Attachment 4 – Service Levels and Service Credits

1. SERVICE LEVELS

1.1. The Supplier shall monitor its performance of this Contract by reference to the relevant performance criteria for achieving the Service Levels shown in this Attachment (the "**Service Level Performance Criterion**"). Annex 1 to this Attachment sets out the Service Levels and the Service Level Performance Criterion which the Parties have agreed to measure.

2. SERVICE CREDITS

2.1. This Paragraph 2 sets out the formula used to calculate Service Credits payable to the Buyer as a result of a Service Level Failure in a given Service Period.

2.2. The amount of any Service Credits shall be determined by the Achieved Service Level, the Service Level Performance Measure and the Service Level Threshold and is calculated by using the straight-line formula below: -

Service Credit % = (m*(a-x) + c) * **Repeat Failure Multiplier** - where:

"m" is a coefficient defined for a particular Service which is calculated from the formula m = (d-c)/(a-b), that is the slope of the straight line;

"d" is the maximum Service Credits (%) payable if the Achieved Service Level reaches the Service Level Threshold;

"c" is the minimum Service Credits (%) payable if the Achieved Service Level falls below the Service Level Performance Measure;

"a" is the Service Level Performance Measure (%) below which Service Credits shall become payable;

"b"` is the Service Level Threshold (%);

"x" is the Achieved Service Level (%) for a Service Period;
and

"Repeat Failure Multiplier" shall have the meaning set out in Paragraph 5 of this Schedule.

2.3. For the avoidance of doubt applicable "Service Level Thresholds" shall be as set out in Annex 1 to this Attachment.

Any Service Credits payable by the Supplier shall be subject to the following minimum and maximum:

Minimum Service Credits %	Maximum Service Credits %
2.5%	10%

2.4. Unless stated otherwise in this Attachment, the amount of the Service Credit (in pounds Sterling) shall be calculated according to the formulae:

Service Credit (£) = Service Credit (%) x 15% of the Charges for the Service Period.

2.5. Service Credits for particular Services shall be cumulative. For the avoidance of doubt, this means that all Service Credits will be added together to make the total Service Credit payable by the Supplier in relation to all Services delivered by the Supplier.

2.6. Where the same Root Cause causes more than one Service Level Failure in a given Service Period, the Service Level Failure attracting the largest Service Credit shall apply in respect of such Service Level Failures.

3. NATURE OF SERVICE CREDITS

3.1. The Supplier confirms that it has modelled the Service Credits and has taken them into account in setting the level of the Charges. Both Parties agree that the Service Credits are a reasonable method of price adjustment to reflect poor performance.

4. SERVICE CREDIT CAP

4.1. For the purposes of this Attachment the Service Credit Cap means 15% of the aggregate Charges payable to the Supplier for the relevant Contract Year.

5. REPEAT FAILURES TO MEET SERVICE LEVEL PERFORMANCE MEASURES

5.1. If the Supplier fails to achieve a Service Level Performance Measure in a Service Period and then fails to achieve the same Service Level Performance Measure in a subsequent Service Period, the failure in the subsequent Service Period shall be a "**Repeat Failure**" save where the Root Cause analysis undertaken demonstrates to the satisfaction of the Buyer that the second failure is the direct result of a different and unrelated Root Cause. The Repeat Failure count shall increment by one (1) for each additional failure.

5.2. The Repeat Failure count shall be reset to zero (0) once there have been two (2) consecutive Service Periods in which the Service Level Performance Measure has been met.

5.3. In this Paragraph the reference to Repeated Failures to achieve a Service Level Performance Measure shall be to the Service Level Performance Measure for one (1) Service Level Performance Criterion.

5.4. For any failure to meet Service Level Performance Measure which is a Repeat Failure, the Service Credit applicable shall be increased as follows (the "**Repeat Failure Multiplier**"):

Repeat Failure count applicable to the Service Period	Repeat Failure Multiplier
0	1

1	1.25
2	1.5
3	1.75
4 and above	2

Repeat Failure example

	Service Period											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Failure to meet Service Level Performance Measure (F)	F	F	P	F	P	P	F	P	F	F	P	F
Repeat Failure count	0	1		2			0		1	2		3

ANNEX 1 - SERVICE LEVELS AND SERVICE CREDITS

1. **Incident & Enquiry Resolution**

1.1. The “**Severity Levels**” shall be defined as set out in the table below:

Severity Level	**Definition**
Level 1	• loss of critical system functionality; and/or • has a critical impact on the ability of the Buyer to carry out its statutory obligations and where no Workaround exists~~;~~ and/or • causes major financial loss to the Buyer; and/or • results in material loss or corruption of any Buyer Data.
Level 2	• has a major (but not critical) adverse impact on the activities of the Buyer; and where no Workaround exists; and/or • causes some financial loss to the Buyer.
Level 3	• has a moderate adverse impact on the activities of the Buyer, and where no Workaround exists;~~.~~
Level 4	• causes minor adverse impact on the provision of the Services to Users.

1.2. Incident Resolution Times shall be calculated from the time of first report of the Incident by the Service Desk to the Supplier until the time that the action has been completed by or on behalf of the Supplier to repair the Root Cause of the Incident or an agreed (agreed with the Buyer) Workaround has been implemented by the Supplier.

1.3. Incident shall be 'closed' only once: (i) Restoration of Service has been achieved; and (ii) the Buyer has confirmed to the Supplier that Restoration of Service has in fact been achieved. Notwithstanding the foregoing, if the Supplier believes that it has achieved Restoration of Service and has made three (3) attempts in good faith to confirm this with the Buyer, but has been unable to contact the Buyer to obtain such confirmation, then the Incident shall be deemed to be closed.

2. Service Levels and Service Credits

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	**Key Indicator**	**Service Level Performance Measure**	**Service Level Threshold**	
SL1: Availability	Availability during Elapsed Hours of applications, systems and underlying infrastructure.	99.90%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL2: Incident - Severity Level 1	Four (4) Elapsed Hours	99.90%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL3: Incident - Severity Level 2	Five (5) Elapsed Hours	99.90%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL4: Incident – Severity Level 3	Eight (8) Operational Hours, where Operational Hours are Monday to Friday 07:00- 19:00 including Bank Holidays and Saturday 07:00 – 17:00.	99.50%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL5: Incident - Severity Level 4	Twelve (12) Operational Hours, where Operational Hours are Monday to Friday 07:00 - 19:00 including Bank Holidays and Saturday 07:00 - 17:00.	99.50%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL6: Asset Management	The Supplier shall maintain software asset licence compliancy details including a) For software assets where the Supplier is responsible for purchasing licenses	99.90%	75%	Refer to the formula in Paragraph 2 for calculation of Service Credit

	• date the Supplier informed the Buyer of the software asset licence non-compliancy Note 1 • date the Supplier resolved the software asset licence non-compliancy. b) For software assets where the Buyer is responsible for purchasing licenses • date the Supplier informed the Buyer of the software asset licence non-compliancy. The Service Level Performance Measure, to be verified every 3 months (January, April, July and October) measures conformance of the above dates with the following timescales: a) For software assets where the Supplier is responsible for purchasing licenses • the Supplier shall have informed the Buyer of the software asset licence non-compliancy within 15 elapsed days • the Supplier shall have resolved the software asset licence non-compliancy within 90 elapsed days. b) For software assets where the Buyer is responsible for purchasing licenses • the Supplier shall have informed the Buyer of the software asset licence non-compliancy within 15 elapsed days. Note: The Supplier shall audit licence compliancy between entitlement and requirement for software assets employed to deliver the Services. The Supplier to present a software asset licence compliancy report to the Buyer as evidence of meeting this Service Level.			

	Note 1: software asset licence non-compliancy means where the number of deployed instances of the software asset exceeds the number of licenced instances of the software asset.			

In respect of the following Service Levels relating to vulnerabilities, the following provisions shall apply:

- The rating of each vulnerability shall be in accordance with Additional Schedule S3 (Security Requirements). The number of vulnerabilities to be remediated shall be counted as the number of patches, or configuration or other changes required over the whole estate in the Supplier's scope of supply, and the number of vulnerabilities to be remediated shall be calculated similarly.
- The Service Level performance shall be calculated, for example, as follows:
    - If 80 servers required 20 IMPORTANT patches each, 1600 IMPORTANT patches require application, if 16 servers have five IMPORTANT patches missing after 15 days, the Service Level performance is 95% and the Service Level 7a is therefore met in respect of IMPORTANT vulnerabilities.
- All references to "remediation" for a vulnerability can include a vendor patch or other mitigation such as stopping of vulnerable Services.
- Service Level 7 applies only to environments related to production data. The Buyer will request a Change in accordance with the Change Control Procedure to measure the Service Level against any non-production environments.
- SL7 (c) and (d) will apply to vulnerability remediations released by third parties for products where the remediation is deployable by an automated mechanism. Where there are consequential risks or known effects of a remediation for a CRITICAL vulnerability these will be raised with the Buyer for a case-by-case decision of the action to be taken. Regardless of whether the Buyer chooses to proceed with an implementation or not, the Supplier shall not be liable for any Service Level breach arising as a consequence of acting in accordance with the Buyer's instructions.
- Where any vulnerability remediation or mitigation requires server or Service restarts that may impact Users, this will be raised with the Buyer for a case-by-case decision of the action to be taken. Where the Buyer chooses to proceed with an implementation, the Supplier shall not be liable for any downtime or Service Level breach arising as a consequence of applying the patch or mitigation.
- Where a CRITICAL vulnerability remediation cannot be fully implemented within these timescales due to the volume of work required, the remediation must be applied as soon as practicable, but the relevant Service Level time will be extended to account for the required time.
- Vulnerability remediation applied under SL7a (Critical), SL7b (Critical), SL7c (Critical) and SL7d (Critical) will not undergo performance testing before application to production systems by default. Vulnerability remediation applied under SL7c (Important), SL7c (Other), SL7d (Important), SL7d (Other) may be performance tested in accordance with the CMS release schedule, or otherwise agreed on a case by case basis.

- Where application of a vulnerability remediation in accordance with the third-party instructions leads to the Service failing, and/or performance issues that require additional activities to restore Service, the Supplier shall not be liable for any downtime or Service Level breach.
- Any vulnerabilities identified within the CMS application components are outside of the scope of SL7 and will be appropriately prioritised and progressed through the joint ADIMS backlog under continuous service improvement capacity.
- The Supplier is responsible for security vulnerability remediation to third-party components as defined in Schedule 9 (Software). The Supplier is not responsible for the vulnerability remediation of any third-party components that are dependencies or sub-components of the primary software components as defined in Schedule 9 (Software). As an example, the Supplier will patch third-party components such as Node.js that are directly integrated and utilised within the Supplier's software. The Supplier will not patch the underlying operating system (e.g. Debian) or any other subcomponent that is not directly integrated into the Supplier's software but is instead a dependency of a third-party component.

Technical Considerations
The following background information may be useful in understanding some influencing factors:

- **Deployment Constraints:**
  - Production environments are currently limited by insufficient resource capacity at busy periods (e.g. Oracle), restricting the ability to perform deployments that necessitate taking nodes offline or rebooting during busy Business-As-Usual (BAU) operational times.
  - The stateful nature of the CMS Classic and its underlying database, combined with the lack of advanced availability mechanisms (e.g., Oracle FAN), necessitates downtime for vulnerability remediation. Consequently, servers cannot be taken in and out of service without causing CMS downtime. This downtime will normally be approved by the Buyer on a case-by-case basis.
  - The release process for CMS Classic currently takes several weeks, so to apply vulnerability remediation within shorter timeframes raises additional risks which may be approved by the Buyer on a case-by-case basis.
- **Continuous Integration/Continuous Deployment (CI/CD) Limitations:**
  - A fully integrated CI/CD pipeline extending into production can be helpful in facilitating the rapid deployment of some vulnerability remediation, for instance addressing open-source software (OSS) vulnerabilities. The current setup does not support this.
- **Performance Testing Challenges:**
  - The current performance testing rig and process are manual, but efficiently managed. This capacity limitation means it is unlikely to be possible to carry out performance assessments of all vulnerability remediation prior to implementation. This is not however a requirement as a risk-based approach will be taken to determine whether performance testing is required for vulnerability remediations.
  - Historical data indicates that a few previous vulnerability remediations, if applied without thorough performance testing, could have caused critical issues in the production environment. This risk-based approach is designed to performance test vulnerability remediations likely to cause performance issues, but it cannot be 100% effective.
- **Technical Debt:**

○ The CMS application carries substantial legacy technical debt, including dependencies on outdated technologies such as IE5.5 compatibility mode, which impedes the ability to update certain OSS components. This, in turn, leads to compounded impacts and limitations in addressing vulnerabilities. ○ There is a significant backlog of vulnerabilities identified in the CMS application through OSS Software Composition Analysis (SCA) tools (e.g., BlackDuck) and static application security testing (SAST) tools (e.g., SonarQube). This backlog results from the historical introduction of these tools and the extensive vulnerability remediation efforts required. Service Levels 7(a) and 7(b) measure vulnerability management for non-CMS only, whilst Service Level 7(c) and 7(d) measure vulnerability management for CMS. The Buyer notes its aspiration to remove Service Levels 7(c) and 7(d) and apply Service Levels 7(a) and 7(b) to both CMS and Non-CMS from twelve (12) months post OSCD and as such the Buyer will work with the Supplier to prioritise any necessary Change to support this being achievable. Any amendment to this Attachment 4 (Service Levels and Service Credits) to include and measure Service Levels 7(a) and 7(b) for CMS will be requested and managed in accordance with Schedule 5 (Change Control) and the Supplier shall be entitled to provide an Impact Assessment to the Buyer.				
SL7 (a)(i): Vulnerability Management (Other-excluding CMS, WMS & MIS)	The remediation of security vulnerabilities rated CRITICAL in within twenty-four (24) Elapsed Hours or as agreed on a case-by-case basis with the Buyer.	90%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL7 (a)(ii): Vulnerability Management (Other-excluding CMS, WMS & MIS)	The remediation of security vulnerabilities rated IMPORTANT in within fifteen (15) elapsed days or as agreed on a case-by-case basis with the Buyer.	90%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL7 (a)(iii): Vulnerability Management (Other-excluding CMS, WMS & MIS)	The remediation of security vulnerabilities rated OTHER in within fifty (50) elapsed days or as agreed on a case-by-case basis with the Buyer.	90%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL7 (b)(i): Vulnerability Management	Security vulnerabilities rated CRITICAL in within forty-eight (48) Elapsed Hours or as agreed on a case-by-case basis with the Buyer.	100%	90%	Refer to the formula in Paragraph 2 for calculation of Service Credit

(Other-excluding CMS, WMS & MIS)				
SL7 (b)(ii): Vulnerability Management (Other-excluding CMS, WMS & MIS)	The remediation of security vulnerabilities rated IMPORTANT in within twenty (20) elapsed days or as agreed on a case-by-case basis with the Buyer.	100%	90%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL7 (b)(iii): Vulnerability Management (Other-excluding CMS, WMS & MIS)	The remediation of security vulnerabilities rated OTHER in within sixty (60) elapsed days.	100%	90%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL7(c)(i): Vulnerability Management (CMS, WMS & MIS Interim)	The remediation of security vulnerabilities rated CRITICAL within twenty-four (24) Elapsed Hours or as agreed on a case-by-case basis with the Buyer. In the case of CRITICAL remediation, the requirements for testing and notification will not apply.	90%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL7(c)(ii): Vulnerability Management (CMS, WMS & MIS Interim)	The remediation of security vulnerabilities rated IMPORTANT within one hundred (100) and OTHER within one hundred and eighty (180) elapsed days or as agreed on a case-by-case basis with the Buyer, excluding Oracle database software which will be within two hundred and seventy (270) days.	90%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL7(d)(i): Vulnerability Management (CMS, WMS & MIS Interim)	The remediation of security vulnerabilities rated CRITICAL within forty-eight (48) Elapsed Hours or as agreed on a case-by-case basis with the Buyer. In the case of CRITICAL remediation, the requirements for testing and notification will not apply.	100%	90%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL7(d)(ii): Vulnerability Management	The remediation of security vulnerabilities rated IMPORTANT within one hundred and thirty (130) and OTHER within two-hundred and ten (210) elapsed days	100%	90%	Refer to the formula in Paragraph 2 for

(CMS, WMS & MIS Interim)	or as agreed on a case-by-case basis with the Buyer, excluding Oracle database software which will be within three hundred (300) days.			calculation of Service Credit
SL7 (e): Anti-Virus Signature Updates	Alerts raised that identify devices as not having up to date antivirus signatures or similar dynamic update designed to mitigate the risk from malware to be Resolved within the following timescales: • Fewer than 10 devices - fixed within 120 Elapsed Hours of alert being raised • 10 or more devices - fixed within 72 Elapsed Hours of alert being raised Where it is agreed between the Parties that a resolution cannot be implemented within these timescales, the resolution must be applied as soon as practicable, but the relevant Service Level time will be extended to account for the required time.	100%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL8: Security Breaches	No Breach of Security caused by the Supplier or its Sub-Contractors.	Zero Breaches of Security	1 Breach of Security	10% Service Credit applied for each Breach of Security
SL9: Not used	Not used	N/A	N/A	N/A
SL10: Not used	Not used	N/A	N/A	N/A
SL11: Resolution of CPS Direct Incidents	Severity Level 1 to 3 Incidents raised by CPS Direct in respect of the Services Resolved within 4 Elapsed Hours.	99.90%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit

SL12: Provision of an triage and assessment in JIRA	The Supplier will undertake triage and assessment of potential work items added to JIRA by the Buyer and update status within 10 Working Days, unless otherwise agreed by the Buyer (such agreement shall not be unreasonably withheld).	99.99%	75%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL13: Not used	Not used	N/A	N/A	N/A
SL14: Provision of Performance Reports	Each Monthly performance report shall be delivered within 5 Working Days of the Month's end.	100%	-	Minimum Service Credit is applied for 1 day late. 1% Service Credit applied for each subsequent day after the agreed Service Level Performance Criterion
SL15: Provision of Finance Reports	The Financial Response Template populated with Actual Charges to be delivered within 10 Working Days of the Month's end for the Month 3 months previous in accordance with Schedule 2 (Charges).	100%	-	Minimum Service Credit is applied for 1 day late. 1% Service Credit applied for each subsequent day after the agreed Service Level Performance Criterion
SL16: Breach of Security Reporting	Notify the nominated security representative from the Agency Manager and the Buyer of all actual or suspected Breaches of Security within 30 minutes of identification.	100%	1 Breach of Security reporting within any given Service Period.	10% Service Credit applied for each failure to report a Breach of Security

SL17: Approved Outages	All Planned Service Outages shall be Approved by the Buyer.	100%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL18: Adherence to Outage Window	The Approved Outage Window shall be adhered to by the Supplier.	99.50%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit
SL19: Service Catalogue Request Fulfilment	The Supplier shall adhere to the published timelines when satisfying Service Catalogue requests.	99.50%	80%	Refer to the formula in Paragraph 2 for calculation of Service Credit

3. Performance Indicators

The following performance indicators will be reported to the Buyer as a means of measuring performance. These performance indicators are not Service Levels, do not attract Service Credits and will not be included in any published Performance Reports.

Performance Criterion	Key Indicator	Performance Measure

KPI9a: CMS/WMS & MIS Data Recovery	Full restoration of an Oracle database from an Oracle backup file on the media server to either the production Oracle instance or the live copy instance within 24 Operational Hours of approval from authorised Buyer representative or within alternative agreed time (not unreasonably withheld) at point of authorisation.	No more than 1 failure to complete technical restore activities within 24 Operational Hours of approval
KPI9b: CMS/WMS & MIS Data Recovery	Restore activities for CMS unstructured data stored on the CMS NetApp NAS, of 1 TiB or less, to be completed within 24 Operational Hours of approval from authorised Buyer representative or within alternative agreed time (not unreasonably withheld) at point of authorisation. Restorations of data greater than 1 TiB to be completed as soon as reasonably practical.	No more than 1 failure to complete technical restore activities within 24 Operational Hours of approval
KPI10: User Data Recovery	Restoration of a snapshot on the Azure NetApp NAS, of 1 TiB or less, to be completed within 24 Operational Hours of approval from authorised Buyer representative or within alternative agreed time (not unreasonably withheld) at point of authorisation. Restorations of data greater than 1 TiB to be completed as soon as reasonably practical.	95%

ANNEX 2

1. Critical Service Level Failure

1.1 A Critical Service Level Failure will be deemed to have occurred if the performance of the Services falls below the same Service Level Threshold on three (3) occasions in any six (6) consecutive Service Periods.

1.2 In the event of a Critical Service Level Failure, the Buyer shall be entitled to:

1.2.1 Compensation for Critical Service Level Failure in accordance with Clause 10; and

1.2.2 exercise its rights under Clause 31.1.3(b) to step-in to itself supply or procure a third party to supply (in whole or in part) the Services and if the Buyer exercises such right the Buyer shall be entitled to charge the Supplier in accordance with Clause 31.2 until Service is restored to a level of quality acceptable to the Buyer.