Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Application Lifecycle	**AL01**	**Secure development and testing practices**	To understand how the supplier implements best practice in development processes, including environmental segregation and testing processes.	Dedicated development environments are in place in which coding and other development practices are performed separately from production environments. Security tests are conducted on applications whilst in development to ensure they are secure prior to release and include consideration of recent threat intelligence. Security testing includes testing of all aspects of the application, including dependent libraries. Identified vulnerabilities are remediated appropriately.
	AL04	**Logging and monitoring - review and reporting**	To determine if application access is restricted to authorised individuals, and application logging is maintained and reviewed.	Access to applications require credentials, including a unique ID and a password, which allow the user to perform specific actions dependent on their access rights. Application logs are effectively maintained through a formal process. All actions performed within an application are recorded including failed access attempts and retained for at least 12 months. Application logs are reviewed regularly, with any suspicious activity alerted to. Access to sensitive application data is restricted and any unauthorised attempts to gain access to it is recorded and denied.
	AL05	**Network connections - external connections**	To determine if applications are protected from unauthorised access, and anomalous traffic is reported.	A web application firewall is in place to block any unauthorised traffic to each application interface within and across said application. Application interface inputs have been modelled against expected activity for a user of a specific level, to ensure anomalous traffic is rejected and alerted on. Controls exists to monitor application interface traffic, both inputs and outputs, and block and alert on any anomalous/suspicious activity where necessary.
	AL07	**Quality assurance - review**	To confirm that application source material is controlled, ensuring authentication, authorisation, validation, and auditing of all changes.	All code repositories have an in-built version control capability. Source code management solution is used to protect version application materials. Application code, binaries and any associated libraries are obtained/utilized from a reputable source, reviewed for integrity, and approved before using.
	AL08	**Asset management**	To ensure applications are maintained and meet the minimum security requirements.	Each application has an assigned owner with an appropriate skillset to maintain it, challenge developers against requirements, and make key decisions. The criteria by which application materials must meet in order to be introduced to either development or production environments is documented and includes security considerations. All security testing is completed prior to promotion to production.

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Application Lifecycle	**AL09**	**Industry Standards**	To understand how security configurations on applications align to relevant industry best practice.	Industry standards such like NIST / ISO / CIS, are utilized in the configuration of security for applications developed. Patches for each application must be obtained from a known reputable source. Where applications are obtained from an external provider, security configurations of the application are assessed and validated prior to being utilised.
	AL10 **AL11**	**Removal of access - controls**	To determine the controls in place to validate sessions and remove access where applicable.	Default credentials, unused identities or accounts in applications are disabled or removed. Unused functionality is blocked per least privilege or removed.
Cryptography	**CL01** **CL02** **CL03** **CL04**	**Cryptographic key lifecycle**	To understand the supplier's cryptographic key lifecycle.	Key management processes are defined and operated for all aspects of the key lifecycle, including key generation, storage, inventory, expiration, destruction. Keys are regularly rotated, and there are processes to manage key compromise events. Prior to key destruction, Impact assessments are performed to understand the impact on associated infrastructure and applications, especially for parent keys. Keys are made logically and physically unrecoverable upon destruction; destruction by third parties is made verifiable.
	CL05 **CL06** **CL07** **CL08** **CL09**	**Protection of cryptographic keys - monitoring**	To understand the supplier's cryptographic key management processes.	Keys used for LLOYDS BANKING GROUP infrastructure/data are stored securely and not shared with any other clients or supplier internal infrastructure. Keys are not reused across development, test or production environments. Keys stored in software are encrypted using a secure parameter. Keys are tracked centrally, and an audit trail is in place for all activities concerning processes in the key management lifecycle and pertaining to maintained hardware security modules. Access to keys is strictly controlled to a small number of trusted individuals. The physical locations of cryptographic functions performed are understood and risk assessed. Backups of cryptographic keys are maintained in the event of the loss of services or storage locations; escrow keys are stored in secure locations and monitored. Incident processes are in place to manage key loss or compromise events. Access to keys in component form are restricted to designated personnel in auditable key management operational procedures. No individual is permitted access to more than one component at any time. Keys in component form are designed with disaster recovery and integrity requirements in mind.

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Cryptography	CL11	**Cryptographic standards**	To confirm how the supplier sources cryptographic functions and protocols and ensures their currency	Cryptographic standards are selected from a maintained list that accounts for regulatory requirements and industry guidance, which are suitable for the lifetime of the data under encryption. Cryptographic functions used account for common sources of weak encryption, including but not limited to weak key derivation, low entropy data, salt selection, and input collisions. Cryptographic standards are reviewed on a regular basis to ensure cryptographic protocols are current and in use. As cryptographic protocols become obsolete, migration programmes are established to upgrade infrastructure to the latest standard.
	CL12			
	CL13	**Cryptographic tamper protections**	To determine what tamper protections are in place for both cryptographic audit trails and the data being protected	Cryptographic tamper-evident protection is in place to ensure that data cannot be created, substituted or modified without being detected. Protections are in place to prevent individuals tampering with the audit trail of cryptographic processes.
	CL14	**Cryptographic certificates**	To understand how the supplier manages cryptographic certificates throughout their lifecycle.	External-facing web domains maintained by the organisation are certified by a respected certification authority (CA). Only pertinent and current CA root certificates are considered trusted. Certificates issued by a Certificate Authority follow a defined process, adhering to naming and parameter requirements, and are uniquely identifiable and recorded. Certificate signing requests are transmitted in a secure manner; certificate delivery mechanisms validate the integrity and identity of the certificate. Certificate lifecycles are managed to avoid unexpected expiry; processes are in place to alert prior to expiry and initiate certificate signing requests.
	CL15			
	CL16			
	CLCSWS04	**Hardware security modules**	To understand how the supplier manages hardware security modules used to generate and control cryptographic keys.	Keys generated through the use of hardware security modules or third party providers and are FIPS 140-2 compliant. All default key values are changed prior to accession to production. Physical security controls are in place to limit access to hardware security modules maintained by the organisation. HSMs are access restricted through dual control mechanisms, and physical keys are removed when the HSM is activated. Network connected HSM security function access requires 2FA for administrative actions and operate role reparation. All cryptographic hardware devices are uniquely referenced and maintained in an inventory. Asset registers include HSMs to manage their lifecycle processes and identification in the event of theft.

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Data Storage & Loss Prevention	**DLN01**	**Network data loss prevention**	To understand how network data loss prevention polices are implemented to monitor and control the flow of data on user egress channels.	A network data loss prevention (DLP) solution has been implemented on the network, which is configured to log, monitor, alert and take action upon unusual activity in user channels. The DLP solution operates clear policies established on where data can be sent, and who has access to data transfer channels. Software, services or features that send information outside of the network boundary are disabled unless approved and appropriately configured for use by the security team.
	DLN02	**Email and web data loss prevention**	To determine how interception and decryption is performed on user egress channels.	Browser-based protection is in place and blocks at a minimum the data transfer functionality of browser-based mail (e.g. Gmail, Hotmail), file sharing sites (e.g. Dropbox, Google Drive), and social media sites (e.g. Facebook, Twitter). Email content filtering tools are in place to ensure the sending of non-public LLOYDS BANKING GROUP data (e.g. sending of card data, account information and personal data etc) is flagged, reviewed and blocked where appropriate. A cloud access security broker (CASB) or equivalent shadow cloud management service is in place to help detect and apply controls to shadow cloud usage.
	DLPE01	**Endpoint data loss prevention**	To confirm how the DLP endpoint solution manages the risk of data loss on managed endpoints.	A DLP endpoint solution is implemented to prevent data loss through external devices connecting to the network, with the configuration of the solution documented and regularly reviewed. Instances of blocked devices attempting to connect to the network are logged, monitored and aggregated for investigation. Use of removable media such as USBs is restricted and controlled; all approved USBs are encrypted under security policy.
Device	**D02**	**High risk countries**	To confirm that the supplier mitigates the risk of employees using devices in, and sending data from or to, countries that pose an inherent security risk.	High Risk countries have been identified and listed. Access to devices by employees from high risk countries is monitored and blocked as required.

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Device	D05	**Device application inventory**	To confirm how the supplier maintains accuracy and currency over applications on managed devices, as well as mitigating controls in place to prevent data loss (e.g. encryption, the use of secure communication channels, etc.)	An inventory of all managed devices is kept and regularly reviewed to ensure completeness. Where managed applications are used on unmanaged devices, segmentation is in place preventing access paths between personal and non-personal areas (e.g. moving data between segments). Portable devices have LLOYDS BANKING GROUP data sufficiently encrypted to mitigate device loss or theft. Unmanaged messaging applications are not to be used to transmit LLOYDS BANKING GROUP data.
	D07	**Device patching**	To understand how the supplier ensures applications on managed devices are kept up to date.	Managed devices either receive scheduled updates by connecting to the network, or in the case of mobile devices, through the MDM solution prompting the user to download and install an update. Users install security updates for applications on managed devices.
	D11	**Removal of devices**	To ensure supplier devices are deprovisioned securely, so that there is no risk of LLOYDS BANKING GROUP data remaining which could be accessed by unauthorised users.	De-provisioning processes are in place for any managed device, which include secure wiping of the device. If a device is stolen or lost, secure wiping of the device can be performed remotely. Data storage devices are securely destroyed upon the completion of their business use.
Identity, Authentication & Access	**IAM01**	**Unique IDs**	To understand how the supplier ties people to their accounts and associated activity, and how they justify and independently approve that access.	New user IDs for network or application accounts are linked to a unique individual; Service accounts or shared accounts are linked to a unique identity and are tied to appropriate business justification and approval; and Approval for service account access is appropriately segregated from those using the account and are subject to ongoing independent review and monitoring.

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Identity, Authentication & Access	IAM02	MFA and password authentication	To determine the identification and authentication protection on systems.	An industry-aligned password policy is in place to authenticate users to the network, applications and devices. Multi-factor authentication applied at the same point of access is in place to allow further control of access where appropriate. Use of authentication controls (i.e. passwords and MFA) are applied on the basis of risk, with higher risk access (e.g. business privilege, system administration, remote access) subject to enhanced password and MFA requirements. Authentication controls are applied consistently across all systems, where technically possible through SSO; users are unable to bypass authentication controls; authentication information is stored securely.
	IAM03	User lifecycle and authorisation	To confirm how access permissions are issued and revoked.	All access permissions are defined and documented at the entitlement level. Entitlements are assigned to any given role, and roles are assigned to users, on the basis of least privileged access. Access requests are reviewed and authorised by appropriate individuals and cannot be raised and approved by the same user. Approval requirements for access requests are determined on the basis of risk. If an employee changes role or leaves the organisation, existing access is reviewed, and any access no longer required is removed. Accounts not used within a reasonable period must be suspended. Account owners of group / shared IDs ensure passwords / PINs are changed whenever a user of the account leaves the organisation.

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Identity, Authentication & Access	**IAM04**	**Access recertification**	To determine how access is monitored and kept up-to-date and appropriate.	Access control lists (also called user access lists) are generated for all relevant applications and networks, detailing the up-to-date and accurate access rights of relevant users and are generated from reliable source. Network and application accounts are recertified on a regular basis (e.g. quarterly) based on the risk associated to the access (e.g. privileged access or financial control access). Following recertification, applicable updates to user access are made and evidence of the activity retained. Entitlements underlying roles are reviewed on a longer term review cycle (annually) to ensure they are appropriate for the role being provisioned to users.
	IAM05	**Segregation of duties**	To understand how segregation of duties is ensured and how conflicts are managed.	A segregation of duties (SoD) matrix has been defined and any toxic combinations of these duties. SoD conflicts are prevented where possible when provisioning access to roles. Where it is not possible to remediate violations, a formal risk acceptance or dispensation process is in place to define compensating controls and manage the risk.
	IAM06	**Protection of authentication information**	To understand how the supplier ensures the confidentiality and integrity of authentication information is maintained.	The generation and distribution of authentication information is performed in a secure manner. Where default passwords are allocated, passwords / PINs are changed upon first successful authentication by the user. Requests for the resetting of authentication is confirmed as coming from the identified owner or a delegate. Compromised or suspected compromised authentication information are promptly changed. Authentication information is classed as Highly Confidential data and is protected whenever stored and transferred (unless explicitly stated otherwise within the standards). Passwords are stored using one-way encryption (e.g. hashing).
	IAM07	**Access audit trails**	To determine how access controls are logged, and how audit trails are stored for future retrieval and review.	Access request logs are retained and stored centrally for a minimum period of 12 months (or longer based on risk) and can be made available to LLOYDS BANKING GROUP on request.

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Information Classification & Handling	ICH01	Information classification	To gain an understanding of the supplier's data classification and handling policy and its alignment to LLOYDS BANKING GROUP requirements.	The approach to classification is documented in a data classification policy/equivalent document which outlines what each classification type means and handling guidelines. All information, including but not limited to: policies; procedural documents; emails; public brochures; intellectual property; files containing personal data; and more, have a classification assigned to them (e.g. public, confidential, highly confidential). Mechanisms of attaching classifications to files at points of creation, and entry and exit from the network, are in use by employees.
	ICH02	Data integrity	To understand how the supplier safeguards the integrity, i.e. accuracy, of LLOYDS BANKING GROUP data under their care, including controls against accidental duplication, record replication, removal or corruption.	Controls are in place at the point of origin and receipt of data to verify properties of the data such as the number of records, to prevent records from being accidentally replicated, or the dataset as whole being duplicated. Sampling is performed against source records at the point of receipt, and whilst at rest, to validate the accuracy of the data and identify data corruption. Mechanisms are in place to restore or re-source data suspected of being corrupted or inaccurate.
	ICH03	Data protection at rest	To determine how the supplier protects its data at rest through use of controls such as encryption, and how these controls are applied to LLOYDS BANKING GROUP data.	Confidential and HC information at rest is encrypted with up-to-date encryption protocols, in network, cloud and application database settings.
	ICH04	Data protection in transit	To understand how the supplier protects LLOYDS BANKING GROUP data in transit, either electronically or physically.	LLOYDS BANKING GROUP Confidential / HC data is encrypted when transferred internally and when transferring outside of the organisation. Physical Highly Confidential data delivery is via secure Point-to Point courier (Same Day Direct Delivery), or else deliver by hand by trusted personnel. Limited and Confidential data delivery uses approved internal delivery services for delivery of internal information, and secure courier track and trace services. Approval for transport is provided by the owner of the data prior to its transit.

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Information Classification & Handling	**ICH05**	**Asset management - protection**	To ensure equipment and media are protected during relocation or decommission	Records are kept which allow unique identification and detailing of equipment and media during relocation or decommissioning Media is protected during transportation and to be sealed with a padlock and one-time use security seal. Cases have a case strap with combination lock, use constrictor technology and tamper indicators. Transportation use point-to-point courier services, and are trackable in real time with anti-bandit locks. Delivery is arranged beforehand with specific day/time and proof of delivery, and processes are in place to notification of failed delivery or suspicion that the media has been tampered with. Process must exist to ensure media can be returned or destroyed securely.
	ICH06	**Asset management - destruction**	To understand how the supplier disposes of both digital and physical data	Data is securely deleted once no longer required. Destruction methods render data forensically unrecoverable. Physical data (including hard copy data, non-reusable storage media, stamped plastic note bags, laminated paper, and credit/debit cards) is disposed of in confidential waste bins. The destruction of any computer equipment or media is recorded and logged to include: What media was disposed of; when all related inventories were updated; and certificates of hardware disposal
Infrastructure & Platform	**IPL01**	**Security configuration development and maintenance**	To understand how the organisation develops and maintains security configurations and reduces the attack surface of their systems.	Supplier uses security configurations that have been approved and uses sources of industry best practice during development. Suppliers have controls in place that allow for regular validation that security configurations are implemented, maintained and reviewed.
	IPL02			Controls to protect shared computing resources (processing, memory and storage) against manipulation Systems provide minimum access/services to complete tasks. Unauthorised executables and scripts are prevented from running.

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Infrastructure & Platform	IPL03	Trusted build media	To ensure the supplier develops, approves, controls and maintains build and platform installation media using a trusted source.	All build and installation systems come from an approved, identifiable, verifiably trusted and controlled by the supplier All build and installation systems must be reviewed for vulnerabilities to validate their security Build and installation systems follow version control processes
	IPL04	Secure state	To understand how the supplier returns to a secure state after an infrastructure or platform failure	Backups/restore points for infrastructure and platforms return to a secure state (patch levels aligned, security enhancing patches applied, security applications i.e. AV running) RTO timelines agreed and approved with infrastructure/platform owners
	IPL05	Time synchronisation	To ensure the supplier synchronises time for authentication and logging services	All system, platforms and infrastructure clocks synchronised using a reliable external time source.
Network Lifecycle	NL01	Network hardening	To understand the measures the supplier has put in place to ensure their network is secured.	An up-to-date network diagram is maintained and approved and includes all aspects of the network relevant to LLOYDS BANKING GROUP services, including firewalls, routers, cloud servers, VPN connections and data centre MLPS connections. Network device and network hardening controls are in place and actively monitored.
	NL03	DDoS protection	To ensure the supplier has taken measures to detect and respond to DDoS attacks.	Distributed Denial of Service (DDoS) protection is in place for any internet facing services to detect and prevent such an attack. The DDoS protection includes capabilities including but not limited to, rate limiting and packet dropping.
	NL04	Network traffic flow	To confirm how traffic flows across the suppliers' network, and to understand the LLOYDS BANKING GROUP data flow.	Network flow diagrams are in place, which clearly outline any flows involving LLOYDS BANKING GROUP data. Suspicious activity on any network is logged, monitored, and investigated in line with the standard incident management procedures. These include incidents such as detection of anomalous user behaviour, attempted DDoS attacks, and others.
	NLNIPS01 NLNIPS02 NLNIPS03 NLNIPS04	Intrusion detection / prevention systems (IDPS)	To understand the controls the supplier has in place to detect and prevent malicious intrusion into the network	Intrusion detection technology is deployed at all ingress points of the network, complete with alerting systems and clear processes on how detected intrusions will be managed. Intrusion prevention technology is deployed which will block any malicious intrusions to the network. Firewalls are in place at all points where data and traffic enters and exits the network, and rulesets are regularly reviewed (at a minimum every six months).

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
				DNS requests from unknown networks are blocked; DNS requests to external malicious websites are blocked / prevented from resolving.
Network Lifecycle	NLWN01	Wireless networks	To understand how the supplier secures wireless networks.	Any enterprise wireless networks have segregated corporate and guest instances. The guest wireless network only allows direct connection to the internet and is ringfenced from any corporate resources. The corporate wireless network is secured through encryption protocols such as WPA2/3 and security features such as SSID hiding and MAC/IP filtering. Connection to the corporate wireless network is subject to adequate authentication measures, such as MFA.
	NLWN02			
	NLWN03			
	NLWN04			
	NLWN05			
	NLWN06			
	NLWN07			
	NLWN08			
	NLWN09			
	NLWN10			
PCI DSS Compliance	PCI01	PCI DSS	To ensure the supplier is PCI DSS compliant and has the relevant documentation.	The supplier can provide evidence of the compliance status of the supplier in relation to the Merchant or Service Provider Level. i.e. Report on Compliance (RoC) or Attestation of Compliance (AoC) depending on Merchant or Service Provider Level Ensure the RoC or AoC is within date and agreed via an appropriate PCI DSS Auditor
	PCI02			
	PCI03			
	PCI04			
	PCI05			
Physical & People	PPS02	Preventative and detective physical controls	To understand how the supplier operates preventative and detective physical security controls to manage staff access to facilities and data, and limit intruders.	Buildings / locations where LLOYDS BANKING GROUP information is processed are restricted at all times. Monitoring and detective controls are in place to capture attempted or successful physical security breaches, and other unusual activity, for investigation. Access rights are reviewed at least annually, and quarterly for restricted areas. Access logs are retained for 12 months. Visitors and temporary access procedures are in place and logs are retained for twelve months.
	PPS03	Physical risk assessments	To ensure employees are aware of the security risks in their physical environment and how they can mitigate them.	Risk assessments (relating to buildings and restricted areas where LLOYDS BANKING GROUP information is stored, or activity conducted) are regularly conducted. Risks are assessed prior to attending offsite locations (including home working). Physical security activities are periodically reviewed. Increased physical security controls from the review are implemented in a timely manner and communicated to all employees. Any change project is assessed to determine any physical and people security impact.

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Physical & People	**PPS06**	**Accountability and reporting**	Understand how the supplier governs the accountability and reporting requirements for physical security	There is a nominated individual responsible for the management physical security. Physical security incidents are reported in a timely manner through well-defined channels. All security incidents are analysed by the security team and reported to senior management / accountable individuals.
Security Control	**SC01**	**Logging and monitoring**	To understand how the suppliers monitors their assets for security incidents, and how incident logs are maintained.	All assets deemed to have material or severe impact to the organisation are continually monitored for security events. Where possible, Highly Confidential data is not captured in these logs. Log files are protected from unauthorised tampering and change. Log files are retained for 12 months.
	SC02	**Anti-malware**	To understand what anti-malware technology is in place to protect the suppliers' assets.	Anti-malware controls are in place and up to date on all endpoint and network assets and at all locations where internet traffic enters the network. Malware signatures and solutions are updated regularly. Any failed updates are identified and remediated in a timely manner. All malware detection events are investigated as potential incidents. Detected malware is deleted and suspected malware is quarantined. All emails are scanned for active content, malicious URLs and malicious attachments.
	SC05	**Vulnerabilities - recording and management**	To understand how the supplier will identify and manage vulnerabilities both internally and externally.	Vulnerabilities are identified, analysed and managed in accordance with defined SLAs consistent with the supplier's risk appetite and LLOYDS BANKING GROUP's contractual terms. Vulnerabilities are assessed as part of any change procedure. Vulnerabilities identified are recorded to include: a description; which systems are affected; the inherent risk; the assessed risk to the business; priority of remediation; and remediation plans and deadlines. Vulnerability scans are performed through a dedicated system or accounts which are authorised through a privileged access management solution

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Security Control	VMWS03	**Infrastructure and platform penetration testing**	To understand how the supplier performs penetration testing on their infrastructure including production platforms / environments	External testing including advanced intrusion testing is performed on all networks and specified infrastructure devices at least annually by an approved testing team and schedule. A formal and documented security configuration testing process is performed by an authorised team/individual on a monthly basis, for all production networks and before a system/service enters production. Any material vulnerabilities identified by pen testing are being remediated in a timely manner.
	VMWS07	**Patch management**	To ensure the supplier manages patching processes and exceptions	A patch management system/process is in place which ensures all patches to operating systems, system software and databases are up to date, obtained from a reputable source, and deployed in a suitable time. All technologies are kept up to date with the latest updates and patches and are tested before release. Exceptions are documented and mitigating controls are agreed.
	VMWS07.01			
	VMWS07.02			
	VMWS07.03			
	VMWS07.04			
Training & Awareness	TA01	**Cyber security training**	To confirm the cyber security training that staff receive upon joining, and how this is assessed and refreshed.	The Information Security Training includes: i) Phishing / Social Engineering ii) Protecting information iii) Passwords iv) Malware v) Reporting incidents, data breaches and areas of non-compliance to management. vi) Policy awareness vii) Remote working where permissible Employees are tested on their knowledge of the training at the end of the module. All staff complete training upon joining the organisation and is refreshed every 12 months. Employees who have not completed the training are chased up by management.

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Training & Awareness	**PPS04**	**Physical security training**	Confirm that staff are trained on relevant areas of physical security in line with their role and LLOYDS BANKING GROUP standards.	Employees are trained to appropriate physical security standards on a regular basis, with any exceptions to training being recorded, escalated and remediated. Training scope includes but is not limited to: wearing staff passes on-premise (and removing them outside the office), avoiding tailgating at access gates, challenging unknown visitors, locking unattended monitors, adhering to clear desk policy (including for printers) and appropriate use of confidential waste disposal bins. Training materials must be updated with any significant business environment or threat assessment change, and metrics are collected each year to evaluate the success of training and inform updates.
Cloud Security	**CS01**	**Cloud register**	To understand how the suppliers manages and maintains a register of all cloud services.	Supplier has a detailed register of all cloud environments in use (provider, SLAs, contract length, services provided) Cloud register is regularly reviewed for accuracy and currency of cloud services in use.
	CS02	**Cloud incident management**	To establish the incident response process.	Supplier has processes in place to establish incident notification mechanisms between the cloud providers and the supplier's SOC. Cloud providers declare security incident information to the supplier quickly with a detailed description of the effect on the supplier. Supplier and cloud providers have agreed SLAs in place for timely notification of incidents and their management.
	CS03	**Cloud DDOS protection**	To establish how the suppliers cloud services are protected from DDoS attacks.	Cloud environments automatically rate limit connections from clients upon detection of a potential DDOS attack
	CS04	**Trusted communication**	To ensure cloud gateways only allow communications from trusted sources.	Cloud environments and their gateways only accept encrypted protocols from trusted and verified sources.
Policy or industry standards	**PIS01**	**Governance / Information Security Management System (ISMS)**	To confirm that there is an Information Security (IS) Policy in place and where appropriate includes supporting policies and procedures.	Supplier has a documented Information Security (IS) Policy in place that must: • Undergo a fit for purpose review at least annually • States compliance with the Security Policy is mandatory for all colleagues • Include information security roles & responsibilities • Identify roles and responsibilities of individuals / teams within each function, e.g. org chart • Be agreed / signed-off by management

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Policy or industry standards	**PIS02**	**ISMS - Legal & reg**	To confirm that there is a formal approach to ensuring that legal and regulatory requirements regarding cyber security are understood and managed.	Legal (e.g. GDPR and Network and Information Systems Regulation (NIS)) and regulatory requirements regarding cyber security, including privacy obligations, must be understood and managed: • Changes to the regulatory requirements in relevant jurisdictions must be monitored • Security program / controls must be updated to reflect changes • Relevant legal / regulatory requirements must be complied with
	PIS03	**ISMS - Scope**	To confirm the scope of the LLOYDS BANKING GROUP service is understood.	The scope of the service must be understood: • What Group data is in scope • Where it is stored / hosted, processed and transmitted • Who has access to it including onward transmission to third parties • Controls to protect it • Data flow mapped including all systems used to provide the service.
	PIS04	**ISMS - MI / Reporting**	To confirm that there is an ISMS compliance management and assessment process in place.	ISMS compliance management and assessment process must be documented and include: • Methods to test compliance to controls within the ISMS • Reporting of compliance and non-compliance to management • A governance framework in place with appropriate escalation • Agreeing exceptions to policy • Identification and update on threats.
	PIS05	**ISMS - Documentation**	To establish that ISMS policy and procedure documentation is in place.	Policies must include the following attributes: • Assigned owner(s) • Review cycle (at least annual) and date of last review • Approval from Senior Management • Date of last issue • Version controlled. Information Security documents must be: • Published • Communicated to all relevant staff • Reviewed at least annually. Minimum standards must: • Be documented but not necessarily at policy level • Be implemented and evidenced

Lloyds Banking Group Third Party Supplier Security Standards

Security Domain	Reference	Control	Goal	Principle Requirements
Policy or industry standards	**PIS06**	**ISMS - Training (standard)**	To establish that staff understand how to protect LLOYDS BANKING GROUP customers and their data.	Staff must know how to protect LLOYDS BANKING GROUP customers and their data: • All relevant staff must complete relevant security awareness training before working on or supporting any service provided to LLOYDS BANKING GROUP • Staff complete the training annually • Staff knowledge is tested to validate a user's understanding of topics covered • Training exceptions must be reported to LLOYDS BANKING GROUP • Non-compliance is identified, recorded and tracked • Training content is reviewed annually.
Risk Assessment & Remediation	**RAR01**	**Risk - Management**	To confirm that there is an Information & Cyber Security risk management process in place.	Information & Cyber Security risks must be identified, documented, owned, regularly reviewed, and tracked through to resolution / risk acceptance.
	RAR02	**Risk - threats**	To establish how the supplier keeps up to date with the external threat landscape.	Outsider threat knowledge must be kept up to date e.g. attending forums and / or external communications such as newsletters and knowledge must be dispersed within the organisation.
Incident Management & Reporting	**IMR01**	**Investigation authorisation**	To understand how the suppliers manage and respond to incidents.	Documented policy / procedure that establishes management responsibilities and procedures for a quick, effective and orderly response to incidents including: • Availability of offline copies of Incident Management playbooks/procedures • Categorisation, e.g. type and potential impact, and how to manage them • Triage and corrective actions to support SLAs • Root cause and trend analysis • Escalation internally and when LLOYDS BANKING GROUP would be notified • Engagement of specialist companies, e.g. who, for what type of incident and how to contact them • Reasonable access to necessary information to assist in any LLOYDS BANKING GROUP /Supplier investigation • Process if criminal or wrongdoing are suspected • Containment, preservation of evidence • Out-of-band communication tooling segregated from enterprise network.