hs2 engine for growth

IT Security Evaluation Methodology

Evaluation of IT Security Qualification Envelope

Qualification Questions			
Evaluation Criteria	**Question**	**Pass**	**Fail**
Data Protection	**Data location:** Please confirm that any data provided during the course of the Solution will not be stored, or processed, outside the United Kingdom.	Yes; or The response to the question was 'No', but sufficient information has been provided that reassures HS2 Ltd about the security of the data storage.	No; and/or Insufficient information has been provided that does not reassure HS2 Ltd about the security of the data storage.
	If the answer to the above is 'No', please confirm the location(s) where the data may be stored and/or processed. The file should be named 'Data Storage'. There is no page limit.		
	Accreditation: Are your data processing centre(s) 'Cyber Essentials' accredited? (See further: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview).	Yes; or The response to the question is 'No', but sufficient information has been provided that reassures HS2 Ltd about the security of the data processing.	No; and/or Insufficient information has been provided that reassures HS2 Ltd about the security of the data processing.
	If the answer to question above is 'No', please provide evidence of how HS2 Ltd.'s information will be protected. The file should be named 'Accreditation' There is no page limit.		
	ICT data protection: Can your organisation demonstrate how information and communications technology (ICT) used to support the solution is designed and managed in alignment / compliant with industry and HM Government best practices and standards? If 'Yes', please demonstrate how your Solution: • Is an effective information security management system (ISMS) as defined by ISO/IEC 27001 standard (2013 version or as superseded); • Complies with HM Government's Security Policy Framework; • Complies with CESG's End User Device Security Principles (gov.uk); • Complies with CESG's Cloud Security Principles (gov.uk); • Complies with PAS555:2013; etc. Your response should be concise and in the form of an attachment with consideration given in regard to content and number of pages. The file should be named ' ICT Data Protection'	Yes; and Sufficient information has been provided that reassures HS2 Ltd about the security of ICT.	No; or If 'Yes', insufficient information has been provided that does not reassure HS2 Ltd about the security of ICT.

Qualification Questions			
Evaluation Criteria	**Question**	**Pass**	**Fail**
	Client data breach: Has your organisation been involved in any privacy breaches involving client data in the last 5 years? If the answer to the question above is 'Yes', please attach further details and include information about whether these were reported to the relevant regulator and confirmation as to whether all corrective measures been taken /acted upon. Your response should be concise and in the form of an attachment with consideration given in regard to content and number of pages. The file should be named ' Data Breach'.	No; **or** The response to the question is 'Yes', but sufficient information has been provided that reassures HS2 Ltd about the security of the data.	Yes; **and** Insufficient information has been provided that does not reassure HS2 Ltd about the security of the data.
	Information law: Has your organisation been involved in any Information Commissioner's Office enforcement / successful civil action in relation to information law (privacy etc.) compliance in the last 5 years? If the answer to the question above is 'Yes', please attach further details and include information about the outcome and the corrective measures taken /acted upon as part of the enforcement / successful civil action. Your response should be concise and in the form of an attachment with consideration given in regard to content and number of pages. The file should be named 'Information Law'.	No; **or** The response to the question is 'Yes', but sufficient information has been provided that reassures HS2 Ltd about the compliance with the law.	Yes; **and** Insufficient information has been provided that does not reassure HS2 Ltd about the compliance with law.
	External interface: Does your organisation have adequate restrictions in place to ensure the security of external system interface? If 'Yes', please provide documentation which evidences: • You inform consumers which networks the solution is accessible from and what interfaces are exposed to those networks. • You have protections in place to prevent unauthorised access to the solution via any exposed interfaces by consumers or outsiders. • You publish guidance to consumers on how to safely connect to the solution whilst minimising risk to the consumer's systems. Your response should be concise and in the form of an attachment with consideration given in regard to content and number of pages. The file should be named 'External Interface'.	Yes; **and** Sufficient information has been provided that reassures HS2 Ltd about the security restrictions in place with regards to external system interface.	No; **or** If 'Yes,' insufficient information has been provided that does not reassure HS2 Ltd about the security restrictions in place with regards to external system interface.
	Data transition: Does your organisation have adequate systems and processes in place to ensure that the data in transit is protected at all times? If 'Yes', please provide documentation which evidences how your data in transit is protected:	Yes; **and** Sufficient information has been provided that reassures	No; **or** If 'Yes', insufficient information has been provided that does not

Qualification Questions			
Evaluation Criteria	**Question**	**Pass**	**Fail**
	- Between the consumer's end user devices and the solution; - Internally within the solution; and - Between the solution and other systems (e.g. where APIs are exposed). Maximum of 1 side of A4. The file should be named 'Data Transition'.	HS2 Ltd about the security of data transition.	reassure HS2 Ltd about the security of data transition.
	Data sanitisation: Does your organisation have adequate processes in place for data sanitisation? If 'Yes', please provide documentation which evidences: - That you inform consumers how long it will be before consumer data (and any backups) is securely sanitised following the termination of the contract or exit from the solution provision; - You securely erase consumer data when resources are moved or reprovisioned, when the consumer leaves the solution and upon request by the consumer; and - Storage media which has held consumer data is sanitised or securely destroyed at the end of its usable lifetime. Maximum of 1 side of A4. The file should be named ' Data Sanitisation'	Yes; **and** Sufficient information has been provided that reassures HS2 Ltd about the data sanitisation processes in place.	No; **or** If 'Yes', insufficient information has been provided that does not reassure HS2 Ltd about the data sanitisation processes in place.
	Equipment disposal: Does your organisation have adequate equipment disposal processes in place? If 'Yes', lease provide evidence that: - All equipment potentially containing consumer data, credentials, or configuration information for the solution identified at the end of its life or prior to being recycled; - Any components containing sensitive data are sanitised, removed or destroyed as appropriate; and - Accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker. Maximum of 1 side of A4. The file should be named 'Equipment Disposal'.	Yes; **and** Sufficient information has been provided that reassures HS2 Ltd about the equipment disposal processes in place.	No; **or** If 'Yes', insufficient information has been provided that does not reassure HS2 Ltd about the equipment disposal processes in place.