Cyber Risk Profile Low

The Low Cyber Risk Profile applies to contracts where it has been assessed the cyber risks to the contract may be basic but are more targeted and where the attackers may be semi-skilled but not persistent. The control measures required to mitigate the cyber risks are shown below. For further information search 'DCPP' on the GOV.UK website.

CSM Low Cyber Risk Profile Requirements
Governance
L.01 Define and assign information security relevant roles and responsibilities.
L.02 Define and implement a policy which addresses information security risks within the supply chain.
Security Culture and Awareness
L.03 Define and implement a policy which ensures all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security.
L.04 Define employee (including contractor) responsibilities for information security.
L.05 Define and implement a policy to provide employees and contractors with information security training.
Information Asset Security
L.06 Define and implement a policy for ensuring sensitive information is clearly identified.
L.07 Define and implement a policy to control access to information and information processing facilities.
Info-Cyber Systems Security
L.08 Maintain Cyber Essentials Scheme Plus Certification.
L.09 Define and implement a policy to control the exchanging of information via removable media.
L.10 Define and implement an information security policy, related processes and procedures.
L.11 Record and maintain the scope and configuration of the information technology estate.
L.12 Define and implement a policy to manage the access rights of user accounts.
Personnel Security
L.13 Define and implement a policy for verifying an individual's credentials prior to employment.
L.14 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.
L.15 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.
Security Incident Management
L.16 Define and implement an incident management policy, which must include detection, resolution and recovery.

DCPP Cyber Risk Profile – Low