ans

Service Definition

Threat Management | Author

1. Operational Services

1.1 Service Description

Normal Business Hours = 9:00 -17:30, Monday to Friday
(excluding bank holidays)
Working Day – 8.5 Normal Business Hours
24x7 = 24 hours a day, 7 days a week

1.1.1 ANS Service

Service	Service Description	Service Hours
Incident Management		
Security Incident Response	Provide data, interpretation, and remediation advice for Customer Incident response for P2, P3, P4 Security Incidents	Normal Business Hours
High Priority Security Incident Response	Provide data, interpretation, and remediation advice for Customer Incident response for P1 Security Incidents	24 x 7
Security Incident Remediation Advice	Provide advice on how to contain and remediate a P2, P3 or P4 Security Incident	Normal Business Hours
High Priority Security Incident Remediation Advice	Provide advice on how to contain and remediate a P1 Security Incident	24 x 7
Service Desk - Non Business Critical Faults	The Supplier provides access with relevant phone and email contact details to the Supplier Service Desk for non-critical system/service down and/or affected scenarios (P2/P3/P4) related to Alert Logic Platform.	Normal Business Hours
Service Desk - Business Critical faults	The Supplier provides 24/7 access with relevant phone contact details to the Supplier Service Desk for critical system down scenarios (P1) only that are related to Alert Logic platform.	24 x 7
Priority Escalation to Alert Logic for faults	Priority escalation to Alert Logic Support for Platform issues	Normal Business Hours
High Priority Escalation to Vendor	High Priority escalation to Alert Logic Support for Priority 1 business critical faults related to Alert Logic Platform.	24 x 7
Change Management & Advisory		
Support Services and PCI Scanning ASV Support	The supplier will provide advice & assistance with Alert Logic PCI scan scheduling and configuration	Normal Business Hours
Vulnerability Scan Configuration	The supplier will provide advice & assistance with configuration & scheduling of internal and external Alert Logic Vulnerability scans	Normal Business Hours
Asset Discovery Configuration	The supplier will configure asset discovery for networks and endpoints specified by the customer.	Normal Business Hours

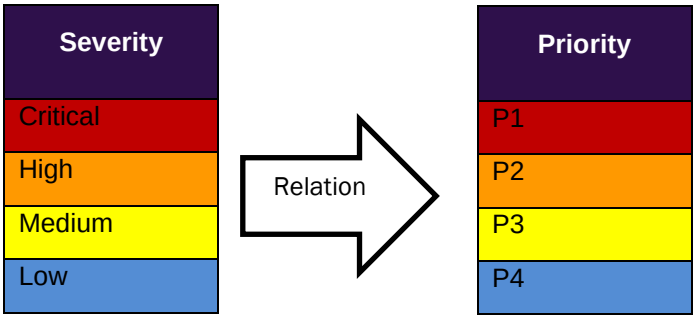
Asset Visibility	The supplier will provide visibility of all networks and endpoints discovered and then current health status within the Alert Logic Console.	24 x 7
Endpoint Protection Configuration	The supplier will provide advice & assistance with endpoint protection, including Alert Logic Appliance and Agent Configuration.	Normal Business Hours
Log Management Configuration	The supplier will provide advice & assistance with Log Management Configuration.	Normal Business Hours
Service Features		
Asset Discovery	Continuous discovery and visualisation of customer supported assets.	24 x 7
Vulnerability Scanning	Ability to run the following vulnerability scans: • PCI Scan • External vulnerability scans run from Alert Logic Datacentres • Internal vulnerability scans run from Alert Logic appliance deployed in the customer environment.	24 x 7
Cloud Security Configuration Checks	Continuous assessment of Cloud Environment configuration against CIS Benchmarks	24 x 7
Extended Endpoint Protection	Monitoring of endpoints attacks including identification of malware and ransom ware (Windows Operating Systems Only)	24 x 7
Threat Risk Index	Threat Risk Index provides a personalized score across customer supported assets, networks, deployments, helping to identify assets most at risk.	24 x 7
Threat Management	Detection of threats in motion through network IDS, log collection and log analytics, generation of actionable incidents with contextual information.	24 x 7
Log management, storage and search	Collection, storage, online search of Infrastructure, Cloud, System, Application and custom logs.	24 x 7
Compliance Readiness	Professional Embedded Security capabilities help to meet key compliance mandates and support compliance audit processes	24 x 7
Service Operations		
Alert Logic Portal Access	Customer read-only access to a portal providing visibility of all Customer Supported Assets covered by the Alert Logic service.	24 x 7
GLASS Portal Access	Customer access to ANS GLASS portal providing visibility of all Service related tickets, alerts and performance dashboards.	24 x 7

Problem Management	ANS Problem Management processes are adhered to for incident, change and event reduction. Problems are reviewed during the Service Management Review.	Normal Business Hours
Service Reviews	Service Management Review (SMR) Reports will be distributed at regular intervals and discussed via a meeting between the Supplier and the Customer. The SMR Report will cover the previous period. Please refer to your Service Statement for SMR frequency and meeting type.	Normal Business Hours
Root Cause Analysis	Applicable to P1 Incidents only, following a successful resolution of a P1 Incident, the Supplier will perform Root Cause Analysis. In the case of recurring Incidents (regardless of priority) further analysis may be undertaken to identify the underlying cause. Where applicable a Service Disruption Report will be created.	Normal Business Hours
Change Management Process	The Supplier will take full ownership of the Change Management Process for the Customer Supported Assets.	Normal Business Hours
Emergency Changes	Following a Security Incident or Business Critical Incident the Supplier will implement Emergency Changes.	24 x 7

1.2 Security Incident Management

A Security Incident is a pattern of potentially malicious activity that implies an identified threat to an information system, violates acceptable use policies, or circumvents standard security practices. The Supplier classifies incidents into four threat severity ratings: Critical, High, Medium, and Low.

1.2.1 Threat Severity Ratings:



1.2.2 Incident Response and Escalation Table:

Incident Priority	Threat Severity Rating	Response SLA	Escalation Notification	Notification Type
P1	Critical	30 Minutes	Immediate	Telephone Call
P2	High	1 Hour	None	Email/GLASS
P3	Medium	4 Hours	None	Email/GLASS
P4	Low	1 Day	None	N/A
P5	Question Query	2 Days	None	N/A

For an Incident “Response” is the time from when the ticket is first logged within the Supplier ITSM Tool to the time that the Supplier responds with a suitably qualified Employed person whether via an email, GLASS Portal update, telephone call (dependant on Priority). For detailed process flow see the current Managed Services Handbook.

From the time of Response until resolution, updates shall be provided to the Named Contacts and/or Escalation Contacts by email or GLASS Portal updates at such frequencies as set out in the table above.

Incident Resolution is handled by the Change Authority of the Supported Asset under investigation.

1.3 Security Incident Remediation

Remediation steps for Security Incidents are shared with the Customer by the Supplier. Resolution of and carrying out remedial steps is the responsibility of the Change Authority of the Supported Asset under investigation.

If the Supported Asset is under a Managed contract with the Supplier then the Service Levels of that contract will comply and the Supplier will remediate via the Suppliers Change Management Process.

Where the Customer is the Change Authority then the Incident will be functionally escalated (assigned) to the Customer to deliver any required remedial actions via Change Management.

1.4 Platform Incident Management

1.4.1 Platform Incident Priority Table:

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

1.4.2 Platform Incident Response and Escalation Table:

Priority	Response SLA	Specialist Review	Escalation Manager	Escalation Director	Notification Frequency	Target Resolution KPI
P1	30 Minutes	1 Hour	Immediate	Immediate	Hourly Email	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

For an Incident related to the Alert Logic platform, “Response” is the time from when the ticket is first logged within the ANS ITSM Tool to the time that the Supplier responds with a suitably qualified Employed person whether via an email, GLASS Portal update, telephone call or in person. For detailed process flow see the current Managed Services Handbook. Support to provide a resolution shall be provided within Service Hours from the time of Response until the Incident has been resolved.

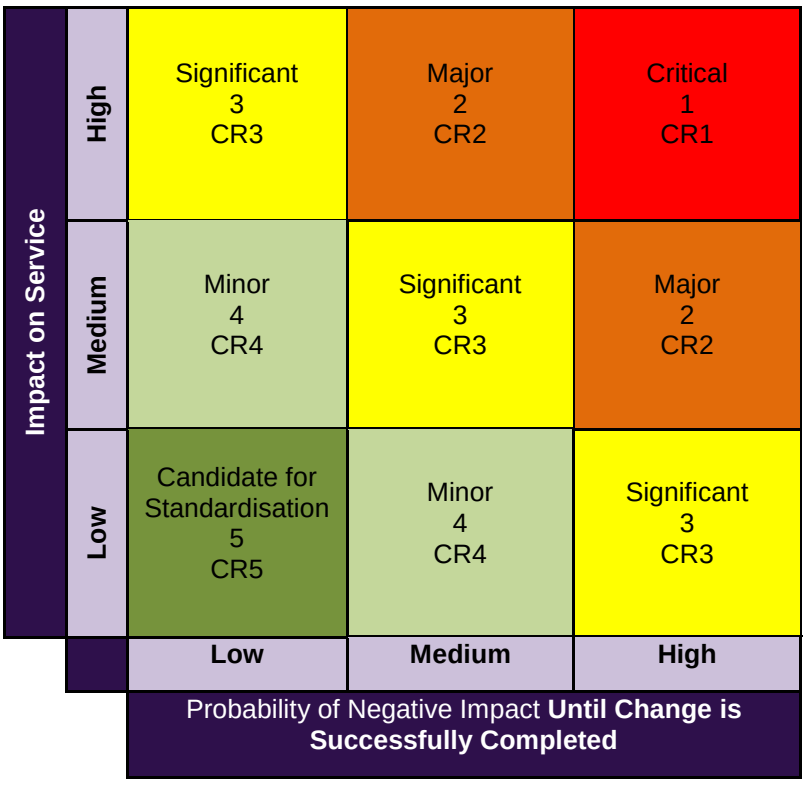
From the time of Response until resolution, updates shall be provided to the Named Contacts and/or Escalation Contacts by email or GLASS Portal updates at such frequencies as set out in the table above.

1.5 Platform Change Management

All Changes to the Alert Logic Platform Configuration require a Request for Change (RFC) form to be completed on the Suppliers GLASS Portal and submitted detailing the required Change. The Supplier will reject unapproved or incomplete RFC forms.

Changes will follow the Change Management Process as defined in the ANS Managed Services Handbook. It should be noted that Emergency Changes will only be carried out in the event of a P1 scenario (either pro-active or reactive) and/or a major Security Incident where the Supplier deems appropriate.

Platform Change Risk Assessment Matrix



1.5.1 Platform Change implementation targets Table:

Change Type	Implementation Start Date
Normal CR1	1 Working Day from CAB Approval
Normal CR2	2 Working Days from CAB Approval
Normal CR3	3 Working Days from CAB Approval
Normal CR4	4 Working Days from CAB Approval
Normal CR5	5 Working Days from CAB Approval
Normal CR6	Project Changes (Informational and Approval only)
Standard	Change to be completed within 4 Working days from logging on ANS ITSM Tool
Emergency	Change to completed in conjunction with Incident Management Process (P1)

Emergency Changes are dealt with in conjunction with the Incident Management Process; further details of this and all other change types are detailed within the Managed Services Handbook.

Standard and Emergency Changes to the Service within the scope of this Contract will be completed by the Supplier at no additional cost.

2. Security Service Levels, Key Performance Indicators and Service Credits

Category	Service Level Target
P1 Incidents	100% of incidents responded to within 30 minutes – 24x7 Service Hours.
P2 Incidents	100% of incidents responded to within 1 Normal Business Hour.
P3 Incidents	100% of incidents responded to within 4 Normal Business Hours.
P4 Incidents	100% of incidents responded to within 1 Working Day.
P5 Incidents	100% of incidents responded to within 2 Working Days.

3. Platform Service Levels, Key Performance Indicators and Service Credits

Category	Service Level Target	Minimum Service Level	Service Credits
P1 Incidents	100% of Incidents responded to within 30 minutes – 24x7 Service Hours.	100%	1st incident missed response time – 5% Service Credit 2nd incident missed response time – 10% Service Credit
P2 Incidents	100% of Incidents responded to within 1 Normal Business Hour.	Service credits apply from 2nd failure within a calendar Month	1st incident missed response time – 0% Service Credit 2nd incident missed response time – 5% Service Credit 3rd incident missed response time – 10% Service Credit
P3 Incidents	100% of Incidents responded to within 4 Normal Business Hours.	80%	<80% - 5% Service Credit
P4 Incidents	100% of Incidents responded to within 1 Working Day.	None	No Service Credit
P5 Incidents	100% of Incidents responded to within 2 Working Days.	None	No Service Credit
Root Cause	100% of P1 Incidents to receive a Root Cause Analysis within 10 Working Days of Resolution	None	No Service Credit

CR1 Change	100% of Changes start implementation within 1 Working Day from CAB Approval	100%	1 Change Missed Implementation time - 5% Service Credit 2 Changes missed Implementation times - 10% Service Credit
CR2 Change	90% of Changes start implementation within 2 Working Days from CAB Approval	85%	5% Service Credit
CR3 Change	90% of Changes start implementation within 3 Working Days from CAB Approval	None	No Service Credit
CR4 Change	90% of Changes start implementation within 4 Working Days from CAB Approval	None	No Service Credit
CR5 Change	90% of Changes start implementation within 5 Working Days from CAB Approval	None	No Service Credit
Standard Change	100% of changes implemented within 4 Working Days	90%	5% Service Credit

Service Credits are calculated as a percentage of the monthly Base Charge and in any event, shall not exceed 10% of the monthly Base Charge in the month that the Service Credit arose. Where a Service Credit is due it shall not accumulate with any other Service Credit and only one Service Credit can be offered within the monthly period.

4. Exclusions

The following are listed as exclusions, but this list shall not be considered complete or exhaustive and the Terms and Conditions should be consulted.

a. Issues resulting from misconfiguration by the Customer outside of the Customer Supported Assets resulting in impact to the Customer Supported Assets
b. Issues resulting from failures in maintenance/administration by the Customer outside of the Customer Supported Assets resulting in impact to the Customer Supported Assets
c. Issues resulting from misconfiguration or development by the Customer and/or the Customers chosen 3rd Party Application provider
d. Issues resulting from Unauthorised Access by the Customer of Customer Supported Assets
e. End User or 1st Line support
f. Technical Advice to any persons not listed as a Named Contact
g. Failure to meet SLA due to Public Cloud provider outages or local environment factors such as Power and Cooling
h. Normal Changes requiring more than 2 hours of implementation time are excluded from the service and will be subject to Additional Service Charges
i. Project Changes (Normal CR6) are excluded from the service and will be subject to Additional Service Charges. Project Changes are recorded within the Supplier ITSM Tool for Informational and approval purposes only.
j. Emergency Changes that are not a direct output of a Priority 1 incident may be subject to Additional Service Charges
k. Major Version Releases will be subject to Additional Service Charges as only dot releases and patches are including as part of the service
l. Change Requests for remediation are not included unless the Supported Asset is covered under a Managed contract with the Supplier

5. Customer Responsibilities

Including but not limited to:

a. The Customer shall have an established end user support function that may be validated by the Supplier
b. Where required, the Customer shall make available appropriately skilled Employed persons while an Incident is being managed
c. The Customer is required to undertake an initial Impact Assessment before logging the Incident with the Supplier. Such Impact Assessment is to include:
    a. Affected Services
    b. Business Impact
    c. Number & Type of users affected
    d. Recent changes on Supported Assets (regardless of perceived impact)
    e. The Customer shall check hardware onsite and ensure the hardware has power and cables are connected as expected (where required)
    f. The Customer shall check LED status of equipment onsite (where required)
d. The Customer shall provide full administrative access to the Supplier to all the services outlined in the Impact Assessment and any subsequently identified services or provide persons with adequate access to allow investigations to proceed
e. The Customer is required to ensure that all Customer Supported Assets are appropriately licenced and have (where required) Supplier recommended hardware and vendor support in place.

f. The Customer is responsible for all configuration backups outside of the Supported Assets without exception.
g. The Customer is responsible for completing a Request for Change (RFC) in accordance with the Supplier's Change Management Process
h. The Customer shall ensure that all relevant Customer employees have access to and have read the Supplier's Managed Services Handbook
i. The Customer shall ensure an on-going availability of suitable Internet connection (if not provided by the Supplier)
j. The Customer shall ensure 24x7x365 availability of a suitable Escalation Contact should the Supplier need to gain approval for an Emergency Change or to engage other aspects of the Customer's support functions
k. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the Customer Supported Assets including environmental changes. Failure to do so may result in Additional Service Charges.
l. 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.
m. During investigations into a potential a hardware or software fault it may be required to reseat certain elements of the device/infrastructure onsite or require a device inspection for LED status. This task sits with the Customer (unless the Supported Asset is located within the Suppliers Data Centres).
n. If the Customer requires the Supplier to provide onsite hands and eyes support then this will be subject to Additional Service Charges.
o. It should be noted that the Customer shall report Business Critical Incidents via telephone only. The Supplier cannot offer any Service Levels or Service Credits for Business-Critical Incidents raised via email.
p. The Customer will ensure that active protection mechanisms (such as web application firewalls or intrusion prevention systems) allow Alert Logic scanning traffic.
q. Alert Logic onboarding will require Customer participation to ensure that the Supplier receives the right level of Customer feedback and activity to ensure a successful deployment.
r. Customers are responsible for installing agents, configuring appropriate firewall access to enable agent communication, and notifying The Supplier when installation of agents is complete.
s. Customers are responsible to ensure that there is no "Scan Interference" as defined in PCI SSC's "ASV Program Guide" during the PCI Scans.
t. Alert Logic depends upon a reliable connection between the Supplier hosted scan technologies and Customer target networks / systems. If a reliable connection is unavailable for any reason, The Supplier will not be responsible for the service level commitments for that period.
u. Alert Logic depends upon reliable vulnerability and scan data from Customer networks. Systems that are off-line, in error, or otherwise in a state that degrades the collection of data inhibit service delivery. Customers are responsible for ensuring that Customer-owned networks, systems, and applications within the scope of the Alert Logic service are maintained and functioning properly.
v. Customers are responsible for racking and installing the physical appliance(s) (if applicable), and/or loading and installing the virtual appliance image. Customers are responsible for providing network access to the appliance(s) for The Supplier personnel, configuring appropriate firewall access to enable appliance communication, and notifying The Supplier when installation of the appliance(s) is complete.
w. Customers are responsible for completing service activation questionnaires and participating in kickoff meetings to agree to the scope of the onboarding process, confirm the minimum deployment configuration and timeline of activities, and provide appropriate technical and security contacts to receive alerts, notifications and escalations. Customers are also responsible for participating in efforts to tune Alert Logic to best fit Customer needs.
x. Customers are responsible for identifying key stakeholders to participate in The Supplier sessions for introduction and handover to service, and to complete the available self-guided training.
y. Service continuity will require Customer participation to ensure that The Supplier receives relevant data for analysis and has the appropriate escalation contacts.
z. Customers are responsible for identifying target systems/networks and AWS/Azure environments/assets to include within the Alert Logic service and ensuring that Alert Logic technologies are installed appropriately for the desired scope of service and properly configured:
    a. to access all monitored networks including any necessary changes to on premise equipment such as firewalls and switches.

b. for the desired level of log collection in their audit log settings.

aa. Customers who have configured and implemented log collection black-out periods (for example, cache log data on local machine during business hours for single upload after business hours) should recognize that this collection configuration will delay log ingestion, aggregation, and normalization by the Alert Logic service.

bb. Customers must ensure that collection for target source log data and networks are properly installed in Alert Logic and validate log and event data is being sent back to The Supplier for storage and analysis.

cc. Customers are responsible for confirming the actual IP addresses, domains, or address ranges are specifically allocated to Customers prior to initiating any scans.

dd. Customers are responsible for participating in ongoing service optimization activities such as performing agreed upon network or application changes and changes to Customer information.

ee. Customers are responsible for communicating all relevant changes to Customer environments that may impact the scope of log and event collection/correlation or vulnerability scanning.

ff. Customers are responsible for configuring escalation alerting and notification options in the The Supplier portal with accurate and updated information. Customers should include both security and technical contacts when they configure notifications so that the appropriate parties may be quickly reached and notified of a given condition.

6. Assumptions

a. All Customer Supported Assets and Production AWS and Azure Accounts within the Customer Supported Assets within this Contract are covered by a valid software maintenance and support agreement in line with this Contract Service Levels
b. All Customer Supported Assets are in a Valid Supported Configuration at the point of contract start date
c. All Customer specific pre-requisites have been completed before contract commencement
d. The Customer will provide a suitable specification platform, operating system and connectivity for the Enterprise Monitoring collector server

7. Pre Requisites

a. On-Boarding Health Check and Documentation
b. Deployment of Alert Logic Appliance and Agents to customer supported assets and environments
c. A limited privilege AWS IAM / Azure role that will allow Alert Logic to perform specific setup tasks.
d. Platform and where applicable WMI access for all monitored services
e. Registered Partner of Record and/or AWS Associated Partner registration (where required)
f. Administrative Access Permissions for ANS Engineers on supported Subscriptions / Accounts and Customer Supported Assets

8. Partner of Record

ANS' Managed Cloud for Azure incorporates Microsoft Signature Cloud Support for any issues that require escalation to Microsoft. In order for this to be able to be fulfilled, Microsoft leverage information collected from the Partner of Record (PoR) system to assign back end support rights. As such ANS must be registered as the digital PoR on any Subscriptions that contain or contribute to assets under support or management for the entire duration of the agreement. Consequently, the Customer shall, prior to the Commencement Date arrange for ANS to be registered as the PoR on all Subscriptions that contain or contribute to assets under support or management for the entire duration of this agreement.

9. Amazon AWS Associated Partner

Amazon AWS' partnership status is heavily reliant on demonstrating working relationships with AWS consumers, Amazon leverage information collected from the associated partner system to assign partnership status. As such ANS must be registered as the associated partner on any accounts that contain or contribute to assets under support or management for the entire duration of the agreement. Consequently, the Customer shall, prior to the Commencement Date arrange for ANS to be registered as the associated partner on all accounts that contain or contribute to assets under support or management for the entire duration of this agreement