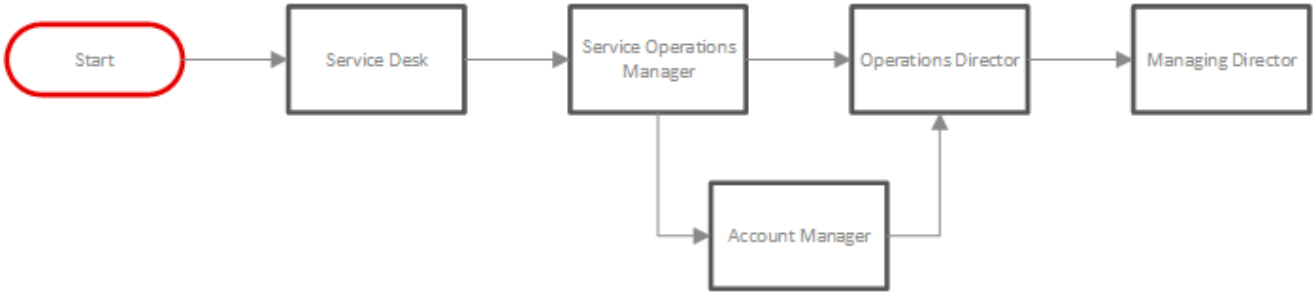
Priority Level	Action
Priority 1 (P1)	Servicedesk provide prioritised, sustained effort using all necessary resources until service is restored
Priority 2 (P2)	Service Desk reprioritise resources from lower priority jobs where necessary to focus on restoring the services
Priority 3 (P3)	Service Desk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