REQUIREMENTS - LOW 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.
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.
L.05 Define and implement a policy to provide employees and contractors with information security training.
Information
L.06 Define and implement a policy for ensuring that sensitive information is clearly identified.
L.07 Define and implement a policy to control access to information and information processing facilities.
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.
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.
Preparing for and Responding to Security Incidents
L.16 Define and implement an incident management policy, which must include detection, resolution and recovery.

REQUIREMENTS - LOW Cyber Risk Profile		
Good Governance		
L.01 Define and assign information security relevant roles and responsibilities.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Identify the senior manager responsible for security in your organisation (preferably at board level)	<Name>	Typically, a board-level representative who has responsibility for managing information security risks. They should understand the strategic business goals of the organisation and how these may be affected by failure of Information Security, in order to ensure that information risks are weighed alongside other factors, such as financial, legal, operational risks. They should ensure compliance with the security requirements mandated by MOD, ensure that Security Policies are defined and subject to regular review and that information security processes and procedures are defined, monitored and reviewed.
Identify the individual who has overall day to day responsibility for security?	<Name>	The person who has responsibility for the day-to-day effectiveness of information security protective measures. They should determine where and what level of compliance is required of delivery partners and suppliers, where equivalent security policies are acceptable and the level of oversight needed to assure them that assets are properly protected. In the event of a Security Incident, they should be the designated point of contact.
Provide a Security Incident Contact:	<Name> <Telephone> <Email>	The person, helpdesk or desk officer to be contacted in the event of a Security Incident being identified. *In the event of a Security Incident, the person, helpdesk or desk officer should ideally be available 24/7.*
General Guidance		

Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook, Chapter 3, Roles and Responsibilities

"Ultimately, responsibility for the success of an organization lies with its senior managers. They establish the organization's computer security program and its overall program goals, objectives, and priorities in order to support the mission of the organization. Ultimately, the head of the organization is responsible for ensuring that adequate resources are applied to the program and that it is successful. Senior managers are also responsible for setting a good example for their employees by following all applicable security practices."

For further details visit:

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

BIS 10 Steps to Cyber Security, Information Risk Management Regime

"Establish a governance framework: A governance framework needs to be established that enables and supports information risk management across the organisation, with ultimate responsibility for risk ownership residing at Board level."

For further details visit:

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

REQUIREMENTS - LOW Cyber Risk Profile		
Good Governance		
L.02 Define and implement a policy that addresses information security risks within supplier relationships.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Supplier-related Information Security Risk Management Policy	<Title> \<Issue No> \<Issue Date> \<Authorised By> \<Document Reference> *<Cross-reference> (see Note)*	Identify the policy that states how Information Security risks within supplier relationships must be managed. *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		
ISO/IEC 27036-1: 2014 - Information security for supplier relationships — Part 1: Overview and concepts "acquirers and suppliers can cause information security risks to each other. These risks need to be assessed and treated by both acquirer and supplier organizations through appropriate management of information security and the implementation of relevant controls." For further details visit: http://standards.iso.org/ittf/PubliclyAvailableStandards/c059648_ISO_IEC_27036-1_2014.zip BIS 10 Steps to Cyber Security, Executive Companion "Effectively managing the process of assessing risks and implementing controls is essential – both in the business and supply chain." For further details visit: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility		

REQUIREMENTS - LOW Cyber Risk Profile		
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.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Information Security Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that addresses how Information Security is managed and that all parts of the business have sufficient and appropriate resources to manage the establishment, implementation and maintenance of information security. *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		

Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook, Chapter 13, Awareness, Training, and Education

"The purpose of computer security awareness, training, and education is to enhance security by:

- improving awareness of the need to protect system resources;
- developing skills and knowledge so computer users can perform their jobs more securely; and
- building in-depth knowledge, as needed, to design, implements, or operate security programs for organizations and systems."

For further details visit:

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

BIS 10 Steps to Cyber Security, Information Risk Management Regime

"Produce supporting policies: An overarching corporate information risk policy needs to be created and owned by the Board to help communicate and support risk management objectives, setting out the information risk management strategy for the organisation as a whole."

For further details visit:

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

REQUIREMENTS - LOW Cyber Risk Profile		
Culture and Awareness		
L.04 Define employee (including contractor) responsibilities for information security.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
User Security Policy / Acceptable Use Policy (AUP)	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines what employees and contractors can and can't do in terms Information Security. *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, 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 - LOW Cyber Risk Profile		
Culture and Awareness		
L.05 Define and implement a policy to provide employees and contractors with information security training.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Information Security Training and Awareness Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how employees and contractors are given Information Security training. *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, User Education and Awareness "It is critical for all staff to be aware of their personal security responsibilities and the requirement to comply with corporate security policies. This can be achieved through systematic delivery of a security training and awareness programme that actively seeks to increase levels of security expertise and knowledge across the organisation as well as a security-conscious culture. Without exception, all users should receive regular refresher training on the cyber risks to the organisation and to them as both employees and individuals." For further details visit: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility		

REQUIREMENTS - LOW Cyber Risk Profile		
Information		
L.06 Define and implement a policy for ensuring that sensitive information is clearly identified.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Information Asset Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how information assets are identified and managed. *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		
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)." See next page.		

General Guidance Continued
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 - LOW Cyber Risk Profile		
Information		
L.07 Define and implement a policy to control access to information and information processing facilities.		
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 - LOW Cyber Risk Profile		
Technology and Services		
L.08 Maintain Cyber Essentials Scheme Plus Certification.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Cyber Essentials	<Certificate ID> <Date of Award> <Certification Body>	Provide details of your Cyber Essentials Scheme Certification.
General Guidance		

The government has worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF) to develop Cyber Essentials, a set of basic technical controls for organisations to use.

The full scheme, launched on 5 June 2014, enables organisations to gain 1 of 2 new Cyber Essentials badges. It is backed by industry including the Federation of Small Businesses, the CBI and a number of insurance organisations which are offering incentives for businesses.

The Cyber Essentials Requirements document sets out the necessary technical controls. The Assurance Framework shows how the independent assurance process works and the different levels of assessment organisations can apply for to achieve the badges. It also contains guidance for security professionals carrying out the assessments.

"Of the basic but successful cyber attacks against UK businesses and citizens of which Government has detailed knowledge, the large majority would have been mitigated by full implementation of the controls under the following, selected categories:

1. Boundary firewalls and internet gateways
2. Secure configuration
3. Access control
4. Malware protection
5. Patch management".

Certification can cover the whole of an organisation's enterprise IT, or a sub-set. Whether the whole or a part of the organisation is subject to certification, the boundary of the part in scope must be clearly defined in terms of the organisation or business unit managing it, the network boundary and physical location.

The name on the certificate must be consistent with the scope.

For further details visit:

https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

REQUIREMENTS - LOW Cyber Risk Profile		
Technology and Services		
L.09 Define and implement a policy to control the exchanging of information via removable media.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Information Exchange Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how the exchange of information 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		
Typically use of removable media would be controlled. Such controls could include: rights to use being limited to a sub-set of the population; data written to removable media being forced to be encrypted; read/write actions being logged and monitored. "[CSC 5-3] Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. [CSC 5-4] Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted." BIS 10 Steps to Cyber Security, Removable Media Controls "Where removable media has to be used, the information should be encrypted. The type of encryption should be proportionate to the value of the information and the risks posed to it." For further details visit: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility		

REQUIREMENTS - LOW Cyber Risk Profile		
Technology and Services		
L.10 Define and implement an information security policy, related processes and procedures.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Information Security Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	This is the high level organisation-wide information security policy which demonstrates the company's commitment to information security.
General Guidance		
Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook, Chapter 5, Computer Security Policy "Because policy is written at a broad level, organizations also develop standards, guidelines, and procedures that offer users, managers, and others a clearer approach to implementing policy and meeting organizational goals. Standards and guidelines specify technologies and methodologies to be used to secure systems. Procedures are yet more detailed steps to be followed to accomplish particular security-related tasks. Standards, guidelines, and procedures may be promulgated throughout an organization via handbooks, regulations, or manuals. Organizational standards specify uniform use of specific technologies, parameters, or procedures when such uniform use will benefit an organization. Standardization of organization wide identification badges is a typical example, providing ease of employee mobility and automation of entry/exit systems. Standards are normally compulsory within an organization." For further details visit: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf		

REQUIREMENTS - LOW Cyber Risk Profile		
Technology and Services		
L.10 Define and implement an information security policy, related processes and procedures.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Information Security Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	This is the high level organisation-wide information security policy which demonstrates the company's commitment to information security.
General Guidance		
Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook, Chapter 5, Computer Security Policy "Because policy is written at a broad level, organizations also develop standards, guidelines, and procedures that offer users, managers, and others a clearer approach to implementing policy and meeting organizational goals. Standards and guidelines specify technologies and methodologies to be used to secure systems. Procedures are yet more detailed steps to be followed to accomplish particular security-related tasks. Standards, guidelines, and procedures may be promulgated throughout an organization via handbooks, regulations, or manuals. Organizational standards specify uniform use of specific technologies, parameters, or procedures when such uniform use will benefit an organization. Standardization of organization wide identification badges is a typical example, providing ease of employee mobility and automation of entry/exit systems. Standards are normally compulsory within an organization." For further details visit: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf		

REQUIREMENTS - LOW Cyber Risk Profile		
Technology and Services		
L.11 Record and maintain the scope and configuration of the information technology estate.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
IT Configuration Management Policy	<Title> \<Issue No> \<Issue Date> \<Authorised By> \<Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how the scope and configuration of your Information Technology estate is maintained. *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.* Confirm that this exists and is being maintained
General Guidance		
Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook, Chapter 7, Computer Security Risk Management "The first step in assessing risk is to identify the system under consideration, the part of the system that will be analyzed, and the analytical method including its level of detail and formality. Different parts of a system may be analyzed in greater or lesser detail. Defining the scope and boundary can help ensure a cost-effective assessment. Factors that influence scope include what phase of the life cycle a system in: more detail might be appropriate for a new system being developed than for an existing system undergoing an upgrade. Another factor is the relative importance of the system under examination: the more essential the system, the more thorough the risk analysis should be." For further details visit: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf		

REQUIREMENTS - LOW Cyber Risk Profile		
Technology and Services		
L.12 Define and implement a policy to manage the access rights of user accounts.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
User Account Management	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy that defines how access rights to user accounts are managed. *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 - LOW Cyber Risk Profile		
Personnel Security		
L.13 Define and implement a policy for verifying an individual's credentials prior to employment.		
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		
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 - LOW Cyber Risk Profile		
Personnel Security		
L.14 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Reporting Security Violations	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy and procedures that define how security violations can be reported in a fair, proportionate and consistent manner, without fear of recriminations. *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, User Education and Awareness "Promote an incident reporting culture: The organisation should enable a security culture that empowers staff to voice their concerns about poor security practices and security incidents to senior managers, without fear of recrimination." For further details visit: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility		

REQUIREMENTS - LOW Cyber Risk Profile		
Personnel Security		
L.15 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Acting against Security Violations	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy or procedures that define how security violations are acted upon. *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, User Education and Awareness "Establish a formal disciplinary process: All staff should be made aware that any abuse of the organisation's security policies will result in disciplinary action being taken against them." For further details visit: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility Government Security Classifications, April 2014, Version 1.0 – October 2013 "Principle Three: Access to sensitive information must ONLY be granted on the basis of a genuine'need to know' and an appropriate personnel security control The compromise, loss or misuse of sensitive information may have a significant impact on an individual, an organisation, or on government business more generally. Access to sensitive information must be no wider than necessary for the efficient conduct of an organisation's business and limited to those with a business need and the appropriate personnel security control The more sensitive the material, the more important it is to fully understand (and ensure compliance with) the relevant security requirements." For further details visit: https://www.gov.uk/government/publications/government-security-classifications		

REQUIREMENTS - LOW Cyber Risk Profile		
Preparing for and Responding to Security Incidents		
L.16 Define and implement an incident management policy, which must include detection, resolution and recovery.		
Evidence Required		
Information	**Supplier's Information**	**Further Information**
Incident Management Policy	<Title> <Issue No> <Issue Date> <Authorised By> <Document Reference> *<Cross-reference> (see Note)*	Identify the policy or procedures that define how security incidents are managed. This must include how incidents are detected, reported, resolved and recovered. *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		

Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook, Chapter 11, Preparing for Contingencies and Disasters

"A computer security contingency is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster

To avert potential contingencies and disasters or minimize the damage they cause organizations can take steps early to control the event. Generally called contingency planning, this activity is closely related to incident handling, which primarily addresses malicious technical threats such as hackers and viruses."

For further details visit:

http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter11-printable.html

BIS 10 Steps to Cyber Security, Executive Companion

"Have robust, regularly tested, incident management processes and contingency planning in place to recover from and reduce the impact of any compromises to the business, Understanding why an attack occurred and what was compromised is critical to recovering successfully and protecting the business in the future."

BIS 10 Steps to Cyber Security, Incident Management

"Establish an incident response capability: The organisation should identify the funding and resources to develop, deliver and maintain an organisation-wide incident management capability that can address the full range of incidents that could occur. The supporting policy processes and plans should be risk based and cover any legal and regulatory reporting or data accountability requirements."

For further details visit:

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

The Policy should include post-incident review and reporting obligations eg to customer and/or national authorities.