Clear.Bank

Minimum Supplier Security Requirements

(MSSRs)

Our Security Requirements for Suppliers

Our Minimum Supplier Security Requirements (MSSRs) form part of our standard contractual agreement with Suppliers that have access to ClearBank Confidential data. These control requirements are aligned with industry best practice and are advised to Suppliers during the procurement process. Unless specifically agreed otherwise, all requirements within the MSSRs will be considered binding Supplier obligations. ClearBank will continually monitor Suppliers' compliance with the MSSRs throughout their relationship with us. Further details of our oversight approach are outlined on page12.

Information Security Control Requirements

These are the minimum security controls we expect our Suppliers to maintain to protect ClearBank's systems, data and services.

Minimum Security Requirements (Physical Security)

Reference	Requirement	Description	Minimum Frequency	Purpose
PH-001	Physical Risk Assessments	Suppliers will ensure that security risk assessments are undertaken to review physical security controls and processes at sites and premises undertaking activities supporting services provided to ClearBank. Assessments must be completed by suitably experienced or qualified individuals and must consider the design and operational effectiveness of physical security controls to mitigate the current threat profile of the facility and any emerging issues that may impact the site.	Annual	Security Risk Assessments provide an accurate snapshot of Suppliers' physical security environments, controls and processes - and their current operational effectiveness.
PH-002	Access Control	Electronic, mechanical or digital physical access controls are to be deployed and managed in all Supplier premises. All security systems are to be installed, operated and maintained in accordance with applicable legal and regulatory requirements. Equipment selection must be proportionate to current physical security threats identified during the Security Risk Assessment conducted for each location.	Continuous	Effective access control is part of a layered approach to protecting premises from unauthorised access and to ensure the security of business assets.
PH-003	Security Personnel	Security personnel must be deployed where it is appropriate and proportionate in view of the Security Risk Assessment conducted for each facility, as per PHY-001.	Continuous	Security personnel are part of the layered controls to protect premises and assets from unauthorised access.
PH-004	Physical Incident Management	Suppliers will maintain procedures to manage security incidents and undertake investigations where appropriate. Where ClearBank data are impacted, incidents should be reported to ClearBank within 24-hours of discovery, with formal reports containing investigation details shared as soon as possible thereafter.	Continuous	Failure to maintain an appropriate incident management procedure may lead to inappropriate or inefficient action being taken following an incident.
PH-005	Data Centres	All data centres and cloud provider facilities used or relied upon by Suppliers must be secured to prevent unauthorised access or damage to ClearBank data. All data centres are to have layered technical and physical controls and procedures in place to protect the perimeter, building and integrity of the data halls. Appropriate controls include, but are not limited to, security cameras, intruder detection systems, physical access controls and security personnel.	Continuous	To protect data and assets held within data centres from the risk of loss, damage or theft resulting from unauthorised access.

Minimum Security Requirements (Information Security)

Reference	Requirement	Description	Minimum Frequency	Purpose
IS-001	Information Security Framework	Suppliers must establish a framework for Information Security governance to ensure there is appropriate understanding of their people, process, technology environment and the effectiveness of their information security controls. The information security framework must be documented and include administrative, technical, and physical measures to protect data from unauthorised access, loss, misuse, alteration or destruction.	Continuous	An effective security governance framework sets the overall security tone and posture for the organisation.
IS-002	Information Risk Management	Suppliers must establish an information security risk management program that effectively assesses, mitigates and monitors security risks throughout and around its environments.	Continuous	Risk Management enables visibility of, and accountability for, security risks impacting the organisation and drives informed decision making.
IS-003	Acceptable Use	Suppliers should publish acceptable use requirements on systems and data to inform all personnel of their individual responsibilities in this area. Appropriate steps should be taken to ensure compliance to these requirements (e.g. training, testing, monitoring and disciplinary action).	Continuous	Acceptable use requirements help to underpin the control environment protecting data and assets.
IS-004	Supply Chain Security	Suppliers must maintain a Supplier security assurance process to ensure their subcontractors are risk assessed, subject to appropriate due diligence, commit to contractual security obligations protecting any ClearBank data they may access, and are subject to regular oversight to ensure that all critical security controls remain design and operationally effective.	Continuous	Provides assurance that Suppliers will maintain appropriate security controls to protect ClearBank's interests.
IS-005	Security Awareness	Suppliers must have a security awareness program established for all employees, contractors, and third-party users of its systems. This will include regular updates on current security threats and relevant procedures, processes and policies.	Quarterly	Effective personnel education and awareness supports all other controls protecting data and assets.
IS-006	Security Training	Suppliers must ensure that all personnel undertake mandatory information security training within one month of joining the organisation, and at least annually thereafter. Training content should include coverage of common threats/attacks, essential controls and policies as well as an assessment to confirm the content was understood.	Annual	Effective personnel training and education supports all other controls protecting data and assets.
IS-007	Security Incident Management	Suppliers must establish a Security incident management process that effectively validates, contains and mitigates security incidents in Suppliers' environment. Suppliers must regularly test incident response plans to ensure effectiveness of response.	Annual Testing	An incident management and response process helps to ensure that incidents are quickly contained and prevented from escalating.
IS-008	Asset Management	Suppliers must maintain an effective asset management process. Asset management should govern the lifecycle of assets from acquisition to retirement, providing visibility of and security to all classes of asset in the environment.	Continuous	A complete and accurate inventory of information and technology assets is essential for ensuring appropriate controls are maintained to protect them.
IS-009	Network Security	Suppliers must ensure all IT Systems operated by it(or are operated on its behalf by a sub-contractor) are protected from lateral movement of threats within its (and any relevant sub-contractors') network. Suppliers must monitor the flows of data transiting its networks to identify and analyse anomalous access patterns or activities in the data.	Continuous	If Network Security controls are not implemented, external or internal networks could be subverted by attackers and unauthorised access could be gained to data and/or systems.

Reference	Requirement	Description	Minimum Frequency	Purpose
IS-0010	Log Management	Suppliers must ensure that there is an established log management framework which confirms that key IT systems including applications, networking equipment, security devices and servers are set to log key events. Logs must be centralized, secured and retained by Suppliers for a minimum period of 12 months.	Continuous	If this control is not implemented, Suppliers will not be able to detect and respond to inappropriate or malicious or anomalous activities within reasonable timescales.
IS-0011	Malware Defenses	Suppliers must have policies, procedures and supporting processes and technical measures in place to prevent the execution of malware on end-point devices (i.e. staff laptops, and mobile devices) and IT infrastructure network and systems components. Malware defenses should include mechanisms that perform behavioral analysis of executable code and sandboxing capabilities.	Continuous	Anti-malware solutions are vital for protection against the impact of Malicious Code.
IS-0012	Secure Configuration Standards	Suppliers must have an established framework to ensure that all systems and networking equipment are securely configured in accordance with Industry Standards (e.g. NIST, CIS).	Continuous	Standard build controls help to protect systems/data from unauthorised access.
IS-0013	Endpoint Security	Suppliers must ensure that endpoints used to access ClearBank Data are hardened to protect against attacks. Endpoint security build must include: • Disk Encryption. • Disabling all un-needed software/services/ ports • Disabling administration rights for local users.	Continuous	If this control is not implemented, endpoints may be vulnerable to attacks.
IS-0014	Data Leakage Pre-vention	Suppliers must maintain measures to protect against inappropriate data leakage including, but not limited to, monitoring and responding to the following: • Email and other communication channels for unauthorised transfer of information outside Suppliers network. • Internet / Web Gateway (including online storage and webmail) • Loss or theft of data on portable electronic media (including data on laptops, mobile devices, and portable media). • Unauthorised transfer of Information to portable media. • Insecure Information exchange with third parties (e.g., subcontractors). • Inappropriate printing or copying of data.	Continuous	Appropriate controls must be operated effectively in order to ensure that confidential information is restricted to those who should be allowed to access it (confidentiality), protected from unauthorised changes (integrity) and can be retrieved and presented when it is required (availability).
IS-0015	Secure Development	Where Suppliers develop applications, the use of secure coding practices, including OWASP Top 10 application risks, must be included. Applications must be developed in a secure environment. Where Suppliers develop applications, a Secure Development Lifecycle (SDLC) framework must be established to prevent security breaches and to identify and remediate vulnerabilities in the code during the development process.	Continuous	Controls protecting application development help to ensure that applications are secure prior to deployment.
IS-0016	Penetration Testing	Suppliers must engage with an independent external security tester to perform an assessment of their IT infrastructure and web applications. Penetration testing must be conducted on an annual basis at minimum to identify, prioritise and resolve any actively exploitable vulnerabilities in a timely manner. Critical findings should follow a predetermined remediation timeline reflective to industry standards.	Annual	If this control is not implemented, Suppliers may be unable to assess the cyber threats they face and the appropriateness and strength of their defenses.

Reference	Requirement	Description	Minimum Frequency	Purpose
IS-0017	Logical Access Management (LAM)	Access to Suppliers' systems and data must be restricted and should be managed in line with the following principles: • The need-to-know principle that people should only have access to Information they are required to know in order to perform their authorised duties; • The principle of Least Privilege that states people should only have the minimum level of privilege necessary to perform their • authorized duties; and • The segregation of duties principle that at least two individuals are responsible for the separate parts of any task to prevent error and fraud.	Continuous	If this control is not implemented, Suppliers will not be able to detect and respond to inappropriate or malicious or anomalous activities within reasonable timescales.
IS-0018	Vulnerability Management	Suppliers must maintain policies, procedures and supporting processes and technical measures to enable the timely detection of vulnerabilities within its applications, infrastructure, network and system components. Critical findings should follow a predetermined remediation timeline reflective to industry standards.	Quarterly	If this control is not implemented, attackers could exploit vulnerabilities within systems to carry out attacks against Suppliers' systems.
IS-0019	Patch Management	Suppliers must maintain policies, procedures and supporting processes and technical measures to enable the timely deployment of new security patches to all end-point devices and IT infrastructure, network and system components. If a system cannot be patched, Suppliers must implement appropriate controls to mitigate the risk.	Monthly	If this control is not implemented, services may be vulnerable to security issues which could compromise data, cause loss of service or enable other malicious activity.

Minimum Security Requirements (Personnel Security)

Reference	Requirement	Description	Minimum Frequency	Purpose
HR-001 HR-002 HR-003	Identity Verification Address Verification Credit Check	Suppliers will perform background checks on all new personnel, including but not limited to the following: • Checking valid, original photographic identity evidence, and retaining evidence. • Ensuring new personnel reside at a fixed abode by obtaining a suitable and recent document addressed to the individual that bears their home address. • Undertaking a credit and bankruptcy check of all new personnel and retain evidence.	One time	Security Risk Assessments provide an accurate snapshot of Suppliers' physical security environments, controls and processes - and their current operational effectiveness.
HR-004	Reference Checks	Suppliers will: • Verify the employment history of new personnel (last three years at minimum). • Conduct reference checks to confirm that the employment history was without incident.	One time	To confirm the suitability and integrity of new personnel and to verify that references provided are genuine.
HR-005	Criminal History Checks	Suppliers will (where permitted by local legislation) undertake, via appropriate agencies, a check for criminal convictions, and retain evidence of such checks.	One time	These checks can help to determine whether personnel are of good character and guard against the unauthorised disclosure of confidential data by individuals with criminal or malicious intent.

Information Security Oversight Approach

This is how we monitor Suppliers' compliance with the MSSRs.

Minimum Security Requirements (Supplier Oversight)

Reference	Requirement	Description	Minimum Frequency	Purpose
SO-001	Security Audit Rights	ClearBank maintains the right to conduct on-site audits of Suppliers' security controls on an annual basis to verify compliance with the MSSRs.	Annual	Audits provide ClearBank with a mechanism to actively verify Suppliers' compliance with the MSSRs and to observe the operational effectiveness of specific controls.
SO-002	Annual Security Questionnaires	ClearBank will require Suppliers to complete and return a security compliance questionnaire annually. These questionnaires must be completed as thoroughly as reasonably possible, attaching appropriate evidence as required. Suppliers must notify ClearBank in the event of material changes being made to security controls and infrastructure referred to in their most recent questionnaire submission.	Annual	ClearBank's security questionnaires provide a high-level, point-in-time overview of Suppliers' security controls.
SO-003	OSINT Scan*	ClearBank will use advanced OSINT (Open-Source Intelligence) tools to non-intrusively assess the security posture of Suppliers on a continuous basis.	Continuous	ClearBank utilises specialist tools to monitor Suppliers' overall security posture by means of publicly accessible data sources.
SO-004	Critical Finding Remediation	Where ClearBank's MSSR oversight mechanisms identify Critical findings, Suppliers must engage with ClearBank (and/or Panorays, if appropriate) to challenge or agree remediation plans in order to resolve such findings in a timely manner.	Continuous	Critical findings must be promptly and effectively managed to ensure that both ClearBank and its Suppliers are not exposed to excessive levels of security risk.
SO-005	Certification / Assurance Documentation	Upon request, Suppliers must provide ClearBank with the latest copies of certifications or reports obtained by Suppliers that demonstrate continued achievement of any Information Security related certifications communicated to ClearBank during the onboarding process.	Annual	Where Suppliers have referred to achieving independently assessed security standards (e.g. ISO 27001), ClearBank will require evidence that these Suppliers have continued to maintain such standards throughout their relationship with us.

What is OSINT and how is it used by ClearBank?

This is an overview of how ClearBank uses open-source intelligence (OSINT) to continually assess and monitor Suppliers' security postures.

Open-Source Intelligence (OSINT & Panorays)

Panorays

In order to effectively manage the level of security risk ClearBank is exposed to by its Suppliers, we use the Panorays open-source intelligence (OSINT) platform to continuously monitor their external security posture. This approach allows us to proactively identify material control weaknesses and work with our Suppliers to ensure these are remedied in an appropriate and timely manner.

Panorays' OSINT platform conducts non-intrusive scans of Suppliers' external facing infrastructure to detect configuration gaps or weaknesses and the geo-location of assets. It also monitors the 'dark-web' for signs of malicious activity and checks social and broadcast media to identify potential data breaches. ClearBank also uses this platform to send our security assurance questionnaires and collect associated evidence.