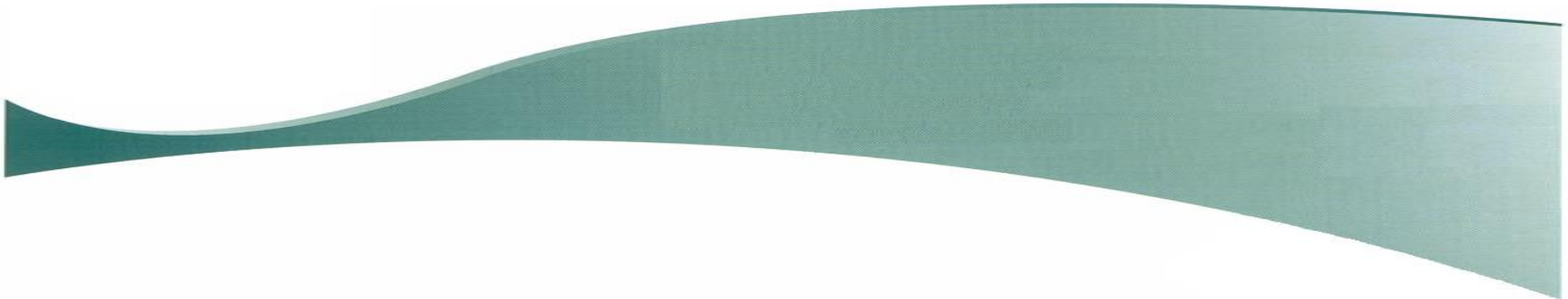




Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

HSE Supplier IT Security Assessment Questionnaire



Version 2.0

Completing the IT Security Assessment Questionnaire

1. The HSE IT Supplier Assessment Questionnaire must be completed by all HSE Suppliers who supply information systems or services to the HSE and who through the provision of these information systems and services to the HSE will or may process HSE information.
2. The purpose of the HSE IT Supplier Assessment Questionnaire is to allow the HSE to ascertain the Technical and Organisational Measures (ToM's) that the Supplier has implemented within their organisation, and not just the ToMs the supplier has in place around the information systems or services they supply to the HSE.
3. The information provided by the Supplier will only be used by the HSE for the purposes of assessing the Suppliers internal ToM's and the HSE will ensure the any information provided is kept confidential at all times.
4. The completed HSE IT Supplier Assessment Questionnaire must be signed by a member of the Supplier's management team or the Suppliers Data Protection Officer (where relevant) and returned to the HSE within **2 weeks (14 days)** of the questionnaire having been issued to the Supplier.
5. When answering the HSE IT Supplier Assessment Questionnaire Suppliers must **not** answer the questions by simply providing a link to a white paper or some other document.
6. Where appropriate the supplier must attach and return copies of certificates, policy documents and any other relevant information and/or documents referenced by the supplier in their answers to the questions.

Supplier Details	
Supplier Name	
Supplier Address	
Description of proposed service(s) and/or information systems provided to the HSE	

IT Security Assessment Questionnaire

Location, Ownership & Outsourcing

Ref	Question	Supplier Response
1	Where (what country(s)) are <u>all</u> the suppliers servers and IT infrastructure located which are used or may be used by the supplier to process HSE data?	
2	What tier of data centres does the supplier use to process HSE data?	
3	Has the suppliers data centres achieved any security accreditations for example, SOC2, SOC3,Trusted Site Infrastructure (TSI), SSAE 16 (Statements on Standards for Attestation Engagements No. 16), SAS 70 (Statement on Auditing Standards No. 70) or equivalent? If yes, please supply a copy of the accreditations.	

Location, Ownership & Outsourcing

Ref	Question	Supplier Response
4	Does the supplier outsource (for example, data centre hosting, provision of IT infrastructure etc) any part of the services which they provide to the HSE to third parties? If yes, please provide the details of the parts of the service which are outsourced and the name of third party who provides these parts of the service on behalf of the supplier	
5	In situations where a supplier is providing an information system to the HSE is the information system hosted within: a) HSE data centres. b) Off-site by the supplier using the suppliers own IT infrastructure and the suppliers own data centre. If yes, please state geographic location of data centre. c) Off-site by the supplier using the suppliers own IT infrastructure within a third party data centre (i.e. colocation data centre). If yes, please state geographic location of data centre. d) Off-site by the supplier within the cloud. If yes, please complete cloud computing section of assessment on pages 28 - 31	

Data Protection

Ref	Question	Supplier Response
6.	Under the General Data Protection Regulation (GDPR) is the supplier legally required to appoint a Data Protection Officer (DPO)? If yes, please provide the name and contact details of the suppliers DPO.	
7.	In relation to data protection roles and responsibilities for the IT information systems and services which the supplier provides to the HSE. Does the supplier consider themselves the Data Processor and the HSE as the Data Controller for any HSE 'personal data' that is processed by the supplier in the course of the HSE using the suppliers IT information systems and services?	
8.	Does the supplier have a documented data protection policy? If yes, please provide the HSE with a copy of this policy	
9.	Does the supplier maintain records of their processing activities which they carry out on behalf of their customers?	

Data Protection

Ref	Question	Supplier Response
10.	Has the supplier been audited by a European Data Protection Supervisory Authority (for example, Irish Data Protection Commissioner, UK ICO etc) in the last 3 years? If yes, please provide the HSE with an overview of the audit findings.	
11	Has the supplier had a personal data breach in the last 3 years which they had to report to a European Data Protection Supervisory Authority? If yes, please provide details of the breach and the steps taken by the supplier to rectify the breach and prevent reoccurrence	
12	Does the supplier regularly conduct GDPR / data protection audits? If yes, please answer the following questions: a) What is frequency of the GDPR / data protection audits? b) When was the last GDPR / data protection audit? c) Are the GDPR / data protection audits carried out by the suppliers own employees or are they carried out by a third party? d) Can the supplier supply the HSE with a copy (or part) of their most recent audit report or a summary of the audit findings? If not, please state why not?	

Data Protection

Ref	Question	Supplier Response
13	Has the supplier audited their third party suppliers / service providers for GDPR / data protection compliance?	
14	Does the supplier feel that they, the services and IT information systems they are currently supplying, or intend to supply to the HSE are fully compliant with the General Data Protection Regulation (GDPR)?	
15	How can the supplier demonstrate their compliance with the GDPR to the HSE?	

IT Security Controls

Ref	Question	Supplier Response
16	Does the supplier have documented IT security policies which the supplier's employees, contractors, temporary employees and third party suppliers and service providers must adhere to? If yes, can the supplier provide a copy of these IT security policies to the HSE? If not, please state why not?	
17	Do the supplier's IT security policies cover the following areas? ▪ Data classification ▪ Data privacy ▪ Data handing ▪ Email use & retention ▪ Data Retention ▪ Data & It equipment disposal ▪ Encryption ▪ Backup & Recovery ▪ Data Access ▪ Security configuration for network, operating systems, applications and computer devices ▪ Change control ▪ Network & user system access ▪ Security incident management ▪ Physical access ▪ External communications ▪ Asset management	

IT Security Controls

Ref	Question	Supplier Response
18	Does the supplier implement network firewall protection? If yes, please provide details.	
19	Does the supplier implement web application firewall protection? If yes, please provide details.	
20	Does the supplier implement host firewall protection? If yes, please provide details.	
21	Does the supplier provide network redundancy? If yes, please provide details	
22	Does the supplier employ Mobile Device Management (MDM) software? If yes, please provide details	

IT Security Controls

Ref	Question	Supplier Response
23	Does the supplier implement Network Based Intrusion Detection Systems (IDS) on their network? If yes, please provide details	
24	Does the supplier implement Host Based Intrusion Detection Systems (IDS)? If yes, please provide details	
25	Does the supplier implement Network Based Intrusion Prevention Systems (IPS) on their network? If yes, please provide details & technology	
26	Does the supplier implement Hosted Based Intrusion Prevention Systems (IPS)? If yes, please provide details & technology	
27	Does the supplier implement a Security Management System? If yes, please provide details	

IT Security Controls

Ref	Question	Supplier Response
28	Does the supplier implement anti-malware software on all their workstations, mobile computer devices and servers? If yes, please provide details of products used and how this is managed and how often this is updated.	
29	Does the supplier implement any file integrity monitoring software on their servers (for example, Tripwire etc)? If yes, please provide details.	
30	Does the supplier employ encryption software? If yes, please answer the following: a) Details of encryption algorithms and protocols used. b) Encryption products used c) Is data encrypted at rest (i.e. on disk / storage)? d) Is data encrypted in transit? e) How encryption keys are managed?	

IT Security Controls

Ref	Question	Supplier Response
31	Does the supplier have a documented patch management policy? if yes, please provide the HSE with a copy of the patch management policy which should address the following: a) Vulnerability identification and patch acquisition b) Risk assessment & prioritisation c) Patch testing d) Patch deployment and verification e) Patch distribution and application tools	
32	Describe how the supplier manages and secures remote connections to the supplier's network and services from their customers and third party suppliers / service providers (for example, VPN, SSL, TLS etc). If the supplier is using SSL or TLS please state what version(s) they are currently using.	
33	Describe what controls the supplier has in place to prevent employees and others from installing unauthorised and potentially malicious software on the suppliers computer devices and network.	
34	Please provide details of which of the suppliers employees and those of the suppliers third party suppliers / service providers will have access to HSE data and what controls the supplier has in place to prevent the unauthorised processing of HSE data.	

IT Security Controls

Ref	Question	Supplier Response
35	Will HSE data be shared with the supplier's parent or group companies? If yes, please describe what HSE data will be shared and for what purpose.	
36	Describe how the supplier manages the secure disposal of information, removable storage devices, computer media, IT devices and other IT equipment at the end of their useful life?	
37	Does the supplier keep a record of all removable storage devices, computer media, IT devices and other IT equipment which they disposed of?	
38	Does the supplier employ managed secure access points on its wireless network?	
39	Does the supplier have a documented password policy? If yes, please answer the following: a) What is minimum password length? b) What is the password refresh cycle? c) What is the password complexity requirements? d) Are passwords stored in cleared text or are they hashed? e) Is account lockout automatically enabled after a number of failed attempts to login? f) Does the supplier's password policy comply with the HSE Password Policy (https://www.hse.ie/eng/services/publications/pp/ict/password-standards-policy.pdf)	

IT Security Controls

Ref	Question	Supplier Response
40	Does the supplier prohibit split tunnelling?	
41	Describe how the supplier approves, manages and monitors it employees, contractors and temporary employees and third parties suppliers / service providers who have privileged access to the suppliers information systems and network.	
42	Describe the authentication methods (i.e. two-factor, multi-factor etc) used by the supplier to authenticate customers and third party suppliers / service providers via external connections	
43	Describe the controls the supplier has in place to ensure the segregation of data between different customers?	
44	Does the supplier feel that they, the services and information systems they are currently supplying, or intend to supply to the HSE are fully compliant with the HSE IT security policies? https://www.hse.ie/eng/services/publications/pp/ict/	

IT Security Management

Ref	Question	Supplier Response
45	Does the supplier have a dedicated IT Security Team? If yes, roughly how many people are on the IT Security Team?	
46	Is the supplier ISO 27001 certified? If yes, please supply a copy of the certification.	
47	Is the supplier Cyber Essentials or Cyber Essentials Plus certified? If yes, please supply a copy of the certifications.	
48	Apart from ISO 27001 & Cyber Essentials does the supplier hold any IT security / Cyber security certifications? If yes, please supply a copy of the certifications	
49	Does the supplier perform regular security audits of their services and information systems? If yes, what is the frequency of these and when were these last undertaken for the current services and information system which are provided to the HSE?	
50	Does the supplier regularly review access permissions for all the supplier's servers, databases and applications? If yes, what is frequency of this?	

IT Security Management

Ref	Question	Supplier Response
51	Does the supplier regularly review system logs for failed logins, or failed access attempts? If yes, what is frequency of this?	
52	Does the supplier regularly review dormant accounts on their information systems and network with a view to removing these? If yes, what is frequency of this?	
53	Does the supplier regularly review network & firewall logs? If yes, what is frequency of this?	
54	Does the supplier regularly review wireless access logs? If yes, what is frequency of this?	
55	Does the supplier regularly perform scanning in order to detect rogue wireless access points? If yes, what is frequency of this?	

IT Security Management

Ref	Question	Supplier Response
56	Does the supplier perform regular vulnerability scanning of their information systems and network? If yes, what is frequency of these?	
57	Does your organisation conduct regular penetration testing on their information systems and network? If yes, please answer the following: a) What is frequency of penetration testing on your information systems? b) When was the last information system penetration test? c) What is frequency of penetration testing on your network? d) When was the last network penetration ? e) Is the penetration testing carried out by the suppliers own employees or is it carried out by a third party company f) If the penetration testing is carried out by a third party is the third party CREST accredited g) Can the supplier supply the HSE with a copy (or part) of their most recent pen test report or a summary of the pen test findings? If not, please state why not?	
58	What, if any security test reports can the supplier make available to their HSE?	

Backup & Recovery

Ref	Question	Supplier Response
59	Does the supplier have a documented backup & recovery policy? If yes, please provide details of the backup routine and schedule (for example, full, incremental, differential, continuous, daily, weekly, monthly, etc).	
60	How often does the supplier test their backups to ensure they can restore any data stored on the backups?	
61	Does the supplier store backups off-site? If yes, please answer the following: a) Is the off-site storage of backups outsourced to a third party? If yes, please provide the name of the third party & the geographic location where the off-site backups are held. b) How does the supplier secure access to off-site backup media? c) How does the supplier secure access to backup media in transit?	

Backup & Recovery

Ref	Question	Supplier Response
62	Are the backups protected from unauthorised access, theft and tampering? If yes, please describe the access controls in place to protect the backup media.	
63	Is backup media encrypted? If yes, please describe the encryption algorithms and protocols used to encrypt the backup media.	
64	Is all backup media (onsite/offsite, full and/or incremental), rendered unreadable at the end of their useful life? If yes, please describe the method used by the supplier to render the backup media unreadable.	
65	Are procedures in place to fully erase all data contained on backup media before they are reused by the supplier? If yes, please describe the procedures used to achieve this.	
66	Does the supplier maintain records of all backup media that is disposed of?	

Disaster Recovery

Ref	Question	Supplier Response
67	Does the supplier have a documented disaster recovery plan? If yes, please answer the following: a) How frequently is the disaster recovery plan tested? b) When was the last time the supplier's disaster recovery plan was tested? c) Has the suppliers disaster recovery plan been independently audit? If yes, when was this carried out. d) Where are the copies of the supplier's disaster recovery plan stored? e) What guarantees does the supplier provide for Recovery Point Objectives (RPO)? f) What guarantees does the supplier provide for Recovery Time Objectives (RTO)? g) Does the supplier have a 'hot site(s)' which can be used to continue to provide services to their customers in the event of a disaster? h) Has the supplier achieved any business continuity certifications or does the supplier adhere to any industry business continuity standards (for example, BS25999, ISO22301 etc)? If yes, please supply a copy of the certification. i) Has the supplier had to invoke their disaster recovery plan in the last 3 years? If yes, please provide a brief description of the reason(s) why the plan was invoked.	

Personnel Security

Ref	Question	Supplier Response
68	Do the supplier's terms & conditions of employment clearly define information security requirements including non-disclosure provisions during and post employment for the supplier's employees, contractors & temporary employees?	
69	Are all the suppliers employees, contractors & temporary employees required to sign a confidentiality agreement?	
70	Please describe the suppliers pre-screening / vetting process for all their employees, contractors and temporary employees?	

Personnel Security

Ref	Question	Supplier Response
71	Are the supplier's employees, contractors & temporary employees prevented from working with the supplier prior to completion of the pre-screening / vetting process? If not, please state why not?	
72	Does the supplier conduct formal information security / data protection awareness training for all its employees, contractors and temporary employees? If yes, describe the training and how often the training is refreshed?	
73	Does the supplier have a formal procedure dictating the actions that must be taken by the supplier when one of their employees, contractors or temporary employees violates the any of the supplier's security or privacy policies?	

Support

Ref	Question	Supplier Response
74	Where the supplier provides support (i.e. hardware, software, technical, application, other) for the services and/or IT information systems they supply to the HSE, please list the type of support provided, the countries where this support is provided from and who provides the support (i.e. the supplier and/or subcontractors)	

Support

Ref	Question	Supplier Response
75	Will any part of the services and/or IT information systems provided to the HSE by the supplier, involve the supplier processing and/or transferring HSE personal data in or to a country or countries outside the European Economic Area (EEA)? If yes, please answer the following questions: a) Name of the country or countries outside the EEA where HSE personal data will be processed and/or transferred in or to? b) The purpose of processing and/or transferring HSE personal data in or to a country or countries outside EEA? c) Description of HSE personal data which is processed and/or transferred in or to a country or countries outside the EEA d) What is the relationship between the supplier and organisation within the country or countries outside the EEA where the HSE data is processed in or transferred to? e) What ‘appropriate safeguards’ have be implemented to facilitate the processing and/or transferring of HSE personal data in or to the country or countries outside the EEA, for example the use of one of the following appropriate safeguards: ➤ EU Standard Contractual Clauses ➤ Supplier has EU approved Binding Corporate Rules (BCR) ➤ The Country or Countries outside the EEA where HSE data is transferred have acquired an EU Commission ‘Adequacy Decision’ ➤ In the case of the USA, Privacy Shield Certified ➤ Other	

Incident Response

Ref	Question	Supplier Response
76	Does the supplier have a documented incident response plan? If yes, please provide the HSE with an over view of this plan and how often it tested.	

Third Party Supplier / Service Provider Management

Ref	Question	Supplier Response
77	Does the supplier have appropriate confidentiality agreements / data protection agreements in place with all their third party suppliers / service providers?	
78	Do the confidentiality agreements / data protection agreements the supplier has in place with their third party suppliers / service providers incorporate the same or similar confidentiality / data protection clauses as those in the HSE Service Provider Confidentiality Agreement? https://www.hse.ie/eng/services/publications/pp/ict/hse-service-provider-confidentiality-agreement-v3-0.pdf	
79	Does the supplier have a third party supplier / service providers assessment process in place? If yes, please describe the process.	
80	How does the supplier ensure that its third party suppliers / service providers comply with the supplier data protection and IT security policies?	

System Development & Maintenance

Ref	Question	Supplier Response
81	What tools & technologies does the supplier utilise to effectively manage the development lifecycle?	
82	Are the suppliers development, test and production environments separated physically or virtually?	
83	Does the supplier use production data in their development and/or test environment? If yes, please explain why and what controls they have in place to protect this data	
84	Does the supplier secure their development and test environments in the same manner as their production environment?	

System Development & Maintenance

Ref	Question	Supplier Response
85	At what stage of a software development project does the supplier typically start to discuss the security design requirements?	
86	Are the supplier's employee's who have specialist security training involved in the technical reviews of application designs?	
87	Have the supplier's software developers been trained in secure coding techniques?	
88	Are security professionals involved in the suppliers testing phase of an application? If yes, are the security professional employees or is this task outsourced to a third party supplier / service provider?	

Cloud Computing

This section of the Assessment is only valid where the supplier is utilising cloud services

Ref	Question	Supplier Response
89	Name of cloud service provider	
90	Geographic location of cloud servers used to process, host and backup HSE data within the cloud	
91	What is the suppliers relationship with cloud service provider	
92	Type of cloud used (for example, public, private, hybrid, community etc)	

Ref	Question	Supplier Response
93	Type of cloud service used (i.e. (for example, Saas, Paas, IaaS etc)	
94	Is the cloud service provider ISO 27001 certified? If yes, please supply a copy of the certification.	
95	Is the cloud service provider ISO 27017 certified? If yes, please supply a copy of the certification.	
96	Is the cloud service provider ISO 27018 certified? If yes, please supply a copy of the certification.	
97	Is the cloud service provider CSA Star certified? If yes, please supply a copy of the certification.	

Ref	Question	Supplier Response
98	Is the cloud service provider EuroCloud Star Audit (ECSA) certified? If yes, please supply a copy of the certification.	
99	Does the cloud service provider adhere to the EU Cloud Code of Code?	
100	Availability of cloud service. Include the following information in your answer: a) What level of service availability is guaranteed, b) How does the cloud service provider ensure availability, How is availability measured c) Has the cloud service provider attained any independent accreditation around availability (for example, Uptime Institute certification etc) d) What is the process for notifying customers in the event of an interruption to the service e) How are customers compensated for unscheduled downtime	
101	Describe the cloud technology stack	

Ref	Question	Supplier Response
102	Describe the level of support provided with the cloud service and the response times for standard calls & emergency calls etc	
103	Describe the interoperability and portability features of the cloud service. Your answer should where possible address the following: a) How does the vendor support interoperability and portability? b) If the Cloud service is compliant with ISO 19941 c) What level of support does the vendor offer for the following standards: ➤ Open Virtualization Format (OVF), ➤ Cloud Data Management Interface (CDMI), ➤ Open Cloud Computing Interface (OCCI), ➤ OASIS Topology Orchestration Specification for Cloud Applications (TOSCA), ➤ OASIS Cloud Application Management for Platforms (CAMP), Cloud Auditing Data Federation (CADF).	

Supplier Declaration

I hereby acknowledge that all the information supplied by my organisation to the HSE in the course of completing this HSE IT Security Questionnaire is true and correct to the best of my knowledge and belief.

Name of Signatory

Position

Contact Details

Signature

Date