Using AWS in the context of UK Healthcare IG SoC process

May 2016

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Table of Contents

Abstract

This whitepaper is intended to assist organisations using Amazon Web Services (AWS) for United Kingdom (UK) National Health Service (NHS) workloads. UK's Department of Health sponsors the Health and Social Care Information Centre (HSCIC) to provide information, data and IT systems for commissioners, analysts and clinicians in health and social care. As part of this role, HSCIC publishes guidance and requirements on Information Governance (IG). IG Statement of Compliance (IG SoC) is a process by which organisations enter into an agreement with HSCIC for access to HSCIC's services, including the NHS National Network (N3), in order to preserve the integrity of those services. Currently, AWS does not directly access services provided by HSCIC including the NHS N3. However, AWS Partners or customers may have or require access to HSCIC services and hence, require them to comply with the IG SoC process. This document aims to help the reader understand:

- The role that the customer and/or partner and AWS play in ownership, management and security of the content stored on AWS
- A reference architecture that demonstrates shared responsibility model to meet IG SoC requirements
- How AWS aligns with each of the 17 requirements for a Commercial Third Party within HSCIC's IG Toolkit requirements

Introduction

All organisations that wish to use HSCIC services, including the N3 network, must complete the IG SoC process. The IG SoC process set out a range of security related requirements that must be satisfied in order for an organisation to provide assurances with respect to safeguarding the N3 network and information assets that may be accessed.

The IG Toolkit is part of the IG SoC process, in that organisations must carry out an annual assessment, evidence their compliance with the requirements and accept the IG Assurance Statement, which confirms the organisation's commitment to meeting and maintaining the required standards of information governance.

For organisations that need to complete the IG SoC process, a 3-step process must be followed as described on the 'IG SoC for Non-NHS Organisations' website. Key steps of this process are described below:

Step 1

- Complete and submit the application form, which includes details of an NHS sponsor.

Additional documentation: Logical Connection Architecture (only if you are connecting DIRECTLY to N3), Offshoring policy and ISMS document.

Step 2

- Review the IG Toolkit assessment for the organisation-type.
- Complete and publish the IG Toolkit assessment annually.

Step 3

- 'Authority to Proceed' notification provided through British Telecom (BT) N3 team.
- BT N3 team will contact applicant to proceed.

Government Security Classifications in context of UK Healthcare workloads

Under the UK Government Security Classifications, HM Government information assets can be classified into three types: OFFICIAL, SECRET and TOP SECRET. Each classification attracts a baseline set of security controls providing appropriate protection against typical threats. AWS customers and partners will be required to follow the HSCIC guidance when managing information assets, which may or may not include patient data. HSCIC offers guidance on looking after information according to the principles of good Information Governance.

Cloud Security Principles and IG SoC

For UK government organisations to use cloud services for OFFICIAL-marked systems, CESG Cloud Security Guidance includes a risk management approach to using cloud services, a summary of the Cloud Security Principles, and guidance on implementation of the Cloud Security Principles.

Our Cloud Security Principles whitepaper provides guidance on how AWS aligns with Cloud Security Principles and the objectives of the principles as part of CESG's Cloud Security Guidance.

For our customers and partners using AWS for UK healthcare information assets marked as OFFICIAL, we have mapped each IG SoC requirement with the appropriate Cloud Security Principle in this whitepaper. For architectures managing OFFICIAL-marked information assets and for more information on using AWS in the context of Cloud Security Principles, we recommend referring to our Cloud Security Principles whitepaper.

G-Cloud framework and GOV.UK Digital Marketplace

The G-Cloud framework is a compliant route to market for UK public sector organisations to source commoditised cloud-based IT services on a direct award basis. The framework supports a more time and cost effective procurement process for buyers and suppliers. The UK Digital Marketplace lists related security questions based on the Cloud Security Principles, and responses for 12 AWS services. These services are listed below, with links to service description and digital marketplace:

1	Amazon Elastic Compute Cloud (Amazon EC2)	Digital Marketplace link
2	Auto Scaling	Digital Marketplace link
3	Elastic Load Balancing	Digital Marketplace link
4	Amazon Virtual Private Cloud (Amazon VPC)	Digital Marketplace link
5	AWS Direct Connect	Digital Marketplace link
6	Amazon Simple Storage Service (Amazon S3)	Digital Marketplace link
7	Amazon Glacier	Digital Marketplace link

8	Amazon Elastic Block Store (Amazon EBS)	Digital Marketplace link
9	Amazon Relational Database Service (Amazon RDS)	Digital Marketplace link
10	AWS Identity and Access Management (IAM)	Digital Marketplace link
11	Amazon CloudWatch	Digital Marketplace link
12	AWS Enterprise Support	Digital Marketplace link

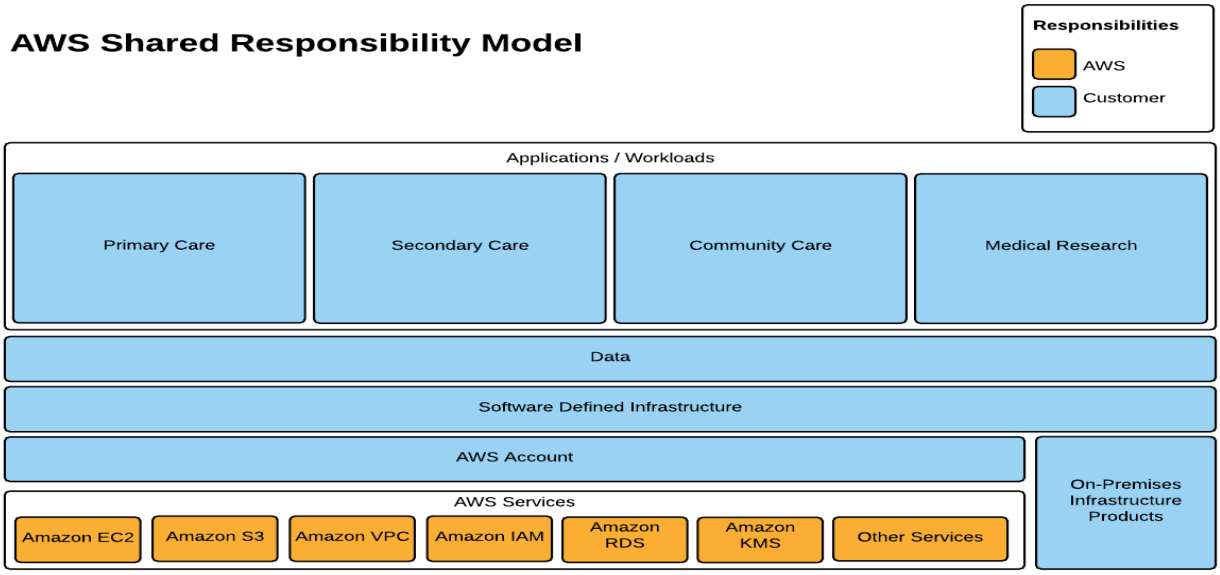
Shared Responsibility Environment

When using AWS services, customers maintain complete control over their content and are responsible for managing critical content security requirements, including:

- What content they choose to store on AWS
- Which AWS services are used with the content
- In what country that content is stored
- The format and structure of that content and whether it is masked, anonymised or encrypted
- Who has access to that content and how those access rights are granted, managed and revoked.

Because AWS customers retain control over their data, they also retain responsibilities relating to that content as part of the AWS "shared responsibility" model. This shared responsibility model is fundamental to understanding the respective roles of the customer and AWS in the context of the Cloud Security Principles.

Under the shared responsibility model, AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. In turn, customers assume responsibility for and management of their operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS-provided security group firewall. Customers should carefully consider the services they choose, as their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations. It is possible to enhance security and/or meet more stringent compliance requirements by leveraging technology such as host-based firewalls, host-based intrusion detection/ prevention, and encryption. AWS provides tools and information to assist customers in their efforts to account for and validate that controls are operating effectively in their extended IT environment. More information can be found on the AWS Compliance center at http://aws.amazon.com/compliance.



IG Toolkit requirements for a Commercial Third Party Version 13

IG Toolkit is a Department of Health (DH) policy delivery vehicle that the HSCIC develops and maintains. It combines the legal rules and central guidance set out by DH policy and presents them in a single standard of information governance requirements. The organisations in scope of this process are required to carry out self-assessments of their compliance against the IG requirements. For Commercial Third Party organisations, the IG Toolkit lists 17 requirements that these organisations must assess within three requirement initiatives – Information Governance Management, Confidentiality and Data Protection Assurance, and Information Security Assurance.

Details on the 17 requirements from the IG Toolkit and how AWS aligns with these requirements with the related assurance approach are described below, with two notes:

- AWS customers and partners providing services to HSCIC should meet and maintain each individual requirement described below using their designated IG responsible staff under the Shared Responsibility Model. The use of AWS and the AWS approach described below does not satisfy their responsibilities for the requirement in its entirety.
- IG Toolkit requirements and the IG SoC process are subject to revision. AWS will attempt to update the guidance in this document to reflect these changes in due course following the revision, but customers should review the HSCIC guidance to confirm applicability.

Information Governance Management

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-114 Requirement Details Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff.	It is important that there is a consistent approach to information handling within the organisation which is in line with the law, central policy, contractual terms and conditions and best practice guidance. This requires one or more members of staff to be assigned clear responsibility for driving any required improvements.	Customers building systems connecting to HSCIC services or N3 network are required to assign Information Governance responsibility to an appropriate member, or members, of staff. AWS has an established information security organization managed by the AWS Security team and is led by the AWS Chief Information Security Officer (CISO). AWS Security establishes and maintains formal policies and procedures to delineate the minimum standards for logical access on the AWS platform and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. The implementation of this requirement is validated independently in ISO 27001, PCI-DSS and SOC certifications.	**Principle 4: Governance Framework**
Requirement 13-115 Requirement Details There is an information governance policy that addresses the overall requirements of information governance.	There is a need to ensure that everyone working for or on behalf of the organisation (including temps, volunteers, locums and students) is aware of the organisation's overall approach to IG and where underpinning procedures and processes can be found. This can be achieved by developing an Information Governance policy.	Information security and governance policies are approved and communicated across AWS to ensure the implementation of appropriate security measures across the environment. The implementation of this requirement is validated independently in ISO 27001, PCI-DSS and SOC certifications.	**Principle 4: Governance Framework**

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-116 Requirement Details All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities.	One of the ways in which an organisation can ensure it fulfills its legal and other responsibilities regarding confidential information is to ensure that all staff members (including temps, locums, students and volunteers) are fully informed of their own obligations to comply with information governance requirements.	All personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Additionally, upon hire, personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy.	**Principle 6: Personnel Security**
Requirement 13-117 Requirement Details All staff members are provided with appropriate training on information governance requirements.	To maintain information handling standards in the organisation staff should be provided with appropriate training on information governance.	AWS customers and partners providing services to HSCIC should meet and maintain this staff training requirement using their designated IG responsible staff under the Shared Responsibility Model. All personnel supporting AWS systems and devices must sign a non-disclosure agreement prior to being granted access. Additionally, upon hire, personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy. AWS maintains employee training programs to promote awareness of AWS information security requirements.	**Principle 6: Personnel Security**

Confidentiality and Data Protection

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-202 Requirement Details Confidential personal information is only shared and used in a lawful manner and objections to the disclosure or use of this information are appropriately respected.	The Data Protection Act 1998 provides conditions that must be met when processing personal information. In addition, where personal information is held in confidence (e.g. details of care and treatment), the common law requires the consent of the individual concerned or some other legal basis before it is used and shared. Staff must be made aware of the right of an individual to restrict how confidential personal information is disclosed and the processes that they need to follow to ensure this right is respected.	AWS does not access any customer's content except as necessary to provide that customer with the AWS services it has selected. AWS does not access customers' content for any other purposes. AWS does not know what content customers choose to store on AWS and cannot distinguish between personal data and other content, so AWS treats all customer content the same (Source: EU Data Protection Whitepaper). The Standard Contractual Clauses (also known as "model clauses") are a set of standard provisions defined and approved by the European Commission that can be used to enable personal data to be transferred in a compliant way by a data controller to a data processor outside the European Economic Area. The Article 29 Working Party has approved the AWS Data Processing Agreement which includes the Model Clauses. The Article 29 Working Party has found that the AWS Data Processing Agreement meets the requirements of the Directive with respect to Model Clauses. This means that the AWS Data Processing Agreement is not considered "ad hoc". In addition to this, alignment with ISO 27018 demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content. AWS' alignment with and independent third-party assessment of this internationally recognized code of practice demonstrates AWS' commitment to the privacy and protection of customers' content. Further information can be found at: https://aws.amazon.com/compliance/eu-data-protection/ https://aws.amazon.com/compliance/iso-27018-faqs/ https://aws.amazon.com/compliance/amazon-information-requests/	**Principle 9: Secure consumer management**

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-206 Requirement Details Staff access to confidential personal information is monitored and audited. Where care records are held electronically, audit trail details about access to a record can be made available to the individual concerned on request. Organisations should ensure that access to confidential personal information is monitored and audited locally and in particular ensure that there are agreed procedures for investigating confidentiality events.	Organisations should ensure that access to confidential personal information is monitored and audited locally and in particular ensure that there are agreed procedures for investigating confidentiality events.	AWS customers and partners looking to access and protect confidential personal information have a great deal of flexibility in how they meet the data protection requirements. AWS CloudTrail is a service that provides audit records for AWS customers and delivers audit information in the form of log files to a specified storage bucket. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. CloudTrail provides a history of AWS API calls for customer accounts, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing. The log file objects written to S3 are granted full control to the bucket owner. The bucket owner thus has full control over whether to share the logs with anyone else. This feature provides confidence and enables AWS customers to meet their needs for investigating service misuse or incidents. More details on AWS CloudTrail and further information on audit records can be requested at http://aws.amazon.com/cloudtrail. A latest version of CloudTrail User Guide is available at: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html	**Principle 13: Audit information provision to consumers**

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-209 Requirement Details All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines.	Organisations are responsible for the security and confidentiality of personal information they process. Processing may include the transfer of that information to countries outside of the UK, and where person identifiable information is transferred, organisations must comply with both the Data Protection Act 1998 and the Department of Health guidelines.	AWS customers and partners providing services to HSCIC should meet and maintain compliance with Data Protection Act 1998 and Department of Health guidelines using their designated IG responsible staff under the Shared Responsibility Model. AWS customers and partners are in control of which AWS Region their data is stored. For compliance guidance on Data Protection Act and the EU Directive, we recommend our EU Data Protection Whitepaper that describes the various considerations and obligations against the data protection principles.	**Principle 9: Secure consumer management**

Requirement 13-210 Requirement Details All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements.	Organisations should ensure that when new processes, services, systems and other information assets are introduced that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements. For best effect, requirements to ensure information security, confidentiality and data protection and information quality should be identified and agreed prior to the design, development and/or implementation of a new process or system.	AWS is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. Protecting this infrastructure is AWS's number one priority. AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form. AWS' development process follows secure software development best practices, which include formal design reviews by the AWS Security Team, threat modeling, and completion of a risk assessment. Static code analysis tools are run as a part of the standard build process, and all deployed software undergoes recurring penetration testing performed by carefully selected industry experts. Our security risk assessment reviews begin during the design phase and the engagement lasts through launch to ongoing operations.	**Principle 9: Secure consumer management**

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-211 Requirement Details All transfers of personal and sensitive information are conducted in a secure and confidential manner.	There is a need to ensure that all transfers of personal and sensitive information (correspondence, faxes, email, telephone messages, transfer of patient records and other communications containing personal or sensitive information) are conducted in a secure and confidential manner. This is to ensure that information is not disclosed inappropriately, either by accident or design, whilst it is being transferred or communicated to, within or outside of the organisation.	AWS customers and partners looking to access and protect confidential personal information have a great deal of flexibility in how they meet the data protection requirements. Customers have a number of options to encrypt their content when using the services, including using AWS encryption features, managing their own encryption keys, or using a third-party encryption mechanism of their own choice. AWS does not access or use customer content for any purpose other than as legally required and to provide the AWS services selected by each customer, to that customer and its end users. AWS never uses customer content or derives information from it for other purposes such as marketing or advertising. AWS offers a comprehensive set of data protection and confidentiality features and services using key management and encryption easy to manage and simpler to audit, including the AWS Key Management Service (AWS KMS). More details on AWS KMS and further information can be requested at http://aws.amazon.com/kms. A latest version of KMS Developer Guide is available at http://docs.aws.amazon.com/kms/latest/developerguide/overview.html.	**Principle 13: Audit information provision to consumers**

Information Security

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-305 Requirement Details Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems.	Organisations should control access to Information Assets and systems by ensuring that system functionality is configured to support user access controls and by further ensuring that formal procedures are in place to control the allocation of access rights to local information systems and services. These procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given to managing access rights which allow support staff to override system controls.	AWS customers and partners providing services to HSCIC should support appropriate access control functionality using their designated IG responsible staff under the Shared Responsibility Model. AWS Identity and Access Management (IAM) provides customers with controls and features to provide confidence that authenticated and authorised users have access to specified services and interfaces. AWS IAM allows the creation of multiple users and the ability to manage the permissions for each of these users within your AWS Account. A user is an identity (within an AWS Account) with unique security credentials that can be used to access AWS. AWS IAM eliminates the need to share passwords or keys, and makes it easy to enable or disable a user's access as appropriate. AWS IAM enables implementation of security best practices, such as least privileged, by granting unique credentials to every user within an AWS Account and only granting permission to access the AWS services and resources required for the users to perform their jobs. AWS IAM is secure by default; new users have no access to AWS until permissions are explicitly granted.	**Principle 9.1: Authentication of consumers to management interfaces and within support channels**

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-313 <u>Requirement Details</u> Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely.	The objective of this requirement is to ensure there is appropriate protection for systems hosted and information communicated over local networks, and for the protection of the supporting infrastructure components (including wireless networks).	AWS customers and partners providing services to HSCIC should implement policies and procedures to operate the ICT networks securely using their designated IG responsible staff under the Shared Responsibility Model. AWS uses various technologies to enable data in transit protection between the consumer and a service, within each service and between the services. Cloud infrastructure and applications often communicate over public links, such as the Internet, so it is important to protect data in transit when you run applications in the cloud. This involves protecting network traffic between clients and servers, and network traffic between servers. The AWS network provides protection against network attacks. Procedures and mechanisms are in place to appropriately restrict unauthorized internal and external access to data, and access to customer data is appropriately segregated from other customers.	**Principle 1: Data in Transit Protection**

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-314 Requirement Details Policy and procedures ensure that mobile computing and teleworking are secure.	Mobile computing and teleworking pose a substantial risk. For example, devices may be lost, damaged, or stolen, potentially resulting in the loss or inappropriate disclosure of data. The information security protection measures required should be commensurate with the risks presented by these working arrangements.	Helping to protect the confidentiality, integrity, and availability of our customers' systems and data is of the utmost importance to AWS, as is maintaining customer trust and confidence. AWS uses techniques described in industry-accepted standards to ensure that data is erased when resources are moved or re-provisioned, when they leave the service or when you request it to be erased. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.	**Principle 2: Asset Protection and Resilience**

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-316 Requirement Details There is an information asset register that includes all key information, software, hardware and services.	The objective is to account for information assets containing patient/service user information to ensure that in the event of damage, destruction or loss, there is awareness of what information is affected and, in the case of loss, whether the information held on the asset is protected from unauthorised access.	AWS applies a systematic approach to managing change so that changes to customer impacting services are reviewed, tested, approved and well communicated. Change management (CM) processes are based on Amazon change management guidelines and tailored to the specifics of each AWS service. These processes are documented and communicated to the necessary personnel by service team management. The goal of AWS' change management process is to prevent unintended service disruptions and maintain the integrity of service to the customer. Change details are documented in Amazon's CM workflow tool or another change management or deployment tool.	**Principle 5: Operational Security**

Requirement 13-317 Requirement Details Unauthorised access to the premises, equipment, records and other assets is prevented.	It is important to ensure that the organisation's assets, premises, equipment, records and other assets including staff are protected by physical security measures.	AWS customers and partners providing services to HSCIC should implement controls to prevent unauthorized access to premises, equipment, records and other assets using their designated IG responsible staff under the Shared Responsibility Model. Amazon has significant experience in securing, designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS provides data center physical access to approved employees and contractors who have a legitimate business need for such privileges. All individuals are required to present identification and are signed in. Visitors are escorted by authorised staff. When an employee or contractor no longer requires these privileges, his or her access is promptly revoked, even if he or she continues to be an employee of Amazon or AWS. In addition, access is automatically revoked when an employee's record is terminated in Amazon's HR system.	**Principle 2: Asset Protection and Resilience**

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-319 Requirement Details There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions.	In the event of a security failure or a disaster, natural, accidental or deliberate, vital business processes still need to be carried out. Having documented business continuity plans and procedures assists this process enabling all staff to know what they need to do in the event of a security failure or disaster.	The AWS Resiliency program encompasses the processes and procedures by which AWS identifies, responds to and recovers from a major event or incident within our environment. This program aims to provide you sufficient confidence that your business needs for availability commitment of the service including the ability to recover from outages are met. This program builds upon the traditional approach of addressing contingency management which incorporates elements of business continuity and disaster recovery plans and expands this to consider critical elements of proactive risk mitigation strategies such as engineering physically separate Availability Zones (AZs) and continuous infrastructure capacity planning. AWS contingency plans and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. Plans are tested and updated through the due course of business (at least monthly) and the AWS Resiliency plan is reviewed and approved by senior leadership annually.	**Principle 2: Asset Protection and Resilience**

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-320 Requirement Details There are documented incident management and reporting procedures.	Information incidents include a loss/breach of staff/patient/service user personal data, a breach of confidentiality or other effect on the confidentiality, information security or quality of staff/patient/service user information. All incidents and near-misses should be reported, recorded and appropriately managed so that where incidents do occur, the damage from them is minimised and lessons are learnt from them. An Information Governance Serious Incident Requiring Investigation (IG SIRI) deemed reportable to national bodies e.g. the Information Commissioner, should be recorded and communicated via the IG Toolkit Incident Reporting Tool.	AWS customers and partners providing services to HSCIC should implement documented incident management and reporting procedures using their designated IG responsible staff under the Shared Responsibility Model. AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS utilizes a three-phased approach to manage incidents: 1. Activation and Notification Phase 2. Recovery Phase 3. Reconstitution Phase In addition to the internal communication mechanisms detailed above, AWS has also implemented various methods of external communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.	**Principle 5: Operational Security**

Requirement	Requirement Description	Customer responsibility and AWS approach	Cloud Security Principle mapping
Requirement 13-323 Requirement Details All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures.	Organisations must ensure that all of their information assets that hold or are personal data are protected by technical and organisational measures appropriate to the nature of the asset and the sensitivity of the data.	AWS customers and partners providing services to HSCIC should implement appropriate organizational and technical measures to protect information assets that hold, or are, personal data, using their designated IG responsible staff under the Shared Responsibility Model. AWS does not access any customer's content except as necessary to provide that customer with the AWS services it has selected. AWS does not access customers' content for any other purposes. AWS does not know what content customers choose to store on AWS and cannot distinguish between personal data and other content, so AWS treats all customer content the same. Alignment with ISO 27018 demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content. AWS' alignment with and independent third-party assessment of this internationally recognized code of practice demonstrates AWS' commitment to the privacy and protection of customers' content. Further information can be found at: https://aws.amazon.com/compliance/eu-data-protection/ https://aws.amazon.com/compliance/iso-27018-faqs/	**Principle 5: Operational Security** **Principle 9: Secure consumer management**

Healthcare Reference Architecture

In order to help customers meet the objectives of the HSCIC IG SoC requirements, AWS has provided a sample architecture diagram (Figure 2 - Sample Reference Architecture) along with recommended AWS Security controls for various healthcare workloads. The sample architecture diagram has been provided for illustrative purposes only and will be referenced throughout this section of the document.

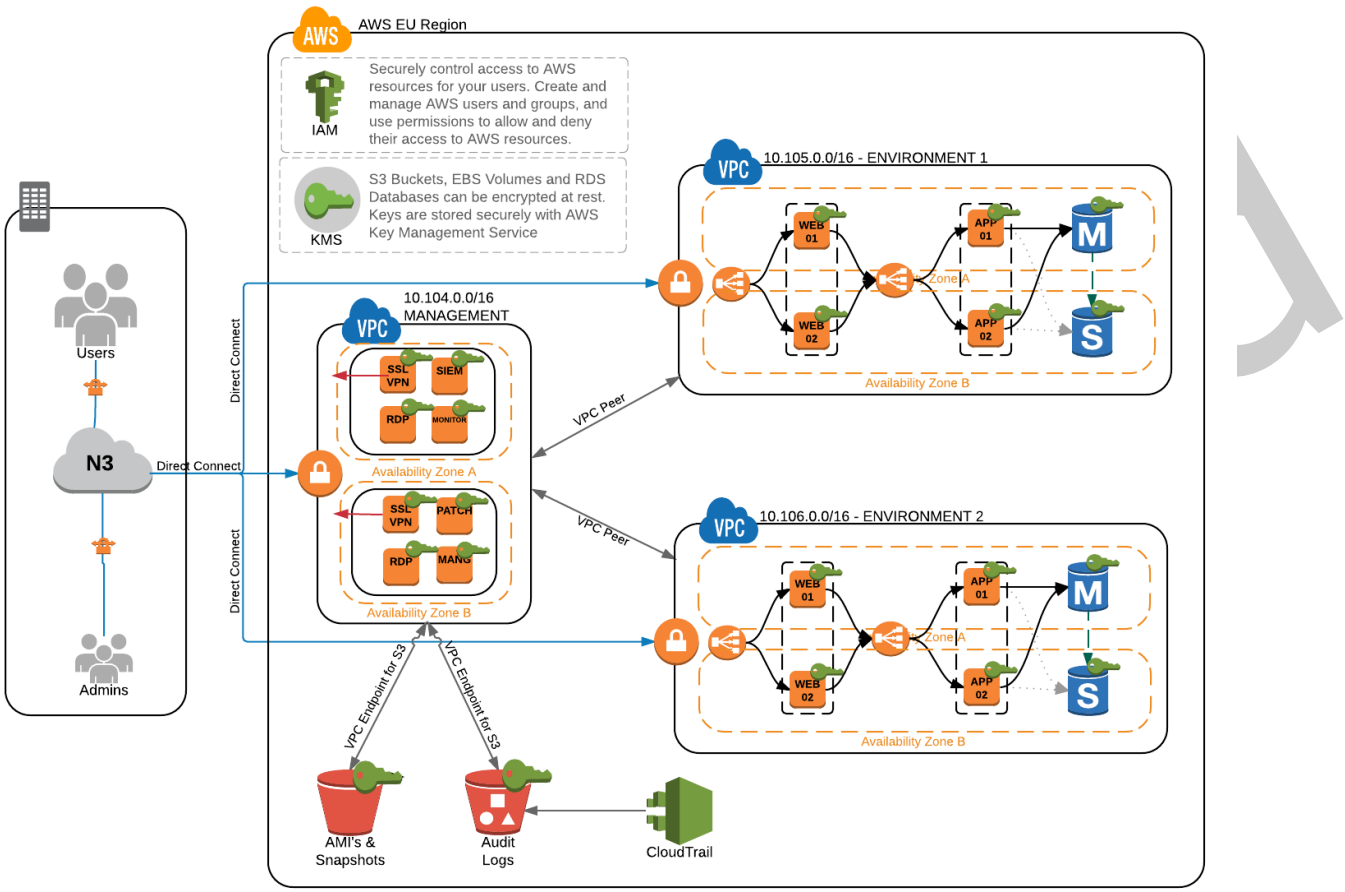


Figure 2 – Sample Reference Architecture

Architecture Overview

The sample reference architecture diagram shows two three-tier web applications, each isolated within their own AWS Virtual Private Cloud (VPC). This architecture also includes a Management VPC where management and monitoring services will be hosted. This may include services such as bastion hosts for administration, configuration management tools or patching and SIEM services. Each VPC hosts only private subnets and no access is available from the public Internet. There is an AWS Direct Connect in place connecting the customer site to the AWS VPC's of their choosing via a dedicated line. This ensures that all application traffic is sent over a private network. SSL/TLS is recommended to encrypt data in transit when accessing these applications. Optionally, you could also host a client side VPN service within the Management VPC for access to administrative systems.

Each Application VPC is isolated from others. This allows you to run multiple versions of an application at different deployment stages whilst maintaining complete network isolation. For example, you could host a Development environment in one VPC, and production in another. VPC Peering connections are in place between the management VPC and the application VPC's, with routes and rules in place to ensure only management traffic is allowed.

Audit Logs, Amazon Machine Images, Snapshots and static assets can be stored in Amazon S3 buckets for highly durable object storage. We access these buckets using VPC Endpoints for S3, which allow you to communicate with those S3 buckets both over a private connection and only from the VPC's that you specify.

AWS Security Implementation

Identity and Access Management

AWS Identity and Access Management (IAM) is a web service that allows you to centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

IAM provides users with granular permissions to allow different people to have access to different AWS resources. Multi-factor authentication (MFA) is recommended and can be added to your account and to individual users for additional security. You can also leverage identity federation if required to enable users who already have passwords elsewhere, for example in your corporate network, to gain temporary access to your AWS account.

Customers should use IAM Roles for Amazon EC2 when accessing other AWS services such as S3 from applications running on Amazon EC2. IAM Roles for EC2 allow you to assign permissions to an EC2 instance instead of a specific user. This role is assigned to an EC2 instance and applications running on that instance that leverage AWS SDK's can securely access other AWS resources such as S3 buckets without have to share API keys.

Protecting Data at Rest

AWS Key Management Service (KMS) provides a simple web services interface that can be used to generate and manage cryptographic keys and operate as a cryptographic service provider for protecting data. AWS KMS offers traditional key management services integrated with other AWS services providing a consistent view of customers' keys across AWS, with centralized management and auditing. Master keys in AWS KMS can be used to encrypt/decrypt data encryption keys used to encrypt data in customer applications or in AWS services that are integrated with AWS KMS. For more information on KMS visit: https://aws.amazon.com/kms/.

AWS services such as Amazon S3, AWS Elastic Block Store (EBS) and Amazon Relational Database Service (RDS) shown in Fig 2 above allow customers to encrypt data using keys that customers manage through AWS KMS.

Protecting Data in Transit

Network traffic must encrypt data in transit. For traffic between external sources and Amazon EC2, customers should use industry-standard transport encryption mechanisms such as TLS or IPsec

virtual private networks (VPNs). Internal to an Amazon Virtual Private Cloud (VPC) for data travelling between EC2 instances, network traffic must also be encrypted; most applications support TLS or other protocols providing in transit encryption that can be configured. For applications and protocols that do not support encryption, sessions transmitting patient data can be sent through encrypted tunnels using IPsec or similar.

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud offers a set of network security features well aligned to architecting for IG SoC compliance. Features such as stateless network access control lists and dynamic reassignment of instances into stateful security groups afford flexibility in protecting the instances from unauthorized network access. Amazon VPC also allows customers to extend their own network address space into AWS. Customers are also able to connect their data centers to AWS via a Virtual Private Network (VPN) or using Amazon Direct Connect to provide a dedicated connection as shown in Fig 2 earlier. VPC Flow logs provide an audit trail of accepted and rejected connections to instances processing, transmitting or storing patient information. For more information on VPC, see https://aws.amazon.com/vpc/.

Elastic Load Balancing

To ensure that data is encrypted in transit end-to-end customers can implement any of two different architectures when using Amazon Elastic Load Balancing (ELB).

Customers can terminate HTTPS or SSL/TLS on ELB by creating a load balancer that uses an encrypted protocol for connections. This feature enables traffic encryption between the customer's local balancer and the clients that initiate HTTPS or SSL/TLS sessions, and for connections between the load balancer and the customer back-end instances. For information see: http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-https-load-balancers.html.

Alternatively, customers can configure Amazon ELB in basic TCP-mode and pass-through encrypted sessions to back end instances where the encrypted session is terminated. In this architecture, customers manage their own certificates and TLS negotiation policies in applications running in their own instances. For information see: http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-listener-config.html

Conclusion

The AWS cloud platform provides a number of important benefits to UK public sector organisations and enables you to meet the objectives of the HSCIC IG SoC requirements. While AWS delivers these benefits and advantages through our services and features, under the aforementioned 'security IN the cloud' shared responsibility model, the individual organisations connecting to HSCIC are ultimately responsible for controls and assurance for the IG SoC requirements. Using the information presented in this whitepaper, we encourage you to use AWS services for your organisations to manage security and the related risks appropriately.

For AWS, security is always our top priority. We deliver services to hundreds of thousands of businesses including enterprises, educational institutions, and government agencies in over 190 countries. Our customers include government agencies, financial services and healthcare providers

who leverage the benefits of AWS while retaining control and responsibility for their data including some of their most sensitive information.

AWS services are designed to give customers flexibility over how they configure and deploy their solutions as well as control over their content, including where it is stored, how it is stored and who has access to it and the security configuration environment. AWS customers can build their own secure applications and store content securely on AWS.

Additional Resources

To help customers further understand how they can address their privacy and data protection requirements, customers are encouraged to read the risk, compliance and security whitepapers, best practices, checklists and guidance published on the AWS website. This material can be found at:

- AWS Compliance: http://aws.amazon.com/compliance
- AWS Security Center: http://aws.amazon.com/security

AWS also offers training to help customers learn how to design, develop, and operate available, efficient, and secure applications on the AWS cloud and gain proficiency with AWS services and solutions. We offer free instructional videos, self-paced labs, and instructor-led classes. Further information on AWS training is available at http://aws.amazon.com/training/.

AWS certifications certify the technical skills and knowledge associated with best practices for building secure and reliable cloud-based applications using AWS technology. Further information on AWS certifications is available at http://aws.amazon.com/certification/.

If further information is required, please contact AWS: https://aws.amazon.com/contact-us/ or contact the local AWS account representative.

Document Revisions

None.