GUIDANCE ON CURRENT MINIMUM SECURITY STANDARDS EXPECTED OF THIRD PARTY SUPPLIERS PROVIDING GOODS AND SERVICES TO LLOYDS BANKING GROUP

DECEMBER 2020

Control (Process)	Minimum Standard
Contract	The supplier **must be fully aware** of the contractual basis on which it provides services to Lloyds Banking Group (LBG), and in particular the mandated security requirements as set out in the Security Schedule (or agreed equivalent contractual terms).
Governance / Information Security Management System (ISMS)	An Information Security Policy must be documented and must: • Be reviewed at least annually or following any changes to the service • include Information Security roles & responsibilities • identify roles and responsibilities of individuals / teams within each function and • be agreed / signed-off by Management committing they understand risk and will treat risk exposures appropriately, i.e. in line with contractual, legal, and regulatory requirements.
Information Security Management System (ISMS) - Legal & Regulatory Requirements	Legal (e.g. General Data Privacy Regulation (GDPR) and Network and Information Systems Regulation) and regulatory requirements regarding security, including privacy obligations, must be understood and managed: • Changes to the regulatory requirements in relevant jurisdictions must be monitored and security program / controls must be updated to reflect changes and • relevant Legal and Regulatory requirements must be complied with.
Information Security Management System (ISMS) - Scope	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 3rd parties • controls to protect it (as per these minimum standards) and • data flow mapped including all systems used to provide the service.
Information Security Management System (ISMS) – Management Information / Reporting	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 and • identification and update on threats.
Information Security Management System (ISMS) - Documentation	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 and • version controlled. Information Security documents must be: • Published

	• communicated to all relevant staff and • reviewed at least annually. Minimum standards must: • Be documented but not necessarily at Policy level and • be implemented and evidenced.
Information Security Management System (ISMS) - Training (standard)	Staff must know how to protect LBG customers and their data: • All relevant staff must complete relevant security awareness training before working on or supporting any service provided to LBG • staff complete the training annually • staff knowledge is tested to validate a user's understanding of topics covered and • training exceptions must be reported to LBG.
ISMS - Training (review)	Training & Awareness media must be reviewed annually to ensure it remains aligned to industry good practice.
ISMS - Training (MI)	Reports / MI should be created and communicated to senior staff and LBG highlighting any non-compliance: • Non-compliance is identified, i.e. people who have not completed training and / or the test and • non-compliance is managed, e.g. escalation to senior management.
Cyber Security Training	In line with ISMS policy, all staff with access to LBG information and / or provision of processes / services to LBG must undergo Information Security training.
Risk - Management	Information & Cyber Security risks must be identified, documented, owned, regularly reviewed, and tracked through to resolution / risk acceptance.
Risk - Threats	Outsider threat knowledge must be kept up to date e.g. attending forums and / or external communications such as newsletters, knowledge must be dispersed within the organisation.
Asset Management - Policy	There must be documented procedures in place to ensure that a current, complete, and accurate information asset inventory is maintained at all times: • Planning: Establish and verify asset requirements • Acquisition: Appropriate and fit for purpose • Operation and Maintenance: Application and management of an asset, including maintenance and support lifecycle management (e.g. tracking of End of Life/Support) and • Decommissioning & Disposal.
Asset Management - Register	The Asset Register must: • Include physical devices & systems; software applications & platforms including websites; external IT systems; critical supplier relationships; virtual / cloud-based assets • be kept up to date • be tested to ensure compliance (e.g. annual check that all applications are included plus sample test of supporting assets every quarter); and • include classification of the asset to at least LBG's standards.
Investigation authorisation	There must be a documented policy / procedure that establishes management responsibilities and procedures for a quick, effective, and orderly response to incidents including: • Process if criminal or wrongdoing are suspected • containment, preservation of evidence including chain of custody • triage and corrective actions to support Service Level Agreements (SLA) • root cause and trend analysis • categorisation, e.g. type and potential impact, and how to manage them • escalation internally and when LBG would be notified • engagement of specialist companies, e.g. who, for what type of incident and how to contact them and • reasonable access to necessary information to assist in any LBG / Supplier investigation.

	Incidents include but are not limited to: • Social Media • unauthorised logical access and • unauthorised physical access.
Investigation authorisation	There must be a documented policy / procedure that establishes management responsibilities and procedures for a quick, effective, and orderly response to incidents including: • Process if criminal or wrongdoing are suspected • containment, preservation of evidence • triage and corrective actions to support SLAs • root cause and trend analysis • categorisation, e.g. type and potential impact, and how to manage them escalation internally and when LBG would be notified • engagement of specialist companies, e.g. who, for what type of incident and how to contact them and • reasonable access to necessary information to assist in any LBG / Supplier investigation.
Joiners Movers Leavers (JML) - policy	What, how and when access is provisioned and removed must be documented, e.g. User Access Policy (this may be LBG owned for LBG systems). • Must include JML process • authorisation for change • re-enablement / reactivation of accounts where disabled for long-term leave must include authorisation by the Line Manager • any circumstances allowing pre-approval, e.g. setup of a laptop allows for setup of remote access • privileged access / special accounts • least privilege / Segregation of Duties • management of shared / system accounts • recycling equipment; and • roles, abilities, and functions defined and documented including trust / permissions (e.g. read only).
Application - ownership	Someone, e.g. an Application Owner, must be accountable for access to the system. Either through policy or technical control: • Specified people may only grant access to the system • access can only be granted after approval provided • segregation of duties must be followed, i.e. authorisers cannot also be system administrators or perform any other function which would allow authorisation and completion of a request • 'least privilege', i.e. access is based on role and function and • Access Control Lists (ACLs) must be maintained for each system.
Application - Privilege Access	In addition to standard user access controls, controls on privileged (including administrator) access must include: • User accounts with privileged access must have this clearly attributed (e.g. recorded in the account properties), and be subject to user access reviews at least every 6 months • the privileged access provisioning and review process must include and record approvals appropriate to the level and type of access being granted, and be mindful of any potential for privileged access to override segregation of duties controls • privileged user access to be logged, tracked, and reported • any privileged action in any environment where Group data is handled or stored must be demonstrably linked to an agreed and approved change/service request • elevated access privileges must only be invoked where required and their use limited (as far as is practical) to the context in which they are required

	• standard user activities such as accessing email, or the internet must not be permitted while elevated access privileges are invoked and • strong authentication is required in order to use elevated access privileges.
Application - Incident Management	Any unauthorised information disclosure must: • Follow Incident Management policy and • lead to an immediate review of current least / privilege access standards.
Protection of authentication information	The supplier must have a documented and adhered to password policy / processes including: • Passwords must be changed in the event of a compromise, real or suspected • process for password change / reset • only allowing passwords to be issued to the correct individual • password changes upon first logon must be enforced, this includes a password reset where a manager or IT desk may know the password • vendor supplied default passwords and security settings must be changed and • passwords must be stored using one-way encryption, e.g. hashing.
Secure System Access Authentication	Where supplier policy states that National Institute of Standards and Technology (NIST) or any other industry standard is followed, this must be documented and referenced including how the standard is met / not met. Where a supplier does not follow a standard, the following requirements must be met: Short passwords: • Minimum length = 8 • users cannot re-use the previous 5 passwords • expires after 90 days • 5 unsuccessful attempts and • locked out for 20 mins. Long passwords: • Minimum length = 12 • users cannot re-use the previous 10 passwords • expires after 90 day • 5 unsuccessful attempts; and • locked out for 60 mins. Privileged passwords: • Minimum Length = 14 • users cannot re-use the previous 5 passwords • expires after 30 days • 3 unsuccessful attempts; and • locked out for 60 mins.
Password - Requirements	All suppliers must meet the following: • Passwords must meet complexity requirements (3 out of upper case / lower case / numbers / special characters); and • user session must time out after a defined period of inactivity not greater than 30 minutes.
Logical Identity Configuration	There must be a documented mandate, e.g. policy and / or procedure, requiring the assignment of unique system ID: • The ID must be associated to a sole, identifiable individual; and • includes all accounts involved in the operational aspects of the service provided including administrator, root, privileged accounts or similar.
Unique ID - Exceptions	All known exceptions, e.g. application that does not support unique IDs or administrator / master accounts: • Must follow a documented standard

	• any compensating controls, e.g. proactive monitoring of event logs, break-glass procedure (this is still a gap to LBG policy) must be recorded • evidence maintained to prove who used what account, when and for what; and • ownership / accountability for the account and any changes.
Ownership of Accounts and Groups	Logs / records must be maintained in order to: • Identify ownership of LBG/Shared Accounts and/or Access Groups for Systems involving LBG Information; and • when and to whom ownership was re-attributed.
Monitoring User Access	Standards must enforce: • Annual recertification for standard accounts • 6 monthly recertification for privileged accounts • method for tracking access and response; and • a process for escalations.
Removal of Access - Policy	There must be documented standard(s) in place that explicitly define the timeframe for the revocation of user accounts to system(s), e.g. application / database / operating system / building, involving LBG Information and include: • Revocation for movers • a process for emergency revocation; and • physical assets, e.g. laptops and door access tokens, must be returned on the last day of work.
Removal of Access - Controls	Access must be removed: • Within 24 hours / 1 working day of leaving • immediately in cases of emergency revocation • if an account has not been used for 31 days (unless otherwise agreed with LBG) • on the last day of service for high risk systems (e.g. AD, VPN, DMS); and • not more than 5 business days following a user leaving or the account is no longer required to provide the service.
Removal of Access - Logs	Logs must be maintained to evidence adherence to the procedure including: • when removal of access was requested and by whom: • Date & time user left; and • date & time account was revoked.
Remote / Administrative Access - Policy	There must be a documented policy / procedure in place to ensure that all remote access must: • Enforce Multi-Factor Authentication (MFA) • enforce encryption • require authorisation and approval prior to being granted • be recertified periodically; and • log events for possible breaches which must be reviewed proactively.
Remote / Administrative Access - Controls	Technical controls must support the Remote Access policy / procedure: • Enforce encryption of the transmission of LBG Confidential and Highly Confidential information; log user activity including who connected and when; and • restrict access to authorised individuals.
Remote / Administrative Access - Management Access / Consoles	Support / management access must be provided securely: • A dedicated secure network to provide management access to infrastructure (including cloud) must be used • access accounts for remote support must only be enabled for the duration needed and monitored when in use • MFA enforced; and • access restricted to specific IP addresses.
Logging and Monitoring - Policy	There must be a documented policy / procedure in place to record events: • Administration activities • activities of staff not associated with LBG work/environment • events by privileged users / privileged access

	• logs must be protected for the duration of their life (at least 12 months); and • logs must be proactively and reactively monitored.
Logging and Monitoring - Configuration	Events recorded / logged must include at least: • All individual access to sensitive data • all actions taken by any individual with root or administrative privileges • access to all audit trails • invalid logical access attempts • use of and changes to identification and authentication mechanisms (e.g. creation of new accounts changes / elevation to privileged accounts) • initialisation, stopping or pausing of audit logs • creation and deletion of system level objects • system logon/logoff (success and failure) • use of escalated rights or administrative functions • access of sensitive system resources (success and failure) • change or escalation of rights/privileges • change to audit policies (success and failure) • change to audit logs (success and failure) • Anti-virus and malware events • Intruder Detection / Prevention System events; and • changes made to virtual machine images regardless of their running state (e.g., dormant, off or running).

Logging and Monitoring - Storage and Security	Logs must be made available and protected from change / deletion:
	• Retained for a minimum period of 12 months
	• Secured
	  ○ physical and logical access to logs / log server must be restricted
	  ○ changes or deletion of logs creates an alert; and
	  ○ log server segregated from the operational environment
	• event data are aggregated and correlated from multiple sources and sensors.

Logging and Monitoring - Review and Reporting	Event logs must be monitored and proactively reviewed: • Events are analysed to understand attack targets and methods • data are aggregated and correlated from multiple sources and sensors; and • if manual, logs must be reviewed at least monthly.
Logging and Monitoring - Review and Reporting	Alerts must be configured and issued when potential breaches have been identified, e.g. brute force attack, and must be investigated as potential incidents which must follow the incident response procedure where appropriate.
System Time	There must be a documented approach to maintaining clock synchronisation across all systems, which must include: • All systems ultimately derive their time from the same authoritative time source; and • time synchronisation status is subject to active monitoring or regular checks (at least weekly), with any failures or out of band devices being identified and investigated.
Data Classification – Policy	There must be a documented Policy and supporting procedures: • LBG information must be classified • assets holding LBG information must be classified • information assets must be protected • unauthorised disclosure of LBG information is prohibited • incidents must be reported; and • LBG information must only be stored on authorised systems, e.g. specific applications, share drives and not local shares / drives.

Data Loss Protection (DLP) - Data at Rest (Confidential)	LBG Confidential data at rest must be protected: • Encryption must be used in off premises cloud and/or shared services providers; • Logical access controls must be applied to restrict access to those working on LBG engagement(s) only; and • must be logically separated from other client data, e.g. database, file share.
DLP - Data at Rest (Highly Confidential)	LBG Highly Confidential data at rest must be further protected: • Data at rest must be encrypted; and • changing access permissions to the content e.g. making shareable must be logged / recorded. Where encryption is not possible, a risk assessment must be performed and agreed with LBG. All the following compensating controls must be considered: • Structured data is hosted inside a data centre or technical room • strong access control, with regular access recertification (minimum every 3 months) • all access requests are subject to independent approval by business area line management • all IT privileged accounts are managed (e.g. via CyberArk) • logging and monitoring are performed in compliance with LBG IT security standards (e.g. security logs are integrated with IT SOC SIEM solution) • database Activity Monitoring is in place (for any database holding highly confidential data; and • LBG Application Owner approves lack of encryption and re-certifies solution annually as part of the risk review process.
DLP - Data at Rest	All environments must be considered including non-production and backups.
DLP - Hard Copy	All Confidential and Highly Confidential must be: • Physically secured e.g. locked cabinet • delivery of Highly Confidential information must be via secure Point to Point courier (Same Day Direct Delivery) or by hand; and • delivery of Confidential information must be via secure Courier Track and Trace (Next Day Delivery) or Royal Mail 'Special Delivery'.
DLP - Clear Desk	Checks must be performed, e.g. a floor walk, at least every three months, to identify where colleagues have failed to clear desks of LBG information.
Data Leakage (Local Drives)	Where LBG information can be saved to hard disk, technical controls must enforce: • Hard disk (HDD) level encryption and • encryption when machines are turned off. Checks must be performed to assure that devices are encrypted: • Records of checks must be maintained; and • exceptions must be reported and investigated.
Data Leakage (Exfiltration)	Where Confidential / Highly Confidential Group data is stored or processed in a production environment, controls must be in place to minimise the risk that users with privileged / administrative access to that production environment exfiltrate that data into other environments such as the supplier's wider corporate IT environment, non-Production environments.
Data Leakage (Internet Content Filtering Tools)	Access to sites (for personal use) where LBG Confidential and Highly Confidential information can be shared must be blocked including, but not limited to: • Webmail, e.g. Gmail • file sharing sites such as Dropbox, Google Drive • social media (Facebook, LinkedIn, etc are allowed but the ability to upload files / copy and paste information into message must be blocked); and • instant messaging.

	Where corporate versions of Gmail, Yahoo, etc are used, access must be restricted to corporate machines only.
Data Leakage (Email Content Filtering Tools)	Controls must be in place to protect LBG Confidential information: • Emails that clearly breach LBG confidentiality requirements must be blocked, e.g. sending of card data, account information and personal data • LBG information must not be sent to webmail accounts • all emails containing LBG Confidential information must be encrypted e.g. TLS; and • exceptions must be approved by LBG.
DLP – Highly Confidential Enhanced Controls	Controls must be in place to protect LBG Highly Confidential information: • LBG data must only be received by people authorised to work on our business and • desktop encrypted email must be used when sending any emails or attachments containing highly confidential data, and it must be encrypted end to end (E2E) between the sender and the recipient. Highly Confidential information must not be shared via the internet or stored on a Cloud service without prior approval from LBG.
Data Leakage (USB and Optical Media Ports)	USB, optical media ports and other potential mechanisms for portable media must be disabled by default. If a legitimate business case requires saving to a USB stick, that must be authorised by LBG: • Any exceptions must be treated as an incident • authorisation must be provided • a company issued media only must be used • media must be encrypted • all files transferred to media must be logged • assets must be tracked, i.e. who given to, purpose, when returned • all data deleted from the USB when no longer required; and • at least quarterly reviews to check if access is still required.
Business Area Decommissioning and Disposal Monitoring	There must be a documented policy / process for secure destruction of equipment exists and includes: • Frequency of destruction • protection of assets until destruction • method to validate the established procedures are carried out; and • identifying and rectifying exceptions or material deviations.
Asset Management - Destruction	Where media is securely disposed of: • Certificates of destruction must be obtained, e.g. bags taken by Confidential waste, certificates for hardware disposal; and • hardware disposed of must align with IT Asset Register.
Technology Provider Approval of Disposal Procedures	Data must be erased securely / wiped before any equipment is recycled/reused using industry approved methods.
Monitoring of Media and Equipment Transportation	There must be a documented procedure including: • Methods of transport e.g. tapes, drives, direct link with Data Centre • method of encryption, i.e. algorithm and key size, e.g. AES 256 • requirement for chain of custody for external / physical media • obtain approval from LBG where its data is to be removed or transferred and • raising an incident for any breaches / exceptions including notification to relevant supplier(s), e.g. loss of hardware.
DLP - Hardware in Transit	Data must be encrypted whilst in transit and in line with Data Classification: • Hardware moves • public internet / private networks and • to / from IT Disaster Recovery / backup sites.

DLP - Hardware in Transit	Hardware transfers must be recorded / logged including: • Type of hardware, e.g. server, tape, hard drive • data in transit, e.g. supplier, application(s), data fields • chain of custody; and • asset numbers.
Data Leakage (Mobile Bring Your Own Device (BYOD))	There must be a documented BYOD policy / procedure: • Use of BYOD for LBG information must be authorised by LBG • information cannot be copied from the protected environment to the personal device • devices must be authenticated before allowing access to the internal network • anti-malware is enforced • encryption of data is enforced; and • what applications / information is allowed to be data sent, received, stored, or processed.
DLP - Incident Management	Incidents must be recorded / logged and investigated following the incident management process where required.
Data Transfer Records	Regular data transfers (including to Cloud based systems) must be recorded: • What data is being transferred • from / to where it is being transferred • how it will be transferred; • reasons for the transfer • any controls required, LBG encryption; and • approvals required and received including LBG's.
Data Transfer Agreements	Agreements must be in place to ensure third parties of the supplier adhere to the supplier's information security and privacy policies. Data transfers not adhering to LBG's classification rules or the supplier's data transfer procedures must be raised as an incident.
Protection of Cryptographic Keys Monitoring	There must be a documented policy / procedure on cryptography / encryption including: • Key lifecycle (generation, storage, transfer, usage, revocation, expiration, renewal, archival) • ownership with appropriate key custodian declaration • how unique keys are generated, e.g. in software or in a hardware security modules (HSM) and implemented, i.e. per client / system / application • HSMs must be certified for verified random number • generators to create random keys in line with FIPS140 or FIPS186 • storage of cryptographic keys separately from virtual images and information assets (e.g. in an HSM certified to FIPS140-2) • segregation of HSMs and other cryptographic material • backups • the storage process for keys that are held in clear (e.g. written on paper or component held in smart cards) • inventory list includes key owners, key/certificate list, algorithms, key length • schedule for key renewal / rotation • incident plan for all keys; and • which industry standards are applicable.
Network Diagrams	Network diagrams must be documented: • Accurate and up-to-date diagrams, e.g. after any change • reviewed at least annually • include all systems • supported by documented control requirements and procedures; and • key systems are on appropriate network segments.
Network Connections -	To prevent data security breaches, external connections to the network must:

External Connections	• Be approved, documented (including purpose, approvals, and business justification) • be subject to periodic (at least 6 monthly) review, which should include checking for any unapproved external connections • be routed through a firewall • be designed and configured to ensure end to end protection of sensitive data in transit • restrict permitted traffic to only required ports, protocols, source, and destination addresses • apply the 'default deny' principle (i.e. any traffic that is not explicitly allowed must be blocked); and • not create a bridge between networks of different trust (i.e. production & corporate, public & private, etc.).
Network Connections - Rulesets	Rulesets and configurations for firewalls and other security enforcing network devices must be: • Verified and approved, i.e. documented change request; and • reviewed and updated regularly (at least 6 months).
Wireless Connectivity	Any wireless access to networks within the scope of the assessment must be secure by design and in operation, including: • Having a documented design/policy/configuration • enforcing appropriate authorisation; and • not permitting known weak / insecure authentication or encryption protocols.
Wireless Separation	Wireless networking that is not intended to permit access to in scope networks must have robust separation (physical or virtual) from the in-scope networks.
Network Security Events and Alerts	Security-related network events from all relevant sources (including Firewalls, IPS/IDS, WAFs, Remote Access Gateways, MDMs, etc.) must be captured and subject to logging, monitoring, and alerting.
System Configuration - Builds	All infrastructure (including network devices, servers, and end user devices) must be built, hardened, and maintained according to a documented standard which is informed by vendor/industry good practice, to include: • Disabling all insecure and unnecessary applications, services, and protocols • changing default passwords • removal of admin rights • installing most recent patches and updates upon first build; and • installing required security software i.e. anti-virus.
System Configuration - Monitoring	All infrastructure endpoints (including servers and end user devices) must be monitored to ensure ongoing compliance to build and hardening standards, to include: • Up to date installs/patches • use or adoption of unsanctioned cloud services or shadow IT • exceptions must be investigated and remediated; and • circumvention of policies as enforced by current standards.
Intrusion Detection / Prevention - Tools	Intrusion detection or prevention tools must be in place at all appropriate locations on its network. This is to analyse all inbound network traffic to identify and stop (or alert on) any possible incidents, imminent threats or violations, including any arising from unauthorised network connections.
Connection Authentication	The internal network must be protected against the connection of rogue/unauthorised devices.
Distributed Denial of Service (DDoS) - Contract	For the systems or environments used in the provision of any of the services to LBG, and which are internet accessible or provide communications critical in the service provided to LBG (including email) to/from/across the internet, there must be a DDoS service contract / specification including any supporting documentation.
Distributed Denial of Service (DDoS) - Solution	For the systems or environments used in the provision of any of the services to LBG and which are internet accessible or rely in any way on communications (including email) to/from/across the internet, the DDoS solution must provide:

	• An adequately scaled DDOS solution (e.g. sizing for peak malicious traffic) allowing them to survive initial surge of attack traffic, prior to mitigation being put in place • dynamic scrubbing capabilities to filter out malicious traffic • built in protection mechanisms (e.g. ACL restrictions on specific traffic types) • active monitoring for DDoS attacks (e.g. traffic patterns / behaviour analysis); and • the ability to capture samples of malicious traffic for forensic analysis internally and sharing with LBG Cyber experts.
Distributed Denial of Service (DDoS) - Incidents	DDoS alerts are security events and must be managed accordingly, i.e. monitored, analysed, raised as an incident and subject to an appropriate response (including DDoS mitigation service invocation where necessary).
Vulnerabilities - Automated Scanning	There must be a documented process/procedure for proactively identifying and managing vulnerabilities in the supplier's systems and environments. This must include: • Technical controls to detect (or prevent) the unauthorised installation of software • regular (at least quarterly) vulnerability scans must be performed on internal and external facing infrastructure and systems • vulnerability scans must include scanning of any virtualisation technologies being used, e.g. virtualization aware • management of vulnerabilities e.g. assessment using risk management process and remediation using IT change management process; and • awareness is maintained of external security threat alerts, and relevant intelligence is acted on.
Service and Application Security Testing Monitoring	There must be a documented penetration test policy/process requiring that: • All in scope environments and systems are tested at least annually (including following any major change) by a competent and independent security testing function • findings from pen testing are recorded and treated as risks, and prioritised and tracked through to remediation in line with Risk Management processes; and • where not being remediated, any findings affecting the service provided LBG must follow the Risk Management process including notification to LBG where these are material.
Vulnerabilities - Scope	Penetration Tests must be designed and scoped by competent persons who have been provided with sufficient information about the system(s)/environment(s) to ensure that applicable types of vulnerability are tested for, and that any technical limitations to the testing are understood.
Vulnerabilities - Recording and Management	Vulnerabilities identified from any source must be recorded and managed including: • Description of the vulnerability • system(s) and/or environment(s) are affected • the inherent risk • the assessed risk (likelihood & Impact) to the business; and • remediation plan, status, and deadline (with priority aligned to risk). Where not being remediated, any findings which may directly or indirectly affect the service provided to LBG must follow the Risk Management process, including notification to LBG where these are material.
Vulnerability and Patch Management Monitoring	Patches must be implemented across the network in accordance with documented procedures, which must include: • Rating and prioritising patches according to their severity and business risk • deployment timeframes for different priorities of patch exception process, e.g. for legacy systems management of exceptions, i.e. tracked / monitored / approved / escalated; and • alignment with Change Policy.
Patch Management	Patching compliance must be monitored, reported, and reviewed including: • How many (%) machines and types of machines not patched

	• reason for exceptions; and • management of exceptions.
Change Management	An established Change Management process is in place which ensures: • Each change has been subject to approval by an appropriate authority • the approval authority is the correct authoriser based on the established procedures • any potential for the approval authority to have a conflict of interest has been addressed; and • Emergency changes are documented and are subject to fast-track approval from an appropriate authority and have a post implementation review carried out.
Malware Monitoring	There must be documented procedures in place covering Malware protection, to include: • Anti-malware tools must be kept up to date (i.e. signature updates to be deployed within 24 hrs. of release) • anti-malware is installed on all systems / devices • failed updates to be identified and remediated; and • virus containment plans/procedures must be in place to prevent the spread of viral outbreaks.
Anti-Malware	Technical solution(s) must be implemented, maintained, and monitored as per malware policy / procedures, and all malware detection events must be investigated as potential incidents.
Software Development Life Cycle (SDLC) - Policy	There must be a documented systems development methodology including: • Support secure by design and good security practices, e.g. Open Web Application Security (OWASP) • development, secure by design / in line with the approved Systems Development Methodology • testing, code and application / penetration testing; and • implementation processes and release management - content version controls and strict processes for the migration of source code from one environment to another.
Software Development Life Cycle (SDLC) - Implementation	Secure SDLC measures must be in place as per policy to: • Prevent manual or systematic processing errors or corruption of data through input and output integrity routines (i.e., reconciliation and edit checks such as MD5/SHA checksums) implemented for application interfaces and databases; and • binaries must be compiled on the supplier premise and only the source code artefacts sent to the hosting, e.g. cloud, provider.
Software Development Life Cycle (SDLC) - Training	Developers must be trained on 'secure by design' approaches, including: • OWASP; and • Secure software development lifecycle.
Segregation of Production and Non-Production Environments	There must be documented policies / procedures to protect production and non-production environments from unauthorised changes and access including: • Current system environment(s) must be documented • development/test environment must be segregated from the production environment • developers/sys admins must have separate accounts with different userIDs, e.g. UserID; test_UserID; dev_UserID; • permissions / access to non-production environments must enforce user access controls commensurate with the environment, such as least privilege and support of Segregation of Duties • change to code in production must be prohibited (except break-glass) • break glass procedures (in line with Change Management) for developers to access the production environment (i.e. overriding the segregation of duties requirement); and • live data must not be used within the test environment. If any live data is to be used in any tests, prior approval from LBG data owner must be obtained and the

	supplier must provide evidence that the controls within its test environment are commensurate with those in the production environment.
Quality Assurance - Standards	There must be a Systems Development Quality Assurance Methodology: • Support of data security standards to include confidentiality, integrity, and availability • checks / code analysis must be carried out by an appropriate person at an appropriate level • potential conflicts of interest must be considered; and • considers external guidance, e.g. OWASP 10 attributes and NIST.
Quality Assurance - Review	Source code: • Must be checked prior to implementation / published • cannot be tampered with by the author or anyone else after it has been reviewed • bugs and security vulnerabilities must undergo triage and remedy; and • debugging and test code elements are removed from released software versions.
PCI DSS Compliance	For Suppliers who have access to Payment Card data, the Supplier Information Security Manager ensures that the company is always appropriately compliant with PCI-DSS .
Cloud Computing Policy and Approval	The supplier's Cloud Computing policy must be documented and: • Be reviewed at least annually or following any changes to the service • identify the roles and responsibilities of individuals / teams in respect of developing, reviewing, maintaining, and applying Cloud Computing policy; and • be agreed / signed-off by management to acknowledge they understand the risk and will treat risk exposures in line with contractual, legal, and regulatory requirements.
Cloud Computing Policy and Approval	The documented roles and responsibilities of individuals / teams in respect of developing, reviewing, maintaining, and applying Cloud Computing policy must be established in practice.
Cloud Computing Policy Content	The Cloud Computing policy must contain as a minimum (but not limited to): • All business use of cloud computing services, and the data to be stored or processed using those services, must be formally approved by the organisation's principle security officer (e.g. CSO / CIO) or with their delegated authority • the requirement for a clear understanding to be established of the Roles and Responsibilities of who operates controls in the cloud (1st party, vendor, 4th party etc) • for any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the CSO / CIO or with their delegated authority • the use of such services must comply with the Supplier's Acceptable Use Policy/Computer Usage Policy/Internet Usage Policy/BYOD Policy • the use of such services must comply with all laws and regulations governing the handling of personally identifiable information, financial data or any other data owned or collected by the Supplier and / or LBG • personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data; and • that any use of Cloud is subject to all appropriate security controls having been confirmed to be in place.
Cloud Computing Service and Deployment Framework	The organisation must have an established Cloud Computing (including Cloud Security) service and deployment approach (framework) which addresses the following as a minimum: • How any use of cloud is identified and managed • the ownership, update, and approval of cloud requirements/policies • identification of the Service Models being used (SaaS, PaaS, IaaS) • identification of the Deployment Models being used (e.g. Private, Public, Community, Hybrid) • ensuring compliance with legal and regulatory requirements

	• ensuring required security controls and responsibilities are established and maintained, and subject to periodic review and testing • data residency of cloud security services; and • the management and control of any subcontractors hosting, storing, and processing clients' data as part of cloud deployment services.
Cloud Computing Service and Deployment Framework	The organisation must manage its use of cloud service in accordance with its established Cloud Computing (including Cloud Security) service and deployment approach (framework).
Cloud User Training and Awareness	For providers of cloud services where LBG is a tenant, there must be a formal, role-based, security awareness training program for cloud-related access and data management issues for all persons with access to tenant data.
Physical Security - Policy	There must be a formally documented physical security policy: • Nominated individual or role to be accountable for physical security • measures in place to prevent and detect the unauthorised removal of systems and devices that store or process LBG's data • access control to enter buildings, specifically for buildings where services are provided to LBG or LBG data is stored; and • aligned to Joiners / Movers / Leavers process.
Physical Security - Training	Training must be given to all employees to provide awareness and responsibilities, with exceptions reported to LBG.
Physical Security - Review	An annual review must be performed on all premises where LBG information is stored, or activity conducted.
Physical Security - Access	Physical access must be reviewed at least annually, quarterly for sensitive / restricted areas.
Physical Security - Controls (Access Control)	Physical security controls must be in place: • Physical barriers to protect against unauthorised access are in place • access control mechanisms for entering the building (i.e. electronic access, security guards, etc.) • sensitive rooms (e.g. server rooms) and specific to those that are used to store and process LBG data, must have additional access control which is proactively monitored • access to cabinets storing LBG data must be secured, e.g. key controls; and • physical protection of access control recording system is in place.
Physical Security - Controls (Access Logs)	Access logs must be retained for 12 months.
Physical Security - Controls (Visitors)	A visitor process must be in place: • Visitors are booked in and out of the facility and allocated a visitor pass; and • visitors are supervised and escorted at all times.
Physical Security - Controls (CCTV)	CCTV coverage and monitoring must be in place: • Premises' entry / exit points and secure areas must be monitored • images must be retained for at least 30 days, or 90 days where customer data is stored (including card data); and • location of the CCTV recording equipment must be physically protected.
Physical Security - Controls (Intrusion Detection)	An intrusion detection system must be in place: • Must be active on all doors and windows in the facility housing LBG data or where services are provided; and • monitored 24/7, 365 days a year.
Physical Security - Controls (Electronic Security)	There must be electronic perimeter access controls: • At every access/egress point to the facility • 24/7; and • exit doors are secured.

Physical Security - Controls (Maintenance)	All electronic security systems must be installed and maintained by an approved, certified authority.
Physical Security - Incidents	Breaches of security defences must be reported and investigated and where appropriate, following the incident management procedures.