fluent technology

Project Name:			
Date:		**Release**:	
Author:			
Approver:			

Version History:

Version	Revision Date	Summary of Changes	Updated by
0.1	<Date>	First draft	

Security Checklist: <Project Name>

Personal Information held	The exact personal information that will be held in the solution and who will have access to this is: • … • … • … The suppliers experience and recommendations on how sensitive personal information is to be managed includes: • … • … • …
Security Frameworks and Regulations	This specific security frameworks that the supplier complies with are: • …. • …. • ….

	The key regulations that the supplier is making continuous steps to ensure compliance with are: • …. • …. • ….
Security Steps and Certifications	The supplier can provide evidence of certification to the following standards: • …. • …. • …. Key individuals working on our project or providing technical and/or infrastructure support are certified to the following standards: • …. • …. • ….
Monitoring Systems	The supplier has provided evidence of the following continuous monitoring systems as part of its solution: • …. • …. • …. The supplier's monitoring systems are audited by and with the following frequency: • …. • …. • …. New threats are identified as follows: • …. • …. • …. The supplier provides visibility of the system and their support activity by: • …. • …. • ….

Integrations	The supplier will integrate with our organisational security policies by: • …. • …. • ….
Interfaces	This project links to other systems and projects as follows: • …. • …. • …. The security of these interfaces will be tested through: • …. • …. • ….
Always on	The supplier is committed to providing an 'always on' solution and provides a solution that meets the following level of availability: • XXX uptime SLA • XXX critical issue response time SLA • XXX standard issue response time SLA
Security Testing Criteria	The suppliers criteria for security testing are: • … • … Quality assurance for the project must ensure that acceptance criteria are defined and met. Security quality assurance for the project will be delivered by: • … • …
Security Testing Approach	The approach to security testing for the project will include the following key activities: • … • … • …

Acceptance criteria	User acceptance criteria therefore are: • … • … Quality assurance for the project will ensure that acceptance criteria are defined and met. Quality assurance for the project will be delivered by: • … • …
Project Approach	The project approach will include the following key activities: • … • … • … • …

Project Management Team Structure	The project management structure for this project is:
	• <Project Manager> will be responsible for the project plan and delivery of the project.
	• <Quality Assurance Name> will provide quality assurance.
	• <Project Sponsor from Senior Management> will be the project sponsor.
	• The project team will include:
	  ○ <Name and Role>
	  ○ <Name and Role>
	  ○ <Name and Role>

Guidance on Required Content:

Purpose: The security checklist is used to validate that the supplier system being considered for implementation meets (ideally exceeds) our minimum security criteria.

Suppliers must demonstrate an ongoing commitment to security testing, risk mitigation and security planning as part of their solution proposal and ongoing product roadmap.

Advice: The following quality criteria should be considered when completing this checklist:

Does the supplier genuinely commit to maintaining and improving the security of their solution in an ever changing security landscape? Is frequent, independent testing the norm with new threat recognition ingrained into security procedures and practices?

Is the supplier willing to share details on their testing approach and is there clear evidence of security practices being part of their design and engineering approach?

Does the supplier have a dedicated security team? If so, what is its structure, responsibilities and individual personal development plan? Responses to this will give you a high-level insight into how seriously the suppliers takes security in their daily operations and processes and their level of expertise.

NB this checklist is designed to illicit an important conversation on system security. Vague answers, promises of things to come are no substitute for security being 'baked into' the solution from design through engineering to implementation. Security should never be ignored as part of system selection.