



HSE Cyber Security Baseline (Stage 1)

Checklist

Health Service Executive (HSE) | 28/7/2026 | Version 1.4

Introduction

At this Stage 1 of this procurement process, only a Yes/No response to each question below is required, except where N/A is expressly permitted. If an answer of 'Yes' indicates that additional evidence is available, the candidate may be asked to provide details in a later stage of the procurement process. A response of 'No' to any question will result in exclusion of the candidate from this procurement process, other than where an N/A response is expressly permitted.

Checklist

Ref	Control Family	Requirement	Do you comply (Yes/No)
1	Governance & Risk Management	Do you have clear and accountable risk ownership up to board level, supported by a formal cybersecurity governance framework (e.g. ISO 27001, NIST CSF, SOC 2 Type II, Cyber Essentials)?	
2	Governance & Risk Management	Can you demonstrate current and ongoing compliance with the GDPR, and provide supporting evidence (e.g. policies, audit reports or privacy assessments) upon request?	
3	Supply Chain Security & Risk Management	Do you have a documented cybersecurity supply chain risk-management programme (policy, selection criteria and contractual controls) that includes ongoing risk assessment and monitoring of your direct suppliers and service providers and their supply chains, including those processing personal data?	
4	Supply Chain Security & Risk Management	Do you have documented controls to ensure that components used in any solution subsequently proposed for HSE are screened against applicable EU trade, sanctions and cybersecurity restrictions, and that components or suppliers identified as restricted or unacceptable under the procurement documents are not used?	
5	Supply Chain Security & Risk Management	Do you allow reasonable third-party or regulatory audits of your security controls, in line with regulatory requirements?	
6	Secure Software Development & Testing	Where your organisation develops, configures or materially customises software, hardware or firmware relevant to services of the type being procured by HSE, have you implemented and can you evidence a secure software development lifecycle (SSDLC), including threat modelling, secure coding standards and appropriate security testing? If no development, configuration or material customisation would be performed, please answer N/A.	
7	Secure Software Development & Testing	Where software, firmware, cloud service components, APIs, integrations or software-enabled products are in scope, does your organisation have the capability and established processes to produce and maintain an SBOM, or equivalent software component inventory, for the components within its control in any solution subsequently proposed for HSE? If no software, firmware, cloud service components, APIs, integrations or software-enabled products are in scope please answer N/A.	
8	Secure Software Development & Testing	Do you perform regular penetration testing (annually or after major changes) and vulnerability scans, and can you provide summaries upon request?	



Ref	Control Family	Requirement	Do you comply (Yes/No)
9	Data Protection & Privacy	Can you confirm that any solution subsequently proposed for HSE will be capable of ensuring that all HSE data remains within the EEA, or in a country subject to a valid adequacy decision, including support and monitoring activities?	
10	Data Protection & Privacy	Can you confirm that any solution subsequently proposed for HSE will provide clear mechanisms for data deletion, including secure disposal, and retention controls aligned with GDPR requirements?	
11	Cryptography & Data Encryption	Can you confirm that any solution subsequently proposed for HSE will support encryption of all sensitive data in transit, using TLS 1.2 or higher, and at rest using modern cryptographic standards such as AES-256 or equivalent?	
12	Identity & Access Management	Can you confirm that any solution subsequently proposed for HSE will support multi-factor authentication, role-based access control for all interactive interfaces, and integration with Microsoft Entra ID / ADFS or another HSE-approved identity integration method for HSE logins?	
13	Human Resources Security & Access Management	Do you have a documented joiners-movers-leavers (JML) process, including background checks where appropriate, personal-data access rights, and regular reviews of privileged access?	
14	Resilience & Incident Response	Do you have a documented and regularly tested incident response plan, including prompt customer notification in the event of a breach?	
15	Resilience & Incident Response	Have you established and tested disaster recovery (DR) and business continuity (BC) plans with defined SLAs, recovery time objectives (RTOs), and recovery point objectives (RPOs)?	
16	Environment Monitoring & SIEM/SOC	Do you either operate or have access to a 24/7 managed SOC capability, or can you demonstrate the capability to provide or integrate a solution that can filter and export relevant security events to an HSE-approved or third-party SIEM solution?	
17	Vulnerability & Patch Management	Do you operate a documented and structured vulnerability management programme with defined SLAs for critical patches?	
18	Basic Cyber Hygiene & Training	Do you maintain baseline standards for endpoint/server hardening, network configuration and system patching, and provide role-specific cybersecurity training for employees, including insider threat awareness?	
19	End-of-Service & Vendor Lock-in Considerations	Do you provide a documented exit strategy with data migration or export capabilities, and commit to continuing security patches for a specified period after an end-of-service announcement?	
20	Overall Compliance & Assurance	Can you demonstrate alignment with the NIS2 Directive and, where applicable, compliance with relevant national implementing legislation?	
21	Inventory Management	Do you maintain an up-to-date inventory of information systems and services, and records of processing activities, relevant to the services, systems and data processing that would be used to deliver any solution subsequently proposed for HSE, including classification and locations of personal and other sensitive data?	
22	Supply Chain Security & Risk Management	Can you confirm that all suppliers, subcontractors and consortium partners involved in the response to the RTP meet the security minimum requirements on this list?	