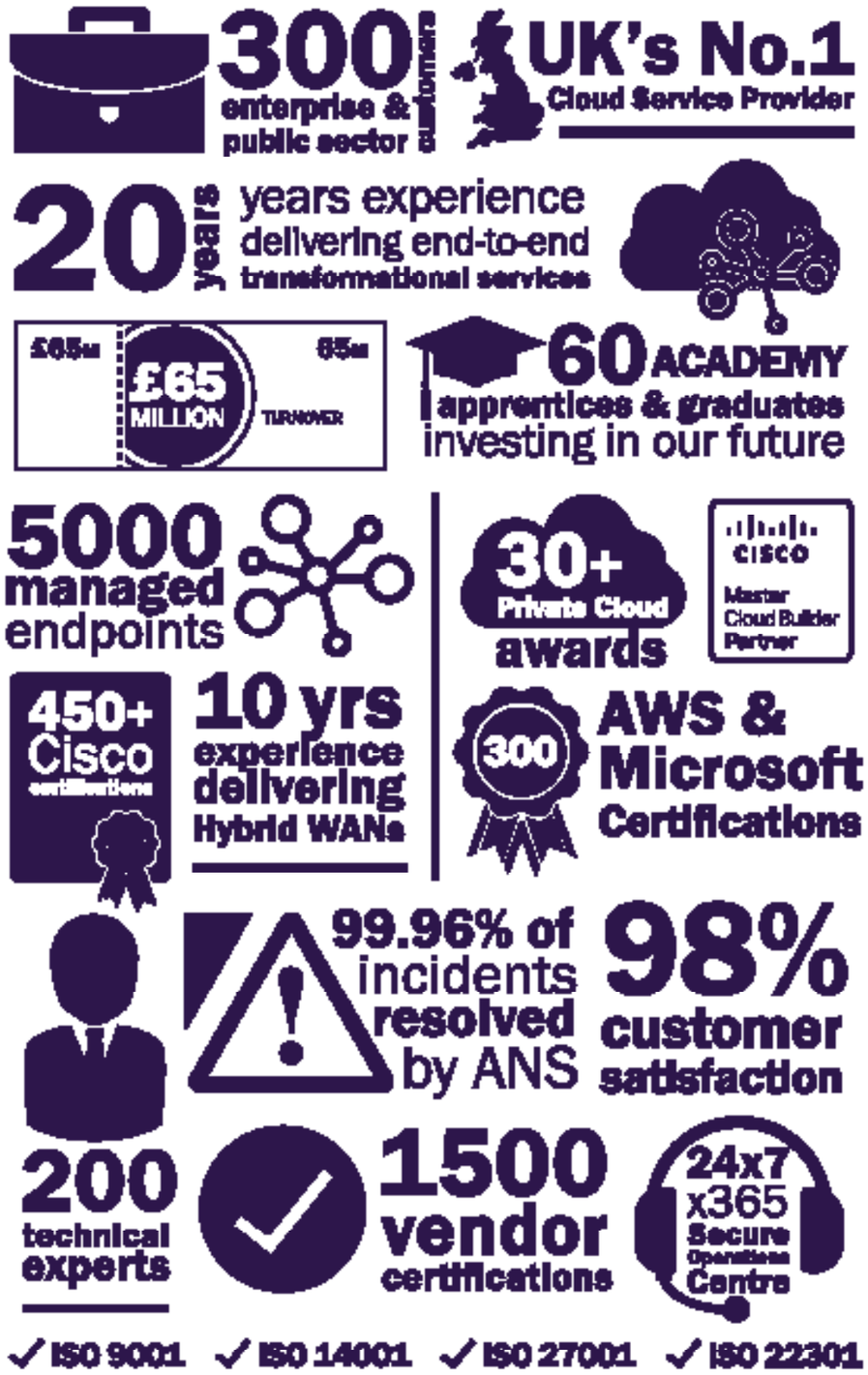
ans

Managed Services Handbook

Contents



1. Introduction.

The ANS Managed Services Handbook is intended to provide details of the Support Service offerings from ANS to our Managed Services customers. This document will further detail working processes, procedures and definitions of terms utilised by ANS in delivering Managed Services.

Customers are advised to refer to their individual Service Definition Document (SDD) for confirmation of specific Service Level Agreements and offerings.

1.1 How to contact ANS

General Enquiries
0161 227 1000

Service Desk 24x7
0333 0142 999

Email
servicedesk@ansgroup.co.uk

GLASS Portal and Mobile App
glass.ans.co.uk

1.2 Service Hours

Normal Business Hours
09:00 - 17:30 Monday to Friday (excluding bank holidays)

24 x 7 x 365
Manned Service Desk

1.3 Service Levels

We know that every business is different and has different challenges. To make sure you have access to a service that best suits your individual needs, we offer Enhanced and Managed levels of support, each providing access to the award-winning ANS GLASS platform, the next generation of service management reporting, review and control.

Enhanced

ANS Enhanced service provides you with 24/7 support, 30 minute responses to SLA's and access to the award-winning ANS GLASS platform. The first step of Enhanced begins with a detailed on boarding health check to understand the intricacies of your environment.

This is followed by the installation of our Enterprise Monitoring System, allowing us to tailor thresholds for such things as Disk Space, CPU Utilisation and System Performance to your specific needs.

Managed

ANS take complete responsibility for the availability of your IT platform with our Managed offering, providing your business with a utility grade SLA to guarantee the availability of your infrastructure.

Managed customers find that more than 75% of all incidents, proactively identified by our Enterprise Monitoring System are assessed and resolved with no interaction needed from the customer, freeing your team up to concentrate on driving your business forward.

Managed Cloud

Managed Cloud from ANS allows you to get the most out of your Public Cloud Investment. ANS' UK based advisory services, technical expertise, governance management and reporting will increase operational value, whilst our financial insights and automation reduce your platform consumption. Managed Cloud operates across 4 key domains: expert access, technical operations, financial insight and security and governance.

Each domain provides several core services to increase technical, financial and operational efficiency so you can focus on innovation and driving your business forward, whilst ANS focus on optimising your Public Cloud environment.

1.4 ANS GLASS

Our innovative digital platform, GLASS will enable you to access a range of key functionalities at your fingertips. The digital portal provides a single view of your service, allows you to run expedient reporting and review service level data.

Developed and driven by the individual requirements of each of our customers, the platform allows complete access and control over real-time updates. Easily view, add and update all incidents and changes within the platform, from any device, anywhere, anytime.

The portal offers an updated and efficient way for you to communicate any requests or notifications with ANS, allowing you to do the following;

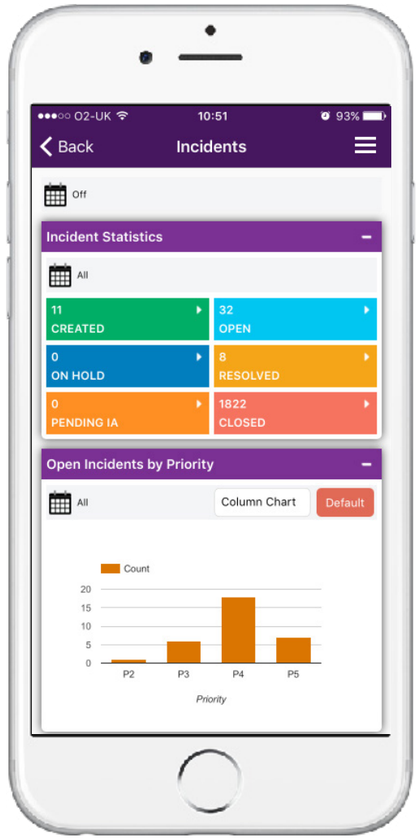
- **Action incidents and changes**
- **Monitor and track key information about your live projects**
- **Monitor your AWS or Azure environment including month to date spend in real time, billing history and cost savings.**
- **Access transparent and detailed contract information**
- **View specific date information such as scheduled changes and consultant days in our calendar view**

Access to the GLASS portal will be provided at the point from which you are on-boarded to your ANS Managed Service. At this point you will be asked to complete a set of security questions in order to complete your account registration.

Should you have any issues when registering or when utilising the portal please contact the ANS service desk.

GLASS is also available on iOS and Android devices, enabling you to add incidents and changes and view updates on the move.

To access our customer portal please go to **glass.ans.co.uk**



1.5 ANS 'AAS' Offerings

ANS offers a catalog of As-a-Service solutions. More information about each service can be found below.

IaaS

The ANS Infrastructure as a Service provides customers with a Managed Hosting Service for running their virtual machines and associated workloads. Over multiple service tiers, the platform can provide flexible topologies and architectures for applications. Security services and internet breakout is also available as remote access and private connectivity

BaaS

The ANS Backup as a Service provides customers with a mechanism to backup systems running on their own infrastructures to the ANS cloud based service. This service provides long term retention models and simple to use restore interfaces in a central web interface. Support for most Operating Systems, Applications & Hypervisors means that the service provides a single pane of glass to our customer's backups/restores.

MaaS

The ANS Monitoring as a Service is used for monitoring our customers' devices and provides fast and efficient processing of all alerts. The services provide proactivity and acts as a warning mechanism to avoid any major disasters. It also reduces the mean time to resolution by allowing analysts to see everything through a single pane of glass.

SECaaS

The ANS SECaaS Authentication Service provides a cloud hosted second factor authentication service, utilising software token devices that can be installed onto mobile phones or laptops, the service supports any device that can utilise the industry standard RADIUS protocol. User provisioning and de-provisioning is fully automated utilising the customers' existing Active Directory infrastructure as an identity source and synchronising users based upon group membership.

DRaaS

Disaster Recovery as a Service from ANS provides business continuity and disaster recovery solutions for virtualised IT within SME and Enterprise organisations. Using hypervisor-based data replication for VMware vSphere estates, ANS DRaaS offers a low impact solution that will ensure a seamless failover in the unfortunate event that offsite recovery is required. Providing RTO and RPO guarantees, customers applications are brought up with minimal to zero data loss.

TMaaS

ANS' Threat Management-as-a-Service solution combines Cloud-based software and innovative analytics to assess, detect and block threats to applications and other workloads. We help you achieve compliance requirements whilst defending against a broad range of server-side threats. By using Alert Logic SaaS threat management, alongside ANS technical experts, we deliver better cloud and web application protection, reduce your risk of adopting cloud whilst accelerating the growth of your business.

Managed Patching

Managed Patching from ANS provides proactive management of your patching requirements removing the administrative overhead on IT Operations staff to ensure IT systems remain compliant and secure. The service includes detection and delivery, for your network and platform endpoints to ensure your systems are up to date with the latest security patches.

2. Incident Management.

All incidents will be recorded in the ANS Service Desk ITSM system under the Incident Management workflow. ANS records the name of the person reporting the incident, the time of the call and any other pertinent information, along with criteria for resolution to ensure that the workflow is initiated correctly.

Please note that support for customer-initiated Business Critical Issues is via telephone only and we cannot offer any SLAs for Business Critical Issues via email.

2.1 Named Contacts

The Incident Management service is available to a defined list of Named Contacts with varying levels of authority for incident, change and escalation.
Escalation Contacts are the relevant Stakeholders within the customer organisation that will be informed of the status of any P1 incidents. This will take the form of automated emails and phone calls (where applicable).
If you require a change to any contacts, please complete a Change Name Contact Request form, which can be downloaded from the ANS extranet at **ansgroup.co.uk/ms-documents**, and send to **servicedesk@ansgroup.co.uk**. Please note that the sender must be also a Named Contact on the SDD.

2.2 Logging a New Incident

Details required when logging a new incident:

- Customer name
- Contact name
- Product/Server/Device/Circuit
- Details of symptoms experienced
- Details of any recent changes
- Impact to the business
- Affect on systems/services

All new incidents will undergo an initial impact assessment. ANS will further look to determine the number of users/systems affected and establish the commercial impact to the client's environment. Please refer to section 2.5.1 for the Incident Impact Assessment Matrix.
When logging an incident via email it is expected that the originator will provide the above information at a minimum, plus any screen shots, diagnostic data and/or diagrams as necessary.
Please note that incident response times will be delayed should this information not be provided.

2.3 Criteria for Resolution

The criteria for resolution are agreed as part of the impact assessment. When the criteria are met the incident is deemed to be resolved, at which point the ANS Service Desk will contact the originator to confirm authority to close the incident.

2.4 Incident Handling

Once logged, incidents are managed within ANS' ITSM system in-line with the assigned priority. All actions and associated updates are logged throughout the incident lifecycle with periodic updates sent to the originator.
On resolution, the ANS Service Desk will contact the originator to confirm authority to close the incident.
Please note that the ANS Service Desk will make a maximum of three attempts to contact the incident originator in order to confirm authority to close.
If all three attempts to make contact are unsuccessful, the incident will be closed automatically with notification sent to the originator via email.
Please refer to Appendix B of this document for the Incident Management workflow.

2.5 Priority Definitions

2.5.1 Incident Assessment Matrix

Affect	Business Impact		
	Minor	Moderate	Major
System / Service Down	P3	P2	P1
System / Service Affected	P4	P3	P2
User Down / Affected	P5	P4	P3

2.5.1.1 Priority 1 (P1)

At this priority level both ANS and the customer must commit to round-the-clock response times and involvement by all necessary and appropriate personnel/systems until a mutually agreeable workaround is provided and the priority is no longer considered to be P1. ANS classifies all P1 incidents as Major Incidents (MI). Please refer to Appendix C for the ANS MI Workflow.
Examples of a P1 incident include: server, site/circuit, node, system or cluster is down, unable to serve data, is in a state of frequent or repeating crash, panic or hang or is in a state of degraded performance sufficient to prevent critical business operations.

2.5.1.2 Priority 2 (P2)

At this priority level ANS is committed to a commercially reasonable effort to provide a workaround and/or restore normal operations as quickly as possible during Normal Business Hours.
Examples of a P2 incident include: when a server, site/circuit, node, system, or cluster is experiencing an infrequent, isolated or intermittent crash, panic or hang, or is in a state of degraded performance that allows business operations to continue but at an inconsistent or less than optimal rate.

2.5.1.3 Priority 3 (P3)

At this priority level ANS will, during Normal Business Hours, work towards a viable and mutually agreeable workaround or propose an upgrade or replacement to mitigate the problem.
Examples of a P3 incident include: server, circuit, node, system, or cluster is experiencing an issue, anomaly or cosmetic defect that inflicts little or no business impact.

2.5.1.4 Priority 4 (P4)

At this priority level ANS will, during Normal Business Hours, provide advice on whether a workaround, upgrade or replacement to mitigate an issue is available.

2.5.1.5 Priority 5 (P5)

At this priority level ANS will, during Normal Business Hours, provide answers to "How do I...?" type queries.

2.6 Out of Hours Service - Night Watch

We monitor your infrastructure 24x7x365 from our Secure Operation's Centre located in our Head Office in Manchester. Operating around the clock ensures that in the event of a major incident (P1), our Technical Analysts are always available, no matter what time you experience a critical error. When a P1 is raised, our team of Technical Analysts initiate the ANS major incident workflow. ANS will then follow the incident management workflow and assign the service request to a Level 3 Analyst so that the request can be worked on immediately.
Please note that this service may be subject to additional service charges if it is not within the scope of your SDD.
Please see Additional Services Charges for more information.
We also have an out of hours Duty Manager that can be contacted when needed by calling **0333 014 2999** and selecting the option for Duty Manager.

3. Service Level Agreements (SLAs) & Key Performance Indicators (KPIs).

Business Impact	Response SLA	Specialist Review	Escalation Manager	Escalation Director/ Vendor	Email Frequency	Target Resolution KPI
P1	30 minutes	1 hour	Immediate	Immediate	Hourly	4 hours
P2	1 hour	2 hours	4 hours	None	GLASS Portal	1 day
P3	4 hours	1 day	2 days	None	GLASS Portal	10 days
P4	1 day	Never	Never	None	GLASS Portal	30 days
P5	2 days	Never	Never	None	GLASS Portal	None

Please note these are our standard SLAs and we would advise our customers to refer to your SDD for information on your specific Service Level Agreements and Key Performance Indicators.

4. Problem Management.

"Our Problem Management function works along-side our Service Management, Event Management and Service Desk Teams to ensure swift identification of Problems. Problems are proactivity identified using trend identification techniques and service management reporting delivering added value to our Managed Service Customers."

STEVE BREEN
HEAD OF MANAGED SERVICES

A problem may be the cause of one or more Incidents, although the potential cause is not usually known at the time the problem record is created. In order to prevent problems and resulting Incidents from reoccurring, Problems are investigated by using a variety of methods to determine root cause and effective resolution or workaround. Once root cause is established it is then documented using ANS' Knowledge Management Process. A Known Error is recorded to help reduce the meantime to resolution of future incidents and to expedite resolution of future problems for other customers. Problem information is reported and discussed during a Service Management Review meeting with your assigned Service Manager.

5. Change Management.

5.1 Request for Change (RFC)

All change requests must be submitted using the ANS Request for Change Form (RFC) on your GLASS portal.
Upon receiving the RFC an ANS Technical Analyst will evaluate the form and determine the nature of the change before confirming with the requester. Once accepted, Standard Changes will be put forward for scheduling whilst Normal changes will be submitted for SME review before CAB approval.
Please note that an incomplete RFC will be rejected by the Service Desk along with an explanation as to what is missing and further details of any actions needed to be taken before re-submission. It will be assumed that all RFCs sent by the customer are pre-approved.
Please refer to Appendix F for full details of the ANS Change Workflow.

5.2 Standard Changes

Standard Changes are pre-approved changes that have been through the full Change Management Process, including Change Advisory Board (CAB) approval at least once. The delivery process and detail is documented and templated within the ANS ITSM Tool to ensure smooth and timely delivery of the change. ANS' Teams can request a Normal Change to become a Standard Change by requesting this in the ANS ITSM Tool which are then reviewed during CAB.
Please visit **ansgroup.co.uk/ms-documents** for the latest list.

5.3 Emergency Changes

ANS classifies an Emergency Change as a Change required in order to resolve or implement a tactical workaround for a P1 incident. All Emergency Changes are subject to approval by both the ANS Emergency CAB and the customer before implementation.
An example of an Emergency Change would be if the Operating System on a Virtual Machine has been corrupted and a replacement Virtual Machine needs to be re-provisioned/restored immediately in order to resolve a P1 Incident.
Please refer to Appendix G for details of the ANS Emergency Change flow.

5.4 Normal Changes

Normal Changes are all Changes that are not classified as Standard or Emergency. Once logged, all Normal Changes are assessed against the following risk matrix and assigned a CR ranking (see right).

Once assessed, the change will then be submitted for further technical review by an ANS Subject Matter Expert (SME) before submission to CAB. Normal Changes will not be implemented until they have been reviewed and approved by the ANS CAB.

Impact on Service	Low	Medium	High
High	Significant 3 CR3	Major 2 CR2	Critical 1 CR1
Medium	Minor 4 4 CR4	Significant 3 CR3	Major 2 CR2
Low	Candidate for Standardisation 5	Minor 4 4 CR4	Significant 3 CR3

Probability of Negative Impact Until Change is Successfully Completed

5.5 Change Advisory Board (CAB)

The ANS Change Advisory Board (CAB) convenes each Tuesday and Thursday during normal business hours. The function of the CAB is to:

- Review and approve or reject all Normal Change requests logged since the last CAB meeting.
- Review all Emergency Changes that have been implemented since the last CAB meeting.
- Review all failed/rejected changes since the last CAB meeting.
- Please note: The deadline for submitting normal changes is 9:30, 1 working day before CAB convenes.

5.6 Emergency Change Advisory Board (ECAB)

The Emergency CAB is available 24x7 and convenes as soon as an Emergency Change request is raised.

A Named Contact from the customers' business must also approve all Emergency Changes before implementation. Once approved, the Emergency Change will be implemented immediately.

Emergency Changes are usually a result of a P1 scenario and will ultimately help to resolve the problem.

5.7 Approval & Rejection of Change

During the assessment stage of a change the ANS analyst will agree an implementation date before submitting to the customer for approval. Once the customer has approved the change only then will the change be submitted to CAB. Change notifications and approval actions will be accessed through Glass. The customer also has the ability to reject a change. If the CAB approves the Change, they will inform the ANS Technical Analyst who logged the RFC that it can proceed.

If the CAB rejects the RFC, they will provide reasons and further actions for the ANS Technical Analyst to communicate to the change originator. The Change should either re-submitted and reviewed at the next CAB meeting or rejected and the customer will be notified.

6. Service Management.

We offer 'high touch' service management and we aim to spark a service focussed partnership with the customer, whether ITIL or DevOps aligned.

ANS Group adheres to a robust Service Management process, including but not limited to the following:

6.1 Service Review

Service Review documents are either sent or presented to customers to detail the service metrics of the Operational Service during a given period.

These metrics include:

- Incident/Problem and Change reporting
- Trend Analysis
- Utilisation statistics
- Capacity reporting/Management*
- Release reporting/Management*
- Performance statistics*
- Vendor incident breakdown
- Quality Issues
- SLA management and measurement
- Contract Renewals

*where applicable

6.2 Cloud Score

Cloud Score is our scoring mechanism to determine and rate a customer's overall cloud health, so that the cloud environment can be improved.

The scoring works by breaking down various elements of your cloud environment, such as cost optimisation, tagging, monitoring, and security. Alongside this, you'll gain a complete insight into how well your environment is operating. A rating is then calculated by our Cloud SME's who will provide recommendations to optimise your environment and increase your overall rating.

7. Customer Responsibilities.

Depending on your level of service from ANS there are some requirements for the maintenance and care for your environment, and guidelines for the term of your service.

Please note that customers can add in scheduled maintenance via GLASS. To find out more about your specific responsibilities, please refer to your SDD.

7.1 Maintenance Windows

In the event of any maintenance work taking place by the customer that may affect the service ANS are providing; notification should be sent to **scheduled.maintenance@ansgroup.co.uk** with the outage notification form that can be found on our website: **ansgroup.co.uk/ms-documents**. Failure to do so may result in additional service charges.

Please consult the ANS Terms and Conditions for ANS' scheduled maintenance details: **ansgroup.co.uk/site-info/terms conditions.**

7.2 Onsite Hands & Eyes

During investigations into a potential a hardware or software fault it may be required to reseat certain elements of the device/ infrastructure onsite. This task sits with the customer (unless within ANS Data Centres that have a colo contract including Level 1 Hands and Eyes). If the customer requires ANS onsite hands and eyes then this will be subject to additional service charges.

7.3 Assets & Locations

The Customer shall request permission from the Supplier in writing in the event that the Customer wishes to change the location of the Customer Assets and/or Supplier Assets from the address specified in the Contract. Any asset that has been moved without notification to ANS will be subject to additional service charges.

8. Enterprise Monitoring & Event Management.

The ANS Enterprise Monitoring System is used for monitoring our customers' infrastructure from the Service Operations Centre (SOC) within our Head Office located in Manchester.

Our Enterprise Monitoring System (EMS) is a SaaS based system which offers data sovereignty; meaning that all data remains in the UK,which negates current concerns that surround data protection. Enterprise Monitoring technology evolved out of the unique monitoring needs of data centres and enterprise networks.

Data centres have SOC Type II assessment and SSAE16 and ISO27001 meaning that the model uses a highly robust infrastructure in a highly resilient and secure data centre. The system has been designed and approved by our own Subject Matter Experts (SME's), who hold high-level accreditations in our core technology areas: NCIE, CCIE, CCIA, VCAP, MCSE AND MVP.

The technology provides comprehensive, flexible, easy-to-use monitoring functionality that provides an improved insight into how customers network, applications and infrastructure are performing. This feature supports the timely detection and notification of impending IT problems across your enterprise.

8.1 Enterprise Monitoring System

ANS will install either a physical or virtual collector server onsite as part of your Managed Service.

The physical or virtual collector will connect back to the datacentre using a secure encrypted connection. This information is then fed through ANS' custom filters, and events are created via rules and agreed thresholds. These Events can be in the form of an email or a telephone call and are displayed on the management consoles for viewing by our Technical Analysts.

Customers will also be given read-only access to our Managed Service Portal which will provide access to view alerts and updates.

8.2 Event types– Warning, Errors & Critical

Events are dependent on type and criticality. They are routed via the EMS Dashboard or automated phone system including updates to the ANS SOC Wallboards. Critical Events take an expedited workflow ensuring urgency and impact are quickly identified. Depending on the service obtained, ANS can deliver a bespoke workflow to allow customers to receive alerts via phone, email or text.
Each event is categorised as one of the three following types:

- **Warning**

Warning Events include systems or processes that may have reached a predefined warning threshold, such as a WAN link bandwidth reaching higher than usual thresholds but not service impacting. Depending on your level of service, the alert will be escalated to you, or the SOC will then review and assess if any further preventative action is required in order to mitigate possible system impact.

- **Error**

Error Events include systems or processes that may have reached a predefined warning threshold, such as Storage Volume capacity reaching 80%. Depending on your level of service, the alert will be escalated to you, or the SOC will then review and assess if any further preventative action is required in order to mitigate possible system impact.

- **Critical**

Critical Events include a System or Process that has either reached a predefined critical warning level such as a Storage Volume capacity reaching 90%, or a System, Service or Device down. The SOC would first assess to ensure the Event is related to a genuine alert before initiating the Incident Management process.

8.3 Security Event Management

Security Events are handled as part of the same process "Event Management". When a Security Event requires action the Incident or Change Management Processes are engaged. Security tickets are kept indefinitely.

9. Release Management.

9.1 Release Management

ANS follows a strict Release Management policy, whereby all new software releases for our supported products are submitted through our internal release testing process. Only on successful completion of this testing process are releases or patches classified as "ANS recommended" or "Safe harbour".

This information is then fed in to the Service Management team to highlight any exposures or recommended upgrades to our customer base.

Please refer to Appendix H for further details on the ANS Release Management Workflow.

9.2 OS Patch Management

As part of the on-boarding of a new Managed OS Service, ANS will endeavour to agree a process that best suits the customer's needs and requirements for OS Patching depending on various factors, such as:

- Frequency
- Deployment technology such as WSUS/ SCCM
- Level of testing UAT required
- Types of patches to be deployed by ANS

Once agreed, this information forms the basis of a Document of Understanding (DoU) between ANS and the customer.

An example of a standard patch process is illustrated in Appendix I.

10. Additional Service Charges.

All services may be subject to Additional Service Charges if outside of the scope of your Service Definition and/or SLA:

Service	Charge
Normal Business Hours (Remote Support)	£250 per hour
Out of Hours (Remote Support)	£450 per hour
Normal Business Hours (Onsite L1 Engineer Support)	£300 per hour
Out of Hours (Onsite L1 Engineer Support)	£500 per hour
Daily Rate (Onsite Consultant)	£1250 plus expenses
Bank Holidays & Weekends Rate (Onsite Consultant)	£1875 plus expenses

Below are examples where Additional Service Charges will occur, including but not limited to:

- Normal Changes above 2 hours (subject to scope of contract)
- Project Work
- Configuration changes not verified by ANS CAB of any supported assets that subsequently causes an outage/Incident to be logged
- Unauthorised change of any supported Asset of any managed asset
- Remediation of supported assets resulting from any power outage
- Logging any non-P1 call Out of Hours (unless covered within the customers service definition document)
- Break-fix only contract customers logging non-hardware P1 calls Out of Hours
- Deviation from the agreed scheduled maintenance window process
- Remediation of security breaches
- Remediation of customer caused incidents
- Remediation of unauthorised changes by the Customer

Please refer to your SDD for full detail of inclusive services.

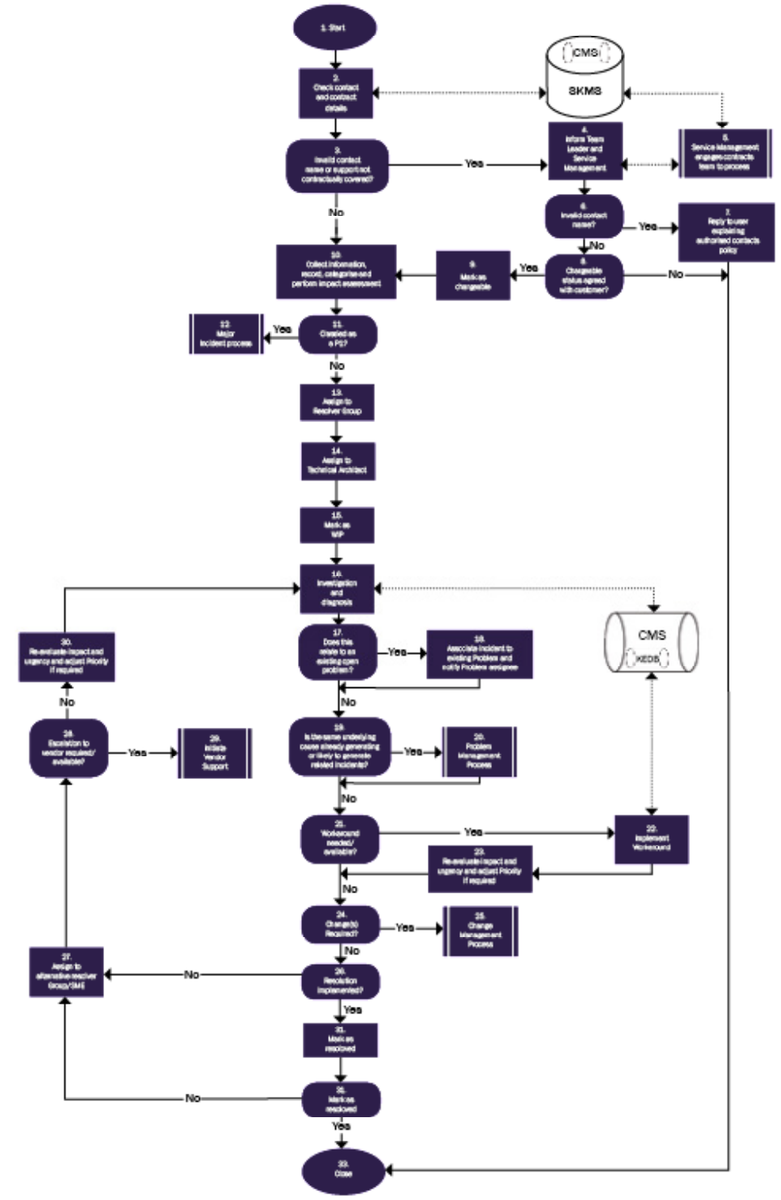
Appendices

11. Appendix A - ANS Escalation

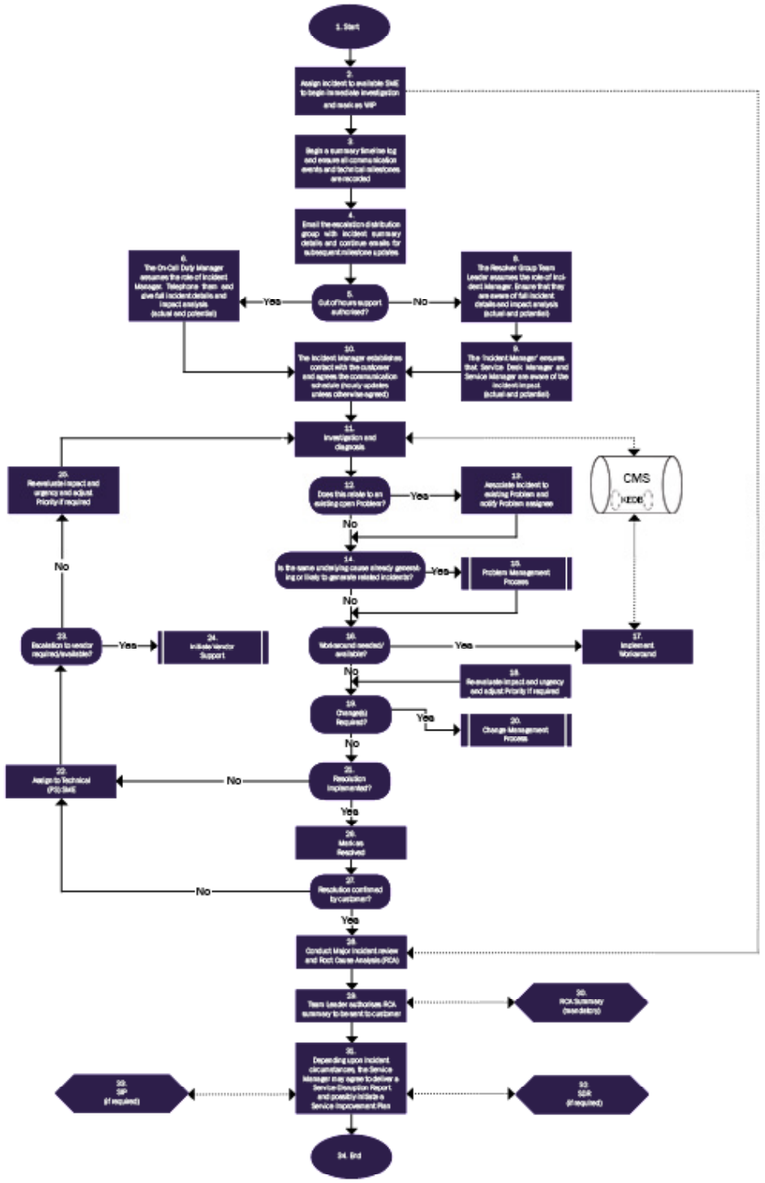
Level	Contact	Definition	Name	Contact	Roles / Responsibilities
1	Service Desk Technical Analyst	Incident is with the Service Desk.	Service Desk	+44 (0)333 014 2999	All tasks involved with incident management.
2	Service Desk Team Leader	Incident has been escalated to Team Leader. Team Leader to monitor incident to resolution, including all P1 Incidents.	Infrastructure Data Centre i3 Infrastructure Network Infrastructure Applications	+44 (0)333 014 2999	Can allocate additional resource and/or equipment.
3	Service Manager	Incident has been escalated to Service Manager or Service Desk Manager.	Service Manager/Simon Brooks (Service Desk Manager)	+44 (0)161 227 1000/ +44 (0)333 014 2999	Prioritisation/re- allocation of equipment and/or additional resource. Help to manage stakeholder communication.
4	SDM	Service Delivery Manager	Melissa Johnson	+44 (0)161 227 1000	Manages the Service Management function to ensure the right level of engagement and activity is taking place. .
5	Head of Managed Services	Head of Managed Services	Steven Breen	+44 (0)161 227 1000	Empowered to use all resources available to ANS. Will discuss incident at ANS Director level.
6	COO	Chief Operating Officer	Chris Hodgson	+44 (0)161 227 1000	Ensures that all other parties of escalation path have acted as expected and utilised all available means to resolve the Incident.

- Escalations are 24/7; however, steps 3 & 4 are replaced with the Duty Manager outside of Normal Business Hours.
- Escalations are automated via ANS' ITSM system but can be manually triggered as required.
- Escalation paths may be expedited depending on Incident priority

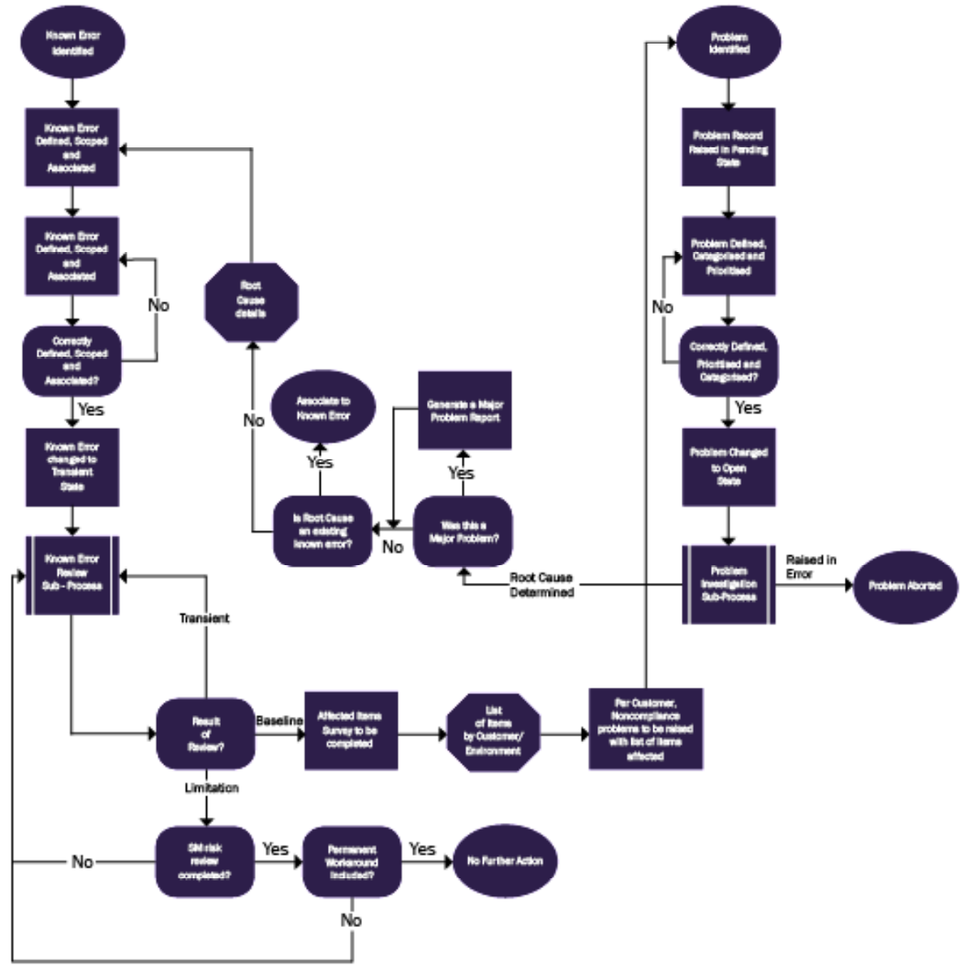
12. Appendix B - ANS Incident Management Workflow



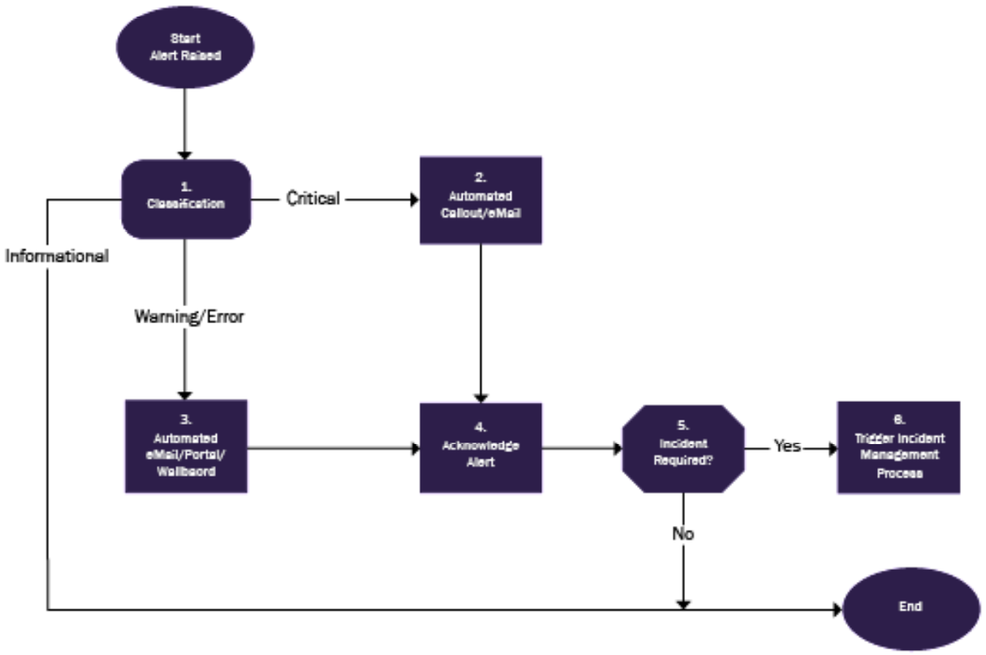
13. Appendix C - ANS Major Incident Management Workflow



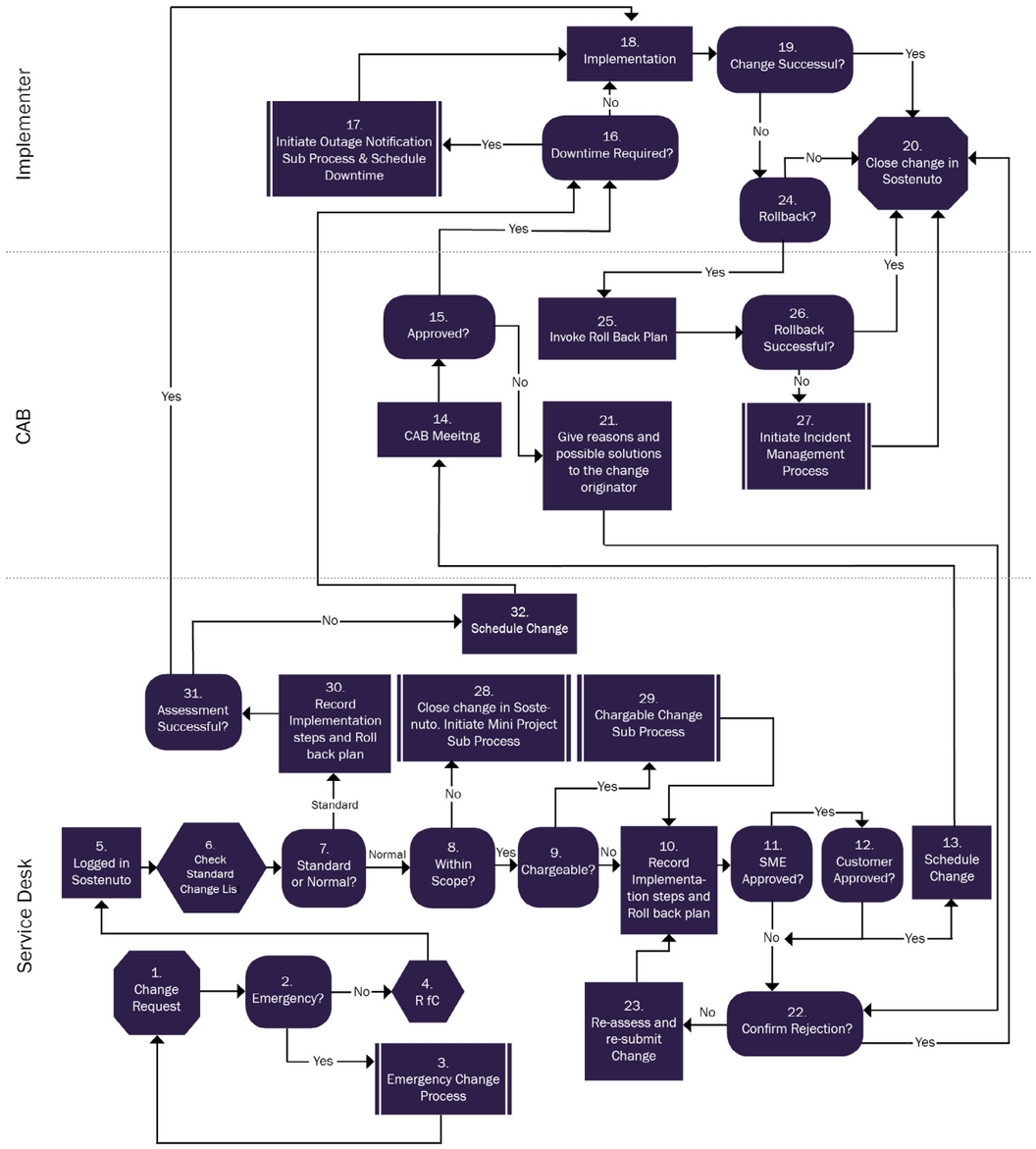
14. Appendix D - ANS Problem Management



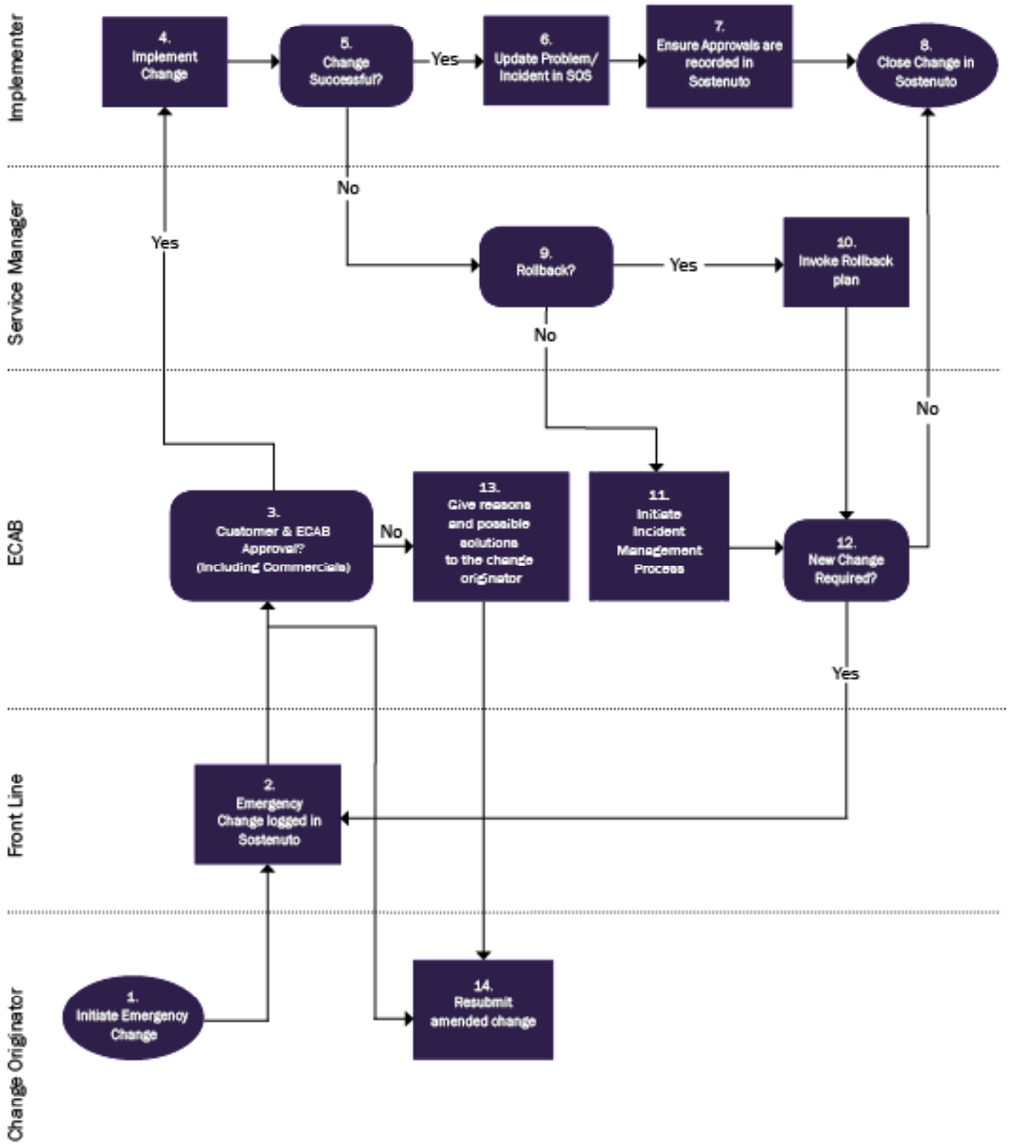
15. Appendix E - ANS Event Management Workflow



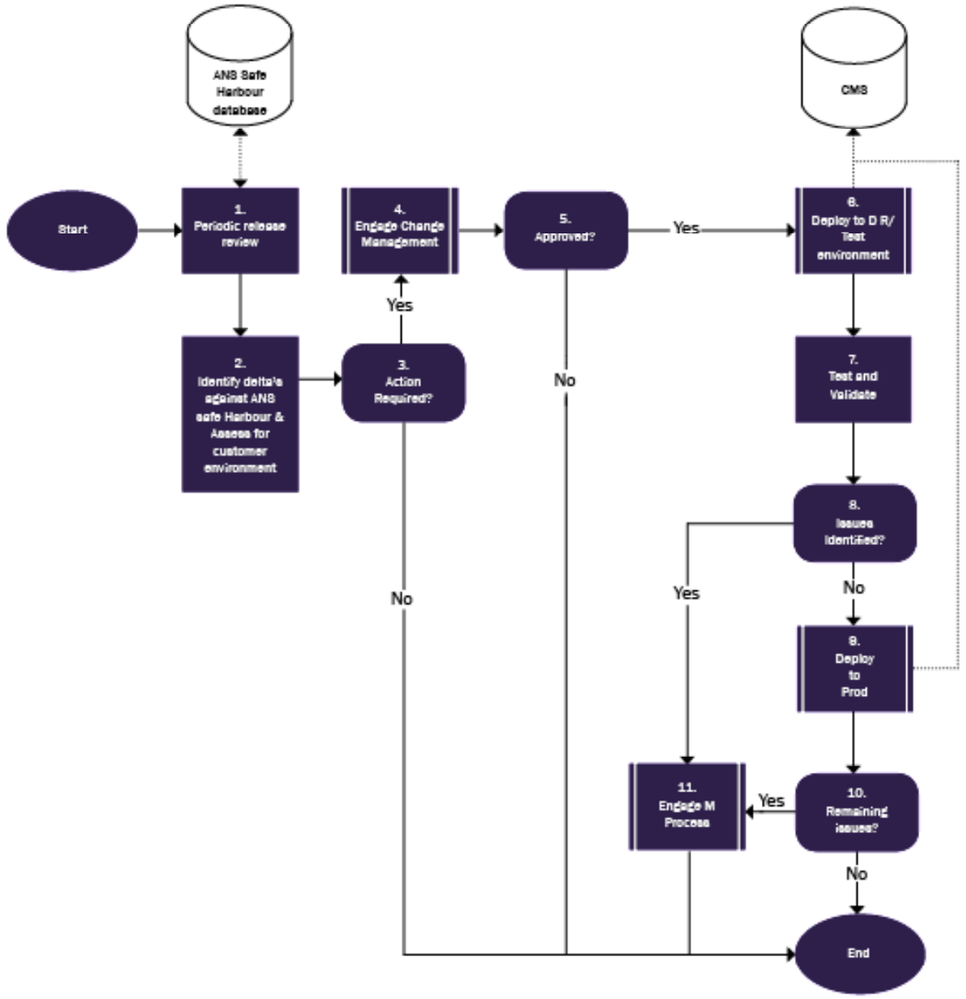
16. Appendix F - ANS Change Management



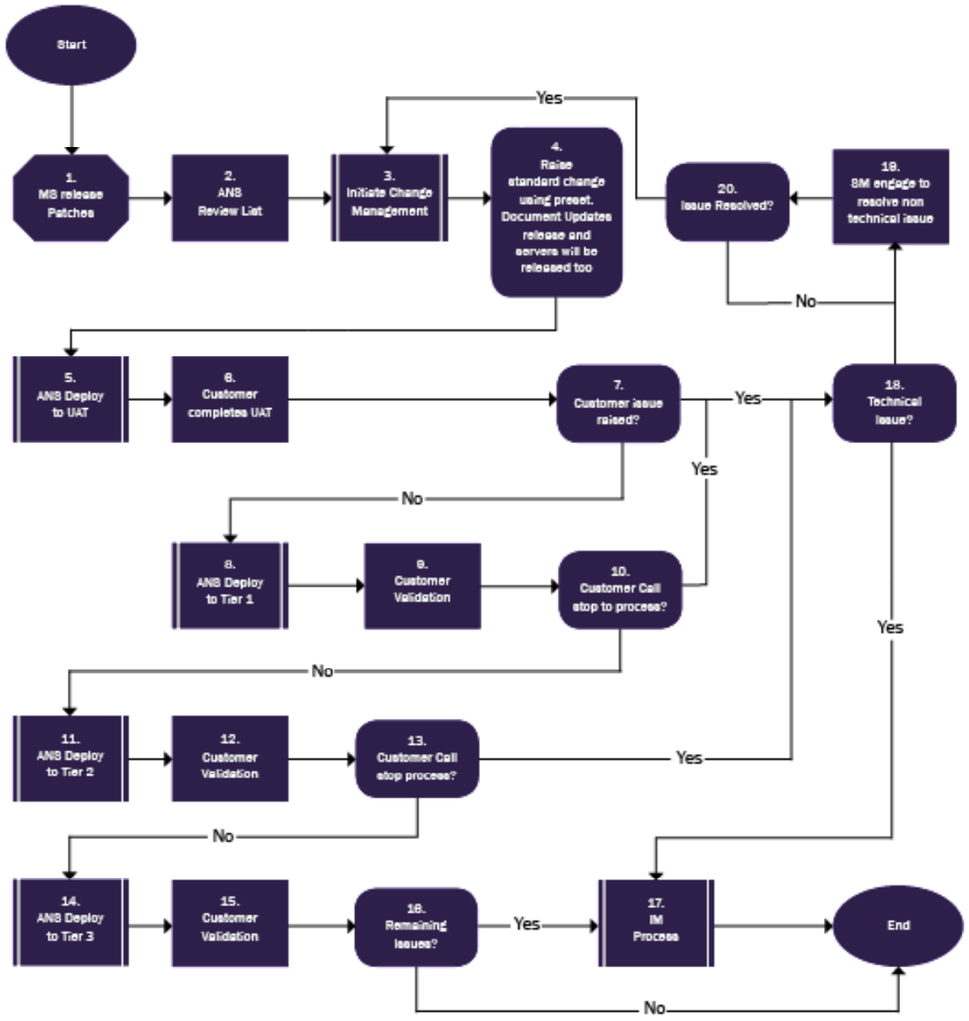
17. Appendix G -



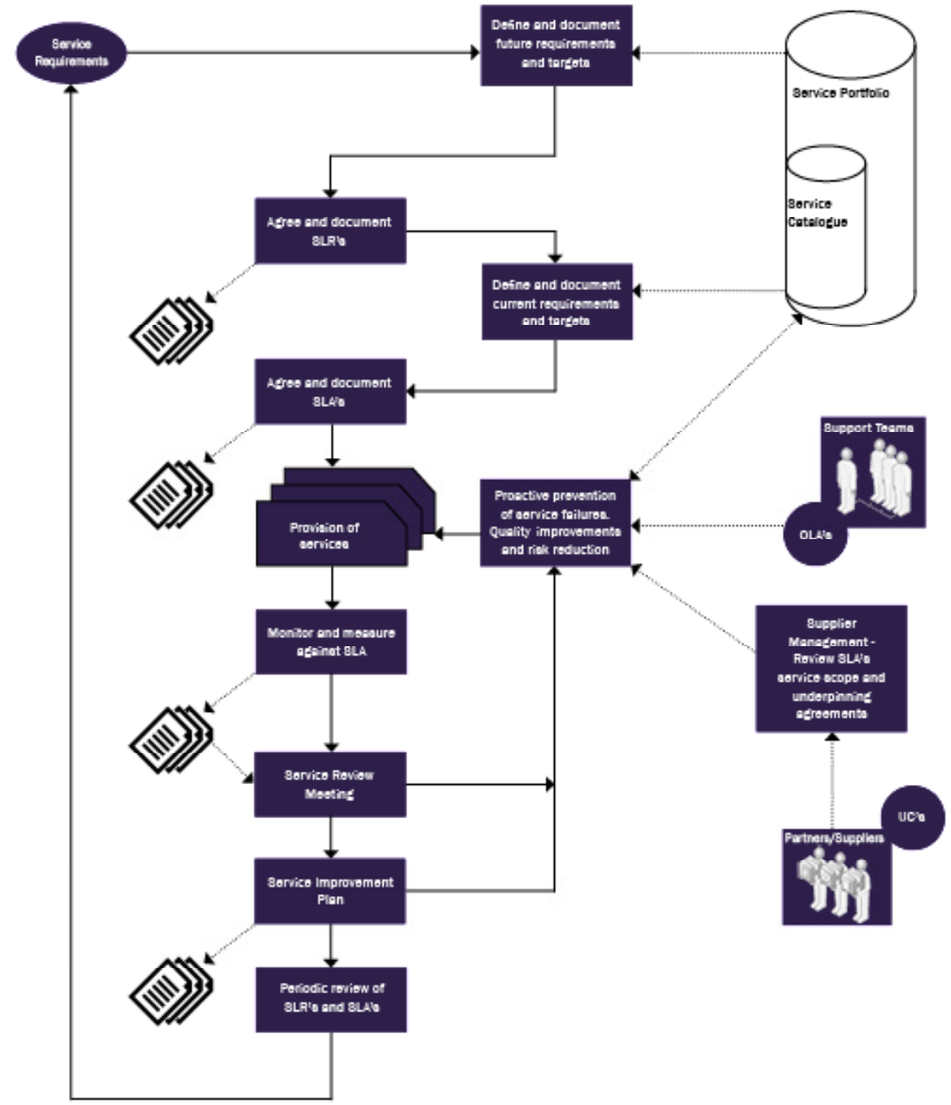
18. Appendix H - Release Management



19. Appendix I - OS Patch Management – Example



20. Appendix J - Service Level Agreement



Notes.

ans

Synergy House, Guildhall Close,
Manchester Science Park,
Manchester, M15 6SY.

T: 0161 227 1000

18 King William Street
London
EC4N 7BP

T: 0207 167 6666