REQUIREMENTS - MODERATE Cyber Risk Profile	
Good Governance	
L.01 Define and assign information security relevant roles and responsibilities.	
L.02 Define and implement a policy that addresses information security risks within supplier relationships.	
M.01 Define and implement a policy that provides for regular, formal information security related reporting.	
Culture and Awareness	
L.03 Define and implement a policy that 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.	**M.02** Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.
L.05 Define and implement a policy to provide employees and contractors with information security training.	
Risk Management	
M.03 Define and implement a policy that provides for repeatable information security risk assessments.	
Information	
L.06 Define and implement a policy for ensuring that sensitive information is clearly identified.	**M.04** Define and implement a policy for storing, accessing, and handling sensitive information securely.
M.05 Define and implement a policy for data loss prevention.	
L.07 Define and implement a policy to control access to information and information processing facilities.	**M.06** Ensure that the organisation has identified asset owners and that asset owners control access to their assets.
Technology and Services	
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.	
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.	
M.08 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.	

<table>
<tr><th colspan="2">REQUIREMENTS - MODERATE Cyber Risk Profile</th></tr>
<tr><td><b>L.12</b> Define and implement a policy to manage the access rights of user accounts.</td><td><b>M.09</b> Define and implement a policy to monitor user account usage and to manage changes of access rights.</td></tr>
<tr><td colspan="2"><b>M.10</b> Define and implement a policy to control remote access to networks and systems.</td></tr>
<tr><td colspan="2"><b>M.11</b> Define and implement a policy to control the use of authorised software.</td></tr>
<tr><td colspan="2"><b>M.12</b> Define and implement a policy to control the flow of information through network borders.</td></tr>
<tr><td colspan="2"><b>M.13</b> Define and implement a policy to maintain the confidentiality of passwords.</td></tr>
<tr><th colspan="2">Personnel Security</th></tr>
<tr><td><b>L.13</b> Define and implement a policy for verifying an individual’s credentials prior to employment.</td><td><b>M.14</b> Define and implement a policy for applying security vetting checks to employees.</td></tr>
<tr><td colspan="2"><b>L.14</b> 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"><b>L.15</b> Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.</td></tr>
<tr><td colspan="2"><b>M.15</b> 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"><b>M.16</b> Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.</td></tr>
<tr><th colspan="2">Preparing for and Responding to Security Incidents</th></tr>
<tr><td colspan="2"><b>L.16</b> Define and implement an incident management policy, which must include detection, resolution and recovery.</td></tr>
</table>

REQUIREMENTS - MODERATE Cyber Risk Profile

Good Governance

M.01 Define and implement a policy that provides for regular, formal information security related reporting.

Evidence Required

Information	Supplier's Information	Further Information
Information Security Reporting	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that identifies what information security reporting occurs. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*

General Guidance

BIS 10 Steps to Cyber Security, Information Risk Management Regime

"Maintain the Board's engagement with information risk: The risks to the organisation's information assets from a cyber attack should be a regular agenda item for Board discussion."

For further details visit:

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

BIS 10 Steps to Cyber Security, Executive Companion

"Risks to all forms of information should be treated in the same way as other financial or business risks, especially where threats and vulnerabilities are constantly changing. Ultimate responsibility for cyber security rests at Board level, with the correct governance, management and culture throughout the business. The Board should seek assurance that key information risks are both assessed and prioritised, and that there is regular monitoring where threats and vulnerabilities are constantly changing."

For further details visit:

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

REQUIREMENTS - MODERATE Cyber Risk Profile

Culture and Awareness

M.02 Define and implement a policy to detail specific employee and contractor responsibilities for information security before granting access to sensitive assets.

Evidence Required

Information	Supplier's Information	Further Information
User Security Policy / Acceptable Use Policy (AUP)		See LOW 04

General Guidance

BIS 10 Steps to Cyber Security, User Education and Awareness

"The organisation should develop and produce a user security policy (as part of their overarching corporate security policy) that covers acceptable use. Security procedures for all ICT systems should be produced that are appropriate and relevant to all business roles.

New users (including contractors and third party users) should be made aware of their personal responsibility to comply with the corporate security policies as part of the induction process."

For further details visit:

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

REQUIREMENTS - MODERATE Cyber Risk Profile		
Risk Management		
M.03 Define and implement a policy that provides for repeatable information security risk assessments.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Information Security Risk Assessment Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that provides for repeatable Information Security risk assessments. A repeatable assessment is one that can be completed in the same way many times. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*
General Guidance		
See next page.		

General Guidance

BIS 10 Steps to Cyber Security, Executive Companion

"Identify the risks to information assets. Assess who has access to those assets and who may wish to target the company. Consider the circumstances in which the risks have or could become a reality. Quantify the level of risk to those assets that the business is willing to accept and communicate your risk appetite across the business, especially to those who implement and manage the company's security. Ensure your assessments keep pace with technological advances, such as Cloud Computing, which may affect the balance of risk over time.

Implement security controls and supporting policies that are commensurate with the level of risk that the business is willing to tolerate.

Regularly review and test the effectiveness of, and adherence to, current controls, and investigate any anomalies."

For further details visit:

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook, Chapter 7, Computer Security Risk Management

"Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.

Both government and industry routinely manage a myriad of risks. For example, to maximize the return on their investments, businesses must often decide between aggressive (but high-risk) and slow-growth (but more secure) investment plans. These decisions require analysis of risk, relative to potential benefits, consideration of alternatives, and, finally, implementation of what management determines to be the best course of action.

While there are many models and methods for risk management, there are several basic activities and processes that should be performed. In discussing risk management, it is important to recognize its basic, most fundamental assumption: computers cannot ever be fully secured. There is always risk, whether it is from a trusted employee who defrauds the system or a fire that destroys critical resources. Risk management is made up of two primary and one underlying activities; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one.

Risk assessment, the process of analyzing and interpreting risk, is comprised of three basic activities: (1) determining the assessment's scope and methodology; (2) collecting and analyzing data; and (3) interpreting the risk analysis results."

For further details visit:

http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

REQUIREMENTS - MODERATE Cyber Risk Profile		
Information		
M.04 Define and implement a policy for storing, accessing, and handling sensitive information securely.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Information Handling Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that addresses accessing and handling sensitive information securely. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.* *LOW 07 – Define information processing facilities. Access in terms of site, room, computer & can computer be removed from site? How does that change things. General guidance in physical security in ISO27001.*
General Guidance		
See next page.		

General Guidance
Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook, Chapter 17, Logical Access Control "Access control is the means by which the ability is explicitly enabled or restricted in some way (usually through physical and system-based controls). Computer-based access controls are called logical access controls. Logical access controls can prescribe not only who or what (e.g., in the case of a process) is to have access to a specific system resource but also the type of access that is permitted. These controls may be built into the operating system, may be incorporated into applications programs or major utilities (e.g., database management systems or communications systems), or may be implemented through add-on security packages. Logical access controls may be implemented internally to the computer system being protected or may be implemented in external devices. A security label is a designation assigned to a resource (such as a file). Labels can be used for a variety of purposes, including controlling access, specifying protective measures, or indicating additional handling instructions. In many implementations, once this designator has been set, it cannot be changed (except perhaps under carefully controlled conditions that are subject to auditing)." For further details visit: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf Government Security Classifications, April 2014, Version 1.0 – October 2013 "Principle One: ALL information that HMG needs to collect, store, process, generate or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection. Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. Each classification provides for a baseline set of personnel, physical and information security controls that offer an appropriate level of protection against a typical threat profile. Security classifications indicate the sensitivity of information AND the typical controls necessary to defend HMG assets against a broad profile of applicable threats. Risk owners should appreciate that information classified at one level cannot be assured to be protected against the threat profile associated with a higher level of classification." For further details visit: https://www.gov.uk/government/publications/government-security-classifications

REQUIREMENTS - MODERATE Cyber Risk Profile

Information

M.05 Define and implement a policy for data loss prevention.

Evidence Required

Information	Supplier's Information	Further Information
Data Loss Prevention Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how the loss of sensitive data is prevented. This should include data recovery in the event of a security or other incident which could compromise the data (fire, flood etc). *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*

General Guidance

Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want. [CSC 15-5]

Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them. [CSC 17-9]

REQUIREMENTS - MODERATE Cyber Risk Profile		
Information		
M.06 Ensure that the organisation has identified asset owners and that asset owners control access to their assets.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Asset Owners	Confirm Asset Owners Identified and suitably informed.	"Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process."
General Guidance		
For further information see: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/365742/Guidance_on_the_IAO_Role.pdf		

REQUIREMENTS - MODERATE Cyber Risk Profile

Technology and Services

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.

Evidence Required

Information	**Supplier's Information**	**Further Information**
Vulnerability Assessment Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that addresses the management of risks that cannot be mitigated. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*

General Guidance

Note: Technical vulnerability management is assumed to have been evidenced under CES+ Certification, which verifies active patch management.

ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls

"address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, … evaluate risks, … define appropriate detective and corrective actions."

The Critical Security Controls for Effective Cyber Defense, Version 5.0, CSC 4: Continuous Vulnerability Assessment and Remediation

"Cyber defenders must operate in a constant stream of new information: software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities has become a continuous activity, requiring significant time, attention, and resources.

Attackers have access to the same information, and can take advantage of gaps between the appearance of new knowledge and remediation. For example, when new vulnerabilities are reported by researchers, a race starts among all parties, including: attackers (to "weaponize", deploy an attack, exploit); vendors (to develop, deploy patches or signatures and updates), and defenders (to assess risk, regression---test patches, install).

[CSC 4-7] Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk."

For further details visit:

https://www.sans.org/media/critical-security-controls/CSC-5.pdf.

REQUIREMENTS - MODERATE Cyber Risk Profile

Technology and Services

M.08 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.

Evidence Required

Information	Supplier's Information	Further Information
Network Monitoring Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how your networks are monitored for indications of potential incidents. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*

General Guidance

BIS 10 Steps to Cyber Security, Monitoring

"Establish a monitoring strategy and supporting policies: Develop and implement an organisational monitoring strategy and policy based on an assessment of the risks. The strategy should take into account any previous security incidents and attacks and align with the organisation's incident management policies.

Monitor all ICT systems: Ensure that the solution monitors all networks and host systems (such as clients and servers).

Monitor network traffic: The inbound and outbound network traffic traversing network boundaries should be continuously monitored to identify unusual activity or trends that could indicate attacks and the compromise of data."

Monitor all user activity: The monitoring capability should have the ability to generate audit logs that are capable of identifying unauthorised or accidental input, misuse of technology or data."

For further details visit:

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

SANS Institute, InfoSec Reading Room, Logging and Monitoring to Detect Network Intrusions and Compliance Violations in the Environment

"In an organization, there are many possible signs of incidents which may go unnoticed each day. These events can be studied mainly by analyzing network behavior or by reviewing computer security event logs. In order to avoid or minimize the losses from an incident outcome, the events need to be analyzed as close to real-time as possible. Logging and intrusion detection systems have the potential to produce very large amount of data, and all that data must be managed, filtered and analyzed."

For further details visit:

https://www.sans.org/reading-room/whitepapers/analyst

REQUIREMENTS - MODERATE Cyber Risk Profile

Technology and Services

M.09 Define and implement a policy to monitor user account usage and to manage changes of access rights.

Evidence Required

Information	**Supplier's Information**	**Further Information**
Network Monitoring Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how your networks are monitored for indications of potential incidents. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*

General Guidance

Note: User Access Control is assumed to have been evidenced under CES+ Certification, which verifies active access control for administrators.

The Critical Security Controls for Effective Cyber Defense, Version 5.0, CSC 16: Account Monitoring and Control

"[CSC 16-10] Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to active employees or contractors.

[CSC 16-11] Monitor attempts to access deactivated accounts through audit logging.

For further details visit:

https://www.sans.org/media/critical-security-controls/CSC-5.pdf.

REQUIREMENTS - MODERATE Cyber Risk Profile

Technology and Services

M.10 Define and implement a policy to control remote access to networks and systems.

Evidence Required

Information	Supplier's Information	Further Information
Remote Access	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how remote access to your networks and systems is controlled. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.* Description of how remote access to networks and systems controlled Date when policy was last reviewed, approved and issued Details of how the effectiveness of the policy is checked

General Guidance

BIS 10 Steps to Cyber Security, Home and Mobile Working

"Assess the risks to all types of mobile working (including remote working where the device connects to the corporate network infrastructure). The resulting mobile security policy should determine aspects such as the processes for authorising users to work off-site, device acquisition and support, the type of information that can be stored on devices and the minimum procedural security controls. The risks to the corporate network from mobile devices should be assessed and consideration given to an increased level of monitoring on all remote connections and the corporate systems being accessed."

For further details visit:

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

The Critical Security Controls for Effective Cyber Defense, Version 5.0, CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

"[CSC 3-7] Do all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC."

The Critical Security Controls for Effective Cyber Defense, Version 5.0, CSC 13: Boundary Defense

"[CSC 13-7] Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.

[CSC 13-8] All enterprise devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (e.g., subcontractors/vendors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access."

For further details visit:

https://www.sans.org/media/critical-security-controls/CSC-5.pdf.

REQUIREMENTS - MODERATE Cyber Risk Profile

Technology and Services

M.11 Define and implement a policy to control the use of authorised software.

Evidence Required

Information	**Supplier's Information**	**Further Information**
Authorised Software Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how the use of authorised software is controlled. The policy should include access to licensing, patching and maintaining an inventory of authorised software. It should also detail how unauthorised software is dealt with. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*

General Guidance

The Critical Security Controls for Effective Cyber Defense, Version 5.0, CSC 2: Inventory of Authorized and Unauthorised Software

[CSC 2-2] Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.

[CSC 2-4] Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level.

For further details visit:

https://www.sans.org/media/critical-security-controls/CSC-5.pdf.

REQUIREMENTS - MODERATE Cyber Risk Profile

Technology and Services

M.12 Define and implement a policy to control the flow of information through network borders.

Evidence Required

Information	**Supplier's Information**	**Further Information**
Network Border Control Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how the flow of information through network borders is controlled. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*

General Guidance

The Critical Security Controls for Effective Cyber Defense, Version 5.0, CSC 13: Boundary Defense

"[CSC 13-1] Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists).

[[CSC 13-6] Design and implement network perimeters so that all outgoing web, file transfer protocol (FTP), and secure shell traffic to the Internet must pass through at least one proxy on a DMZ network. … Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter. Proxies can also be used to encrypt all traffic leaving an organization"

The Critical Security Controls for Effective Cyber Defense, Version 5.0, CSC 17: Data Protection

"[CSC 17-13] Block access to known file transfer and e-mail exfiltration websites"

For further details visit:

https://www.sans.org/media/critical-security-controls/CSC-5.pdf.

REQUIREMENTS - MODERATE Cyber Risk Profile		
Technology and Services		
M.13 Define and implement a policy to maintain the confidentiality of passwords.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Password Protection Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how password confidentiality is maintained, including how those held on networks and systems are protected. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*
General Guidance		
The Critical Security Controls for Effective Cyber Defense, Version 5.0, CSC 16: Account Monitoring and Control "Configure all systems to use encrypted channels for the transmission of passwords over a network. [CSC 16-16] "Verify that all password files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system." [CSC 16-17] For further details visit: https://www.sans.org/media/critical-security-controls/CSC-5.pdf.		

REQUIREMENTS - MODERATE Cyber Risk Profile		
Personnel Security		
M.14 Define and implement a policy for applying security vetting checks to employees.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Security Vetting Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how and when security vetting checks are applied. *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*
General Guidance		

Information on how to apply for security vetting can be found at:

https://www.gov.uk/security-vetting-and-clearance

HMG Personnel Security Controls, Version 2.0, April 2014

"The purpose of personnel security controls (such as recruitment checks or national security vetting) is to confirm the identity of individuals (employees and contractors) and provide a level of assurance as to their trustworthiness, integrity and reliability. Whilst personnel security controls cannot provide guarantees, they are sensible precautions that provide for the identity of individuals to be properly established. In circumstances where risk assessments indicate that the necessary thresholds are met, they provide for checks to be made of official and other data sources that can indicate whether individuals may be susceptible to influence or pressure which might cause them to abuse their position or whether there are any other reasons why individuals should not have access to sensitive assets.

National security vetting comprises a range of additional checks and may be applied where a risk assessment indicates it is proportionate to do so. The risk assessment process takes account of the access an individual may have to sensitive assets (physical, personnel or information) at risk from a wide range of threats."

For further details visit:

https://www.gov.uk/government/publications/hmg-personnel-security-controls

REQUIREMENTS - MODERATE Cyber Risk Profile

Personnel Security

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.

Evidence Required

Information	Supplier's Information	Further Information
Personnel Risk Assessment Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how and when personnel risk assessments are undertaken *Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy's Title and cross-reference to the relevant section.*
Personnel Risk Assessments	< List Security Certifications > < List Relevant Experience > < List Security Certifications > < List Relevant Experience >	The individuals in these roles have been identified within LOW.01. Those with specific responsibilities for information security must have suitable, professional certifications and appropriate levels of appropriate experience. *The levels of suitable, professional certifications and experience will vary from organisation-to-organisation but should be commensurate with the organisation's threat assessment (as identified within LOW.03), business context, and complexity of the network topology and extent of its critical assets (see LOW.1)..*

General Guidance

CPNI, Personnel Security Risk Assessment, A Guide, 4th Edition

"Personnel security risk assessment focuses on employees, their access to their organisation's assets, the risks they could pose and the adequacy of existing countermeasures. This risk assessment is crucial in helping security and human resources (HR) managers, and other people involved in strategic risk decisions, communicate to senior managers the risks to which the organisation is exposed.

The use of appropriate personnel security measures can prevent or deter a wide variety of insider attacks, from staff fraud through to the facilitation or conduct of a terrorist attack. However some of these measures can also be labour intensive and costly, and may result in delays to business processes such as recruitment or movement of staff between different business areas, so it is important that they are implemented in a way that reflects the severity of the risk. Risk management provides a systematic basis for proportionate and efficient personnel security."

For further details visit:

http://www.cpni.gov.uk/advice/Personnel-security1/risk-assessment/

<table>
<tr><th colspan="3">REQUIREMENTS - MODERATE Cyber Risk Profile</th></tr>
<tr><th colspan="3">Personnel Security</th></tr>
<tr><td colspan="3"><b>M.16</b> Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.</td></tr>
<tr><th colspan="3">Evidence Required</th></tr>
<tr><th>Information</th><th>Supplier’s Information</th><th>Further Information</th></tr>
<tr><td><b>Leavers Policy</b></td><td>&lt;Title>
<Issue No>
<Issue Date>
<Authorised By> <Document Reference>
<i>&lt;Cross-reference> (see Note)</i></td><td>Identify the policy that defines how the information security risks associated with leavers are assessed and what actions are undertaken.
<i>Note: If addressed within a policy for which details are provided elsewhere (against another CSM requirement), simply quote the Policy’s Title and cross-reference to the relevant section.</i></td></tr>
<tr><th colspan="3">General Guidance</th></tr>
</table>

NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

"PS-4 Personnel Termination

The organization, upon termination of individual employment:

a. Disables information system access;

b. Terminates/revokes any authenticators/credentials associated with the individual;

c. Conducts exit interviews;

d. Retrieves all security-related organizational information system-related property;

e. Retains access to organizational information and information systems formerly controlled by terminated individual.

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment.

The organization:

(a) Notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and

(b) Requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process."

For further details visit:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf