

**We released this document in response  
to a Freedom of Information request.  
Over time it may become out of date.**

Department for Work and Pensions

**SCHEDULE 4 ANNEX C: Hosting Service Levels**

Measurement Period:  
 Date Compiled:  
 Compiled by:

Hosting Service Elements	No.	PI Component	Details	Measured? (Y/N)	Measurement details	Raw Performance Score	Weighting	Maximum Possible Score	Actual Weighted Score
A. Data Centre Space Rental	A1	Power	99.95% available, 24x7.	Y			2	10	0
					>=99.95	5			
					<99.95	0			
	A2	Air-conditioning	99.95% available, 24x7.	Y			2	10	0
					>=99.95	5			
					<99.95	3			
			Air-conditioning failure which results in temperatures outside the acceptable range outlined in Schedule 2, Annex A (paragraph 3.5(B)) but which DOES NOT result in any impact to services or in requirement to power down IT equipment.						
			Air-conditioning failure which results in temperatures outside the acceptable range outlined in Schedule 2, Annex A (paragraph 3.5(B)) but which DOES result in impact to services and/or requires IT equipment to be powered down.		<99.95	0			
	A3	Network connectivity - GPS	99.7% available, 24x7.	Y			2	10	0
					>=99.7	5			
<99.7					0				
A4	Network connectivity - Internet	99.95% available, 24x7.	Y			2	10	0	
				>=99.95	5				
				<99.95	0				
		- Power failures that do not impact running of Hosting Services due to built in resilience will not incur penalty.  - Air-conditioning failures that do not result in temperatures outside the acceptable range outlined in Schedule 2, Annex A (paragraph 3.5(B)) will not incur penalty.							
								Actual QSI Data Centre	0
								Amount of Data Centre Service Credits Due (if any)	0
B. Network Operations Centre	B1	Critical Alert response	100% of Alerts responded to with defined action, within 5 minutes limited to a cap of 30 Critical Alerts per hour. Once cap is reached in any given hour, CONTRACTOR's obligation will be limited to notifying the AUTHORITY of the quantity of Alerts received in not less than 15 minute intervals.	Y			1	5	0
					100%	5			
					1-2 breaches	2			
			>2 breaches	0					
	B2	Non-Critical Alert response	100% of Non-Critical Alerts responded to with defined action, within 15 minutes limited to a cap of 30 Non Critical Alerts per hour. Once cap is reached in any given hour, CONTRACTOR's obligation will be limited to notifying the AUTHORITY of the quantity of Alerts received in not less than 30 minute intervals.	Y			1	5	0
					100%	5			
					1-2 breaches	2			
			>2 breaches	0					
	B3	Operational tasks	100% of defined daily, weekly, monthly and yearly checks completed and recorded in auditable NOC checklists.	Y			1	5	0
100%					5				
1-2 breaches					2				
		>2 breaches	0						

*For the purposes of item B1, a Critical Alert shall be defined as an Alert or series of Alerts which has the potential to impact the availability of the Hosting Services.*

*For the purposes of item B2, a Non Critical Alert shall be defined as an Alert or series of Alerts which does not have the potential to impact the availability of the Hosting Services.*

*Item B3 will be based on operational checklist template(s) for daily, weekly, monthly and yearly tasks, created by the CONTRACTOR and approved by the AUTHORITY. Any changes to items on these templates will require agreement from both the CONTRACTOR and the AUTHORITY.*

C. Incident Management									
C1	Assign Severity Levels	All Incidents relating to Hosting Services to be assigned a Severity Level.	N						
C2	Incident Management control	Management owner to be assigned for all Incidents involving the Hosting Services as per agreed procedures.	N						
C3	Escalation	Incidents escalated to appropriate level in accordance with the escalation procedure.	N						
C4	Incident occurrence	Number of Severity 1 Incidents attributable to the Hosting Services in any 1 Measurement Period should not exceed targets as set out below: Severity 1 Incidents: 0	Y			5	30	0	
					0	6			
					1	1			
					>1	0			
C4	Incident occurrence	Number of Severity 2 Incidents attributable to the Hosting Services in any 1 Measurement Period should not exceed targets as set out below: Severity 2 Incidents: 0	Y			4.5	22.5	0	
					0	5			
					1	3			
					>1	0			
C5	Incident resolution	Percentage of Incidents Resolved within target timescales for Severity Level: Severity 1 within 2 hours (98%) Severity 2 within 6 hours (98%) Severity 3 within 2 days (95%) Severity 4 within 5 days (95%)	Y			1	5	0	
					All 4 percentage targets met	5			
					Sev 1, 2 & 3 percentage targets met, Sev 4 percentage target not met	3			
					Sev 1 & 2 percentage targets met, Sev 3 percentage target not met	2			
					Sev 1 and 2 targets not met	0			
		<i>"Resolved" means the Problem will be fully corrected or an agreed action is in place, or actions to circumvent the Problem (service restoration) have been taken.</i>  <i>Severity 2 Incidents raised for faults in the Hosting Services which result in single leg operation shall be excluded from Service Credit measurements if they result in zero (0) impact to Gateway services.</i>  <i>Severity 1 Incidents raised for complete loss of either GSi or Internet connectivity to the Gateway shall be excluded from Service Credit measurements if they do not breach the network availability SLA targets defined above for items A3 &amp; A4.</i>							
D. Problem Management									
D1	Introduced Faults	No more than qty 1 or 5% (whichever shall be greater) of Problems raised in the quarter are caused by the implementation of RFCs relating to Hosting Services.	Y			1	5	0	
					=< 1 or 5%	5			
					> 1 or 5%	0			
D2	Escalation	All Problems escalated to appropriate level in accordance with the escalation Procedure.	N						
D3	Agreed and implemented action plan	All Problems to have solution documented and actioned at closure of Problem ticket.	Y			1	5	0	
					100%	5			
					<100%	0			
D4	Problem logging	Problem tickets to be logged for all Severity 1 and Severity 2 Incidents & for any Severity 3 Incidents where it is agreed that further Root Cause Analysis (RCA) is required.	N						

	D5	Problem prioritisation	All Problems to be assigned a Severity Level. Severity Level to be based to be based on risk of reoccurrence versus impact algorithm.	N					
	D6	Repeat Problems	No more than qty 1 or 5% (whichever shall be the greater) of Problems raised during the Measurement Period which are attributable to the Hosting Services are repeat Problems.	Y			1	5	0
					=< 1 or 5%	5			
					> 1 or 5%	0			
	D7	Root Cause Analysis	No fewer than qty 1 or 75% (whichever shall be the greater) of Problems associated with the Hosting Services outstanding for 2 weeks or greater will have Root Cause identified.	Y			1	5	0
					>= 1 or 75%	5			
					< 1 or 75%	0			
	D8	Root Cause Analysis	No fewer than qty 1 or 90% (whichever shall be the greater) of all closed Problems associated with the Hosting Services will have Root Cause identified.	Y			1	5	0
					>= 1 or 90%	5			
					< 1 or 90%	0			
<b>E. Service Level Management</b>									
	E1	Produce and issue statistics for Measurement Period	Network utilisation, NOC and Service Level statistics available by 5th day of the next Measurement Period.	Y			1	5	0
					Available by due date	5			
					1 day late	3			
					> 1 day late	0			
	E2	Produce and issue Service Report for Measurement Period	Report circulated by 10th day of the next Measurement Period.	Y			1	5	0
					Published on time	5			
					Not published on time	0			
	E3	CSIP improvements	90% of documented CSIP improvements delivered to schedule.	N					
	E4	Submission of accurate invoices	Accurate VAT invoices to be issued on agreed date, with clear detail.	Y			1	5	0
					Issued on time	5			
					Up to 1 week late	3			
					> 1 week late	0			
			<i>Where invoices are found to be inaccurate, submission date will be recorded as the date when updated, accurate invoice is submitted.</i>						
	E5	Attend service review for Measurement Period	Meeting to be held by 15th day of the next Measurement Period unless otherwise agreed.	N					
	E6	Manage third parties to agreed SLAs	All exceptions where third party performance impacts Hosting Service Levels are to be reported in monthly meeting and CONTRACTOR to arrange third party attendance at meeting if appropriate. <i>Where due date falls on a non Working Day it will carry over to the next Working Day without penalty.</i>	N					
<b>F. Change Management</b>									
	F1	Change logging	All Changes relating to the Hosting Services to be logged with priority and business impact classifications.	Y			1	5	0
					100%	5			
					1-2 breaches	2			
					>2 breaches	0			
	F2	Authorisation	All Changes to be authorised as per procedure.	N					
	F3	Failed Change	Failed Changes causing service impact will be 0%.	N					
	F4	Backed out	Percentage of Changes backed out in the quarter. Not to exceed qty 1 or 1% (whichever shall be the greater) of Changes.	Y			1	5	0
					Met	5			
					Not met	0			
	F5	Emergency Operational Changes	Percentage of Changes to the Hosting Services in the quarter that are Emergency Operational Changes, not to exceed qty 1 or 5% (whichever shall be the greater).	Y			1	5	0
					Met	5			
					Not met	0			
	F6	Change Request Impact Assessments	98% of Change Request Impact Assessments produced in agreed timescales.	Y			1	5	0
					98% or greater	5			
					< 98% but > 75%	2			
					75% or less	0			

G. Release Management								
Note. Some measures can only be reviewed quarterly or yearly.	G1	Release Schedule	An agreed schedule for Releases involving the Hosting Services produced each quarter based on the overarching Release strategy.	N				
	G2	Releases requiring downtime	100% of Releases not to exceed advertised outage window.	N				
	G3	Releases backed out	Percentage of Releases backed out for reasons relating to the Hosting Services not to exceed 5% of all Releases in a quarter.	N				
	G4	Delivery of schedule	95% of scheduled activity in the quarter completed to planned timetable.	N				
	G5	Testing	No Releases relating to the Hosting Services to result in any impact to services above those advertised in Release documentation	N				
	G6	Documentation	Documentation to be produced for all Releases relating to the Hosting Services as defined in Release Procedures.	Y		1.5	7.5	0
			<i>Any over-running of advertised outage windows are to be classified as unscheduled outages (Incidents) for the duration of the over-run.</i>					
H Configuration Management								
	H1	Maintenance of CMDB	Configuration Report availability within 3 days of request for all Configurable Items relating to the Hosting Services.	N				
	H2	CMDB in line with Change Management process	Configuration Report to be 99% accurate for configuration of all Hosting Services CIs at the quarterly review. <i>Configurable Items (CIs) include all Assets and components relating to the Hosting Services</i>	N				
I. Capacity Management								
	I1	Production of Capacity Reports for Measurement Period	Capacity reports produced for Measurement Period including historical trends, thresholds and recommendations for all forecasted capacity issues, by 15th day of the next Measurement Period.	Y		1	5	0
					Met	5		
					Not met	0		
	I2	Incidents arising from Capacity Problems	Percentage of Incidents arising from Capacity Problems not forecasted in Capacity Reports (not to exceed 2% per quarter).	N				
	I3	Future Variance Reports and Historic Exception Reports	Produced within 3 days of request.	N				
J. Availability Management								
	J1	Data Restoration	Requests for tape retrieval to be actioned within 15 minutes of request.	Y		1	5	0
					Met	5		
					Not met	0		
	J2	Data Restoration	Loading of tapes for data restores to commence within 15 minutes of receipt of tape.	Y		1	5	0
					Met	5		
					Not met	0		
	J3	Data Restoration	No occurrences of human error by NOC staff which result in extension of restores beyond 10 minutes	Y		1	5	0
					Met	5		
					Not met	0		
K. IT Service Continuity Management.								
	K1	ITSCM plan	Maintain the existing ITSCM plan for the Hosting Services and formally review quarterly.	N				
	K2	ITSCM test	Participate in ITSCM test once per year.	N				
	K3	ITSCM process and escalation documentation	Maintain and update any ITSCM procedural documentation that relates to the Hosting Services and formally review quarterly.	N				
	K4	Fail over testing	Participate in fail-over test twice per year for any Hosting Services tasks.	N				
	K5	Recovery test	Participate in data / service recovery tests twice per year and successfully perform any tasks relating to the Hosting Services.	N				

<b>L. Operations and Security</b>	L1	Security clearance	Documented staff lists with SC status. All new staff or temporary staff to be processed through agreed Procedure.	N					
	L2	Security access system	All changes to access system to be logged.	N					
	L3	Visitor Logging	All visitors to be logged.	N					
	L4	Report Security Incidents	All Security Incidents to be reported in line with UNIRAS timescales and approach.	N					
	L5	Security log exported (Any security logs or CCTV footage managed under the Hosting Services)	Within 4 hours of request.	N					
	L6	Data imports and exports	As agreed.	N					
	L7	Access penetration tests	Access penetration tests undertaken each quarter.	N					
	L8	Security breaches	Zero security breaches formally raised by the AUTHORITY as a result of issues within the Hosting Services (AUTHORITY will notify CONTRACTOR if this occurs).	Y			1	5	0
					Met	5			
					Not met	0			
<b>M. Business</b>	M1	Asset Management	All Assets tagged and recorded on Asset Register.	N					
	M2	Disposal	All redundant Assets are disposed of following agreed process.	N					
	M3	Training and skills	Documented key skills register and training plans for all staff, to be reviewed quarterly to ensure staff are adequately trained and all required skillsets are accounted for.	N					
	M4	Knowledge base	Changes made to knowledge base relating to Hosting Services procedures are reviewed quarterly.	N					
								Actual QSI Data Centre Operations NOC	0
								Amount of Data Centre Operations Service Credits Due (if any)	0