Cyber Risk Profile High

The High Cyber Risk Profile applies to contracts where it has been assessed the cyber risks to the contract may be subjected to Advanced Persistent Threats (APT). Attackers at this level will typically be organised, highly sophisticated, well-resourced and persistent. APT attacks may be sustained over long periods and the attack may lay dormant for months or years after an initial approach. The control measures required to mitigate the cyber risks are shown below. For more information search 'DCPP' on the GOV.UK website.

<table>
<tr><th colspan="2">CSM High Cyber Risk Profile Requirements</th></tr>
<tr><th colspan="2">Security Governance</th></tr>
<tr><td colspan="2">L.01 Define and assign information security relevant roles and responsibilities.</td></tr>
<tr><td colspan="2">L.02 Define and implement a policy which addresses information security risks within supplier relationships.</td></tr>
<tr><td colspan="2">M.01 Define and implement a policy which provides for regular, formal information security related reporting.</td></tr>
<tr><th colspan="2">Security Culture and Awareness</th></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>L.04 Define employee (including contractor) responsibilities for information security.</td><td>M.02 Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.</td></tr>
<tr><td colspan="2">L.05 Define and implement a policy to provide employees and contractors with information security training.</td></tr>
<tr><th colspan="2">Information Asset Security</th></tr>
<tr><td>L.06 Define and implement a policy for ensuring sensitive information is clearly identified.</td><td>M.04 Define and implement a policy for storing, accessing, and handling sensitive information securely.</td></tr>
<tr><td colspan="2">M.05 Define and implement a policy for data loss prevention.</td></tr>
<tr><td>L.07 Define and implement a policy to control access to information and information processing facilities.</td><td>M.06 Ensure the organisation has identified asset owners and asset owners control access to their assets.</td></tr>
<tr><th colspan="2">Info-Cyber Systems Security</th></tr>
<tr><td colspan="2">L.08 Maintain Cyber Essentials Scheme Plus Certification.</td></tr>
<tr><td colspan="2">H.01 Maintain patching metrics and assess patching performance against policy.</td></tr>
<tr><td colspan="2">H.02 Ensure wireless connections are authenticated.</td></tr>
<tr><td colspan="2">L.09 Define and implement a policy to control the exchanging of information via removable media.</td></tr>
<tr><td colspan="2">L.10 Define and implement an information security policy, related processes and procedures.</td></tr>
<tr><td colspan="2">L.11 Record and maintain the scope and configuration of the information technology estate.</td></tr>
<tr><td colspan="2">M.07 Define and implement a policy to assess vulnerabilities identified for which there are no countermeasures (e.g. a patch) available, undertake risk assessment and management.</td></tr>
</table>

<table>
<tr><th colspan="2">CSM High Cyber Risk Profile Requirements</th></tr>
<tr><td rowspan="3">M.08 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.</td><td>H.03 Deploy network monitoring techniques which complement traditional signature-based detection.</td></tr>
<tr><td>H.04 Place application firewalls in front of critical servers to verify and validate the traffic going to the server.</td></tr>
<tr><td>H.05 Deploy network-based Intrusion Detection System (IDS) sensors on ingress and egress points within the network and update regularly with vendor signatures.</td></tr>
<tr><td>L.12 Define and implement a policy to manage the access rights of user accounts.</td><td>M.09 Define and implement a policy to monitor user account usage and to manage changes of access rights.</td></tr>
<tr><td colspan="2">M.10 Define and implement a policy to control remote access to networks and systems.</td></tr>
<tr><td>M.11 Define and implement a policy to control the use of authorised software.</td><td>H.06 Define and implement a policy to control installations of and changes to software on any systems on the network.</td></tr>
<tr><td>M.12 Define and implement a policy to control the flow of information through network borders.</td><td>H.07 Control the flow of traffic through network boundaries and police content by looking for attacks and evidence of compromised machines.</td></tr>
<tr><td colspan="2">M.13 Define and implement a policy to maintain the confidentiality of passwords.</td></tr>
<tr><td colspan="2">H.08 Undertake administration access over secure protocols, using multi-factor authentication.</td></tr>
<tr><td colspan="2">H.09 Design networks incorporating security countermeasures, such as segmentation or zoning.</td></tr>
<tr><td colspan="2">H.10 Ensure Data Loss Prevention at egress points to inspect the contents of information and take appropriate action to prevent its inadvertent or malicious release.</td></tr>
<tr><th colspan="2">Personnel Security</th></tr>
<tr><td>L.13 Define and implement a policy for verifying an individual’s credentials prior to employment.</td><td>M.14 Define and implement a policy for applying security vetting checks to employees.</td></tr>
<tr><td colspan="2">L.14 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.</td></tr>
<tr><td colspan="2">L.15 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.</td></tr>
<tr><td colspan="2">M.15 Undertake personnel risk assessments for all employees and contractors and ensure those with specific responsibilities for information security have sufficient appropriate qualifications and appropriate levels of appropriate experience.</td></tr>
<tr><td colspan="2">M.16 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.</td></tr>
<tr><th colspan="2">Security Incident Management</th></tr>
<tr><td colspan="2">L.16 Define and implement an incident management policy, which must include detection, resolution and recovery.</td></tr>
<tr><td colspan="2">H.11 Proactively verify security controls are providing the intended level of security.</td></tr>
<tr><td colspan="2">H.12 Define and implement a policy to ensure the continued availability of critical asset(s)/information during a crisis</td></tr>
</table>