Appendix X Secure by Design Principles Evaluation Table

[*Please illustrate **how** you will meet the supplier requirements linked to the UK Government Secure by Design Principles in the table below.*]

Secure by Design Principle as published on gov.uk	**Requirements**	**How will the Supplier meet the requirement?**
Principle 1 ***Create responsibility for cyber security risk*** *Assign a designated risk owner to be accountable for managing cyber security risks for the service within the contract. This must be a senior stakeholder with the experience, knowledge and authority to lead on security activities.*	The Supplier designates a senior individual within their organisation who has overall accountability for ensuring the Secure by Design are met as part of the overall security requirements stated within the contract.	
	The Supplier designates a senior individual within the supplier delivery team - who will be reporting to the SRO, service owner or equivalent - with overall responsibility for the management of cyber security risks of digital services and technical infrastructure during their delivery.	
	The Supplier provides adequate and appropriately qualified resources to support the Authority with following the government Secure by Design approach as part of service delivery.	

Secure by Design Principle as published on gov.uk	Requirements	How will the Supplier meet the requirement?
	These resources must be reviewed at the beginning of each of the delivery phases during the delivery lifecycle of the service as agreed with the Authority.	
Principle 2 ***Source secure technology products*** *Where third-party products are used, perform security due diligence by continually assessing platforms, software and code for security vulnerabilities. Mitigate risks and share findings with suppliers to help them improve product security.*	The Supplier carries out proportionate (risk-driven) security reviews of third-party products before they are considered as a component of the digital service. The type and details of the review should be based on the significance associated with the product and are subject to agreement with the Authority.	
	The Supplier takes reasonable steps to reduce potential cyber security risks associated with using a third-party product as part of the service to a level that meets the Authority's security risk appetite for the service. Where the risk cannot be mitigated to such level, the Authority should be informed and asked to accept the risk associated with using the product.	

Secure by Design Principle as published on gov.uk	Requirements	How will the Supplier meet the requirement?
	The Supplier takes reasonable steps to assess third-party products used as a component of the digital service against legal and regulatory obligations and industry security standards specified by the Authority. Where the product doesn't meet the required obligations, the Supplier must discuss with the Authority the residual risks associated with using the product.	
Principle 3 ***Adopt a risk-driven approach*** *Establish the project's risk appetite and maintain an assessment of cyber security risks to build protections appropriate to the evolving threat landscape.*	As provided by the Authority, the Supplier should share the risk appetite across the supplier's delivery team from the outset.	
	The Supplier supports the Authority with identifying the cyber threats and attack paths as part of ongoing threat modelling during digital service delivery.	

Secure by Design Principle as published on gov.uk	Requirements	How will the Supplier meet the requirement?
	The Supplier supports the Authority with assessing cyber security risks and providing risk analysis details to help risk owners make informed risk decisions. During the assessment, risks to the digital service are identified, analysed, prioritised, and appropriate mitigation is proposed taking into account the risk appetite during the lifecycle of the service.	
	The Supplier produces an output from the risk management process containing a clear set of security requirements that will reduce the risks in line with the agreed risk appetite and cyber security risk management approach.	
	The Supplier factors in the legal and regulatory requirements provided by the Authority in the risk management process and service design and	

Secure by Design Principle as published on gov.uk	Requirements	How will the Supplier meet the requirement?
	build.	
Principle 4 ***Design usable security controls*** *Perform regular user research and implement findings into service design to make sure security processes are fit for purpose and easy to understand.*	The Supplier ensures that security requirements that are defined and documented as part of user research activities (for example user stories and user journeys) are fed into the design of the digital service.	
	The Supplier ensures that business objectives informing security requirements listed in the business case for the digital service are taken into consideration when designing security controls.	
Principle 5 ***Build in detect and respond security*** *Design for the inevitability of security vulnerabilities and incidents. Integrate appropriate security logging, monitoring, alerting and response*	The Supplier responsible for building the digital service ensures that proportionate security logging, monitoring and alerting mechanisms able to discover cyber security events and vulnerabilities documented in the threat and risk assessment are designed into the	

Secure by Design Principle as published on gov.uk	Requirements	How will the Supplier meet the requirement?
capabilities. These must be continually tested and iterated.	service.	
	The Supplier responsible for building the digital service integrates incident response and recovery capabilities that are in line with the requirements and timescales documented in the service resilience or similar documentation.	
	The Supplier responsible for building the digital service regularly tests digital services and infrastructure to identify and fix weaknesses within systems.	
Principle 6 ***Design flexible architectures*** *Implement digital services and update legacy components to allow for easier integration of new security controls in response to changes in business*	As agreed with the Authority, the Supplier responsible for building the digital service uses flexible architectures and components that allow integration of new security measures in response to changes in business requirements, cyber threats	

Secure by Design Principle as published on gov.uk	Requirements	How will the Supplier meet the requirement?
requirements, cyber threats and vulnerabilities.	and vulnerabilities.	
	The Supplier responsible for building the digital service tests security controls and verifying they are fit for purpose before deployment.	
Principle 7 ***Minimise the attack surface*** *Use only the capabilities, software, data and hardware components necessary for a service to mitigate cyber security risks while achieving its intended use.*	The Supplier responsible for building the digital service implements risk-driven security controls which meet the risk appetite and appropriate baseline as agreed with the Authority.	
	The Supplier responsible for building the digital service follows secure coding practices and, with consultation with the Authority's delivery team, identifies and mitigates vulnerabilities proactively reducing the number of vulnerabilities that potential attackers can exploit.	

Secure by Design Principle as published on gov.uk	Requirements	How will the Supplier meet the requirement?
	The Supplier retires service components (including data) securely when they are no longer needed, or at the end of their lifecycle.	
Principle 8 ***Defend in depth*** *Create layered controls across a service so it's harder for attackers to fully compromise the system if a single control fails or is overcome.*	The Supplier responsible for building the digital service adopts a defence in depth approach when designing the security architecture for the digital service.	
	The Supplier responsible for building the digital service implements security measures to incorporate segmentation.	
	The Supplier responsible for building the digital service implements mechanisms to keep the impact of potential security incidents contained.	

Secure by Design Principle as published on gov.uk	Requirements	How will the Supplier meet the requirement?
	The Supplier responsible for building the digital service tests security controls and verifying they are fit for purpose before deployment.	
Principle 9 ***Embed continuous assurance*** *Implement continuous security assurance processes to create confidence in the effectiveness of security controls, both at the point of delivery and throughout the operational life of the service.*	The Supplier responsible for building the digital service reassess controls during build to ensure they operate effectively and that no known vulnerabilities exist.	
	The Supplier responsible for building the digital service reassesses security controls against changes in the service or threat landscape during the build phase.	
	The Supplier responsible for building the digital service reports on how the delivery team follows the Secure by Design approach and adheres to the Secure by Design principles by contributing to the maintenance of the Secure by Design Self Assessment Tracker.	

Secure by Design Principle as published on gov.uk	Requirements	How will the Supplier meet the requirement?
Principle 10 ***Make changes securely*** *Embed security into the design, development and deployment processes to ensure that the security impact of changes is considered alongside other factors.*	The Supplier responsible for building the digital service works with the Authority to assess the security impact of changes before these are made to digital services and infrastructure.	
	The Supplier responsible for building the digital service records any residual unmitigated risks to the cyber security risk register and shares this with the accountable individuals and security function responsible for incorporating these into the organisation's risk registers.	