BARCLAYS

Supplier Control Obligation (SCO)

Information and Cyber Security (ICS)

Final Version 13.0

Control Area / Title	Control Description	Why this is important
1. Approved Usage	The Supplier should ensure information and other associated assets are appropriately protected, used, and handled. Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented, and implemented. Supplier employees including contractors, sub-contractors, sub-processors of their responsibilities using or having access to the organisation's information and other associated assets should be made aware of the information security requirements for protecting and handling the organisation's information and other associated assets. They should be responsible for their use of any information processing facilities. The organisation should establish a topic-specific policy on the acceptable use of information and other associated assets and communicate it to anyone who uses or handles information and other associated assets. The Supplier must take appropriate steps to ensure conformance to the acceptable use requirements. The following topics may 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	An acceptable use requirement helps to underpin the control environment protecting Information Assets.

	• Risk and consequences of misuse of the above items and/or any illegal, harmful, or offensive outcomes resulting from such misuse.	
2. Boundary and Network Security	The Supplier must ensure that all the Systems and applications operated by Supplier and/or its sub-contractor/sub processors that support Barclays services(s) are protected from inbound and outbound network threats. Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorized access. The Supplier must Identify, Protect, Detect and Respond to any security alerts and breaches. Network Security controls ensure the protection of information in networks and its supporting information processing facilities, must include but not be limited to the following areas: • Maintain an up-to-date inventory of all of the organisation network boundaries (through a Network Architecture/Diagram) and must review it at least annually. • External connections to the Supplier network are documented, verified, and approved prior to the connections being established to prevent security breaches. • Supplier networks must be protected through applying defense-in-depth principles (e.g., network segmentation, firewalls, etc.). • The Supplier must have network intrusion prevention technologies to detect and prevent malicious traffic for all inbound/outbound traffic and update signature databases in line with best industry best practice and apply updates from the solution provider in a timely manner. • The Supplier must ensure that private connectivity between virtual private clouds (VPCs) and third-party on-premises networks is encrypted, and that traffic is not exposed to the public internet • Internet network traffic should pass through a proxy that is configured to filter unauthorised connections. • Logical separation of device management ports/interfaces from user LAN/ traffic; appropriate authentication controls. • Secure communications between devices and management stations/ console. • Ensure that logging and monitoring includes detection and alerting of suspicious activity (using behavior and indicators of compromise triggers) such as via an SIEM. • 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.	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.

	• Supplier must review the firewall rules (External and Internal Firewall) and must review it at least annually. • The Supplier must ensure that access to the internal network is monitored through appropriate network access controls. • All wireless access to the network is subject to authorisation, authentication, segmentation, and strong encryption protocols to prevent security breaches. • Supplier must have segregated network (logically) for Barclays service(s). The Supplier must ensure that any servers and applications used to provide service to Barclays are not deployed on untrusted networks (networks outside your security perimeter, that are beyond your administrative control e.g., internet-facing) without appropriate security controls. The Supplier hosting Barclays Information (including sub-contractors, sub-processors) in a data centre or cloud must hold a Best Industry Practice certification for network 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/ last mile termination router or 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 includes detection and alerting of suspicious activity (using behavior and indicators of compromise triggers) such as via an SIEM. The third-party provider must ensure that any systems and applications providing services which Barclays considers to be, and communicates to the Supplier to be high risk, must be network segmented. The partitioning of a business application and its core underpinning infrastructure components (excluding shared and pervasive critical infrastructure) into its own network segment utilising approved Barclays security technologies (firewalls or other equivalent technologies) to meet the principles below. i. A Segmentation approach must be taken to limit risk exposure, inhibit lateral movement across the network and reduce network broadcast risk. Applications	

	must be deployed to self-contained segments to help limit risk as far as is reasonably possible. Example: Faster Payments zone. All business application(s) related infrastructure and data must be deployed to a self-contained secure Application zone where possible and segregated from the Barclays internal network using a CSO approved enforcement technology (e.g., network firewalls, approved segmentation solution). Note – Some scenarios may warrant splitting components such as the application and database across multiple zones e.g., where shared platforms are leveraged. Each Application must be assessed individually, with the most appropriate approach defined and agreed with a CSO Security Consultant. ii. Services must be physically or logically segregated. The underlying network fabric (e.g., cabling / switches) can be shared with other applications and services i.e., segments can be logically defined without the requirement to enforce segmentation through physical separation from the rest of the Barclays network. iii. Application zones must restrict traffic flows to and from other zones (including the internal CIPE network), on the basis of those required for the service to operate and any approved management, monitoring and security tools. Configurations must stipulate specific ports, protocols, and IP addresses for permitted communication paths, all other communication must be restricted by default. Rules which contain ranges should be avoided and approved by exception only to ensure only the minimum connectivity requirements are enabled. iv. Containers must be robustly segregated with strong logical controls preventing inter-container lateral movement, thus enforcing isolation. Compromise of one container must not lead to the compromise of other containers running on the same host/cluster. v. All segmentation implementations must offer a centralised policy management capability with functionality (or integration) to verify and report policy compliance (see Firewall Compliance document) and provide auditable log of changes. vi. Stateful inspection/controls should be operated where possible/feasible. vii. Segmentation capabilities must operate in a 'fail safe' manner e.g., should the capability fail, approved rulesets to block/allow traffic must remain enforced. viii. Any traffic between production and non-production systems on Application zones must only be permitted by exception and must be logged. **Guidance for Cloud Service customer (Supplier) used for providing service(s) to Barclays** The Cloud Service Customer (CSC) must ensure that appropriate Network Security controls are implemented to safeguard Barclays service -	

	• The cloud service customer (CSC) should define its requirements for segregating networks to achieve tenant isolation in the shared environment of a cloud service and verify that the cloud service provider meets those requirements. • The cloud service customer's access control policy for the use of network services should specify requirements for user access to each separate cloud service that is used. *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.*	
3. Denial of Service Detection	Supplier must maintain a capability to detect and protect against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Supplier must ensure that Internet connected or external channels supporting services supplied to Barclays must have adequate DDoS/DoS protection to ensure availability. If the Supplier is hosting systems and applications providing services and holding Barclays data or underpinning resilience categories 0 or 1 service, this must have adequate DoS protection to ensure availability.	If this principle is not implemented, Barclays and its Supplier may be unable to prevent a denial-of-service attack from achieving its objective.
4. Remote Working (Remote Access)	The Supplier must ensure the security of information while employees are working remotely. Security measures should be implemented to protect information accessed and processed outside the organisation's premises while working remotely. The Supplier should provide instructions to staff members regarding working from home. Remote Access to Barclays Network Remote access to Barclays network via Barclays Citrix application is not provisioned by default. To access Barclays Network from unapproved locations/out of office/from home, and any remote access, prior approval, and authorisation from Barclays (Chief Security Office – ECAM Team (externalcyberassurance@barclayscorp.com) must be obtained. The Supplier must ensure following controls are established for remote access: • Access to the Barclays network requires an RSA Token (Soft) and a supported version of Citrix Workspace App; Barclays will provide details • Supplier must maintain an up to date and correct record of its employees approved to work remotely / hybrid with business justification for each approved employees including sub-contractor/sub-processors.	Remote Access controls help to ensure unauthorized and insecure devices are not connected to the Barclays environment remotely.

	• The Supplier must perform reconciliation of all the remote access employees on a quarterly basis followed by an intimation of its results to Barclays (Chief Security Office - ECAM team (externalcyberassurance@barclayscorp.com). • 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 of date of exit/ Last Day in Office (LDIO) • 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 to Barclays information systems remotely must be configured securely (e.g., patch level, status of anti-malware, etc.). • Services which have remote printing access via a Barclays Citrix application must be approved and authorized by Barclays (Chief Security Office – ECAM Team - externalcyberassurance@barclayscorp.com). Supplier must maintain records and perform quarterly reconciliation. • Personal devices/ BYOD (limited to Laptops/Desktops) must not be allowed to access Barclays environment and/or Barclays data residing/ stored within Supplier managed environment (which includes Supplier Staff, Consultants, Contingency workers, contractors and Managed Service Partners, sub-contractor/sub-processors). Note: Remote access to Barclays network and Barclays data is not permissible unless specifically approved and authorised by Barclays. Remote Access to Supplier Environment/Network Remote access to Supplier managed environment for service delivery which includes Barclays data residing/stored and/or processed within Supplier environment / network. The Supplier must ensure following controls are established for Supplier corporate network for remote access • Remote login access to the Supplier network must be strongly encrypted during data in transit and use multi-factor authentication. • Supplier may use virtual desktop for remote access • Supplier must maintain records of individuals who have been working remotely / hybrid.	

	• Supplier should perform reconciliation of all the remote users as per Supplier timelines • Supplier will deactivate authentication credentials the access is no longer needed (e.g., employee termination, project reassignment, etc.) within twenty-four (24) hours. of date of exit/ Last Day in Office (LDIO) • Personal devices/ BYOD (limited to Laptops/desktops) must not be allowed to access Barclays data residing/ stored within Supplier managed environment (which includes Supplier Staff, Consultants, Contingency workers, contractors, and Managed Service Partners). Employees should be provided with rules from the Supplier on working from home, including Do's and don'ts. Remote (including from home) working capabilities is prohibited during normal course of business where third parties are contractually obliged to provide services from Bank Dedicated Space or Supplier premises or where regulatory requirements are applicable. However, provisions are allowed in third parties business continuity plans in the event of a disaster recovery / crisis / pandemic response in agreement with Barclays and any security requirements mandated for remote working as part of the contractual agreement.	
5. Security Log Management	The Supplier must have a well-established supporting audit and log management framework. The framework must include key IT systems including applications, networking equipment, security devices and servers set to log key events. To record events, generate evidence, ensure the integrity of log information, logs should be untamperable, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations. The Supplier must ensure that logs are centralised, appropriately secured against tampering and/or deletion and retained by the Supplier for a minimum period of 12 months or regulatory requirement whichever greater.	If this control is not implemented, Supplier will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.

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

Security log management framework should cover the following areas:

- 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, and/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'.
- 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).
- 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.

	• Log analysis should cover the analysis and interpretation of information security events, to help identify unusual activity or anomalous behavior, which can represent indicators of compromise. • 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 incidents and/or breaches of access rights occurring in relation to the Supplier Systems. • Test periodically that the framework continues to meet the requirements above. **Guidance for Cloud Service customer (Supplier) used for providing service(s) to Barclays** The Cloud Service Customer (CSC) must ensure that appropriate Security Log Management controls are implemented to safeguard Barclays service - • The cloud service customer should define and document its requirements for event logging and verify that the cloud service meets those requirements. • If a privileged operation is delegated to the cloud service customer, the operation and performance of those operations should be logged. The cloud service customer should determine whether logging capabilities provided by the cloud service provider are appropriate or whether the cloud service customer should implement additional logging capabilities. • The cloud service customer should request information about the clock synchronization used for the cloud service provider's systems. • The cloud service customer should request information from the cloud service provider of the service monitoring capabilities available for each cloud service.	
6. Malware Defenses	In alignment with Best Industry Practice, the Supplier must have established policies and procedures established, 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 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 • Update signature database on a regular basis	Anti-malware solutions are vital for the protection of Barclays Information assets against Malicious Code.

	• 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 malware and attacks on mobile devices used for Barclays services. • The email gateway scans all incoming, outbound, and internal email communications, including attachments and URLs for signs of malicious or harmful content. NB. Anti-malware to include detection for (but not limited to), unauthorised mobile code, viruses, spyware, key logger software, botnets, worms, Trojans, etc.	
8. Endpoint Security	The Supplier must adopt unified endpoint management approach to ensure their endpoints used to access Barclays network, or access and/or process Barclays Information Assets/Data, must be hardened to protect against any malicious attacks. Best Industry Practices must be in place and endpoint secure build must include, but need not be limited to: • Full Hard Disk Encryption. • Disable all un-needed software/services/ports. • Disable administration rights access for local user. • Supplier Employee will not be allowed to change the basic settings like default Service Pack, System Partition, and default services, Anti-Virus etc. • Disable USB to copying of Barclays Information/data to external media • Updated with the latest anti-virus signatures and security patches. • Disable Print Spooler Service • Data prevention tool to protect against Barclays data breach • The Supplier must ensure to block exfiltration of Barclays data to social network sites, webmail services and sites that could store information such as but not limited to google drive, Dropbox, iCloud. • Disable sharing/ transferring of Barclays data on instant messaging tools/software. • Detect, stop, and remediate presence and/or use of unauthorised software including malicious software. • Lock screen times out, Limit TCP IP connection to only the corporate network, Advanced EPS security agent to detect suspicious behaviour NB. Removable media / portable devices should be disabled by default and only enabled for legitimate business reasons.	If this control is not implemented, Barclays and Supplier network and endpoints may be vulnerable to cyber-attacks.

	The Supplier should maintain secure images or templates for all systems in an enterprise based on the organisation's approved configuration standards. Any new system deployment or existing system that has been compromised should be configured using approved 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 Relationship Manager/ Barclays IT support team/ECAM Team. Mobile devices used for Barclays Services - • Supplier must ensure they implement unified end point management (UEM) or 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. • Supplier must ensure have and use mobile device remote lock and wipe capabilities to protect information in the event of a lost, stolen or a compromised device • Encrypt Barclays data stored and/or processed on the mobile device Data • Supplier must ensure mobile devices are not rooted and strong authentication policy is enabled	

9. Data Leakage Prevention	The Supplier must use management approved effective framework to secure Barclays data from leakage/exfiltration and include but not limited only to data leakage channels: -
	
	• Unauthorised transfer of information outside the internal network/ Supplier network
	  ○ Email
	  ○ Internet / Web Gateway (including online storage and webmail)
	  ○ 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 via connectable (e.g., serial, USB) and wireless (e.g., Bluetooth, Wi-Fi).
	• Insecure Information exchange with third parties (sub-contractors, sub-processors).
		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

	• Inappropriate printing or copying of Information. Data leakage prevention measures should be applied to systems, networks and any other devices that process, store, or transmit Barclays data/ information.	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
10. Data Security	The Supplier must secure Barclays data held and/or processed by them through a combination of encryption, integrity protection and data loss prevention techniques. The access to Barclays data must be restricted to its authorized employee only and protected against contamination, aggregation attacks, inference attacks, storage threats including but not limited to threats from cloud computing environments. Data security controls should cover, but not be limited to, the following areas: 1. Supplier is obligated at all times to comply with any and all applicable data protection laws. 2. Establish Policy, Processes and Procedures, supporting business processes and technical measures. Document and maintain data flows for data resident within the service's geographical location (physical and virtual). It should cover details related to applications and systems components part of data flow. 3. Maintain data flow diagram of Barclays data resident within geographical locations (including physical and virtual) in applications and system components. 4. Maintain an inventory of all Barclays sensitive/confidential information stored, processed, or transmitted by the Supplier. 5. Ensure all Barclays data are classified and tagged based on the management approved Information Classification and Protection standard. 6. Protect Data at rest; a. Strongly encrypt data at rest to prevent exposure of Barclays information assets 7. Database activity monitoring; a. Monitor and log database access and activity to quickly and effectively identify malicious activity. 8. Protect Data in use; a. Ensure access management capability controls to processing of sensitive information 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. Protect Data in transit;	

	a. Leverage strong encryption capabilities to ensure data is protected while in transit. b. Strong 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: 10. Transport Layer Security (TLS) (following the Best Industry Practice of modern cryptography, including use / rejection of protocols and cyphers) 11. All data stored in production and non-production environment should protect with encryption (refer to control 16 Cryptography)	
11. 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 Software Development framework to integrate security into the lifecycle of software development. The Supplier must test and remediate vulnerabilities in the software before delivering to Barclays. 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.

	• Establish and adopt management approved Secure coding standards aligned with Best Industry Practices to prevent vulnerabilities and service interruptions. • 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. • Have 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. • Should not copy sensitive information into the development and testing system environments unless equivalent controls are provided for the development and testing systems. • 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 Information) is not 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). • Prohibit use of public code repositories 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 type of application. 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 feasible, a host-based web application firewall should be deployed. Supplier must ensure that all Internet facing Software as a Service (SaaS) based application solution used for Barclays Service(s) must have supplemental access control (authentication control) in addition to a traditional authentication control (username/password).	

	Supplier must include but not be limited to the following areas: • Multifactor authentication (e.g., token, SMS) • SSO (Single Sign-on) • IP Address based access control Supplemental access control must be provisioned for Supplier employees/ sub-contractor/sub processors/Barclays employees/ clients and/or customers of Barclays.	
12. Logical Access Management (LAM)	Access to Information Assets (incl. Software, Hardware and Data) must only be granted on the need-to-know basis, following the principle of Least Privilege. The IT System/Information Asset Owner is accountable for providing a list of all accounts that have access to the system/information asset, as well as defining the Logical Access Security Model, incl. Access Profiles and Segregation of Duties (SoD) Rules. The Supplier hosted Web applications are in-scope of Barclays LAM Onboarding, and Barclays LAM controls must be implemented for these. • The need-to-know basis means that employees should only have access to the Information they need to know in order to perform their authorised duties. E.g., if an employee deals exclusively with UK-based customers, they do not "need to know" Information pertaining to customers based in the US. • The principle of Least Privilege means that employees should only have the minimum level of access necessary 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 (SoD) is an approach to structuring tasks in such a way that a task cannot be completed by a single individual, intended principally to mitigate the risk of fraud. For example, an employee who requests an account creation should not be the one who approves the request. Access Management processes must be defined, documented, and enforced as per Industry Best Practice, where as per Barclays Group Information & Cyber Security Policy and the Identity & Access Management (IAM) Standard this requires the following: • Barclays LAM Onboarding: The Supplier must ensure that access management processes is leveraging the central Barclays IAM Toolset to facilitate LAM Controls. IT	Appropriate LAM controls help to ensure that Information Assets are protected from inappropriate usage. Access management controls helps ensure that only approved Users can access the Information Assets.

	System Access Control Lists (ACLs) must be submitted to IAM team as part of the process of onboarding the IT System to the IAM Toolset. To ensure the most effective operation of downstream LAM controls, the optimal feed frequency is a daily automated feed, however as a minimum requirement this must be supplied on a monthly basis. • Joiner Controls: all access must be appropriate and approved prior to provisioning. • Mover Controls: all access must be reviewed ahead of the transfer day to confirm access that must be retained, revoked, and enabled. Access confirmed for revocation must be removed ahead of the transfer day. • Leaver Controls: all access used to access Barclays information resources and/or provide services to Barclays must be removed on the employee's contract end date with Supplier. • Account Ownership: Unique account must be associated with a single employee, who shall be accountable for any activity carried out using the account. Account details and passwords must not be shared with any other employee. • Dormant Accounts: accounts that are not used for 60 or more consecutive days must be suspended/ disabled (and appropriate records kept). • Recertification of Access: all access must be reviewed – every 12 months (for non-privileged access), and every 6 months (for privileged access), to ensure access remains appropriate. • Identity Verification (ID&V): controls must be in place to ensure access management processes include mechanisms for identity verification.. • Authentication: all accounts must be authenticated before logical access is granted. Applications and authentication mechanisms must not display passwords or PINs. Appropriate password length and complexity, password history, frequency of password changes, multi-factor authentication, and secure credential management must be in place. • Non-personal Credentials: non-personal credentials (i.e. passwords and secrets) must be onboarded onto a suitable Credential Management tool (e.g. CyberArk). Where this is not possible, the credentials must be secured so no human can ever use them. Where human use of the account is required, the access must be temporary and time bound, and the credentials need to be reset afterwards. • Credential Management: Personal account passwords must be changed at least every 90 days. Passwords for privileged and interactive accounts must be changed every 90 days or after every human use so that no human has knowledge of the password or, if the password is 50 characters or more, every 365 days or after every human use so	

	that no human has knowledge of the password. Passwords for interactive accounts must be different from the previous 12 passwords. • Time-bound Access: Personal Privileged Access to Production and Disaster Recovery Infrastructure used by Barclays staff or Barclays non-permanent staff must be time-bound, with appropriate approvals in place. • Privileged Activity Monitoring: Privileged Activity Monitoring must be undertaken. Guidance for Cloud Service customer (Supplier) used for providing service(s) to Barclays The Cloud Service Customer (CSC) must ensure that appropriate Logical Access Management controls are implemented to safeguard Barclays service - • The cloud service customer should use sufficient authentication techniques (e.g., multi-factor authentication) for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service according to the identified risks. • The cloud service customer should ensure that access to information in the cloud service can be restricted in accordance with its access control policy and that such restrictions are realised. This includes restricting access to cloud services, cloud service functions, and cloud service customer data maintained in the service. • Where the use of utility programs is permitted, the cloud service customer should identify the utility programs to be used in its cloud computing environment and ensure that they do not interfere with the controls of the cloud service.	
13. Vulnerability Management	The Supplier must run an effective vulnerability management program through established policies and procedures, supporting processes / organisational measures, and technical measures, for effective monitoring, timely detection and remediation of vulnerabilities within Supplier owned or managed applications or developed application/ Code, 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. • The Service provider will conduct vulnerability scans on a routine basis using updated vulnerability signatures (as regularly as dictated by Best Industry Practice)	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.

that effectively identify known and unknown vulnerabilities across all asset classes in the environment.

- Utilize a risk-rating process to prioritise the remediation of discovered vulnerabilities.
- 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/ or with Patch Management program).
- Establish a vulnerability remediation validation process that quickly and effectively verifies remediation of vulnerabilities across all asset classes in the environment.
- 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 (including communicated **high risk third parties)**

- 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 (30 max days)
P2	High	60
P3	Medium	180
P4	Low	No SLA

All security issues and vulnerabilities, which could have a material effect on Barclays' hosting infrastructure/ 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 - externalcyberassurance@barclayscorp.com).

Guidance for Cloud Service customer (Supplier) used for providing service(s) to Barclays

	The Cloud Service Customer (CSC) must ensure that appropriate Vulnerability Management controls are implemented to safeguard Barclays service - • The cloud service customer should request information from the cloud service provider about the management of technical vulnerabilities that can affect the cloud services provided. The cloud service customer should identify the technical vulnerabilities it will be responsible to manage, and clearly define a process for managing them.	
14. Patch Management	The Supplier must have a Patch Management program supported by established policies and procedures, business processes / organisational measures, and technical measures, to monitor / track the need for patching and deploy security patches to manage the entire Supplier environment/estate. The Supplier must ensure that Servers, Network devices, applications and endpoint devices are kept up to date with the latest security patches and in accordance with Best Industry Practice, ensuring that: • Supplier should evaluate and 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 support future auditing, investigation, troubleshooting and analysis requirements. • Supplier must verify 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.
15. Penetration Testing/ IT Security Assessment	The Supplier must engage with an independent qualified security service provider to perform an IT security assessment / Penetration Testing 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 exploitable vulnerabilities that could breach the security 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.	If this control is not implemented, Supplier 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

<table>
<tr>
<td></td>
<td>For Supplier services related to Hosting infrastructure / applications on behalf of Barclays (including communicated high risk third parties)

The Supplier must inform and agree with ECAM 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).
Supplier should share the latest security assessment report on an annual basis with Barclays (Chief Security Office-ECAM Team - externalcyberassurance@barclayscorp.com)
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).

<table>
<tr><th>Priority</th><th>Rating</th><th>Closure Days (maximum)</th></tr>
<tr><td>P1</td><td>Critical</td><td>15 (30 max days)</td></tr>
<tr><td>P2</td><td>High</td><td>60</td></tr>
<tr><td>P3</td><td>Medium</td><td>180</td></tr>
<tr><td>P4</td><td>Low</td><td>No SLA</td></tr>
</table>
</td>
<td>service may occur leading to regulatory or reputational damage.</td>
</tr>
<tr>
<td>16. Cryptography</td>
<td>The Supplier must ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of Barclays data/information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.

When using cryptography, the following should be considered:

the topic-specific policy on cryptography defined by the organisation, including the general principles for the protection of information. A topic-specific policy on the use of cryptography is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.

</td>
<td>Up to date and appropriate encryption protection and algorithms ensures the continued protection of Barclays Information Assets.</td>
</tr>
</table>

	• identifying the required level of protection and the classification of the information and consequently establishing the type, strength and quality of the cryptographic algorithms required.
	• the use of cryptography for protection of information held on storage media and transmitted over networks to such devices or storage media.
	• the approach to key management, including methods to deal with the generation and protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys.
	• Cryptography Rationale – The Supplier must document the rationale for utilising cryptographic technology and review this to ensure that it is still fit for purpose.
	• 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. The Supplier must retire its keys after the service period is over or set up a mandatory key rotation program.
	• 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.
	• 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.
	• 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.
	  ○ 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:
	  ○ In the cryptographic boundary of a hardware certified security device/module.
	  ○ In encrypted form under another established or password derived key.	

	○ In split component parts split between distinct custodian groups. ○ 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. ○ Keys for regulated services where HSMs are mandated. ○ Certificates representing Barclays from public CAs. ○ Root, Issuing, OCSP and RA (registration authority) Certificates used for issuance of Certificates protecting Barclays services. ○ 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 is 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: • IT support team • Related assets • 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.	

	• 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.	
17. Cloud Computing	The Supplier (Cloud Service Customer CSC) must ensure that cloud service used for Barclays service(s) must have a well-defined security controls framework to meet goals 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 27001or SOC 2 or similar cloud security framework or 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 Information within the cloud and the cloud service provider CSP's is responsible for the security of the cloud computing environment. 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.	If this cloud control is not implemented, Barclays Data could be compromised, which may result in regulatory or reputational damage.

	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) • Secure Data deletion/data purging • Cryptography, Encryption and Key Management - CEK • Logging and Monitoring • Virtualization • Services Segregation Barclays Information Assets / Data including Personal Information stored in the cloud as part of the service to Barclays must be approved by Barclays (Chief Security Office - ECAM team). The Supplier shall provide Barclays with locations of data zones, and failover data zones where Barclays data will be stored or held.	

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** Extranet 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

18.1 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.

18.2 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 regulated and monitored by physical access control mechanisms to ensure that only authorised employee is allowed access (role specific) and approved (by BDS service owner). • An authorised electronic access card to access the BDS areas of the premises. • Supplier must conduct on a quarterly basis check 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, movers and absconding employee (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: For authorised employee: o Photo ID badge which is visible at all times o proximity card readers are implemented o Anti-pass back mechanism is enabled and monitored • Supplier must have processes and procedures for the control and monitoring of external persons, including sub-contractors, sub-processors with physical access to BDS areas for the purpose of maintenance and cleaners.
18.3 BDS - Video Surveillance	• Implement video surveillance for BDS areas to effectively record or alerting unauthorized access and/or malicious activity and aid in investigations. • All entry and exit points of BDS area to be video surveillance. • Testing of cameras for operation and quality also 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.
18.4 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 (RSA 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.) **date of exit/last working day/ LDIO date received** with the Supplier.

	• 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 have 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 - 4. Remote Working (Remote Access)
18.5 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). Remote (including from home) working capabilities is prohibited during normal course of business where third parties are contractually obliged to provide services from Bank Dedicated Space or Supplier premises or where regulatory requirements are applicable. However, provisions are allowed in third parties business continuity plans in the event of a disaster recovery / crisis / pandemic response in agreement with Barclays and any security requirements mandated for remote working as part of the contractual agreement.
18.6 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 - 2. Boundary and Network Security
18.7 BDS – Wireless Network	Disable Wireless network for BDS network provision for Barclays services.
18.8 BDS - Endpoint Security	Secure desktop builds (including laptops) 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: • Full hard disk Encryption. • Disable all un-needed software/services/ports. • Disable administration rights access for local user. • Supplier employee will not be allowed to change the basic settings like default Service Pack, and default services etc. • Disable USB to copying of Barclays Information/data to external media • Updated with the latest anti-malware signatures and security patches. • Disable printer spooler service • Sharing/ Transferring of Barclays Information Assets / Data should be disabled using instant messaging tools/ software. • Detect, stop and remediate presence and/or use of unauthorised software including malicious software. • Lock screen times out, Limit TCP IP connection to only the corporate network, Advanced EPS security agent to detect suspicious behaviour Refer to control - 8. Endpoint Security

18.9 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.

18.10 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/Sub-processors to develop, test, enhance, maintain or operate the Supplier Systems used in the Services, in order to review the Supplier compliance with its obligations to Barclays. The Supplier must also allow Barclays to carry out an inspection on at least an annual basis and/or immediately after a security incident.

Any non-conformance to controls identified by Barclays during an inspection must be risk assessed by Barclays and Barclays must specify a remediation timeframe. The Supplier must 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. The documentation needs to be completed and returned back to Barclays promptly. Supplier also must support Barclays with assessment questioner along with evidence requested during any assurance review.

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 sub-contractors, sub-processors 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 Information	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.
Virtual Machine:	The complete environment that supports the execution of guest software. NOTE – A virtual machine is a full encapsulation of the virtual hardware, virtual disks, and the metadata associated with it. Virtual machines allow multiplexing of the underlying physical machine through a software layer called a hypervisor.

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 support 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 B: 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 C: 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// Prospect 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

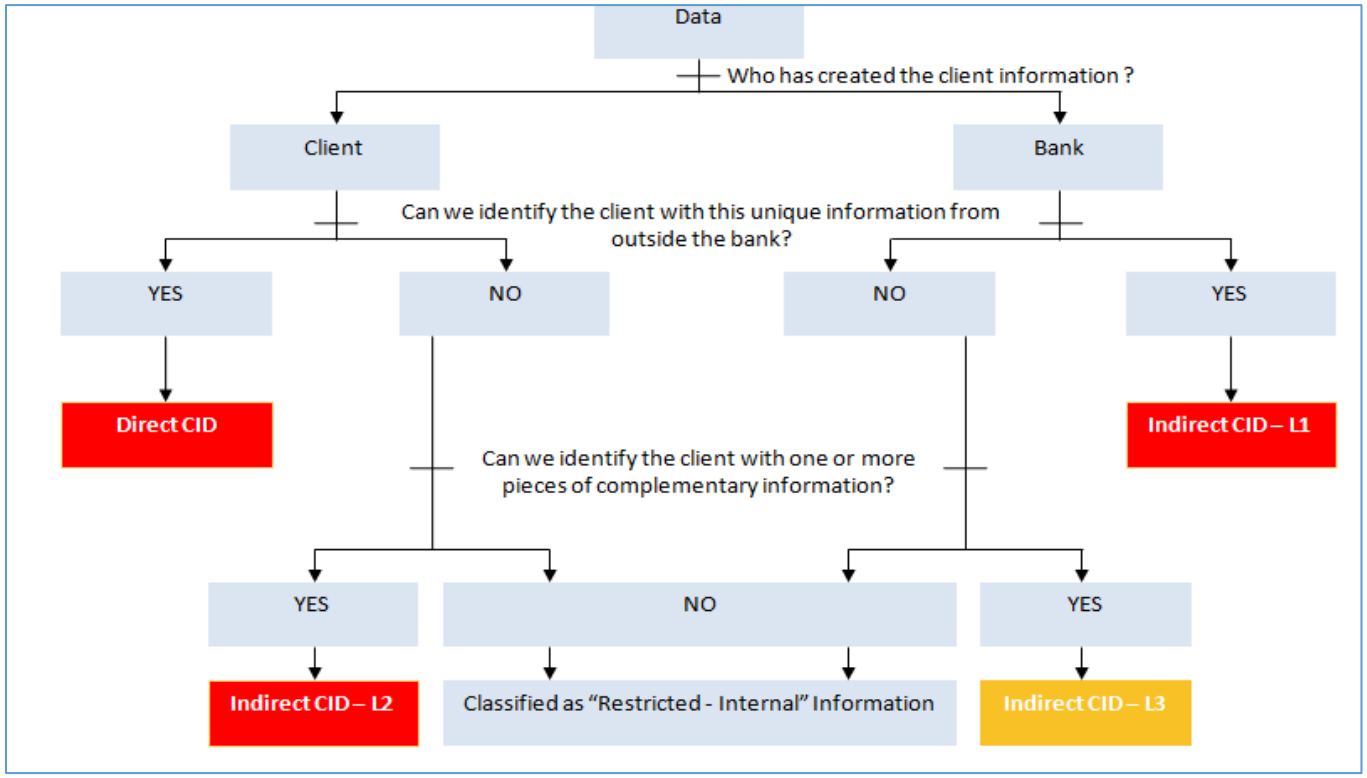
(DCID) = Banking Secrecy Breach

2. Container ID

(L1 ICID) = Banking Secrecy Breach

3. Wealth situation + Nationality

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



Appendix D: Barclays Information Labelling Schema

Table D1: 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 permission. The audience	• 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.

	may include external recipients at the explicit authorisation of the information owner.	• 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 Information. • 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 D2: 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 Supplier 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 Supplier 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 Supplier 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.