CMORG
CROSS MARKET OPERATIONAL
RESILIENCE GROUP

CLOUD CONTROL FRAMEWORK

JULY 2025

TLP CLEAR

CLOUD CONTROL FRAMEWORK (CCF)

SUMMARY

THE PURPOSE (WHAT)

This initiative has been delivered through the CMORG CIO Forum, initially including technical leadership from industry participants. Wider engagement and validation has been conducted through the CMORG CIO Forum and Cyber Coordination Group (CCG), and with the major Cloud Service Providers (CSPs).

The CCF has been aligned to the US Cyber Risk Institute (CRI) Cloud profile, which provides more technical detail and therefore should be used in conjunction with this document. It is anticipated the CCF will evolve to meet future developments in cloud implementation, and alignment will be maintained with other industry frameworks where relevant.

Cloud is recognised as a key strategic enabler for the financial sector. As such, it is essential that finance sector (FS) firms can adopt cloud services with confidence and effectively manage the key risks associated with these solutions. Developing a minimum set of controls to support the active management of these risks, both by firms and CSPs, will enhance consistency for management of the control environment for cloud solutions across the sector. It will also drive capability improvements among less mature firms.

Cloud solutions and deployments bring a different set of risks from managing solutions on an ‘on-premise’ basis. This initiative has been scoped to address a core consideration in the management of cloud risks – dealing with the shared responsibility model, with multiple controls owned by FS firms and CSPs across the different variations of cloud models (infrastructure-as-a-service/IaaS, platform-as-a-service/PaaS, and software-as-a-service/SaaS).

Many FS firms and CSPs have already conducted significant work in this area, which can be leveraged to drive a more consistent approach across the sector, while also recognising that more detailed implementation of controls is likely to vary for each firm and CSP. The ultimate intent of this initiative is to support sector-wide adoption of the CCF and an approach for agreeing responsibility, which would then be aligned to the service arrangements with CSPs.

Finally, it is noted that while this is a UK-based initiative, it has been designed with ‘global in mind’. As highlighted above, key thinking has been developing in collaboration with the CRI in its development of a Cloud Profile to support cross-jurisdictional coherence. This global approach has been reflected in sector engagements with the CSPs.

The approach of defining a baseline control approach across the shared responsibility model will drive consistency and raise standards whilst allowing FS firms and CSPs to utilise existing detailed practices where they have already been developed. The CCF will be complementary to any detailed standards or practices developed through other industry initiatives.

CLOUD CONTROL FRAMEWORK (CCF)

SUMMARY

CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

DESIGN (HOW)

The CCF has 12 sections or control groupings that reflect the areas where appropriate controls are to be applied. There are 86 individual controls. The CCF recognises that across the IaaS, PaaS and SaaS cloud service models, the responsibility for operation of individual controls will vary between the FS firm and CSP. The CCF is designed to apply to both the firm and CSP – requiring appropriate controls to be applied by both parties.

As with any control framework, its value comes from ensuring it is applied consistently and with the right coverage. Given that CSPs already provide substantial reporting, MI and dashboards, there are existing capabilities in place that will be able to support this. However, it is noted that much of that reporting is delivered to customers and therefore will be for the firms to consume and utilise as part of any evidencing of the controls they are responsible for. Where controls are operated by the CSP for services that are not directly visible to the firm, but are essential for the delivery of the service, then closer bilateral engagement between the FS firm and CSP will be required to provide sufficient illustration as to how these controls are being implemented.

The involvement and engagement of the CSPs is essential to delivering the benefits of the CCF. With the shared responsibility model for cloud, FS firms must work alongside CSPs to operate the control environment, and this framework provides a common and consistent basis to do that. In addition to providing a consistent baseline approach, this initiative is also intended as a tool for enabling the CSPs to confirm their adoption and operation of the CCF as part of their broader firm engagement processes. This would be achieved through CSPs committing to operate the CCF for UK FS-regulated firms, rather than for the detail of the CCF to be included in any legal agreements. Such a commitment would be substantive and would support the objectives of this initiative, while also being achievable without material changes to existing contractual arrangements for CSPs.

FS firms and the CSPs will already have their own standards, processes and existing controls, many of which will be relevant to these controls. With 86 controls covering such a broad area, these are worded in a way that provides flexibility as to how the outcomes are achieved. This is an important principle in ensuring ease of adoption, with the reuse of existing practices, processes, standards, and automation wherever possible.

OBJECTIVES (WHY)

- The purpose of the CCF is to **establish a baseline that sets out minimum control standards for financial services FS firms and CSPs, operating across the shared responsibility model inherent to cloud.**
- **These standards will drive improved capability and consistency across the financial sector, while also helping to clarify the key objectives during cloud adoption to firms**. The approach outlined in the CCF is intended to balance a need for granularity, particularly through the definition of specific controls, while also providing sufficient flexibility to allow for existing investments in standards, processes, procedures and automation to be leveraged by firms and CSPs.

EVIDENCING COMPLIANCE

PRINCIPLES AND CONSIDERATIONS

Principles for Approach to Evidencing

- Firms will have existing policies, procedures, standards and processes that will relate to the various controls. These policies may have differing technical standards and levels of assurance, which is appropriate when comparing a small specialist FS firm against a large retail or wholesale firm. It therefore remains at firm discretion how high a threshold they set when executing against individual controls, e.g., Control 1.5 Vetting.
- Firms will already evidence controls through the equivalent of an Enterprise Risk Management Framework. Such a framework is likely to have some controls that are evidenced annually, e.g. a SOC 2 report under Control 7.4, and others that are evidenced more frequently (quarterly or monthly), e.g. Identity Recertification under Control 2.8.
- With increased automation of controls, particularly by the CSPs, more regular evidencing should be possible. The aim is to agree more regular evidencing for appropriate controls with the CSPs and to allow a move away from a traditional annual due diligence assessment (although some elements of that process will still apply).
- Where control exceptions are identified, FS firms will already have procedures and protocols to escalate and report within their own governance and to regulators if required. A key requirement will be that material exceptions arising from the CSPs are reported and escalated to the FS firm clients in the same way that FS firms already have this obligation on any third party outsourcing arrangements.

Specific Considerations for the CSPs

- It is recognised that given the scale of the CSPs, some of the controls (e.g. People), would not apply to all of their staff, but should apply to those staff who may have potential access to FS firm data or systems, e.g. for investigation or critical support functions.
- The CSPs currently provide extensive reporting and evidence through Compliance Portals (static reports) as well as though automated dashboards. Moving to a more frequent evidencing regime may require additional quarterly or monthly reporting to be provided to FS firms alongside clear protocols for material exceptions. It is noted that much of the automated reporting is for the benefits of the clients (the firms) and the controls they are responsible for. Increased visibility and assurance into the controls the CSPs operate to keep the platform secure are a key outcome.
- Thresholds for escalation of material exceptions may need to be defined.

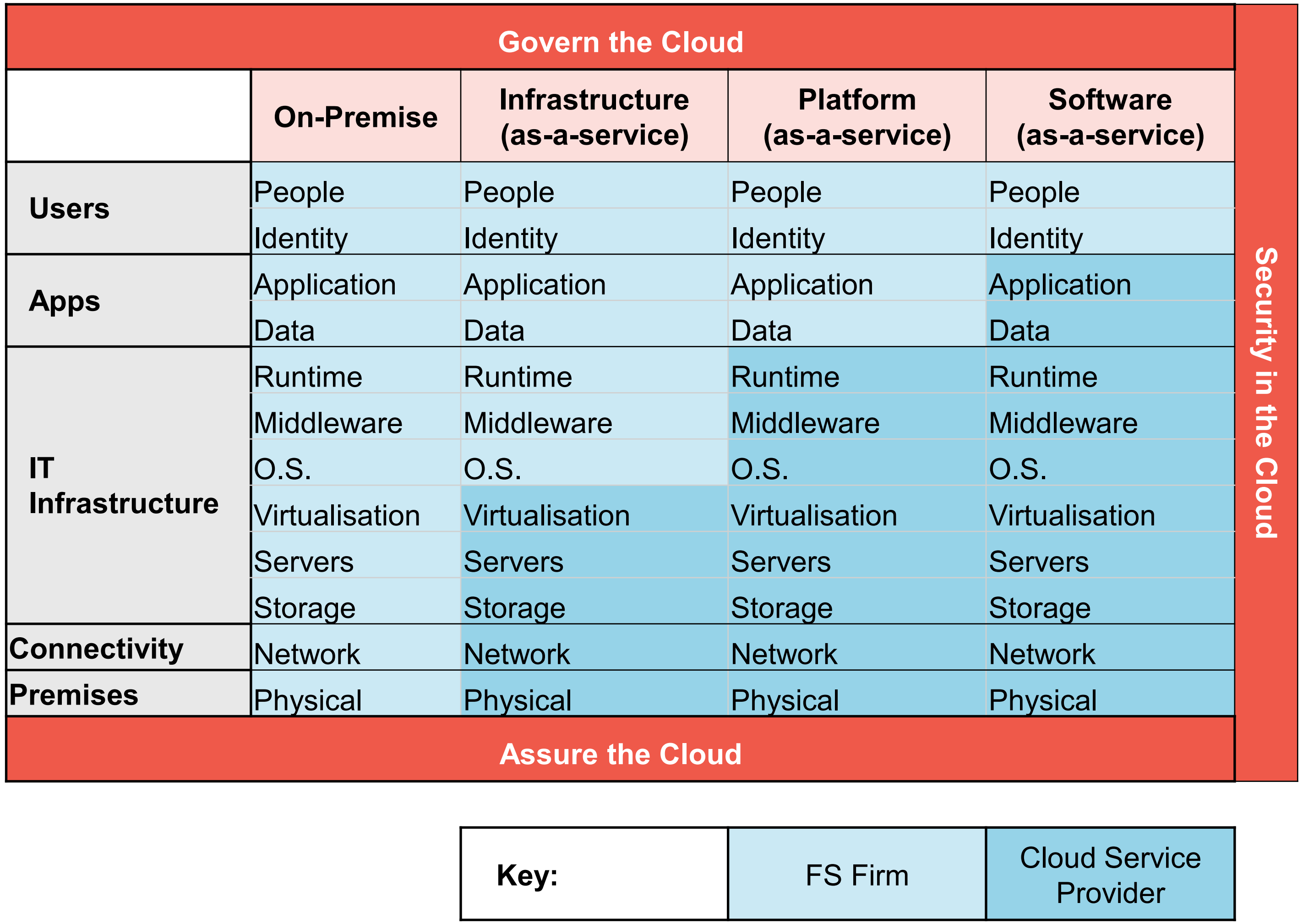
CLOUD CONTROL FRAMEWORK OVERVIEW

KEY CONTROL GROUPS

CMORG CROSS MARKET OPERATIONAL RESILIENCE GROUP

KEY CONTROL GROUPS

1. **People:** Sufficient and appropriately skilled cloud colleagues are in place and monitored, with clear operation and change roles and responsibilities.
2. **Identity and Access Management:** Known people and machines with known, authorised access.
3. **Application Security:** Production and use of robust, safe and secure software.
4. **Data Security:** Protected data to preserve business value and meet regulatory obligations.
5. **Infrastructure Security:** Infrastructure scope understood, secure by design and meeting security standards.
6. **Network Security:** Protecting the underlying network technology and the data it carries.
7. **Physical:** Protection and monitoring of buildings and enclosures holding IT systems.
8. **Change and Config Management:** Change is managed, reviewed and approved, with quality assurance and security vulnerability assessment.
9. **Resilient-by-Design:** Our ability to absorb, respond and recover quickly from a security breach.
10. **IT and Security Operations:** Maintaining visibility of the technology environment and responding to security threat.
11. **Suppliers:** Managing cyber risk of suppliers through selection, contracts and on-going assurance.
12. **Assurance:** Continuous assessment of controls and configurations.



Govern the Cloud

	On-Premise	Infrastructure (as-a-service)	Platform (as-a-service)	Software (as-a-service)
Users	People	People	People	People
	Identity	Identity	Identity	Identity
Apps	Application	Application	Application	Application
	Data	Data	Data	Data
IT Infrastructure	Runtime	Runtime	Runtime	Runtime
	Middleware	Middleware	Middleware	Middleware
	O.S.	O.S.	O.S.	O.S.
	Virtualisation	Virtualisation	Virtualisation	Virtualisation
	Servers	Servers	Servers	Servers
	Storage	Storage	Storage	Storage
Connectivity	Network	Network	Network	Network
Premises	Physical	Physical	Physical	Physical

Assure the Cloud

Security in the Cloud

Key:	FS Firm	Cloud Service Provider

CONTROL GROUPS

GOALS AND OBJECTIVES

#	Grouping	Goal	Control objective
1	People	Sufficient and appropriately skilled cloud colleagues are in place and monitored, with clear operational roles and responsibilities.	People working in and interacting with the organisation will be security aware and skilled in performing their security tasks. We will minimise the impact of any accidental or deliberate actions placing data or systems/assets at risk.
2	Identity and Access Management	People and machines will be positively identified where needed and then will only be given access to data and systems functions for which they have been authorised.	Known people and machines with known, authorised, access.
3	Application Security	Applications, APIs and micro-services are secure by design and security tested, with ongoing update and patching.	Production and use of robust, safe and secure software.
4	Data Security	Data is understood, managed throughout its lifecycle and protected appropriately when stored, processed, or transmitted.	Protected data to preserve business value and meet regulatory obligations.
5	Infrastructure Security	Infrastructure and platform products and services are secure by design, with segregation across all environments and ongoing update and patching.	Infrastructure scope understood, secure by design and meeting security standards.
6	Network Security	Virtual networks and on-premise connectivity are secure by design, with segregation across all environments.	Protecting the underlying network technology and the data it carries.
7	Physical	Buildings, computer systems and their supporting facilities (e.g. alarms, CCTV, Power, HVAC) will be physically protected and monitored.	Protection and monitoring of buildings and enclosures holding IT systems.
8	Change and Config Management	Change is managed, reviewed and approved, with quality assurance and security vulnerability assessments.	Software is engineered securely from the outset, starting with an agreed, then following proven processes to minimise bugs and vulnerabilities.
9	Resilient-by-Design	Platforms and workloads are resilient by design, with business continuity, disaster recovery and incident response plans and proving in place.	We will be able to absorb, detect, respond/contain and initiate recovery at a pace which minimises the impact of the breach.
10	IT and Security Operations	Service and security operation is monitored and managed, with incident and security event detection and resolution.	Maintaining visibility of the technology environment and responding to security threat. Monitoring the security of data and systems and investigating and responding to anomalous behaviours.
11	Suppliers	Cloud provider and third-party service contracts and control positions are understood, assessed and managed.	Managing cyber risk of suppliers through selection, contracts and ongoing assurance. Suppliers should be assessed to a level appropriate to the risk and used only when the security is deemed to be equivalent or better than the organisation would provide for its own managed systems.
12	Assurance	Risks and compliance to organisations policy and standards and regulation is identified and managed.	Gaining confidence that controls are working and correctly configured. Perform continuous assessment of controls and configurations to a degree and frequency appropriate to the risk being managed. This should include active monitoring, testing, reviews and attestations.

CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

APPENDIX

I. CCF CONTROL GROUP DESCRIPTIONS

CONTROL GROUP

PEOPLE

1. People: Sufficient and appropriately cloud skilled colleagues are in place and monitored, with clear operation and change roles and responsibilities		
Control Ref.	**Subject**	**Description of control**
1.1	Operating Model	Document and maintain an up-to-date view of the cloud operating model that provides clear operation and change roles and responsibilities across all in-scope cloud products, services and tooling, including support teams and hours of service. Implement and regularly maintain a Cloud Governance Framework.
1.2	Colleague Capacity	Document and maintain an up-to-date view of cloud skills and capabilities that demonstrates sufficient operation and change capacity is in place, covering all in-scope cloud products, services and tooling, in line with the organisation's policy. Recruitment and/or development plans should be in place for all identified gaps. Identify key cloud IT personnel and implement strategy for succession planning, covering eventualities of replacement. Evaluation of staffing requirements on a regular basis to ensure sufficient human resources are available to support enterprise goals, objectives, processes and controls.
1.3	Colleague Capabilities	Document and maintain an up-to-date view of the organisations cloud skills and capabilities that demonstrates a network of appropriately skilled cloud colleagues are in place, covering all in-scope cloud products, services and tooling, in line with the organisation's policy and security Standards. Development plans should be in place for all identified skills gaps. Conduct regular performance reviews to support development and assess performance goals. Include a process for reward and recognition for attaining performance goals.
1.4	Cloud Training	Ensure that adequate training has been undertaken for the roles with responsibilities for the controls outlined in this framework. Implement verification of cloud competency skills on a periodic basis.
1.5	Vetting	Both the organisation and the cloud supplier staff will be vetted and screened to verify their identity, confirm they have no criminal convictions, and assess them for any signs of financial irresponsibility which could indicate vulnerability to financial inducement. Screening checks should be ongoing and according to local laws, regulations, ethics and contractual constraints, and proportional to the data classification an employee will have access to before joining the organisation. There should be a requirement for employees to sign an employee agreement that covers confidentiality or non-disclosure agreements. Personnel who are given access to confidential information, should sign such an agreement prior to being given access to information and other associated assets.

CONTROL GROUP

IDENTITY AND ACCESS MANAGEMENT

2. Identity and Access Management: People and machines will be positively identified where needed and then will only be given access to data and systems functions for which they have been authorised

Control Ref.	Subject	Description of control
2.1	Identity and Device Inventory	Identify, document and maintain an inventory of all human and non-human identities and devices that allow access to cloud platforms, applications and tooling. Compliance assurance with exception reporting to be reported based on level of risk.
2.2	Identity Provisioning and Management	Review, approve, provision and manage all cloud platform, application and tooling human and non-human identity creation and change requests, ensuring they are identifiable through unique IDs, in line with the organisation’s trust and least-privilege principles, policy and security standards.
2.3	Privileged Identity Provisioning and Management	Review, approve, provision and manage all cloud platform, application and tooling human and non-human privileged identities, with access granted for approved time periods, in line with the organisations trust and least privilege policy, principles, and security standards. Compliance assurance with exception reporting to be reported based on level of risk.
2.4	Access Management	Design and implement identity and access management in line with need to know, least privilege principles and separation of duties. Compliance assurance with exception reporting to be reported based on level of risk.
2.5	Identity Authentication	Design, implement and manage authentication for all cloud platform, application and tooling human and non-human identities, considering multi-factor authentication, password-less authentication, and conditional access policies where appropriate, in line with the organisation’s policy and security standards.
2.6	Device Authentication	Design, implement and manage authentication for all registered devices when accessing the cloud platform, applications and tooling, in line with the organisation’s policy and security standards.
2.7	Identity De-Provisioning Review and Management	Design, implement and manage human and non-human identity de-provisioning, based on regular identity recertification, identity usage reviews and mover/leaver requests for cloud platform, application and tooling, in line with the organisation’s policy and security standards.

CONTROL GROUP

APPLICATION SECURITY

3. Application Security: Applications, APIs and micro-services are secure by design and security tested, with ongoing updates and patching.

Control Ref.	Subject	Description of control
3.1	Application Ownership	Document and maintain application and tooling ownership, in line with the organisation's policy and security standards.
3.2	Application Design and Configuration	Document and maintain security configuration baselines and informed by threat models and identified vulnerabilities.
3.3	API Manager Design and Configuration	Document and maintain Application Programming Interface (API) technical and security designs and configuration, in line with the organisation's policy, security standards, and security configuration baselines, and informed by threat models and identified vulnerabilities.
3.4	API and Micro-service Design and Configuration	Document and maintain all API and micro-service technical and security designs and configuration, in line with the organisation's policy, security standards, and security configuration baselines, and informed by threat models and identified vulnerabilities.
3.5	Application Security Testing	Implement, execute and manage application security testing prior to change deployment, including the identification, prioritisation, and remediation of identified security vulnerabilities based on risk.
3.6	Evergreen Applications and Tooling	Implement and manage application and tooling (including monitoring and security tooling) ongoing currency, updates and patching, enforced and automated where appropriate, and in line with the organisation's policy and security standards.
3.7	Application Components	A framework should be maintained to accurately record the components (inc. Open-Source elements) used to build the various software applications, APIs, micro-services, and underlying cloud platform services"

CONTROL GROUP

DATA SECURITY

4. Data Security: Data is understood, managed throughout its lifecycle, and protected appropriately when stored, processed, or transmitted.

Control Ref.	Subject	Description of control
4.1	Data Inventory	Document and maintain an inventory of critical data based on risk level, in line with the organisations policies and standards.
4.2	Data Ownership and Classification	Document, review and approve the ownership and classification of critical data according to its, confidentiality, integrity and availability and in line with the organisation's policy and security standards.
4.3	Data Lifecycle Management	Create data flow documentation and manage all data throughout the lifecycle, from creation to destruction and ensuring electronic data discovery (eDiscovery), according to its classification and in line with the organisation's policy and security standards.
4.4	Personal Data Processing and Impact Assessment	Review and impact assess all personal data and processing, in line with the organisation's policy and relevant personal data regulation e.g. Data Protection Impact Assessment. This should include sub processing of personal data in the supply chain management. Personal Data breaches should be notified to relevant parties (e.g. regulators, impacted parties) according to applicable laws and regulations (GDPR Article 33 for EEA/UK).
4.5	Data and Secrets Encryption	Implement encryption at-rest and data in use (see DORA article 9) using approved algorithms, functions and protocols, for all data according to its classification and in line with the organisation's policy and security standards.
4.6	Cryptographic Key Inventory Management	Document and maintain all managed cryptographic keys, with registered owners, in line with the organisation's policy and security standards.
4.7	Cryptographic Key Management	Implement, segregate and manage all customer and cloud provider managed cryptographic keys throughout their lifecycle (generation, transmission, retention, usage, renewal, revocation, deletion and compromise), in line with the organisation's policy and security standards.
4.8	Secrets Inventory Management	Document and maintain all customer and cloud provider managed secrets, with registered owners, in line with the organisation's policy and security standards.
4.9	Secrets Management	Manage all organisations managed secrets throughout their lifecycle (generation, transmission, retention, usage, update, deletion and compromise) in line with the organisation's policy and security standards.
4.10	Certificate Management	Implement and manage all organisations certificates throughout their lifecycle (generation, transmission, retention, usage, renewal, revocation, deletion and compromise), in line with the organisation's policy and security standards.
4.11	Data Loss Prevention	Implement and manage Data Loss Prevention (DLP) technologies and policies to monitor endpoints and perimeters, in line with the organisation's policy and security standards.
4.12	Live Data in Test	Use manufactured data in non-production environments, with suitable access control and data masking in place for exceptions where sensitive production data use is required, in line with the organisation's policy and standards.

CONTROL GROUP

INFRASTRUCTURE SECURITY

5. Infrastructure Security: Infrastructure and platform products and services are secure-by-design, with segregation across all environments and ongoing updates and patching.

Control Ref.	Subject	Description of control
5.1	Design and Configuration	Document and maintain all infrastructure and platform product and service technical and security designs and configuration, including the decommissioning of redundant resources, in line with the organisation's policy, security standards, and security configuration baselines, and informed by threat models and identified vulnerabilities. Technical guardrails should be employed wherever possible.
5.2	Segregation and Segmentation	Implement and maintain infrastructure and platform resource segmentation, across all non-production and production environments, in line with the organisation's policy and security standards. Where the service does not offer sufficient segregation, additional logical segregation (e.g. encryption) must be applied.
5.3	Evergreen Infrastructure and Platforms	Implement and manage infrastructure and platform product and service ongoing currency, updates and patching, enforced and automated where appropriate, and in line with the organisation's policy and security standards.

CONTROL GROUP

NETWORK SECURITY

6. Network Security: Virtual networks and on-premise connectivity are secure by design, with segregation across all environments

Control Ref.	Subject	Description of control
6.1	Network Design and Configuration	Document and maintain the virtual network boundary and on-premise connectivity technical and security design and configuration, in line with the organisation's policy, security standards, and security configuration baselines, and informed by threat models and identified vulnerabilities. Intrusion detection should be in place to monitor the network traffic and analyse the signs of possible intrusions, such as exploit attempts and incidents that may be imminent threats to the network.
6.2	Network Segregation and Micro-segmentation	Implement and maintain virtual network segregation and workload micro-segmentation, across all non-production and production environments, in line with the organisation's policy and security standards.
6.3	Boundary / Web Filtering	Implement and manage boundary / web filtering technologies and policies to restrict network ingress, with allowlist review and maintenance, in line with the organisation's policy and security standards.
6.4	DDoS Management	Implement and manage denial of service protection technologies and policies, in line with the organisation's policy and security standards.
6.5	Encryption	All network connections must be encrypted, utilising protocols and algorithms that are up-to-date and approved by the organisation.

CONTROL GROUP

PHYSICAL

7. Physical: Buildings, computer systems and their supporting facilities (e.g. alarms, CCTV, Power, HVAC) will be physically protected and monitored		
Control Ref.	**Subject**	**Description of control**
7.1	User Access	Physical access to information assets and functions by users and support personnel shall be restricted. Policies and procedures must be implemented to ensure this. Individuals must be checked to ensure their access is not excessive or presents a heightened combination risk.
7.2	Controlled Access	Physical security perimeters must be implemented to safeguard sensitive data and information systems. Policies and procedures must be implemented to ensure this.
7.3	Geolocation Policy	Policies and procedures shall be established that ensure data, services and information systems are not located in jurisdictions which are restricted by the organisation.
7.4	Secure Area Authorisation	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.
7.5	Changes	All directly relevant major physical changes (e.g. transfer of hardware or location, destruction of hardware) should be communicated and agreed with the organisation.

CONTROL GROUP

CHANGE AND CONFIGURATION MANAGEMENT

8. Change and Configuration Management: Change is managed, reviewed, and approved, with quality assurance and security vulnerability assessment.

Control Ref.	Subject	Description of control
8.1	Change Lifecycle	Manage all change, including the preparation of new workload hosting, in line with the organisation's policy and the appropriate delivery approach as specified in the organisation’s change approach and security standards.
8.2	Change Governance	Review and approve technology and security design changes in line with the organisation's policy and security standards.
8.3	Change Risk	Implement, execute and manage threat and risk modelling prior to change deployment, including the remediation of identified security vulnerabilities based on risk, automated where appropriate and in line with the organisation's policy and security standards.
8.4	Code Repository and Management	Utilise an approved code repository to store all code, with source code versioning and management in place, in line with the organisation's policy and security standards. Take measures to ensure ongoing integrity of code.
8.5	Code Classification and Ownership	Document and maintain the ownership and classification of all code, according to its type, confidentiality, integrity and availability and in line with the organisation's policy.
8.6	Code Review	Enforce the review and approval of all code change prior to its deployment, with authorised approvers and in line with the organisation's policy and security standards.
8.7	Open Source Code Vulnerability Scanning	Open source code is obtained from trusted and approved sources, with the implementation and execution of open source scanning prior to change deployment, including the remediation of identified security vulnerabilities based on risk, in line with the organisation's policy and security standards.
8.8	Quality Assurance Testing	Implement, execute and manage all functional/non-functional testing throughout the change lifecycle, using automated methods where appropriate and in line with the organisation's policy, change approach, and security standards. Defects should be tracked and resolved prior to production deployment.
8.9	Security Assurance Testing (including Penetration Tests)	For FS managed cloud infrastructure, implement, execute and manage penetration testing, including the remediation of identified security vulnerabilities based on risk, automated where appropriate and in line with the organisation's policy and security standards.
8.10	Change Deployment	Manage all change deployments via approved and automated CI/CD pipelines, with approved change requests and backout plans for production deployments, in line with the organisation's policy and security standards.

CONTROL GROUP

RESILIENT-BY-DESIGN

9. Resilient-by-Design: Platforms and workloads are resilient by design, with business continuity, disaster recovery and incident response plans and proving in place.

Control Ref.	Subject	Description of control
9.1	Resilience Requirements Assessment	Review, document and approve resilience requirements and in line with the organisation's policy and security standards. Define Service Recovery Time Objectives (SRTO) and recovery time objectives (RTO) for IT Systems and applications.
9.2	Resilience/Recovery Design and Configuration	In line with risk profile design, configure, and maintain resilient, highly available and recoverable platforms, applications and tooling. Consider the use of multi-regions and availability zones taking the associated concentration risk and impact on operations into consideration.
9.3	Capacity Management	Design, configure and maintain resource-level and application and tooling capacity, with auto-scaling rules in place where appropriate, and in line with the organisation's policy. Storage alerts should indicate when storage space falls below certain thresholds.
9.4	Data Backup	Identify, implement, and maintain data backups (including cryptographic keys), in line with the organisation's policy and security standards. Have appropriate “offline” or “separated backups” to protect for ransomware scenarios and data corruption. Alerts should indicate when failed backups occur.
9.5	Response and Recovery Planning	Document, approve, and maintain (i) business continuity and (ii) disaster recovery plans, in line with the organisation's policy. Testing and execution of recovery plans should occur at least annually or upon significant change.
9.6	Response and Recovery Proving	Execute (i) business continuity plans, (ii) disaster recovery plans and (iii) incident response exercises, in line with the organisation's policy.
9.7	Portability and Exit Strategy	Review, document and approve a cloud exit (standard and stressed) and portability strategy, in line with the organisation's policy.

CONTROL GROUP

IT AND SECURITY OPERATIONS

10. IT and Security Operations: Service and security operation is monitored and managed, with incident and security event detection and resolution

Control Ref.	Subject	Description of control
10.1	Cloud Resource Inventory	Document and maintain a centralised inventory of all cloud and relevant physical resources, in line with the organisation's policy and security standards.
10.2	Clock Synchronisation	Implement and maintain a reliable time source across all cloud platforms and resources.
10.3	Audit Log Retention	Enable and retain audit logging across all cloud platform components and tooling, including resource, activity, access, network, and security logs, in line with the organisation's policy and security standards.
10.4	Audit Log Security	Manage and protect audit logs from unauthorised access, change and deletion, in line with the organisation's policy and security standards.
10.5	Monitoring and Alerting	Implement and manage monitoring and alerting across all cloud platform components, applications and tooling, automated where appropriate. This should include resource-level health and security, unauthorised access and change, and security events, in line with the organisation's policy and security standards.
10.6	Batch Management	Schedule and manage all batch jobs, with automation and auto-scaling where appropriate, in line with the organisation's policy. Monitor jobs and apply corrective action in case of failure
10.7	Incident Escalation and Notification	Review, manage and recover from all the organisations and supplier IT and security incidents and events, in line with associated service availability requirements, and the organisation's policy and security standards. Root cause analysis should be performed for recurring incidents.
10.8	Anti-Malware Management	Implement, execute and maintain anti-malware scanning technologies and policies to monitor endpoints and perimeters, including the identification, prioritisation, and remediation of identified security vulnerabilities based on risk, in line with the organisations security standards.
10.9	Vulnerability Management	Implement, execute and maintain vulnerability scanning technologies and policies to monitor endpoints, perimeters and change deployment, including the identification, prioritisation, and remediation of identified security vulnerabilities based on risk, in line with the organisation's policy and security standards. If material vulnerability identified that is impacting the FSF then invoke 10.7 above. Interactive-use end points should be configured to require an auto lock screen.
10.10	Digital Forensics	Systems will be designed to enable the collection of evidential forensic data retrieval, in line with external legislation and the organisations requirements.
10.11	Threat Intelligence	Threat intelligence will be monitored and shared bi-directionally between the organisation and CSP for wider analysis, control improvement or incident response. Cross organisation information sharing as well as notification to regulatory bodies where required.
10.12	Cloud Resource Consumption Charging	Implement, monitor and manage resource-level consumption and charging, in line with the organisation's policy.

CONTROL GROUP

SUPPLIERS

11. Suppliers: Cloud provider and third party service contracts and control positions are understood, assessed and managed.

Control Ref.	Subject	Description of control
11.1	Supplier Management	Engage and complete the organisation’s sourcing process if (i) a new cloud supplier and/or third party service requires onboarding and/or (ii) an existing cloud supplier and/or third party service requirements have changed, with the management of any associated risks, in line with the organisation's policy.
11.2	Supply Chain Agreements	The contract with the CSP shall incorporate mutually agreed upon provisions/terms that as a minimum include: roles and responsibilities, SLAs, accountabilities, liabilities and exit policies.
11.3	Geographical Infrastructure	The full service, including infrastructure and applications provisioned specifically for the UK FS organisation and also shared management services, shall be designed, developed, and deployed in accordance with mutually agreed-upon reasonable geographical concentration limits, service and capacity-level expectations, as well as IT governance and service management policies and procedures.
11.4	Supply Chain Management	Policies and procedures must be implemented to ensure that appropriate initial and ongoing due diligence is undertaken by the CSP provider on its own supply chain relationships (third parties, fourth…etc.).
11.5	Right of Audit and Review	The CSP supplier shall ensure the organisation has the right, and access to undertake periodic active security assurance.
11.6	Security Incidents	The CSP will notify the FS customer of any security incidents affecting the confidentiality, integrity or availability of the FS customer’s services or data. Ongoing communication of incidents until resolution must be agreed between CSP and FS customer.
11.7	Industry Accreditations	The CSP shall comply with all reasonable industry standards and provide proof to verify that suitable accreditations are obtained and maintained.
11.8	Concentration Risk	The CSP will inform the UK FS organisation of any areas of known or suspected concentration risk, arising from concentration of their service and/or customers to a single infrastructure component, service, counterparty, sector or country, or where their service is less diverse to provide high-levels of assurance over operational resilience.

CONTROL GROUP

ASSURANCE

12. Assurance: Risks and compliance to organisations policy and standards and regulation is identified and managed.

Control Ref.	Subject	Description of control
12.1	Compliance Assessment	Identify, implement, manage, review and demonstrate compliance to the organisation's policy, standards and all relevant regulatory frameworks, via the use of enforced policies and guardrails as appropriate, in line with the organisation's policy and security standards. Exceptions and risks must be raised and approved where compliance cannot be achieved.
12.2	Cloud Usage and Concentration	Review cloud supplier, product and service usage to identify concentration risk, with updates to a central cloud register for regulator notifications as applicable, in line with the organisation's policy.
12.3	Cloud Risk Assessment and Management	Identify, record and manage delivery and operational risks, and complete the appropriate cloud service risk assessment governance, in line with the organisation's policy.
12.4	Regulatory and Legal Compliance Management	Identify, implement, manage, review and demonstrate regulatory and legal compliance, in line with the organisation's policy and security standards.
12.5	Audit, Control Testing, Governance	All cloud implementations must be subject to regular audit to ensure assurance and insight into the effectiveness and efficiency of cloud controls and cloud risk management processes.