BARCLAYS

External Supplier Control Obligation

Information and Cyber Security (ICS)

Version 11.0 Dated October 2021

Control Area / Title	Control Description	Why this is important
1. Information /Cyber Security Governance, Framework	The Supplier must have an established and consistent industry standard framework for Information and Cyber Security governance in accordance with Best Industry Practice (current industry best programs include NIST, ISO/IEC 27001, ITIL, COBIT) as well as any applicable industry requirements. This will enable the Supplier to ensure there are safeguards or countermeasures of their process, technology and physical environment. A well-structured, enterprise-wide information governance program must ensure that the core concepts of availability, integrity and confidentiality are supported by adequate controls designed to mitigate or reduce the risks of loss, disruption or corruption of information and the Supplier must ensure that Barclays requirement controls are in place and operating effectively to protect Barclays service(s). The Security Governance framework must be developed, documented, approved, and implemented which includes administrative, organizational, technical, and physical safeguards to protect assets and data from unauthorized loss, misuse, access, disclosure, alteration, and destruction. The security program should include, but not be limited to, the following areas: • Policy, procedures, standard program that effectively creates, implements, and continuously measures the effectiveness of the Information and Cyber Security policy and standards implementation. • A comprehensive security program with clear leadership structure, escalation mechanisms, and executive oversight to create a culture of accountability and awareness for security. • Policies, procedures, and processes which are approved and communicated across the organization. • Ensure that Information and Cyber Security policies and procedures/standards are routinely reviewed (at least annually or any material changes) and adapted in line with current Cyber Security practices and the evolving threat landscape. • The Supplier should ensure that there is individual accountability for information and security systems by ensuring that there is appropriate ownership of critical business environments, information and security systems and that this is assigned to capable individuals.	If this principle is not implemented, Barclays or its Suppliers may not have and be able to demonstrate appropriate oversight of Information/Cyber Security. A strong security governance framework sets the security tone for the whole organisation.

	• The Supplier coordinates and aligns roles and responsibilities for personnel. implementing, managing, and overseeing the effectiveness of the security strategy and framework with internal and external partners. • The Supplier should implement a secure infrastructure and control framework to protect the organisation from any threats (including Cyber Security) • Independent expert reviews and assessments should be performed at least annually to ensure that the organisation addresses nonconformities of established policies, standards, procedures, and compliance obligations. **The Supplier must ensure that Barclays is notified (in writing) as soon as they are legally able to do so if the Supplier is subject to a merger, acquisition or any other change of ownership.**	
2. Security Risk Management	The Supplier must establish a security risk management program that effectively evaluates, mitigates, and monitors evolving security risks across the Supplier controlled environment. The risk management program should include, but not be limited to, the following areas: • The Supplier should have a Security risk management framework that is approved by the appropriate governing authority (e.g., the Board or one of its committees). This should be incorporated into the overall business strategy and risk management framework. • Aligned to the risk framework, formal risk assessments should be performed at least annually or at planned intervals, or be triggered on an event driven basis e.g. in response to an incident or associated lessons learnt (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance). • Select an appropriate security risk treatment options, taking account of the risk assessment results. • Formulate a security risk treatment plan; and the risk acceptance criteria through appropriately qualified and accountable individuals. Such criteria should include, but not be limited to, the sensitivity of such data and its business criticality.	If this control is not implemented, Suppliers may not able to demonstrate appropriate measures implemented to manage security risks.

	• The Supplier should ensure identified risks are minimized or eliminated in the environment through the prioritisation of risk and implementation of protective measures. • Risks should be mitigated to an acceptable level. Acceptance levels based on risk criteria should be established and documented in accordance with reasonable resolution time frames and stakeholder approval. • Risk assessments associated with data governance requirements should consider the following: o Data classification and protection from unauthorized use, disclosure, access, loss, destruction, alteration, and falsification. o Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure. o Compliance with defined retention periods and end-of-life disposal requirements. • Supplier should perform as a minimum an annual security risk assessment in relation to security and based on the specific environments, consider a more frequent cadence. **Supplier must make a record of and notify Barclays if they are unable to remediate or reduce any material areas of risk that could impact Barclays Data and/or the service being provided to Barclays.**	
3. Roles and Responsibilities	Supplier is responsible for making sure that all individuals who are involved in providing service to Barclays are aware of, and adhere to, the Barclays control requirements of this document. For Barclays control requirements, Supplier should ensure that a suitable specialist team and/or individuals with appropriate skills, with defined roles and responsibilities to manage Barclays control requirements are in place and operating effectively to protect Barclays service(s). The Supplier must define and communicate roles and responsibilities for all security domains covered by the control requirement. These must be reviewed regularly (and in any event not less than once every 12 months) and after any material change to the Supplier operating model or business. Key roles must include a senior executive, accountable for Information & Cyber Security. It is Supplier's responsibility to ensure that their employees/staff are familiar and comply with the control requirements of this standard and associated policies and	Clear definition of roles and responsibilities supports the implementation of the Information and Cyber Security SCO

	standards. The Supplier must appoint a point of contact for any escalation who will liaise with Barclays.	
4. Approved Usage	The Supplier should produce and publish acceptable use requirements informing all supplier personnel (including contractors and third-party users of the organisation's systems) of their responsibilities. The following topics must be considered: • Use of the Internet; • Use of Software as a Service (SaaS) based; • Use of Public Code repositories; • Use of browser based plugins and freeware / shareware; • Use of Social Media; • Use of corporate email; • Use of instant messaging; • Use of IT equipment provided by the Supplier; • Use of IT equipment not provided by the Supplier (e.g. Bring Your Own Device); • Use of portable/removable storage devices; • Responsibilities when handling, saving, and storing Barclays Information Assets; • Output of data leakage channels; and • Risk and consequences of misuse of the above items and/or any illegal, harmful, or offensive outcomes resulting from such misuse. The Supplier must take appropriate steps to ensure compliance to the acceptable use requirements.	An acceptable use requirement helps to underpin the control environment protecting Information Assets.
5. Education and awareness	The Supplier must have a security education and awareness training program established for all employees, contractors, and third-party users of the organization's systems and mandated when appropriate. All individuals with access to Barclays data/ information must receive appropriate education and awareness training and regular updates in technical and organisational procedures, processes, and policies relating to their professional function relative to the organisation. The levels of education, training, and awareness must be commensurate to the roles being undertaken and recorded in a suitable learning management platform.	Education and awareness supports all other controls within this schedule. If this principle is not implemented, relevant employees will be unaware of cyber risks and attack vectors and would be unable to detect or prevent attacks.

	The Supplier must ensure that all personnel under their control undertake mandatory security information training (continually updated to compensate for evolving threats and industry-specific risks), which includes Best Industry Practice and protection of Barclays data within one month of joining the organisation and refreshed at least on an annual basis. The below should be included where appropriate: High-risk groups, such as those with Privileged Access or in sensitive business functions (including privileged users, senior executives, Information and Cyber Security personnel and third-party stakeholders), should receive enhanced Information and Cyber Security situational awareness training according to their roles and responsibilities. If and where appropriate, this training should be provided by external third-party experts.	
6. Security Incident Management	The Supplier must establish a Security Incident management framework that effectively validates, efficiently escalates, contains, and remediates a Security Incident from the Supplier environment. The Supplier must ensure that there are tailored written incident response plans for each category of known security risk/incident that define the roles of personnel, escalation mechanisms, and phases of incident handling/management: • Incident validation - Establish an incident validation process that leverages various sources of data and is integrated across the enterprise to effectively validate a Security Incident (this relies on the Supplier having effective and appropriate monitoring and detection mechanisms in place across is IT environment). • Incident classification - Establish an incident classification process that effectively and quickly classifies a validated incident across all event types. • Incident escalation – Establish appropriate mechanisms to escalate the incident (dependent on the classification) to appropriate stakeholders, accountable individuals, and where appropriate external specialists, enabling rapid incident response activities. • Incident containment - Utilise people, process, and technology capabilities to quickly and effectively identify the attack vector and accordingly, contain the Security Incident in the environment. • Remediation - Leverage people, process, and technology capabilities to quickly and effectively remediate any security threat and/or its components from the	An incident management and response process helps to ensure that incidents are quickly contained and prevented from escalating.

environment. Effective remediation will ensure against attacks of a similar nature in the future.

The Supplier should seek to establish that incident response activities are improved where possible by incorporating lessons learned from current and previous detection/response activities.

The Supplier should ensure that incident response teams and processes are tested, at least annually, to ensure the Supplier is able to respond to Cyber Security Incidents.

- Simulations and testing must demonstrate that Barclays will be notified of a Security Incident of impact to it; this would be evidenced by Supplier demonstrating the ability to contact appropriate persons in the event of such an incident.
- Communication – The Supplier must appoint a point of contact for any Security Incidents who will liaise with Barclays in the event of an incident. The Supplier should notify Barclays of the individual(s) Contact details and any changes to them, including any out of hours' contacts and telephone numbers.

Details should include: Name, responsibilities within the organisation, role, email address and telephone number

The Supplier will (and shall, if applicable, procure that any of its subcontractors shall) inform Barclays within a reasonable timeframe upon becoming aware of any incident that impacts or is suspected might impact the service to Barclays or Barclays Information/ Data, and in any event, no later than **two (2) hours** from the time the Supplier becomes aware of the Security Incident.

In the event of either a suspected or known data breach (including a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data), the Supplier shall inform Barclays of such incidents within a reasonable timeframe upon becoming aware of any such incidents, and in any event, no later than **two (2) hours** from the time Supplier becomes aware of such an incident.

In addition to the initial notification as detailed above, the Supplier will provide a report to Barclays within **twenty-four (24) hours** of becoming aware of any incident that impacts the service to Barclays or Barclays Information/ Data. The report should include the following details:

	• Date and time Supplier became aware of the Security Incident • Suspected impacted jurisdictions • Type and brief summary of Security Incident • Impact and likely consequences to services to Barclays and/or Barclays Information/Data (and, if applicable, affected data subjects) • Status of Security Incident (for example, have forensic experts been onboarded, relevant authorities notified, attack vector known, enhanced monitoring in place, containment effected) • Action taken or planned to remediate against the Security Incident • Details of any data compromised These incidents, as well as all ongoing updates relating to remediation efforts and notices to data subjects, should be reported to the Barclays Supplier Manager, and the Barclays Joint Operations Centre within **Barclays Chief Security Office (CSO) Joint Operations Centre (JOC) - gcsojoc@barclays.com**. **Please make the subject of the email "[Insert Supplier name] – Security Incident – Urgent Attention Required." If the incident is very urgent and needs to be flagged immediately, the JOC can be reached at its 24/7 hotline:** • UK: +44 330 041 5586 • US: +1 201 499 1900 • India: +91 788 781 9890	
7. Information Classification and Protection	The Supplier must have an established and appropriate information classification, handling, and storage framework/scheme (aligned to Best Industry Practice and/or Barclays requirements) which covers, but is not limited to, the following components: • Continually reviewing existing and new Barclays Information/Data • Assigning Barclays Information/Data the correct Information Label Schema. • Handling and storing Barclays Information/Data securely and appropriately, in line with its assigned level of classification. • Ensuring that all staff are aware of the Supplier/Barclays labelling, storage, and handling requirements and how to apply correct information classification. The Supplier must refer to the Barclays Information Labelling Schema and handling requirements (Appendix B, Table B1 and B2), or an alternative scheme to ensure that Supplier protects and secures the Barclays Information held and/or processed. This requirement applies to all Information Assets held or processed on behalf of Barclays.	If these requirements are not implemented, it may result in Barclays Data being vulnerable to unauthorised modification, disclosure, access, damage, loss or destruction, which may result in regulatory and reputational damage.

8. IT Asset Management (Hardware & Software)	The Supplier must ensure an effective asset management program is established throughout the asset lifecycle. Asset management should govern the lifecycle of assets from acquisition to retirement, providing visibility and security to all asset classes in the environment. The Supplier must maintain a complete and accurate inventory of business-critical assets located at all sites and/or geographical locations which provide service(s) to Barclays including any Barclays equipment hosted in Supplier premises and/or subcontractor provided by Barclays, ensure that there is at least one test annually to validate that the asset inventory is current, complete and accurate. At a minimum, the Asset Management process should cover the following areas: • All Information Assets and infrastructure is continually mapped/updated. • Information Assets and infrastructure are then protected based on their classification, criticality, and business value. • Supplier must have controls in place that assure the recording and ongoing maintenance of hardware asset data throughout the Asset's lifecycle. • Supplier must maintain up-to-date asset inventory • **Suppliers with a Tier1, Tier 2 and Tier 3 setup must maintain current, complete, and accurate asset inventories (including, all endpoints, network equipment, RSA tokens and/or any Barclays provided assets).** • **Supplier must perform reconciliation of all the Barclays assets (Hardware & Software) on annual basis and provide attestation to Barclays (Chief Security Office - ECAM team).** • Ensure that unauthorised assets are either removed from the network or quarantined and that the inventory is updated in a timely manner. • Maintain an up-to-date list of all authorized software that is required for Barclays service delivery. • Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organisation's authorised software inventory. Unsupported software should be tagged as unsupported in the inventory system. Software nearing end-of-life should also be tagged as such in the inventory system. The Supplier should ensure effective and efficient procedures are implemented in a timely manner for the mitigation of non-supported technologies and the end-of-life,	A complete and accurate inventory of Information assets is essential for ensuring appropriate controls. If this principle is not implemented, Barclays assets or assets used by Suppliers to service Barclays could be compromised, which may result in financial losses, loss of data, reputational damage and regulatory censure.

	retirement, and destruction of assets and data to eliminate the risk of data compromise.	
9. Disposal/ Destruction of Physical Assets and Data Remanence of Electronic Information	Destruction or erasure of Barclays Information Assets, stored in either physical or electronic form, must be performed in a secure manner appropriate to its associated risk, ensuring that Barclays Data is not recoverable. Supplier should have effective policies and procedures in place to continually assess and determine when the destruction or deletion of Barclays Information Assets stored in either physical or electronic form is appropriate and required, pursuant to contract or for information security, legal or regulatory purposes. Via written request, Barclays may also seek destruction of Barclays Information Assets. The Supplier should establish procedures with supporting business processes and technical measures that are implemented for the secure disposal and secure removal/erasure of Barclays Data (including backup copies) from all storage media, ensuring data is not recoverable by any computer forensic means. Barclays Data stored in media must be wiped to a sufficient level so that data is not recoverable, preferably using appropriate data erase techniques like secure wipe, purging, data clearing, or data destruction or software-based method to overwrite the data or use the industry standard framework on data disposal (NIST). All equipment must be disposed of at the end of its operational life (faulty, decommissioned due to service, retired or no longer required, used in a trial or proof of concept, etc.). Data erasure services can be utilised for equipment that is to be reused. Disposal requirements apply to Supplier 4th party/subcontracted agencies used to provide the service to Barclays. Disposal of hardcopy information must be shredded to a minimum of P4 DIN66399 standard using a cross cut shredder (this includes payment card information) or may be incinerated in compliance with BS EN15713:2009. For Barclays, evidence of data disposal must be kept, providing audit trail, evidence and tracking, and should include: • Proof of destruction and/or disposal (including date undertaken and method used). • System audit logs for deletion. • Data disposal certificates.	Secure destruction of Information Assets helps to ensure that Barclays Information assets cannot be recovered for any data breach or loss or malicious activity.

	• Who undertook the disposal (including any disposal partners, third parties, or contractors). • A destruction and verification report must be generated to confirm the success or failure of any destruction / deletion process (i.e. an overwriting process must provide a report that details any sectors that couldn't be erased). During exit, Supplier must ensure Barclays Data is securely destroyed upon notification and authorisation from Barclays.	
10. Boundary and Network Security	The Supplier must ensure that all IT Systems operated by the Supplier or its sub-contractor that support Barclays services(s) are protected from **inbound and outbound network threats** within the Suppliers' (and any relevant sub-contractors') network. The Supplier must monitor, detect, prevent, and if necessary remediate the flow of information transferring across networks of different trust levels with a focus on security breaches. Network integrity mechanisms should include but not be limited to the following areas: • Maintain an up-to-date inventory of all of the organisation's network boundaries (through a Network Architecture/Diagram). • The design and implementation of the network, as well as potential vulnerabilities and need to retire and renew infrastructure of the network, must be reviewed at least annually or if there is an event driven requirement which causes changes. • External connections to the Supplier network are documented, routed through a firewall, verified and approved prior to the connections being established to prevent security breaches. • The Suppliers networks are protected through applying defense-in-depth principles (e.g. network segmentation, firewalls, physical access controls to network equipment, etc.). • The Supplier should have network intrusion prevention technologies to detect and prevent malicious traffic from entering the network. • Use of strong network firewall capabilities to provide a layer of perimeter defense against malicious network attacks. • Internet network traffic should pass through a proxy that is configured to filter unauthorised connections. • Ensure that logging and monitoring must be enabled.	If this principle is not implemented, external or internal networks could be subverted by attackers in order to gain access to the service or data within it.

	• Network devices are securely hardened to prevent a malicious attack. • Logical separation of device management ports/interfaces from user traffic; appropriate authentication controls. • All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule. • Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organisation's network boundaries. • Perform regular scans from outside each trusted network boundary to detect any unauthorised connections which are accessible across the boundary. • Secure communications between devices and management stations/ console. • Configure monitoring systems to record network packets passing through the boundary at each of the organisation's network boundaries. • Network connection between interoffice/ cloud service provider/ data centres must be encrypted over secure protocol. Barclays Information Assets / Data in transit within Supplier Wide Area Network (WAN) must be encrypted. • Supplier must review the firewall (External and Internal Firewall) rules on an annual basis. • All wireless access to the network is subject to authorisation, authentication, segmentation and encryption protocols to prevent security breaches. • The Supplier must ensure that access to the internal network must be monitored and only authorised devices must be allowed through appropriate network access controls. • Remote login access to the Supplier network must use multi-factor authentication. • Supplier must have segregated network for Barclays service(s). The Supplier must ensure that any servers used to provide the service to Barclays are not deployed on untrusted networks (network's outside your security perimeter, that are beyond your administrative control e.g., internet-facing) without appropriate security controls. The Supplier hosting Barclays Information (including subcontractor) in a data centre or cloud must hold a Best Industry Practice certification for security management. T2 and T3 Network -	

	• T2 network must be logically segregated from Supplier corporate network by a Firewall, all inbound and outbound traffic to be restricted and monitored. • Routing configuration must ensure only connections to the Barclays network and must not route to any other Supplier networks. • Supplier Edge router connecting to Barclays extranet gateways must be securely configured with a concept of limiting controls of ports, protocols and services; o Ensure that logging and monitoring must be enabled. *N.B. The term "network" as used in this control refers to any non-Barclays network for which the Supplier is responsible for, including the Supplier's sub-contractor's network.*	
11. Denial of Service Detection	The Supplier must maintain a capability to detect and protect against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The Supplier must ensure that Internet connected or external channels supporting services supplied to Barclays must have adequate DoS protection to ensure availability. If the Supplier is hosting an application which is internet facing and holding any restricted data or underpinning a resilience category 0 or 1 service, this must be protected down to layer 7 using appropriate technologies which must be approved by Barclays.	If this principle is not implemented, Barclays and its Suppliers may be unable to prevent a denial of service attack from achieving its objective.
12. Remote Working (Remote Access)	Remote Access to the Barclays network via Barclays Citrix applications and/or Barclays data residing/ stored within Supplier managed environments/networks, if the Supplier or any of its subcontractors access Barclays Data or Barclays Personal Data or any sensitive information provided to the Supplier on a need to know basis, whether in physical or virtual form, to be accessed, shared or processed remotely, in particular where its staff may be working from home, the Supplier will seek prior approval from Barclays (Chief Security Office – ECAM Team) for these arrangements. The Supplier must ensure the following components are established, at a minimum, for Remote Access: • Remote login access to the Supplier network must be encrypted during data in transit and always use multi-factor authentication. • Access to the Barclays network must be via a Barclays Citrix application with RSA Token (Hard & Soft) provided by Barclays.	Remote Access controls help to ensure unauthorized and insecure devices are not connected to the Barclays environment remotely.

	• Supplier to maintain an inventory of all RSA tokens (Hard & Soft) provided by Barclays and a management process that will include review and monitoring of allocation, usage and return of the tokens (Hard token). • Supplier must maintain records of individuals who have been asked to work remotely and the rationale for such requirement • **Supplier to perform reconciliation of all the remote users on a quarterly basis and provide attestation to Barclays (Chief Security Office - ECAM team).** • Barclays will promptly deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed one month). • Supplier must ensure that end point used for connecting Barclays information systems remotely must be configured securely and in accordance with Best Industry Practice (e.g. patch level, status of anti-malware, Endpoint Detection & Response EDR solution, logging etc.). • Services which have remote printing access via a Barclays Citrix application must be approved and authorized by Barclays (Chief Security Office – ECAM Team). Supplier must maintain records and perform quarterly reconciliation. • **Personal devices/ BYOD must not be allowed to access Barclays' environment and/or Barclays Data residing/ stored within Supplier managed environment (which includes, but is not limited to, Supplier staff, consultants, contingency workers, contractors, and Managed Service Partners (MSPs)).** Where the endpoints' (Laptop/Desktop) access is granted to the Barclays network via Barclays Citrix applications over Internet, the Supplier shall install the End Point Analysis (EPA) tool provided by Barclays to validate the endpoint security and operating system compliance, only devices that pass the End Point Analysis checks will be granted Remote Access to Barclays' network via the Barclays Citrix application. If the Supplier is unable to install or use the EPA tool this must be raised with your Barclays Supplier Manager. NB: Barclays will deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) within **twenty-four (24) hours.**	
13. Security Log Management	The Supplier must ensure that there is an established audit and log management framework which confirms that key IT systems and processes including applications, networking equipment, databases, endpoints, security devices, infrastructure, and servers are producing the required logs, in accordance with Best Industry Practice and	If this control is not implemented, Supplier will not be able to detect and respond to inappropriate or

guidance. Such logs should be appropriately secured, held centrally, and retained by the Supplier for a minimum period of 12 months or basis on below categories with proper rational.

Category	Low impact systems/ Service	Medium impact systems/ Service	High impact systems/ Service
Retention of Logs	3 months	6 months	12 months

At a minimum, the security log management process should cover the following areas:

- Supplier should establish policies and procedures for log management.
- Supplier should create and maintain a log management infrastructure.
- Supplier should define the roles and responsibilities of individuals and teams who are expected to be involved in log management.
- Collect, manage, and analyses audit logs of events in order to help monitor, detect, understand, or recover from an attack.
- Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.
- Sample event logs might include:
  - IDS/IPS, Router, Firewall, Web Proxy, Remote Access Software (VPN), Authentication servers, Applications, database logs.
  - Successful logins, Failed login attempts (for example wrong user ID or password), creation, modification and deletion to/of user accounts
  - Configuration change logs.
- Barclays services related to business applications and technical infrastructure systems on which appropriate and Best Industry Practice logging must be enabled, including those that have been outsourced or are ‘in the cloud’.
- Analysis of security-related event logs (including normalisation, aggregation and correlation).
- Synchronisation of time stamps in event logs to a common, trusted source
- Protection of security-related event logs (e.g. via encryption, MFA, access control, and backup).
- Taking necessary actions to remediate any issues identified and respond to Cyber Security Incidents in a fast, effective manner.

malicious use of their service or data within reasonable timescales.

	• Deployment of Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis. • Deployment of tools as appropriate to perform real-time central aggregation and correlation of anomalous activities, network and system alerts, and relevant event and cyber threat intelligence from multiple sources, including both internal and external sources, to better detect and prevent multifaceted cyber-attacks. The key events logged must include those that have the potential to impact the confidentiality, integrity and availability of the Services to Barclays and that may assist in the identification or investigation of material incidents and/or breaches of access rights occurring in relation to the Supplier Systems.	
14. Malware Defenses	In alignment with Best Industry Practice, the Supplier must have policies and procedures established, and supporting business processes and technical measures implemented, to prevent the execution of malware on entire IT environment. The Supplier must ensure malware protection is applied to all applicable IT assets at all times to prevent service disruption or security breaches. Malware protection should have or include, but not be limited to, the following: • Centrally managed anti-malware software to continuously monitor and defend organisation's IT environment. • Ensure that the organisation's anti-malware software updates its scanning engine and signature database on a regular basis and in accordance with Best Industry Practice. • Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting. • The Supplier should implement appropriate controls to safeguard against mobile malware and attacks for mobile devices connecting to Barclays or Supplier networks and accessing Barclays data. • Processes should be in place for regular meetings / forums (such as on a monthly basis) to discuss potential vulnerabilities / updates required. Action to remediate should be taken in a prioritised and timely fashion. Records of reporting, forums, and remedial action taken should be retained. NB. Anti-malware to include detection for (but not limited to), unauthorised mobile code, viruses, spyware, key logger software, botnets, worms, Trojans, etc.	Anti-malware solutions are vital for the protection of Barclays Information assets against Malicious Code.

15. Secure Configuration Standards	The Supplier must have an established framework to ensure that all configurable systems/ networking equipment are securely configured in accordance with Best Industry Practice (e.g. NIST, SANS, CIS). Configuration standard process should cover, but not be limited to, the following areas: • Establishes policies, procedures / organisational measures, and tools to allow for implementation of Best Industry Practice security configuration standards for all authorized network devices and operating Systems, applications, and servers. • Performs regular (annually) enforcement checks to ensure that non-compliance with baseline security standards is promptly rectified. Appropriate checks and monitoring are in place to ensure the integrity of the builds / devices are maintained. • Systems and network devices are configured to function in accordance with security principles (e.g. concept of limiting controls of ports, protocols and services, no unauthorised software, removing and disabling unnecessary user accounts, changing default account passwords, removing unnecessary software, etc.). Ensure configuration management governs secure configuration standards across all asset classes, and detects, alerts and effectively responds to configuration changes or deviations.	Standard build controls help to protect Information Assets from unauthorized access. Compliance with standard builds and controls that ensure changes are authorized helps to ensure that Barclays Information Assets are protected.
16. Endpoint Security	The Supplier must ensure that endpoints used to access the Barclays network, or access/process Barclays Information Assets / Data, must be hardened to protect against any malicious attacks. Best Industry Practices must be in place and endpoint security build must include, but need not be limited to: • Disk Encryption. • Disable all un-needed software/services/ports. • Disable administration rights access for local user. • Supplier Personnel will not be allowed to change the basic settings like default Service Pack, System Partition, and default services etc. • USB port must be disabled to prohibit copying of Barclays data to external media • Updated with the latest anti-virus signatures and security patches.	If this control is not implemented, Barclays and Supplier network and endpoints may be vulnerable to cyber-attacks.

	• Data loss prevention limited to no cut-copy-paste and print-screen of Barclays data • By default, printer access must be disabled. • Supplier should restrict the ability to access social networking sites, webmail services and sites with the ability to store information on the internet like google drive, Dropbox, iCloud. • Sharing/ transferring of Barclays Information Assets / Data should be disabled using instant messaging tools/ software. • Capability and processes to detect unauthorised software identified as malicious and prevent installation of unauthorised software. NB. Removable media / portable devices should be disabled by default and only enabled for legitimate business reasons. The Supplier should maintain secure images or templates for all systems in the enterprise based on the organisation's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates. Where the endpoints (Laptops/Desktops) access is granted to Barclays' network via Barclays Citrix application over Internet, the Supplier shall install End Point Analysis (EPA) tool provided by Barclays to validate the endpoint security and operating system compliance, only devices that pass the End Point Analysis checks will be granted Remote Access to Barclays' network via Barclays Citrix application. If the Supplier is unable to install or use the EPA tool this must be raised with your Barclays Supplier Manager. Mobile devices used for Barclays Services - 1. Supplier must ensure they implement mobile device management (MDM) capabilities to securely control and manage mobile devices throughout the lifecycle that have access and/or contain classified Barclays information, reducing the risk of data compromise. 2. Supplier must ensure mobile device remote lock and wipe capabilities are implemented to protect information in the event of a lost, stolen or compromised device. 3. Encrypt Mobile Device Data (Barclays Data).	

17. Data Leakage Prevention	The Supplier must have an established framework to ensure that protection against inappropriate data leakage is in place ensuring protection includes the following data leakage channels (but not limited to): • Unauthorised transfer of information outside the internal network/ Supplier network o Email o Internet / Web Gateway (including online storage and webmail) o DNS • Loss or theft of Barclays Information Assets on portable electronic media (including electronic Information on laptops, mobile devices, and portable media). • Unauthorised transfer of Information to portable media. • Insecure Information exchange with third parties (4th parties or subcontractors). • Inappropriate printing or copying of Information.	Appropriate controls must be operated effectively in order to ensure that Barclays' 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). If these requirements are not implemented, it may result in Barclays Sensitive Information being vulnerable to unauthorized modification, disclosure, access, damage, loss or destruction, which may result in legal and regulatory sanction, reputational damage, or loss / disruption of business
18. Data Security	The Supplier must ensure that Barclays Information Assets / Data residing in Supplier custody/ network has proper security of data which is achieved through a combination of encryption, secure means for accessing the data, integrity protection, and data loss prevention techniques. It is important that proper care must be taken to limit the access to the Barclays Information Assets / Data, including Personal Data, and to make that access secure. Data security controls should cover, but not be limited to, the following areas: 1. Supplier is obliged at all times to comply with any and all applicable data protection laws. 2. Policies and procedures should be established, and supporting business processes / organisational measures, and technical measures implemented, so as to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties. 3. Maintain an inventory of all sensitive /confidential information (Barclays Information Assets / Data) stored, processed, or transmitted by the Supplier. 4. Establish a data classification standard to ensure sensitive information (Barclays Information Assets / Data) is classified and protected appropriately.	

	5. Ensure all Barclays data are classified and tagged based on the Information Classification and Protection standard. 6. Data at rest protection; a. At a minimum, encrypt data at rest to prevent exploitation of sensitive information through unauthorized access. 7. Database activity monitoring; a. Monitor and log database access and activity to quickly and effectively identify malicious activity. 8. Data in use protection; a. Ensure viewing and use of sensitive information is controlled via access management capabilities to protect against exploitation of sensitive information. b. Utilise data masking and obfuscation technologies to effectively protect sensitive data in use from inadvertent disclosure and/or malicious exploitation. 9. Data in transit protection; a. Leverage strong encryption capabilities to ensure data is protected while in transit. b. Encryption of data in transit is typically achieved using Transport or Payload (Message or Selective Field) encryption. Transport encryption mechanisms include but are not limited to: • Transport Layer Security (TLS) (following the Best Industry Practice of modern cryptography, including use / rejection of protocols and cyphers) • Secure Tunneling (IPsec) • Secure Shell (SSH) c. Transport security protocols must be configured to prevent negotiation of weaker algorithms and/or shorter key lengths, when both end points support the stronger option.	

	10. Data Backup – a. Provisions must be made to ensure Information is adequately backed up and recoverable (and can be recovered within a reasonable time) in compliance with requirements agreed with Barclays. b. Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services. c. Ensure that all Barclays data is automatically backed up on a regular basis.	
19. Application Software Security	The Supplier must develop applications using secure coding practices and in a secure environment. Where the Supplier develops applications for use by Barclays, or which are used to support the service to Barclays, Supplier must establish a secure development framework to prevent security breaches and to identify and remediate vulnerabilities in the code during the development process. Application software security should cover, but need not be limited to, the following areas:	Controls protecting application development helps to ensure that applications are secured at deployment.

	• Secure coding standards must be in place and adopted in line with Best Industry Practice to prevent security vulnerabilities and service interruptions which at the same time defends against possible well known vulnerabilities. • Establish secure coding practices appropriate to the programming language. • All development must be undertaken in a non-production environment. • Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments. • Segregation of duty for production and non-production environments. • Systems are developed in line with secure development Best Industry Practice (e.g. OWASP). • Code should be securely stored and subject to quality assurance. • Code should be adequately protected from unauthorised modification once testing has been signed off and delivered into production. • Only use up-to-date and trusted third-party components for the software developed by the Supplier. • Apply static and dynamic analysis tools to verify that secure coding practices are being adhered. • The Supplier must ensure that live data (including Personal Data) will not be used within non-production environments. • Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with Best Industry Practice (e.g., OWASP for web applications). The Supplier should protect web applications by deploying web application firewalls (WAF) that inspect all traffic flowing to the web application for current and common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	
20. Logical Access Management (LAM)	Access to Information must be restricted, and with due consideration of the need-to-know, the Least Privilege and the segregation of duties principles. The Information Asset Owner is accountable for deciding who needs what access.	Appropriate LAM controls helps to ensure that Information Assets are protected from inappropriate usage.

	• The need-to-know principle is that people should only have access to Information which they need to know in order to perform their authorised duties. For example, if an employee deals exclusively with UK-based customers, they do not "need to know" Information pertaining to customers based in the US. • The Least Privilege principle is that people should only have the minimum level of privilege necessary in order to perform their authorised duties. For example, if an employee needs to see a customer's address but will not be required to change it, then the "Least Privilege" they require is read-only access, which they should be given rather than read/write access. • The segregation of duties principle is that at least two individuals are responsible for the separate parts of any task in order to prevent error and fraud. For example, an employee who requests an account creation should not be the one who approves the request. The Supplier must ensure access to Personal Information is appropriately managed and restricted to those who require access in order to provide the service. Access management processes should be defined as per Best Industry Practice and include the following: • The Supplier should ensure that access management processes and decisions must be documented and apply to all IT Systems (which store or process Barclays Information Assets), and when implemented they must provide appropriate controls for: Joiner /Mover/ Leaver/ Remote Access. • Controls must be in place for authorisation to ensure the process for granting, modifying and revoking access includes a level of authorisation commensurate with the privileges being granted. • Controls must be in place to ensure access management processes include appropriate mechanisms for identity verification. • Each account must be associated with a single individual, who shall be accountable for any activity carried out using the account. • Recertification of access - Controls must be in place to ensure access permissions must be reviewed at least every 12 months, to ensure that they are commensurate with their purpose. • All Privileged Access permissions must be reviewed at least every six (6) months and adequate controls must be implemented for Privileged Access requirements.	Access management controls helps ensure that only approved Users can access the Information Assets.

	• Mover controls – Access amended within twenty-four 24 hours of the move date (and appropriate records to be kept); • Leaver controls – All logical access used to provide services to Barclays removed within twenty-four 24 hours of leave date (and appropriate records to be kept), • Remote Access - Remote Access controls must only be permitted via mechanisms agreed by Barclays (Chief Security Office - ECAM team) and Remote Access must use Multi-Factor Authentication. • Authentication - appropriate password length and complexity, frequency of changes of passwords, multi-factor authentication, secure management of password credentials or other controls must be followed as per Best Industry Practice. • Dormant accounts - not used for 60 or more consecutive days should be suspended/ disabled (and appropriate records to be kept). • Passwords for interactive accounts should be changed at least every 90 days and should be different from the previous twelve (12) passwords. • Privileged accounts should be changed after each use, and every 90 days minimum. • Interactive accounts should be disabled after a maximum of five (5) consecutive failed attempts or a lower maximum, if Best Industry Practice dictates.	
21. Vulnerability Management	The Supplier must have policies and procedures established, supporting processes / organisational measures, and technical measures implemented, for effective monitoring, timely detection and remediation of vulnerabilities within Supplier-owned or managed applications, infrastructure network and system components to ensure the efficiency of implemented security controls. Vulnerability management should cover, but need not be limited to, the following areas: • Defined roles, responsibilities, and accountabilities for monitoring, reporting, escalation, and remediation. • Appropriate tools and infrastructure for vulnerability scanning. • Conduct vulnerability scans on a routine basis (as regularly as dictated by Best Industry Practice) that effectively identify known and unknown vulnerabilities across all asset classes in the environment.	If this control is not implemented, attackers could exploit vulnerabilities within systems to carry out cyber-attacks, which may result in regulatory and reputational damage.

- Utilize a risk-rating process to prioritise the remediation of discovered vulnerabilities.
- Establish a vulnerability remediation validation process that quickly and effectively verifies remediation of vulnerabilities across all asset classes in the environment.
- Ensure vulnerabilities are effectively addressed through robust remediation activities and patch management to reduce the risk of vulnerability exploitation (remediation to occur in a timely fashion and in accordance with Best Industry Practice).
- Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.

For Supplier services related to **Hosting infrastructure / applications** on behalf of Barclays,

- The Supplier must immediately notify Barclays if any Critical/High vulnerabilities are identified.
- Supplier must remediate vulnerabilities in line with the table below or in agreement with Barclays (Chief Security Office - ECAM team).

Priority	Rating	Closure Days (maximum)
P1	Critical	15
P2	High	30
P3	Medium	60
P4	Low	180
P5	Informational	360

All security issues and vulnerabilities, which could have a material effect on Barclays' hosting infrastructure/ web applications provided by the Supplier, that the Supplier has decided to risk accept must be communicated / notified to Barclays promptly and agreed in writing with Barclays (Chief Security Office - ECAM team).

22. Patch Management	The Supplier must have policies and procedures established, supporting business processes / organisational measures, and technical measures implemented, to monitor / track the need for patching and deploy security patches to managed the entire Supplier environment/estate. The Supplier must ensure that the latest security patches are applied to systems / assets / Networks/applications in a timely manner, and in accordance with Best Industry Practice, ensuring that: • Supplier should test all patches on systems that accurately represent the configuration of the target production systems before deployment of the patch to production systems and that the correct operation of the patched service is verified after any patching activity. If a system cannot be patched, deploy appropriate countermeasures. • All key IT changes prior to implementation must be logged, tested and approved via an approved, robust change management process to prevent any service disruption or security breaches. • Supplier must ensure that patches are reflected in production and disaster recovery (DR) environments.	If this control is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.
23. Threat Simulation/ Penetration Testing/ IT Security Assessment	The Supplier must engage with an independent qualified security provider to perform an IT security assessment / threat simulation covering IT infrastructure including disaster recovery site and web applications related to the service(s) that the Supplier provides to Barclays. This must be undertaken at least annually to identify vulnerabilities that could be exploited to breach the confidentiality of Barclays Data through cyber-attacks. All vulnerabilities must be prioritised and tracked to resolution. The test must be undertaken in line with Best Industry Practice. For Supplier services related to **Hosting infrastructure/ application** on behalf of Barclays, • The Supplier must inform and agree on the scope of security assessment with Barclays, in particular start and end date/times, to prevent disruption to key Barclays' activities. • Any or all issues which are risk accepted must be communicated and agreed with Barclays (Chief Security Office - ECAM team).	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. Barclays information may be disclosed and /or loss of service may occur leading to regulatory or reputational damage.

<table>
<tr>
<td></td>
<td>
<ul>
<li><b>Supplier should share the latest security assessment report on an annual basis with Barclays (Chief Security Office - ECAM team)</b></li>
<li>Supplier must immediately notify Barclays if any Critical/ High vulnerabilities are identified.</li>
<li>Supplier must remediate vulnerabilities in line with the table below or in agreement with Barclays (Chief Security Office - ECAM team).</li>
</ul>
<table>
<tr><th>Priority</th><th>Rating</th><th>Closure Days (maximum)</th></tr>
<tr><td>P1</td><td>Critical</td><td>15</td></tr>
<tr><td>P2</td><td>High</td><td>30</td></tr>
<tr><td>P3</td><td>Medium</td><td>60</td></tr>
<tr><td>P4</td><td>Low</td><td>180</td></tr>
<tr><td>P5</td><td>Informational</td><td>360</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>24. Cryptography</td>
<td>
<ul>
<li>Cryptography Rationale – The Supplier must document the rationale for utilising cryptographic technology and review this to ensure that it is still fit for purpose.</li>
<li>Cryptography Lifecycle Procedures - The Supplier must hold and maintain a documented set of cryptography lifecycle management procedures detailing the end to end processes for key management from generation, loading, distribution to destruction.</li>
<li>Manual operations approval - The Supplier must ensure all human managed events for keys and digital certificates, including the registration and generation of new keys and certificates, are approved at an appropriate level and a record of the approval retained.</li>
<li>Digital Certificates - The Supplier must ensure all certificates are procured from a set of approved and vetted Certificate Authorities (CA) which have revocation services and certificate management policies and must ensure Self Signed certificates are only utilised where technically unable to support a CA based solution and must have manual controls in place to ensure the integrity, authenticity of the keys and timely revocation and renewal is achieved.</li>
</ul>
</td>
<td>Up to date and appropriate encryption protection and algorithms ensures the continued protection of Barclays Information Assets.</td>
</tr>
</table>

	• Key generation and cryptoperiod - The Supplier must ensure that all keys must be randomly generated by either certified hardware or a Cryptographically Secure Pseudo Random Number Generator (CSPRNG) in software. o The Supplier must ensure that all keys must then be subject to a limited and defined cryptoperiod lifetime by which time they are replaced or deactivated. This must also be in line with National Institute of Standards and Technology (NIST) and applicable Best Industry Practice. • Key Storage Protection - The Supplier must ensure that secret/private cryptographic keys only exist in the following forms: o In the cryptographic boundary of a hardware certified security device/module. o In encrypted form under another established or password derived key. o In split component parts split between distinct custodian groups. o Clear in host memory for the period of the cryptographic operation, unless required in HSM protection. • The Supplier must ensure that keys are generated and held within the boundary of the memory of HSMs for high risk keys. This includes; o Keys for regulated services where HSMs are mandated. o Certificates representing Barclays from public CAs. o Root, Issuing, OCSP and RA (registration authority) Certificates used for issuance of Certificates protecting Barclays services. o Keys protecting stored aggregated repositories of keys, authentication credentials or PII data. • Key backup and storage - The Supplier maintains a backup of all keys to prevent the service from being interrupted if the keys become corrupted or require restoration. Access to the back-ups are restricted to secure locations under split knowledge and dual control. Key backups must have at least as strong cryptographic protection over them as the keys in use. • Inventory - The Supplier maintains a complete and up-to-date inventory of cryptographic use in the services they provide to Barclays that details all cryptographic keys, digital certificates, cryptography software and cryptographic hardware managed by the Supplier to prevent damage in case of an incident. It is evidenced by signing of the inventory reviewed at least every quarter and provided to Barclays. The inventories must include where relevant: o IT support team o Related assets	

	o Algorithms, key length, environment, key hierarchy, certificate authority, fingerprint, key storage protection and technical and operational purpose. • Functional and operational purpose - Keys must have a single functional and operational purpose and not be shared between multiple services or beyond Barclays services. • Audit trails - Supplier shall perform and retain evidence of an auditable records review every quarter at a minimum for all key and certificate lifecycle management events that demonstrate a complete chain of custody for all keys including generation, distribution, loading and destruction to detect any unauthorized usage. • Hardware - The Supplier stores the hardware devices in secure areas and maintains an audit trail throughout the key lifecycle to ensure that the chain of custody of cryptographic devices is not compromised. This trail is reviewed on a quarterly basis. o The Supplier must ensure cryptographic hardware is certified to at least FIPS140-2 Level 2 and achieving Level 3 in Physical Security and Cryptographic Key Management or PCI HSM. The Supplier may choose to allow Chip Based smartcards or FIPS certified e-Tokens as acceptable hardware for storing keys representing and held by individual people or customers when held off site. • Key compromise - The Supplier maintains and monitors a key compromise plan to ensure replacement keys are generated independently of the compromised key to prevent the compromised key from providing any information regarding its replacement. If a compromise incident occurs, Barclays should be notified at Barclays **Chief Security Office (CSO) Joint Operations Centre (JOC) - gcsojoc@barclays.com** • Strength of algorithms and keys - The Supplier ensures that the algorithms and length of keys in use are compliant with National Institute of Standards and Technology (NIST) and applicable Best Industry Practice.	
25. Cloud Computing	The Supplier must ensure that cloud service used for Barclays service(s) must have a well-defined security controls framework to protect the core concepts of confidentiality, integrity, and availability and to ensure that security controls are in place and operating effectively to protect Barclays service(s). The Supplier should be certified to ISO/IEC 27017 or 27001 or SOC 2 or similar cloud security framework or	If this cloud control is not implemented, Barclays Data could be compromised, which may result in regulatory or reputational damage.

	Best Industry Practice to have an established and security measures implemented to ensure that all use of cloud technology is secure. Ensure that cloud service provider is certified to Best Industry Practice, including appropriate controls equivalent to the latest version of the Cloud Security Alliance, Cloud Controls Matrix (CCM). The Supplier is responsible for ensuring data security controls related to Barclays Information Assets / Data including Personal Data within the cloud and the cloud service provider CSP's is responsible for the security of the cloud service. Supplier remains responsible for configuration and monitoring of implementing security controls to protect from any Security Incidents including data breaches. Supplier must implement security measures across all aspects of the service being supplied including the cloud shared responsibility model, such that it safeguards the confidentiality, integrity, availability and accessibility by minimising the opportunity of unauthorised individuals from gaining access to Barclays Information and the services utilised by Barclays. Cloud security controls should cover, but need not be limited to, the following domains for deployment models (IaaS/PaaS/SaaS): • Governance & Accountability mechanisms • Identity and Access Management • Network Security (including connectivity) • Data Security (Transit/Rest/Store) • Cryptography, Encryption and Key Management - CEK • Logging and Monitoring • Virtualization • Services Segregation Barclays Information Assets / Data including Personal Data stored in the cloud as part of the service to Barclays must be approved by Barclays (Chief Security Office - ECAM team). Where sensitive data (personal and restricted) is being held with a cloud service provider, the Supplier shall furnish Barclays will the locations, data zones, and failover data zones where this data will be held.	

26. Bank Dedicated Space (BDS)	For services provided which require formal Bank Dedicated Space (BDS), specific BDS physical and technical requirements must be in place. (If BDS is a requirement for the service, the control requirements would be applicable.) The different types of BDS are: Tier 1 (First class) - The entire IT infrastructure is managed by **Barclays** via the provision of a **Barclays** managed LAN, WAN & Desktop to a Supplier site with a Barclays dedicated space. Tier 2 (Business class) - The entire IT infrastructure is managed by the **Supplier** and connects to **Barclays** Internet gateways - LAN, WAN & Desktop devices is owned and managed by the Supplier. Tier 3 (Economy class) –The entire IT infrastructure is managed by the **Supplier** and connects to **Barclays** Internet gateways - LAN, WAN & Desktop devices is owned and managed by the Supplier.	If this control is not implemented, appropriate physical and technical controls may not be in place leading to service delays or disruption or Cyber Security breaches / Security Incidents occurring.
26.1 BDS - Physical Separation	The physical area occupied must be dedicated to Barclays and not shared with other companies / vendors. It should be logically and physically segregated.	
26.2 BDS - Physical Access Control	• Supplier must have a physical access process that covers access methods and authorisation to BDS where services are provided. • Ingress and egress to BDS areas must be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access. • An authorised electronic access card to access the BDS areas of the premises. • Supplier must conduct on a quarterly basis checks to ensure only authorised individuals are provided with BDS access. Exceptions are investigated thoroughly through to resolution. • Access rights are removed within 24 hours for all leavers and movers (and appropriate records to be kept). • Utilise guards to routinely patrol the BDS interior to effectively identify unauthorized access or potentially malicious activity • Secure automatic controls must be operating for access to BDS including: If for authorised personnel: o Photo ID badge which is visible at all times o proximity card readers are implemented o Anti-pass back mechanism is enabled • Supplier must have processes and procedures for the control and monitoring of external persons, including 3rd Party's with physical access to BDS areas for the purpose of maintenance and cleaners.	

26.3 BDS - Video Surveillance	• Implement video surveillance for BDS areas to effectively detect unauthorized access or malicious activity and aid in investigations. • All entry and exit points of BDS area to be video surveillance. • security cameras are positioned appropriately and provide clear and identifiable images at all times to capture malicious activity and aid in investigations. The Supplier must store the captured CCTV footage for 30 days and all CCTV recordings and recorders must be securely located to prevent modification, deletion or the 'casual' viewing of any associated CCTV screens and access to the recordings must be controlled and restricted to authorised individuals only.
26.4 BDS - Access to Barclays Network and Barclays Authentications Tokens	• Every individual user must only authenticate to the Barclays network from the BDS using a Barclays provided multi factor authentication token. • Supplier must maintain records of individuals who have been provided Barclays authentication tokens and Supplier must perform a reconciliation on a quarterly basis. • Barclays will deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) within twenty-four (24) hours. • Barclays will promptly deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed one month). • Services which has remote printing access via a Barclays Citrix application must be approved and authorized by Barclays (Chief Security Office – ECAM Team). The Supplier must maintain records and perform a quarterly reconciliation. Refer to control - 12. Remote Working (Remote Access)
26.5 BDS - Out of Office Support	Remote Access to BDS environment is not provided by default for out of office hours/out of business hours/ work from home support. Any Remote Access must be approved by relevant Barclays teams (including Chief Security Office – ECAM team).
26.6 BDS - Network Security	• Maintain an up-to-date inventory of all of the organisation's network boundaries (through a Network Architecture/Diagram). • The design and implementation of the network must be reviewed at least annually. • BDS network must be logically segregated from Supplier's corporate network by a Firewall and all inbound and outbound traffic to be restricted and monitored. • Routing configuration must ensure only connections to the Barclays network and must not route to any other Supplier networks. • Supplier Edge router connecting to Barclays extranet gateways must be securely configured with a concept of limiting controls of ports, protocols and services; o Ensure that logging and monitoring must be enabled.

	• BDS network must be monitored and only authorised devices must be allowed through appropriate network access controls Refer to control - 10. Boundary and Network Security
26.7 BDS – Wireless Network	Wireless networks must be disabled for Barclays network segment to provision Barclays services.
26.8 BDS - Endpoint Security	Secure desktop builds must be configured in accordance with Best Industry Practice for computers within the BDS network. Best Industry Practices must be put in place and BDS endpoint devices security build must have, but need not be limited to: • Disk Encryption; • Disable all un-needed software/services/ports; • Disable administration rights access for local user; • Supplier Personnel will not be allowed to change the basic settings like default Service Pack, and default services etc.; • USB port must be disabled to prohibit copying of Barclays data to external media; • Updated with the latest anti-virus signatures and security patches; • Data loss prevention limited to no cut-copy-paste and print-screen or print capture tool of Barclays data; • By default, printer access must be disabled; • Sharing/ Transferring of Barclays Information Assets / Data should be disabled using instant messaging tools/ software; • Capability and processes to detect unauthorised software identified as malicious and prevent installation of unauthorised software; Refer to control - 16. Endpoint Security
26.9 BDS - Email and Internet	• Network connectivity must be securely configured to restrict email and internet activity on the BDS network. • Supplier must restrict the ability to access social networking sites, webmail services and sites with the ability to store information on the internet like google drive, Dropbox, iCloud. • Unauthorised transfer of Barclays data outside the BDS network must be protected from Data leakage: • Email • Internet / Web Gateway (including online storage and webmail) • Enforce network-based URL filters that limit a system ability to connect to only Internal or Internet websites of Supplier organisation • Block all attachments and/ or upload feature to websites. • Ensure that only fully supported web browsers and email clients are allowed.

26.10 BDS - BYOD/Personal Device	**Personal devices/ BYOD must not be allowed to access Barclays environment and/or Barclays data**	
Right of Inspection	The Supplier must allow Barclays, upon Barclays giving not less than ten (10) Business Days written notice, to conduct a security review of any site or technology used by the Supplier or its Sub-contractors to develop, test, enhance, maintain or operate the Supplier Systems used in the Services, in order to review the Supplier's compliance with its obligations. The Supplier must also allow Barclays to carry out an inspection on at least an annual basis or immediately after a Security Incident. Any non-compliance of controls identified by Barclays during an inspection must be risk assessed by Barclays and Barclays should specify a remediation timeframe. The Supplier should then complete any required remediation within that timeframe. The Supplier must provide all assistance reasonably requested by Barclays in relation to any inspection and documentation submitted during inspection needs to be completed and return back to Barclays.	If not agreed, Suppliers will be unable to provide full assurance of compliance to these security obligations.

Appendix A: Glossary

Definitions	
Account	A set of credentials (for example, a user ID and password) through which access to an IT system is managed using logical access controls.
Backup, Back-up	A backup or the process of backing up refers to making copies of data so that these additional copies may be used to restore the original after a data loss event.
Bank Dedicated Space	Bank Dedicated Space (BDS) means any premises in the possession or control of a Supplier Group Member or any Subcontractor that is exclusively dedicated to Barclays and from which the Services are performed or delivered.
Best Industry Practice	Using best and current market leading practices, processes, standards, and certifications; and exercising that degree of skill and care which would reasonably be expected from a highly skilled, experienced, and market leading professional organisation engaged in the provision of services which are the same as or similar to the services provided to Barclays.
BYOD	Bring your own devices
Cryptography	The application of mathematical theory to develop techniques and algorithms that can be applied to data to ensure goals such as confidentiality, data integrity and/or authentication.
Cyber Security	The application of technologies, processes, controls, and organisational measures to protect computer systems, networks, programs, devices, and data from digital attacks which may involve (but are not limited to), unauthorised disclosure, destruction, loss, alteration, theft of or damage to hardware, software, or Data.
Data	A recording of facts, concepts or instructions on a storage medium for communication, retrieval and processing by automatic means and presentation as information that is understandable by humans.
Denial of Service (Attack)	An attempt to make a computer resource unavailable to its intended users.
Destruction / Deletion	The act of overwriting, erasing or physically destroying information such that it cannot be recovered.
ECAM	External Cyber Assurance and Monitoring team which assess the security posture of Supplier
Encryption	The transformation of a message (data, voice or video) into a meaningless form that cannot be understood by unauthorised readers. This transformation is from plaintext format into cipher text format.
HSM	Hardware Security Module. A dedicated device which provides secure cryptographic key generation, storage and use, including acceleration of cryptographic processes.
Information Asset	Any information that has value, considered in terms of its confidentiality, integrity, and availability requirements. Or any singular piece or grouping of Information that has a value for the organisation.
Information Asset Owner	The individual within the organisation who is responsible for classifying an asset and ensuring that it is handled correctly.
Least Privilege	The minimum level of access/permissions which enables a User or account to perform their business role.
Network Device/ Networking Equipment	Any IT device that is connected to a network that is used to manage, support or control a network. This could include, but is not limited to routers, switches, firewalls, load-balancers.

Malicious Code	Software written with the intent to circumvent the security policy of an IT system, device or application. Examples are computer viruses, Trojans and worms.
Multi-Factor Authentication (MFA)	Authentication requiring two or more different authentication techniques. One example is the use of a security token, where successful authentication relies upon something that the individual holds (i.e. the security token) and something the user knows (i.e. the security token PIN).
Personal Data	Any information related to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Privileged Access	Designation of special (above standard) access, permissions, or abilities to a user, process, or computer.
Privileged Account	An account that provides an elevated level of control over a specific IT system. These accounts are typically used for system maintenance, security administration or configuration changes to an IT system. Examples include 'Administrator', 'root', Unix accounts with uid=0, Support Accounts, Security Administration Accounts, System Administration Accounts and local administrator accounts
Remote Access	Technology and techniques used to give authorised users access to an organisation's networks and systems from an off-site location.
System	A system, in the context of this document, is people, procedures, IT equipment and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement.
Should	This definition means that the implications will be fully understood and carefully assessed.
Security Incident	Security Incidents are defined as those events which include, but are not limited to: • Attempts (either failed or successful) to gain unauthorised access to a system or its data. • Unwanted disruption or denial of service. • Unauthorised use of a system for the processing or storage of data. • Changes to the system hardware, firmware or software characteristics without the owner's knowledge, instruction or consent. • An application vulnerability which results in unauthorised access to data.

Appendix B: Barclays Information Labelling Schema

Table B1: Barclays Information Labelling Schema

Label	Definition	Examples
Secret	Information must be classified as **Secret** if its unauthorised disclosure would have an adverse impact on Barclays, assessed under the Enterprise Risk Management Framework (ERMF) as "Critical" (financial or non-financial). This information is restricted to a specific audience and must not be distributed further without the originator's permission. The audience may include external recipients at the explicit authorisation of the information owner.	• Information on potential mergers or acquisitions • Strategic planning information – business and organisational • Certain information security configuration information • Certain audit findings and reports • Executive committee minutes • Authentication or Identification & Verification (ID&V) details – customer/client & colleague • Bulk volumes of cardholder Information • Profit forecasts or annual financial results (prior to public release) • Any items covered under a formal Non-Disclosure Agreement (NDA)
Restricted - Internal	Information must be classified as **Restricted - Internal** if the expected recipients are only Barclays authenticated employees and Barclays Managed Service Providers (MSPs) with an active contract in place and which is restricted to a specific audience. Unauthorised disclosure would have an adverse impact on Barclays, assessed under the ERMF as "Major" or "Limited"(financial or non-financial). This Information is not intended for general distribution but may be forwarded or shared by recipients according to the need-to-know principle.	• Strategies and budgets • Performance appraisals • Staff remuneration and Personal Data • Vulnerability assessments
Restricted - External	Information must be classified as **Restricted - External** if the expected recipients are Barclays authenticated employees and Barclays MSPs with an active contract in place and which is restricted to a specific audience or external parties that are authorised by the information owner. Unauthorised disclosure would have an adverse impact on Barclays, assessed under the ERMF as "Major" or "Limited" (financial or non-financial).	• New product plans • Client contracts • Legal contracts • Individual/low volume customer/client Information intended to be sent externally • Customer/client communications. • New issue offering materials (e.g. prospectus, offering memo) • Final research documents • Non-Barclays Material Non-Public Information (MNPI) • All research reports

	This Information is not intended for general distribution but may be forwarded or shared by recipients according to the need-to-know principle.	• Certain marketing materials • Market commentary • Audit findings and report
Unrestricted	Information must be classified as Unrestricted if it is either intended for general distribution, or would not have any negative impact on the organisation if it were to be distributed.	• Marketing materials • Publications • Public announcements • Job advertisements • Information with no impact to Barclays

Table B2: Barclays Information Labelling Schema – Handling Requirements

*** System security configuration Information, audit findings, and personal records may be classed as either Restricted – Internal or Secret, depending on the impact of unauthorised disclosure to the business

Lifecycle Stage	Secret	Restricted – Internal	Restricted – External
Create and Introduce	• Assets must be assigned an Information Asset Owner.	• Assets must be assigned an Information Asset Owner.	• Assets must be assigned an Information Asset Owner.
Store	• Assets (whether physical or electronic) must not be stored where unauthorised people may be able to view or access them. • Electronic assets in storage must be protected through encryption or appropriate compensating controls if there is a significant risk that unauthorised people may be able to access them. • All private keys that are used to protect Barclays Data, identity and/or reputation, must be protected by a FIPS 140-2 Level 3 or above certified hardware security modules (HSMs).	• Assets (whether physical or electronic) must not be stored in public areas (including public areas within the premises where visitors may have unsupervised access). • Information must not be left in public areas within premises where visitors may have unsupervised access.	• Assets (whether physical or electronic) must not be stored where unauthorised people may be able to view or access them. • Electronic assets in storage must be protected through encryption or appropriate compensating controls if there is a significant risk that unauthorised people may be able to access them.

Access & Use	• Assets (whether physical or electronic) must not be worked on or left unattended where unauthorised people may be able to view or access them. Assets may be worked on if suitable controls are in place (e.g. privacy screens). • Printed assets must be printed using secure printing tools. • Electronic assets must be protected by appropriate Logical Access Management controls	• Assets (whether physical or electronic) must not be left in public areas outside the premises. • Assets (whether physical or electronic) must not be left in public areas within the premises where visitors may have unsupervised access. • Electronic assets must be protected by appropriate Logical Access Management controls if required	• Assets (whether physical or electronic) must not be worked on or left unattended where unauthorised people may be able to view or access them. Assets may be worked on if suitable controls are in place (e.g. privacy screens). • Printed assets must be retrieved immediately from the printer. If this is not possible, secure printing tools must be used. • Electronic assets must be protected by appropriate Logical Access Management controls.
Share	• Hard copy assets must carry a visible Information label on every page. • Envelopes containing hard copy assets must carry a visible Information label on the front and be sealed with a tamper-evident seal. They must be placed inside an unlabelled secondary envelope prior to distribution. • Electronic assets must carry an obvious Information label. Electronic copies of multi-page documents must carry a visible Information label on every page. • Assets must only be distributed using systems, methods, or Suppliers approved by the organisation. • Assets must only be distributed to people employed by, or under an appropriate contractual obligation to, the organisation, or as part of a clearly recognised business need such as contract negotiation. • Assets must only be distributed to people specifically authorised to receive them by the Information Asset Owner. • Assets must not be faxed.	• Hard copy assets must be given a visible Information label. The label must be on the title page at a minimum. • Electronic assets must carry an obvious Information label. • Assets must only be distributed using systems, methods, or Suppliers approved by the organisation. • Assets must only be distributed to people employed by, or under an appropriate contractual obligation to, the organisation, or as part of a clearly recognised business need such as contract negotiation.	• Hard copy assets must carry a visible Information label. The label must be on the title page at a minimum. • Envelopes containing hard copy assets must carry a visible Information label on the front • Electronic assets must carry an obvious Information label. Electronic copies of multi-page documents must carry a visible Information label on every page. • Assets must only be distributed using systems, methods, or Suppliers approved by the organisation. • Assets must only be distributed to people employed by, or under an appropriate contractual obligation to, the organisation, or as part of a clearly recognised business need such as contract negotiation. • Assets must only be distributed to people with a business need to receive them. • Assets must not be faxed unless the sender has confirmed that the recipients are ready to retrieve the asset.

	• Electronic assets must be encrypted using an approved cryptographic protection mechanism when in transit outside the internal network. • A chain of custody for electronic assets must be maintained.		• Electronic assets must be encrypted using an approved cryptographic protection mechanism when in transit outside the internal network.
Archive and Dispose	• Hard copy assets must be disposed of using a confidential waste service. • Copies of electronic assets must also be deleted from system “recycle bins” or similar facilities in a timely manner. • Media on which Secret electronic assets have been stored must be appropriately sanitised prior to, or during, disposal.	• Hard copy assets must be disposed of using a confidential waste service. • Copies of electronic assets must also be deleted from system “recycle bins” or similar facilities in a timely manner	• Hard copy assets must be disposed of using a confidential waste service. • Copies of electronic assets must also be deleted from system “recycle bins” or similar facilities in a timely manner.

Banking Secrecy

Additional controls only for Banking Secrecy Jurisdictions (Switzerland/Monaco)

Control Area / Title	Control Description	Why this is important
1. Roles and Responsibilities	The Supplier must define and communicate roles, responsibilities, and accountabilities for the handling of Client Identifying Data (hereafter CID). The supplier must review documents highlighting roles, responsibilities, and accountabilities for CID after any material change to the Supplier's operating model (or business) or at least once a year and distribute them with the appropriate banking secrecy jurisdiction. Key roles must include a senior executive, accountable for the protection and oversight of all activities related to CID (Please refer to Appendix A for the definition of CID). The number of CID accessing staff must be kept to the minimum, based on the need-to-know principle.	Clear definition of roles and responsibilities supports the implementation of the External Supplier Control Obligations Schedule.
2. CID Breach Reporting	Documented controls, processes, and procedures must be in place to ensure any breaches that impact CIDs are reported and managed. Any breach of the handling requirements (as defined in table B2) must be responded to by the Supplier and reported to the corresponding Barclays entity subject to Banking Secrecy immediately (at the latest within 24 hours). An incident response process for timely handling and regular reporting of events involving CID must be established and regularly tested. The Supplier must ensure that identified remedial actions following an incident are addressed with a remediation plan (action, ownership, delivery date) and shared and agreed with the corresponding banking secrecy jurisdiction. Remedial action should be taken by the Supplier in a timely fashion. In case the external supplier provides consultancy services, and an employee of that supplier has triggered data loss prevention incidents, the Bank will notify the incident to the Supplier and where applicable the Bank has the right to request replacement of the employee.	An incident response process helps to ensure that incidents are quickly contained and prevented from escalating. Any breach that impact CID could have strong reputational, damage to Barclays and could lead to fines and loss of the banking license in Switzerland or Monaco

3. Education and awareness	Supplier employees that do have access to CIDs and/or handle them must complete a training* which covers the CID Banking Secrecy Requirements, after any change in regulations or at least once a year. The Supplier must ensure that all new supplier employees (that have access to CIDs and/or handle them), within reasonable time period (circa 3 months), complete training which ensures they understand their responsibilities with regards to CID. Supplier must keep track of employees that completed training. * banking secrecy jurisdictions to provide guidance on the training expected content.	Education and awareness supports all other controls within this schedule.
4. Information Labelling Schema	***Where appropriate****, the Supplier must apply the Barclays Information Labelling Schema (Table E1 of Appendix E), or an alternative scheme that is agreed with the banking secrecy jurisdiction, to all Information Assets held or processed on behalf of the banking secrecy jurisdiction. The handling requirements for CID data are provided in Table E2 of Appendix E. * "***where appropriate***" *refers to the benefit of labelling balanced against the associated risk. For example, it would be inappropriate to label a document if doing so would breach regulatory anti-tampering requirements.*	A complete and accurate inventory of Information assets is essential for ensuring appropriate controls.
5. Cloud Computing/ External Storage	All use of cloud computing and/or external storage of CID (in servers out of the banking secrecy jurisdiction or out of the Supplier infrastructure) used as part of the service to that jurisdiction must be approved by corresponding relevant local teams (including Chief Security Office, Compliance and Legal); and controls must be implemented in accordance with the laws and regulations applicable in corresponding banking secrecy jurisdiction to protect CID information with regards to the high-risk profile they present.	If this principle is not implemented, inappropriately protected Customer data (CID) could be compromised, which may result in legal and regulatory sanction, or reputational damage.

Appendix C: Glossary

** Client Identifying data are special data due to the Banking Secrecy laws in force in Switzerland and Monaco. As such, the controls listed here are complement to those listed above.

Term	Definition
CID	Client Identifying Data
CIS	Cyber and Information Security
Supplier employee	Any individual directly assigned to the Supplier as a permanent employee, or any individual providing services to the Supplier on a limited period of time (such as a consultant)
Asset	Any singular piece or grouping of information that has a value for the organisation
System	A system, in the context of this document, is people, procedures, IT equipment and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement.
User	An account appointed to a Supplier employee, consultant, contractor or agency worker who has authorised access to a Barclays owned system without elevated privileges.

Appendix D: CLIENT IDENTIFYING DATA DEFINITION

Direct CID (DCID) can be defined as unique identifiers (owned by the client), which allow, as is and by itself, to identify a client without access to data in Barclays banking applications. This must be unambiguous, not subject to interpretation, and can include such information as first name, last name, company name, signature, social network ID etc. Direct CID refers to client data that is not owned or created by the bank.

Indirect CID (ICID) is split up into 3 levels

- **L1 ICID** can be defined as unique identifiers (owned by the Bank) which allow to uniquely identify a client in the cases where access to banking applications or other **third party applications** is provided. The identifier must be unambiguous, not subject to interpretation, and can include identifiers such as the account number, the IBAN code, credit card number, etc.
- **L2 ICID** can be defined as information (owned by the client) which, in combination with another, would provide inference to the identity of a client. While this information cannot be used to identify a client on its own, it can be used with other information to identify a client. L2 ICID must be protected and managed with the same rigor as DCID.
- **L3 ICID** can be defined as unique but anonymised identifiers (owned by the Bank) which allow to identify a client if access to banking applications is provided. The difference with L1 ICID is the Information Classification as Restricted - External instead of banking secrecy, meaning they are not subject to the same controls.

Please refer to Figure 1 CID Decision Tree for an overview of the classification method.

Direct and Indirect L1 ICID must not be shared with any person located outside of the Bank and must respect the need-to-know principle at any time. L2 ICID can be shared on a need-to-know basis, but must not be shared in conjunction with any other piece of CID. By sharing multiple pieces of CID there is a possibility of creating a 'toxic combination' which could potentially reveal the identity of a client. We define a toxic combination starting from at least two L2 ICID. L3 ICID can be shared as they are not classified as Banking Secrecy level information, unless recurrent usage of the same identifier can result in the gathering of sufficient L2 ICID data to reveal the identity of the client.

Information Classification	Banking Secrecy			Restricted - Internal
Classification	Direct CID (DCID)	Indirect CID (ICID)		
		Indirect (L1)	Potentially Indirect (L2)	Impersonal Identifier (L3)
Type of Information	Client name	Container number / Container ID	Place of Birth	Any strictly internal identifier of CID hosting/processing application
	Company name	MACC (money account under an Avaloq Container ID) number	Date of birth	Dynamic identifier
	Account statement	SDS ID	Nationality	CRM Party Role ID
	Signature	IBAN	Title	External container ID
	Social network ID	eBanking logon details	Family situation	
	Passport number	Safe deposit number	Post code	
	Phone number	Credit card number	Wealth situation	
	Email address	SWIFT message	Large Position/Transaction Value	
	Job title or PEP title	Business Partner Internal ID	Last Customer Visit	
	Artist Name		Language	
	IP Address		Gender	
	Fax number		CC Expiration Date	
			Primary Contact Person	
			Place of Birth	
			Account Opening Date	

Example: If you send an email or share any document with external people (including third parties in Switzerland/Monaco) or internal colleagues in another affiliate/subsidiary located in Switzerland/Monaco or other countries (e.g. UK)

1. Client name

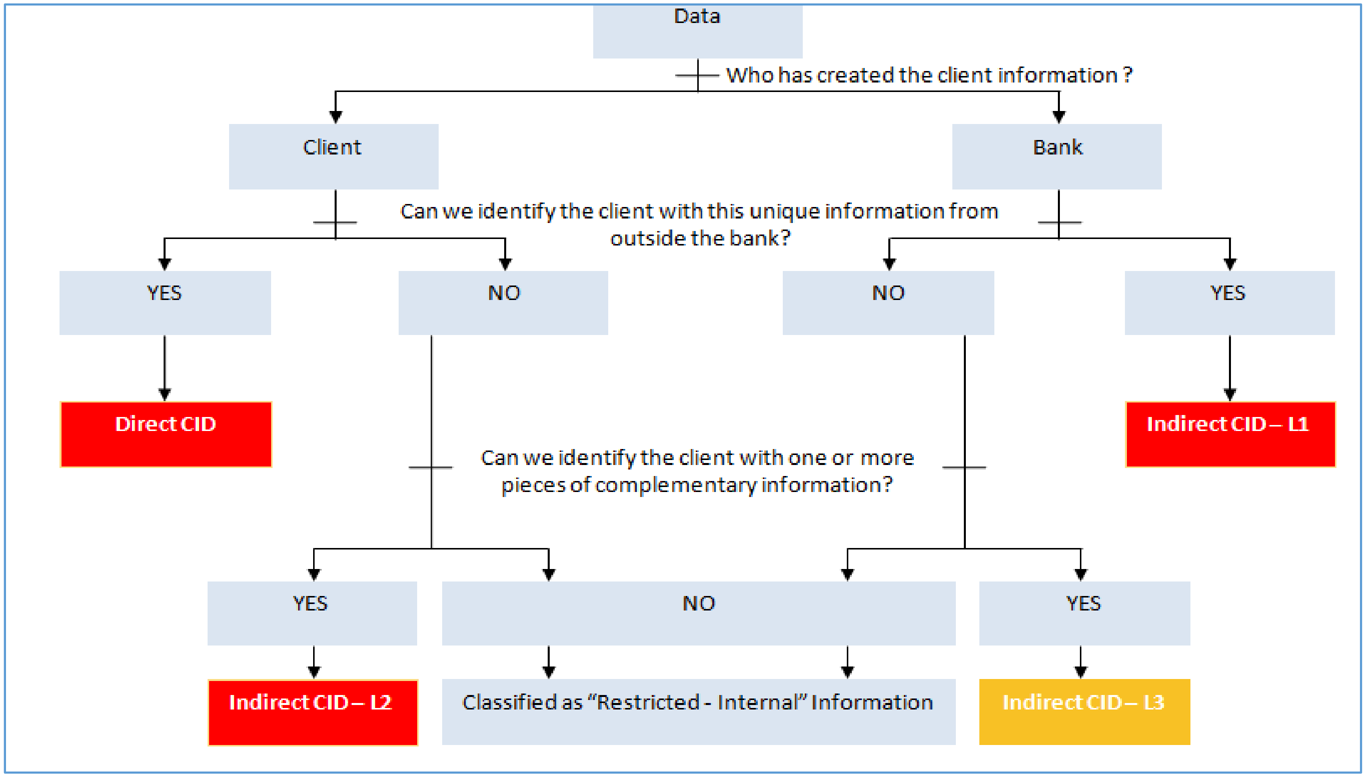
   (DCID) = Banking Secrecy Breach

2. Container ID

   (L1 ICID) = Banking Secrecy Breach

3. Wealth situation + Nationality

(L2 ICID) + (L2 ICID) = Banking Secrecy Breach


Data
Who has created the client information ?
Client
Bank
Can we identify the client with this unique information from outside the bank?
YES
NO
NO
YES
Direct CID
Indirect CID – L1
Can we identify the client with one or more pieces of complementary information?
YES
NO
YES
Indirect CID – L2
Classified as "Restricted - Internal" Information
Indirect CID – L3

Appendix E: Barclays Information Labelling Schema

Table E1: Barclays Information Labelling Schema

** The Banking Secrecy label is specific to Banking Secrecy jurisdictions.

Label	Definition	Examples
Banking Secrecy	Information which is related to any Swiss, Direct or Indirect Client Identifying Data (CID). The 'Banking Secrecy" classification applies to information which is related to any Direct or Indirect Client Identifying Data. Therefore, access by all employees, even located in the owning jurisdiction is not appropriate. Access to this information is only required by those with a need-to-know to fulfil their official duties or contractual responsibilities. None authorised disclosure, access or sharing both internally and externally of the entity of such information may have a critical impact and may lead to criminal proceedings and have civil and administrative consequences such as fines and loss of the banking license, if it were disclosed to unauthorised personnel both internally and externally.	• Client name • Client address • Signature • Client's IP address (further examples in appendix D)

Label	Definition	Examples
Secret	Information must be classified as Secret if its unauthorised disclosure would have an adverse impact on Barclays, assessed under the Enterprise Risk Management Framework (ERMF) as "Critical" (financial or non-financial). This information is restricted to a specific audience and must not be distributed further without the originator's	• Information on potential mergers or acquisitions. • Strategic planning information – business and organisational. • Certain information security configuration information. • Certain audit findings and reports. • Executive committee minutes. • Authentication or Identification & Verification (ID&V) details – customer/client & colleague.

	permission. The audience may include external recipients at the explicit authorisation of the information owner.	• Bulk volumes of cardholder Information. • Profit forecasts or annual financial results (prior to public release). • Any items covered under a formal Non-Disclosure Agreement (NDA).
Restricted – Internal	Information must be classified as Restricted - Internal if the expected recipients are only Barclays authenticated employees and Barclays Managed Service Providers (MSPs) with an active contract in place and which is restricted to a specific audience. Unauthorised disclosure would have an adverse impact on Barclays, assessed under the ERMF as “Major” or “Limited” (financial or non-financial). This Information is not intended for general distribution but may be forwarded or shared by recipients according to the need-to-know principle.	• Strategies and budgets. • Performance appraisals. • Staff remuneration and Personal Data. • Vulnerability assessments. • Audit findings and reports.
Restricted – External	Information must be classified as Restricted - External if the expected recipients are Barclays authenticated employees and Barclays MSPs with an active contract in place and which is restricted to a specific audience or external parties that are authorised by the information owner. Unauthorised disclosure would have an adverse impact on Barclays, assessed under the ERMF as “Major” or “Limited” (financial or non-financial). This Information is not intended for general distribution but may be forwarded or shared by recipients according to the need-to-know principle.	• New product plans. • Client contracts. • Legal contracts. • Individual/low volume customer/client Information intended to be sent externally. • Customer/client communications. • New issue offering materials (e.g. prospectus, offering memo). • Final research documents. • Non- Barclays Material Non-Public Information (MNPI). • All research reports • Certain marketing materials. • Market commentary.

Unrestricted	Information either intended for general distribution, or which would not have any impact on the organisation if it were to be distributed.	• Marketing materials. • Publications. • Public announcements. • Job advertisements. • Information with no impact to Barclays.

Table E2: Information Labelling Schema – Handling Requirements

** Specific handling requirements for CID data to ensure their confidentiality as per regulatory requirements

Lifecycle Stage	Banking Secrecy requirements
Creation and Labelling	As per "Restricted-External" and: • Assets must be assigned an CID Owner.
Store	As per “Restricted-External” and: • Assets must only be stored on removable media for as long as explicitly required by a specific business need, regulators or external auditors. • Large Volumes of Banking Secrecy Information Assets must not be stored on portable devices/media. For more information, contact local Cyber and Information Security Team (hereafter CIS). • Assets (whether physical or electronic) must not be stored where unauthorised people may be able to view or access them, according to the need-to-know or need-to have principle. • Secure workplace practices such as Clear Desk and Desktop locking must be followed for safekeeping of assets (whether physical or electronic). • Removable media information assets must only be used for storage for as long as it is explicitly required, and locked away when not in use. • Ad-hoc data transfers to portable devices/ media requires the data owner, compliance and CIS approval.
Access & Use	As per “Restricted-External” and: • Assets must not be removed / viewed off site (Barclays premises) without formal authorisation from the CID Owner (or deputy). • Assets must not be removed / viewed out of the client booking jurisdiction without formal authorisation from the CID Owner (or deputy) and the client (waiver/ Limited Power of Attorney).

	- Secure remote working practices, ensuring no shoulder surfing is possible, must be followed when taking physical assets off site.
	- Ensure that unauthorised persons cannot observe or access the electronic assets containing CID through the use of restricted access to business applications.
Share	As per "Restricted-External" and: - Assets must only be distributed in accordance with the "need to know principle" AND within the originating Banking Secrecy jurisdiction's information systems and staff. - Assets being transferred on an ad-hoc basis using removable media requires the information asset owner and CIS approval. - Electronic communications must be encrypted while in transit. - Assets (hard copy) sent by mail must be delivered using a service that requires a confirmation receipt. - Assets must only be distributed in accordance with the "need to know principle".
Archive and Dispose	As per "Restricted-External"

*** System security configuration information, audit findings, and personal records may be classed as either Restricted – Internal or Secret, depending on the impact of unauthorised disclosure to the business

Lifecycle Stage	Restricted – Internal	Restricted – External	Secret
Create and Introduce	• Assets must be assigned an Information Asset Owner.	• Assets must be assigned an Information Asset Owner.	• Assets must be assigned an Information Asset Owner.
Store	• Assets (whether physical or electronic) must not be stored in public areas (including public areas within the premises where visitors may have unsupervised access). • Information must not be left in public areas within premises where visitors may have unsupervised access.	• Assets (whether physical or electronic) must not be stored where unauthorised people may be able to view or access them. • Electronic assets in storage must be protected through encryption or appropriate compensating controls if there is a significant risk that unauthorised people may be able to access them.	• Assets (whether physical or electronic) must not be stored where unauthorised people may be able to view or access them. • Electronic assets in storage must be protected through encryption or appropriate compensating controls if there is a significant risk that unauthorised people may be able to access them. • All private keys that are used to protect Barclays Data, identity and/or reputation, must be protected by a FIPS 140-2 Level 3 or above certified hardware security modules (HSMs).
Access & Use	• Assets (whether physical or electronic) must not be left in public areas outside the premises. • Assets (whether physical or electronic) must not be left in public areas within the premises where visitors may have unsupervised access. • Electronic assets must be protected by appropriate Logical Access Management controls if required	• Assets (whether physical or electronic) must not be worked on or left unattended where unauthorised people may be able to view or access them. Assets may be worked on if suitable controls are in place (e.g. privacy screens). • Printed assets must be retrieved immediately from the printer. If this is not possible, secure printing tools must be used. • Electronic assets must be protected by appropriate Logical Access Management controls.	• Assets (whether physical or electronic) must not be worked on or left unattended where unauthorised people may be able to view or access them. Assets may be worked on if suitable controls are in place (e.g. privacy screens). • Printed assets must be printed using secure printing tools. • Electronic assets must be protected by appropriate Logical Access Management controls

Share	• Hard copy assets must be given a visible information label. The label must be on the title page at a minimum. • Electronic assets must carry an obvious information label. • Assets must only be distributed using systems, methods, or Suppliers approved by the organisation. • Assets must only be distributed to people employed by, or under an appropriate contractual obligation to, the organisation, or as part of a clearly recognised business need such as contract negotiation.	• Hard copy assets must carry a visible information label. The label must be on the title page at a minimum. • Envelopes containing hard copy assets must carry a visible information label on the front • Electronic assets must carry an obvious information label. Electronic copies of multi-page documents must carry a visible information label on every page. • Assets must only be distributed using systems, methods, or Suppliers approved by the organisation. • Assets must only be distributed to people employed by, or under an appropriate contractual obligation to, the organisation, or as part of a clearly recognised business need such as contract negotiation. • Assets must only be distributed to people with a business need to receive them. • Assets must not be faxed unless the sender has confirmed that the recipients are ready to retrieve the asset. • Electronic assets must be encrypted using an approved cryptographic protection mechanism when in transit outside the internal network.	• Hard copy assets must carry a visible information label on every page. • Envelopes containing hard copy assets must carry a visible information label on the front and be sealed with a tamper-evident seal. They must be placed inside an unlabelled secondary envelope prior to distribution. • Electronic assets must carry an obvious information label. Electronic copies of multi-page documents must carry a visible information label on every page. • Assets must only be distributed using systems, methods, or Suppliers approved by the organisation. • Assets must only be distributed to people employed by, or under an appropriate contractual obligation to, the organisation, or as part of a clearly recognised business need such as contract negotiation. • Assets must only be distributed to people specifically authorised to receive them by the Information Asset Owner. • Assets must not be faxed. • Electronic assets must be encrypted using an approved cryptographic protection mechanism when in transit outside the internal network.

			• A chain of custody for electronic assets must be maintained.
Archive and Dispose	• Hard copy assets must be disposed of using a confidential waste service. • Copies of electronic assets must also be deleted from system “recycle bins” or similar facilities in a timely manner	• Hard copy assets must be disposed of using a confidential waste service. • Copies of electronic assets must also be deleted from system “recycle bins” or similar facilities in a timely manner.	• Hard copy assets must be disposed of using a confidential waste service. • Copies of electronic assets must also be deleted from system “recycle bins” or similar facilities in a timely manner. • Media on which Secret electronic assets have been stored must be appropriately sanitised prior to, or during, disposal.