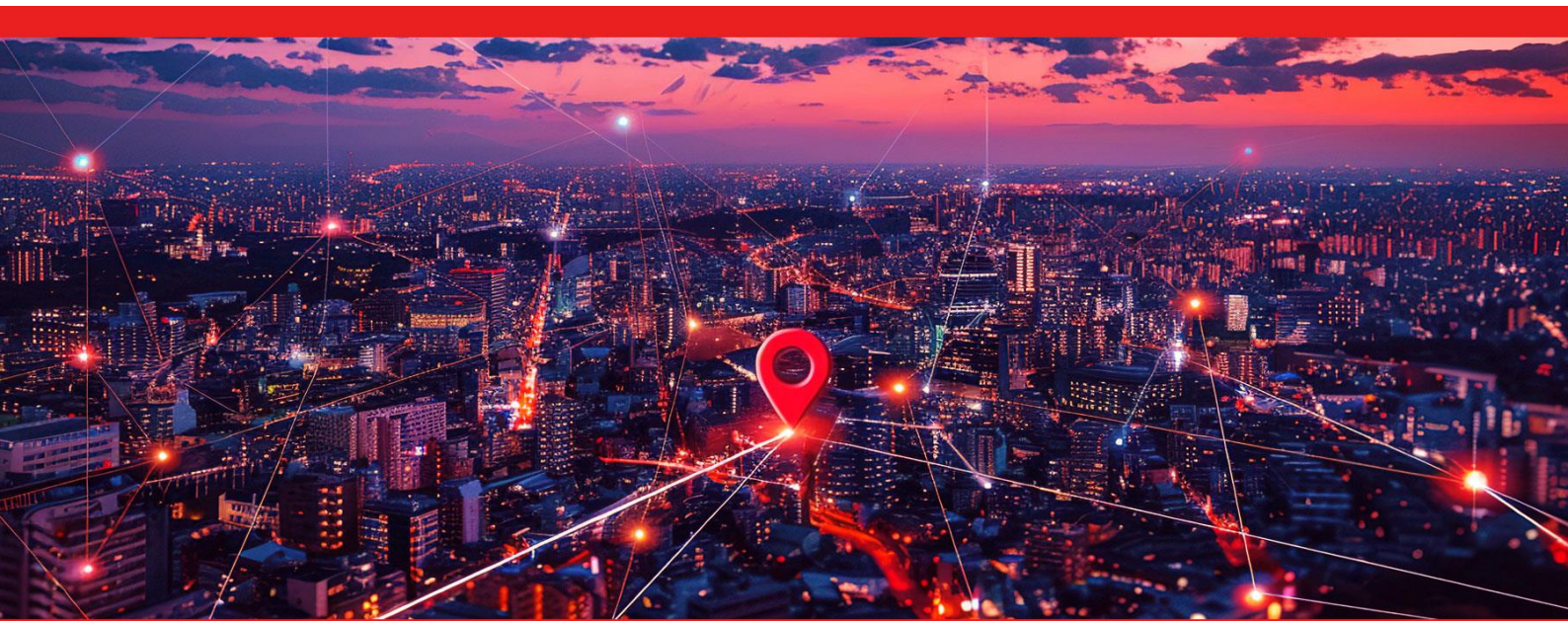# Cloud and Infrastructure Monitor

Service Description

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 It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without Koris365's prior permission in writing.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

Contents

1   Summary

1.1   Overview

Cloud and Infrastructure Monitor provides customers with a managed server and network monitoring and alerting solution. Cloud and Infrastructure Monitor can be delivered as a standalone service or as part of a more comprehensive managed solution.

1.2   Features

Features available in the Cloud and Infrastructure Monitor service include:

- Monitoring of server infrastructures
- Monitoring of applications and backup jobs
- Inclusive installation and ongoing maintenance of monitoring solution
- Email alerting of threshold breaches and service issues
- Server management portal options
- Monthly reporting

1.3   Suitable Customers

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

- Organisations with limited, or no, proactive monitoring capability
- Organisations struggling to deploy an effective internal monitoring solution
- Organisations not getting any value from their existing monitoring solution
- Organisations looking to remove the burden of managing a monitoring solution
- Organisations requiring monitoring ownership and accountability
- Organisations looking for a centralised remote server management tool

1.4   Pricing

Cloud and Infrastructure Monitor pricing is based on the number and type of devices that require monitoring.

2 Detailed Service Description

2.1 Pre-requisites

To provide the Cloud and Infrastructure Monitor service, Koris365 will require the following:
- The customer must provide a comprehensive list of devices to be monitored complemented with a good standard of documentation
- Koris365 must be provided with the necessary service accounts and permissions for the systems that require monitoring
- The customer will need to provide at least one named decision maker
- The customer must provide contact details for at least one technical person who will receive alerts

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. Koris365 makes initial deployment
5. Koris365 compares initial deployment with documentation and if required liaises with customer to perform fine tuning
6. Koris365 customer documentation is updated
7. Koris365 completes final deployment
8. Alert notifications and applicable portal access created
9. Business as usual monitoring and alerting commences

IMS 090 v1.0

2.3 Deliverables

Server	Included
Virtual Microsoft Windows Server	Anti-Virus (AV) status (vendor dependant), clock drift, CPU, memory, disk space, network connectivity, reboots, Windows services up/down
Physical Microsoft Windows Server	Hardware health (vendor dependant), AV status (vendor dependant), clock drift, CPU, memory, disk space, network connectivity, reboots, Windows services up/down
VMware ESXi Server	Network connectivity, datastore space, hardware health (vendor dependant), memory, CPU, maintenance mode, Network Interface Controller (NIC) status, logical drive performance, licensing status

Roles/Applications	Included
On-Premises Microsoft Exchange	Exchange specific Windows services up/down, HTTPS connectivity, SSL certificate status, back-pressure events, unexpected Database (DB) dismount events, information store performance warnings, DB mount status
Microsoft SQL	SQL specific Windows services up/down, SQL port availability, performance warnings
Microsoft Hyper-V	Hardware health (vendor dependant), AV status (vendor dependant), clock drift, CPU, memory, disk space, network connectivity, reboots, Windows services up/down, Hyper-V performance alerts

Storage	Included
Storage Area Network (SAN)	Network connectivity, hardware health (vendor and device dependant)
Network Attached Storage (NAS)	Network connectivity

Backup	Included
Veeam Backup and Replication	Backup and replication success/fail
Acronis Backup	Backup success/fail

2.4 Exclusions

- Any remediation without exception is not covered by Cloud and Infrastructure Monitor
- Remediation of issues caused by customer or third-party changes (this will be considered chargeable)
- Although performance/resource threshold monitoring is included and may allow customers to proactively prevent an outage, sudden unpredictable outages do occur of which there will be no warning
- Development of monitoring and management features
- This is not a security monitoring or Security Information and Event Management (SIEM) service
- Service wide outages that are beyond our control such as Internet Service Provider (ISP) failures will generate alerts but will also prevent polling, resulting in any coinciding issues becoming undetectable for the duration of the outage
- End of life operating systems, applications, and devices
- Renotification of repeat failures where the customer has not carried out remediation or recommendations

3 Service Level Agreement (SLA)

3.1 Hours of Service

Service	Mon - Fri	Weekends	Bank holidays
24/7	Monitoring and alerting are automated and running 24/7. 08:00 – 18:00 for monitoring alterations or platform help	Monitoring and alerting are automated and running 24/7.	Monitoring and alerting is automated and running 24/7.

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

IMS 090 v1.0
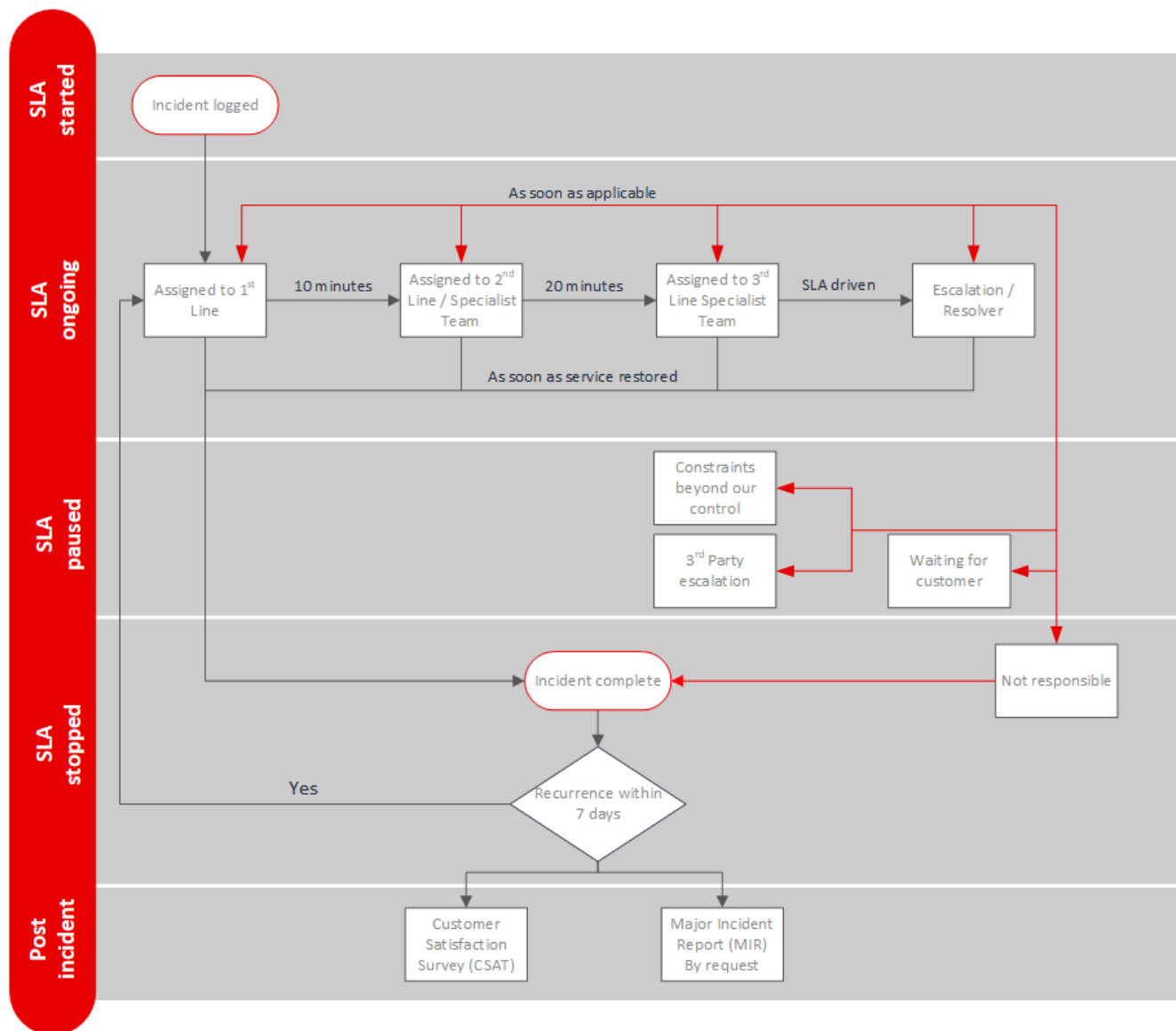
3.7.2 P3 and P4 Ticket Flow
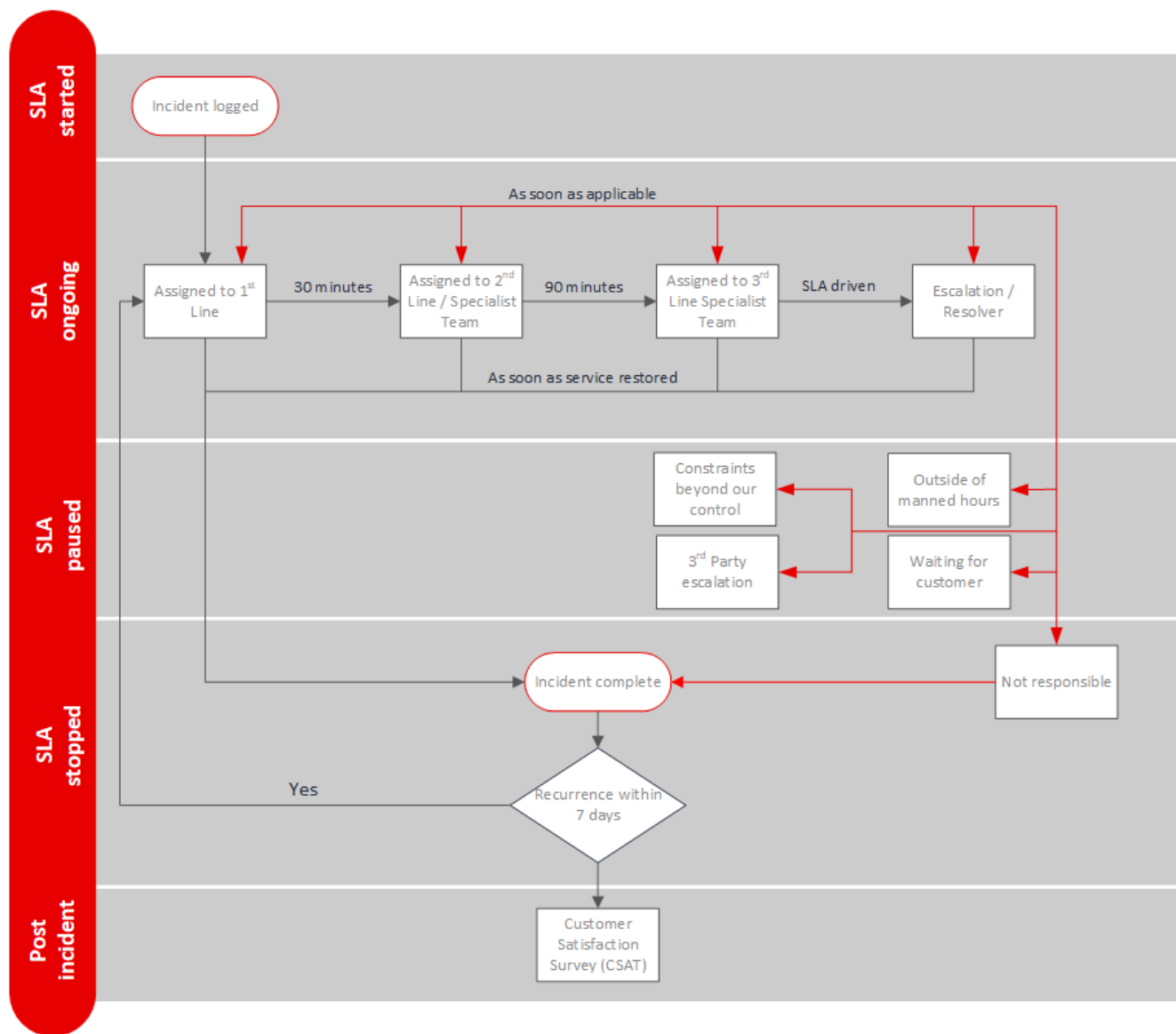
3.7.3 Customer Escalation

IMS 090 v1.0
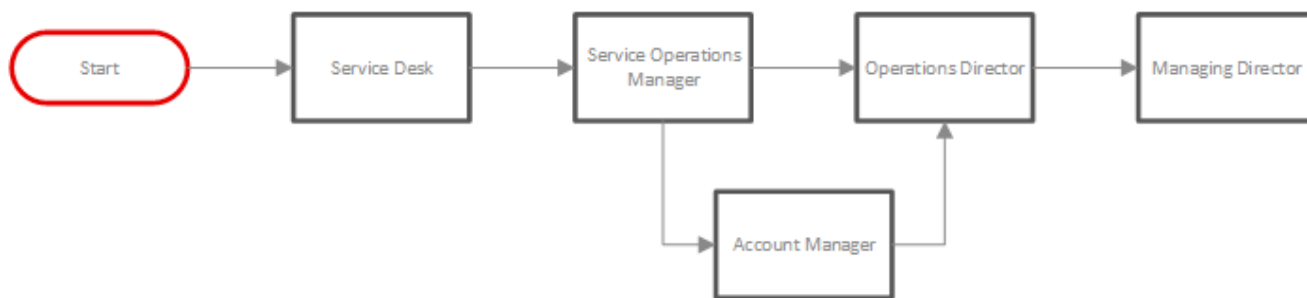
4 Offboarding Procedure

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