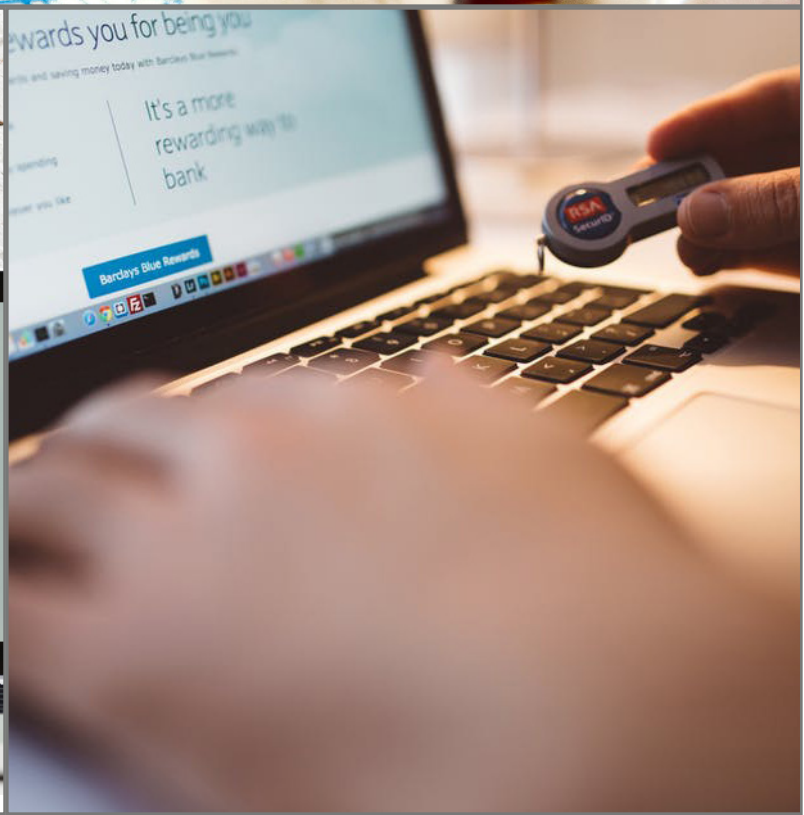
CLOUD STRATEGY



Cloud Strategy Policy

Author	Cyber security
Issue Number	0.1
Issue Date	11/12/2018
Document ID	CYB-EX-STD-029-Cloud Strategy - 01
Security Classification	OFFICIAL
Review Date	Draft+1year

Contents

1 Overview

Cloud Strategy is a critical aspect of the organisation's information security, as we increasingly move towards hosted solutions. It is vital that the surrounding security wrappers are cohesive, comprehensive and appropriate to protect the organisation's information assets.

2 Purpose

This document defines the requirements for the organisation's administrators to follow in order that essential systems hosted in the 'cloud 'are brought into service with appropriate respect to security. gaining access to information they are not authorised to see

3 Scope

This policy applies to all projects and managers looking to outsource to cloud service providers or to take advantage of applications available through cloud connectivity.

4 Applicability

This policy applies to all ICT devices used to store, process or communicate the organisations information. No device should be used for these purposes without being configured by an authorised administrator and tested for compliance with appropriate guidance. Cloud Strategy is particularly applicable to ICT system administrators who are responsible for the creation, management and termination of device use. The policy is furthermore applicable to managers and stakeholders including information asset owners for the assurance it renders.

Disclaimer

This policy is a draft document that has been provided to relevant personnel for information, to assess compliance with an initial set of requirements and to solicit feedback during the Policy Compliance & Controls Assessment GRA pilot scheme. An uplifted final version will be delivered following the completion of the GRA pilot schemes.

5 Cloud Strategy Policy

This policy is written to ensure that the following outcomes to meet Cyber Security Principles are addressed:

- Systems are built to defend themselves from compromise.
- Data Loss is minimised.
- Unauthorised access to information assets is minimised.
- Inappropriate applications are not operated on devices containing sensitive information assets.
- Malicious software is not promulgated.

5.1 Data In Transit

Policy ID	Policy Requirement
5.1.1	User data transiting networks should be adequately protected against tampering and eavesdropping. *This should be achieved through a combination of:* • network protection - denying your attacker the ability to intercept data' • encryption - denying your attacker the ability to read data.
5.1.2	Encryption of data in transit shall be through implementing TLS 1.2 or TLS 1.3 .

5.2 Data at Rest

Policy ID	Policy Requirement
5.2.1	User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.
5.2.2	Service providers shall present detailed information on all locations where data is stored and processed and where they manage the service from.
5.2.3	The service provider shall present information on the security controls around their (or their suppliers') data centres.
5.2.4	The service provider should confirm that their data centre protections are certified against a recognised and appropriate standard that covers physical security. Appropriate standards include: CSA CCM v3.0 or SSAE-16 / ISAE 3402.
5.2.5	The service provider should confirm that their data centres meet the Uptime criteria for Tier 3, with redundant and dual-powered servers, storage, network links and other IT components. are powered with multiple, active and independent sources of power and cooling resources.

5.2.6	The service provider should state that their scale, obfuscation techniques, or data storage 'sharding' make it infeasible for a determined attacker with physical access to a data centre to locate a specific customer's data.
5.2.7	The service provider should employ a recognised standard (256-bit AES encryption (Advance Encryption Standard)) of encryption to ensure that no data is written to disk in an unencrypted form.
5.2.8	The service provider shall confirm their policy that storage which is no longer required is sanitised according to a specified procedure, detailed in their confirmation, before being reallocated to another user.
5.2.9	The service provider shall confirm their policy that a third-party, preferably HMG approved, destruction service which specialises in secure disposal of equipment is used.

5.3 Separation of Users

Policy ID	Policy Requirement
5.3.1	The service provider should use well-designed virtualisation technologies to provide separation.
5.3.2	The service provider should utilise "compute separation" provided by a hypervisor. Network and storage virtualisation techniques are also to be employed.
5.3.3	Where other software controls, such as operating systems, web servers or other applications, provide separation between users of the service, the service provider shall provide evidence of • regular penetration tests of infrastructure and any relevant web applications. • security reviews of the design of the service. • an engineering approach that ensures security is a key consideration in developing the service.
5.3.4	The service provider should allow an independent review of the scope of a penetration test, and review of the mitigations it identified, to give a higher degree of confidence that penetration testing successfully achieved the objectives set out above.

5.4

Policy ID	Policy Requirement
5.4.1	The service provider shall provide evidence of a security governance framework which coordinates and directs its management of the service and information within it.
5.4.2	The service provider should present a clear structure (diagram) identifying a named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer'.

5.4.3	The service provider should present a documented framework for security governance, with policies governing key aspects of information security relevant to the service.
5.4.4	Security and information security should be part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk.
5.4.5	The service provider should present processes to identify and ensure compliance with applicable legal and regulatory requirements.

5.5 Operational Security

Policy ID	Policy Requirement
5.5.1	The service provider shall present evidence of configuration change control including test, acceptance and risk measurement of changes.
5.5.2	The service provider shall present evidence of vulnerability management and should have processes in place to identify, triage and mitigate vulnerabilities.
5.5.3	The service provider shall declare its processes to: • Assess potential new threats, vulnerabilities or exploitation techniques which could affect service and take corrective action (software updates/patching etc.). • Monitor relevant sources of information relating to threat, vulnerability and exploitation techniques. • Consider the severity of threats and vulnerabilities within the context of the service and use this information to prioritise the implementation of mitigations. • Use a suitable change management process to track known vulnerabilities until mitigations have been deployed. • Address the above in a timely fashion.
5.5.4	The service provider shall declare its policy on protective monitoring and as a minimum: • The service generates adequate audit events to support effective identification of suspicious activity. • These events are analysed to identify potential compromises or inappropriate use of your service. • The service provider takes prompt and appropriate action to address incidents.
5.5.5	The service provider shall declare its policy on incident handling and as a minimum: • Incident management processes are in place for the service and are actively deployed in response to security incidents. • Pre-defined processes are in place for responding to common types of incident and attack.

	• A defined process and contact route exists for reporting of security incidents by consumers and external entities. • Security incidents of relevance to you will be reported in acceptable timescales and formats.
5.5.6	The service provider should be invited to substantiate the above minimum requirements with certification to a recognised, audited standard such as ISO/IEC 27001:2013.

5.6 Personnel Security

Policy ID	Policy Requirement
5.6.1	The service provider shall confirm that it carries out background checks on its personnel and personnel screening is in place which includes or exceeds the requirements of BS7858:2012.
5.6.2	The service provider shall confirm that access control is in place which ensures anyone accessing the organisation's data or the platform on which it is stored, are strongly authenticated.

5.7 Secure Development

Policy ID	Policy Requirement
5.7.1	The service provider shall confirm that new and evolving threats are reviewed and the service improved in line with them.
5.7.2	The service provider shall confirm that development is carried out in line with industry good practice regarding secure design, coding, testing and deployment.
5.7.3	The service provider shall confirm that configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.
5.7.4	The service provider should confirm the number of security standards with supporting certification mechanisms which exist and could be used to demonstrate conformance with the goals outlined above. These include: • CESG CPA Build Standard • ISO/IEC 27034 • ISO/IEC 27001 • CSA CCM v3.0

5.8 Supply Chain Security

Policy ID	Policy Requirement
5.8.1	The service provider should clearly state how information, that is their responsibility to store on behalf of the organisation, is shared with, or accessible to, third party suppliers and *their* supply chains.
5.8.2	The service provider should clearly state how they manage security risks from third party suppliers.

5.8.3	The service provider should clearly state how their procurement processes places security requirements on third party suppliers.
5.8.4	The service provider should clearly state how they manages the conformance of their suppliers with security requirements.
5.8.5	The service provider should clearly state how they verify that hardware and software used in the service is genuine and has not been tampered with.
5.8.6	Security controls should be implemented in the supply chain through the application of a relevant standard with supporting certification such as ISO/IEC 27001 or ISO/PAS 28000:2007
5.8.7	Where cloud services are layered - built on top of third party IaaS or PaaS products, the service shall identify all parties including relative responsibilities for implementing which security functions. This should form part of a cohesive communications and incident management plan.

5.9 Secure User Management

Policy ID	Policy Requirement
5.9.1	Service providers should set out the mechanisms in place to ensure that management requests which could have a security impact are performed over secure and authenticated channels. only authorised individuals from your organisation can use those mechanisms to affect your use of the service.
5.9.2	Service providers shall put in place mechanisms to ensure approved, named members of the organisation can make requests for management reports/investigations etc. but that these shall all use secure authentication and be recorded.
5.9.3	The service provider should have sufficient controls in place to ensure that only authorised users from your organisation can affect your account via support channels and can demonstrate that they regularly test their security via these channels (e.g. through using social engineering techniques), and the tests are documented.

5.10 Identity and Authentication

Policy ID	Policy Requirement
5.10.1	Service providers shall demonstrate that access to service interfaces (web applications and APIs) should be constrained to authenticated and authorised individuals.
5.10.2	There shall be no evidence of weak authentication mechanisms to these interfaces that could enable unauthorised access to information assets, resulting in the theft or modification of data, changes to service, or a denial of service.

5.10.3	The service provider should ensure the service supports authentication over TLS using an X.509v3 client certificate that identifies an individual user and employs strong encryption.
5.10.4	The service provider should demonstrate that key management is secure, particularly addresses concern regarding: • creation and management of certificates. • safeguards in place on end user devices. • protection against theft of client certificates. • malware. • additional factor of authentication. • Processes to revoke lost or compromised credentials.
5.10.5	The service provider should support federating to another authentication scheme, such as a corporate directory, an OAuth or SAML provider.
5.10.6	Multi-Factor authentication shall be supported as well as strong password enforcement.

5.11 External Interface Protection

Policy ID	Policy Requirement
5.11.1	Services providers shall provide evidence they protect data by limiting an attacker's opportunity to connect. This can be done by only providing the service to a limited set of networks, locations or devices.
5.11.2	Cloud services wherever possible should be accessible via a community network (with other levels of protection) such as the Public Sector Network.

5.12 Secure Service Administration

Policy ID	Policy Requirement
5.12.1	The service provider should provide a clear description of the service administration model (dedicated, shared, private) it has selected demonstrate that the model chosen is appropriate to its client organisations.
5.12.2	The service provider should provide a risk assessment where potential threat actors are considered which include all those operands in the selected service model.

5.13 Audit Information for Users

Policy ID	Policy Requirement
5.13.1	The service provider shall clearly describe the audit information that will be provided as well as how and when it will be made available, the format of the data, and the retention period associated with it.
5.13.2	The service provider shall demonstrate that the audit information available will meet the needs for investigating misuse or incidents.

5.13.3	The service provider should make specific audit data available to users. The timetable, method, format and retention period of the data is specified.
5.13.4	For IaaS and PaaS services, the service provider or a third party should offer value-add protective monitoring services and these should be tailored to legal requirements such as keeping the original data for forensic and prosecution purposes, and retention of data for periods legally binding – financial, contractual, personal.

5.14 Secure Use of the Service

Policy ID	Policy Requirement
5.14.1	The service provider must discuss with the organisation the correct usage of the system and the requirements expected of the organisation's users and administrators.
5.14.2	The service provider should provide Standard Operating Procedures (SOP) and where applicable Security Operating Procedures (SyOPs).