Abstract

The Department of Public Expenditure and Reform’s (DPER) Cloud Computing Cloud Advice Note (the Cloud Advice Note) reflects the growing importance of cloud technology to public sector bodies (PSBs). This report sets out the advantages of cloud services and encourages PSBs to take a cloud-first approach. Other government strategies such as the Irish Public Service Innovation Strategy, which promotes a policy of innovation, digital transformation, and the advancement of public services through the use of new and emerging technologies, reinforces this messaging.

In February 2021, the Office of Government Procurement (OGP) released a Cloud Services Procurement Guidance Note (the Guidance Note), providing information on contractual and commercial considerations to better enable PSBs to purchase cloud services. The Guidance Note, which represents an important accompaniment to the Cloud Advice Note, aims to ease the transition for PSBs from a traditional on-premises approach to one that harnesses the power of cloud instead.

There is an increasing recognition across the Irish public sector—as evident from recent statements by both the Minister for Public Expenditure and Reform, and the Minister of State for Public Procurement and eGovernment—that cloud adoption will be key to realising the government’s wider digital transformation ambitions. Cloud use affords access to a full range of innovative technologies that can revolutionise the delivery of services to better serve people in Ireland while also improving efficiency, security, and value for money.

Read this eBook to gain additional information that can help you successfully implement the advice provided by the Cloud Advice Note. Learn from real-life Amazon Web Services (AWS) case studies, gathered from over 15 years of experience. By deep diving on key themes presented in the Cloud Advice Note, you will gain the practical information needed to assist you in your cloud-driven digital transformation.
1. Introduction

In recent years, the increasing deployment of new technologies have helped deliver innovative public services. Tools such as artificial intelligence (AI), machine learning (ML), and data analytics—all of which largely rely on cloud computing—stand at the forefront of a fast-evolving digital landscape and are changing the way people interact with public services.

Strong government messaging around the wider use of cloud computing complements official publications such as the Department of Public Expenditure and Reform’s (DPER) Cloud Computing Cloud Advice Note (Cloud Advice Note) and the Office of Government Procurement’s (OGP’s) Cloud Services Procurement Guidance Note (Guidance Note). For example, when speaking in February 2021, Ossian Smyth (Minister of State for eGovernment) said, “It’s government policy that cloud computing should be the default option for new ICT investment. Existing systems should be reviewed to see if they can also be moved to the cloud.”

At AWS, we recognise that public sector bodies (PSBs) may face challenges in achieving the government’s vision of a cloud-powered approach. Resources can be limited and, at times, elements of the digital transformation may seem daunting. But with over a decade of experience working with public sector customers in more than 190 countries and territories, AWS has learnt how to help make this transition as smooth as possible. In May 2021, AWS published Adopting Cloud Technology, a document that offers a cloud agnostic, high-level explanation of cloud computing to provide useful information and assist PSBs in their cloud adoption journey.

In a similar manner, this eBook will draw on AWS’s proven track record to further support the Irish public sector’s adoption of cloud technology in line with instruction provided by the Cloud Advice Note. This practical guidance aims to be a helpful resource that PSBs can use to successfully harness the AWS Cloud, thereby lowering costs, innovating faster, achieving greater levels of security, and providing a path to achieve the government’s vision of the further digitalisation of modern public services.

Important themes within the Cloud Advice Note have been broken down into key concepts, which will be addressed herein. These include the division of responsibilities between cloud service providers (CSPs) and PSBs, cloud infrastructure, data obligations, compliance, solution offerings, cost management, and migration. A mapping table of the Cloud Advice Note’s considerations to corresponding sections of this eBook, is provided in Appendix A.
In 2007, AWS opened the first AWS Region outside of the United States in Ireland, and today we support over 8,700 jobs across the Irish economy. As a hyperscale CSP, AWS provides cloud technology across all classification levels. The AWS Cloud is used by over 7,500 government agencies, 14,000 academic institutions, and 35,000 nonprofit organisations around the world. Both internationally and in Ireland today, PSBs are starting to realise the potential of the cloud—including the World Health Organisation (WHO), the Cork Institute of Technology, and the Health Service Executive (HSE). The HSE’s COVID Tracker application that runs on AWS is a good example of our technology in practice; government of Ireland chief information officer (CIO) Barry Lowry described it as a “perfect example” of how digital government should work. \(^5\) Further information on these case studies is provided in Appendix B.

Digitalisation is accelerating in Ireland and traditional server room models no longer represent long-term solutions. The AWS Cloud provides a low-friction path to cloud computing, with levels of scale, reliability, and security that are cost prohibitive for private cloud models and often not possible with on-premises data centres. By harnessing the secure access to expanding amounts of data provided by our economies of scale, PSBs in Ireland can re-invent the way organisations deliver modern public services.

As workloads shift to the cloud, PSBs can use the same infrastructure, services, application programming interfaces (APIs), and tools to help digital transformation projects get up and running faster. PSBs can modernise and manage all their applications through a broad set of hybrid capabilities and keep their data in the Ireland Region. PSBs can rapidly migrate application workloads suited for the cloud and keep other components on-premises designed to ensure continued operation with existing investment where needed.
2.1. Supporting Skills Enablement

AWS works hard to support the public sector workers who deliver cloud-powered services. We provide guidance for PSBs to help bridge skill gaps identified in the Cloud Advice Note through investment in training programmes in cloud technology and infrastructure. AWS offers a range of resources (many at no-cost) including classroom and online training, self-paced labs, and whitepapers designed to help organisations build the cloud skills they need. Our AWS certification programmes are recognised as four of the top 10 IT certifications that professionals plan to pursue.7

Not only does AWS aim to empower existing public sector workers, we also hope enable the next generation of tech practitioners and future builders. We have collaborated with Technological University Dublin (TU Dublin) to develop a bursary programme that enables students to learn valuable technical skills, and we work with a number of other Irish universities and colleges as part of our AWS Educate and AWS Academy programmes designed to upskill students for careers in the cloud.

Additionally, the AWS re/Start programme prepares unemployed and underemployed individuals without any existing experience or qualifications for careers in the cloud. AWS collaborates with local organisations around the world, including Generation in Ireland, to provide learners with the technical and soft skills needed for an entry level cloud role, as well as CV and interview coaching to prepare them for employer meetings and interviews. Upskilling people in this way not only reduces unemployment but also creates a pipeline of cloud talent to support the economy as digital transformation ensues.

UK DVSA Streamlines Innovation on AWS

The United Kingdom (UK) Driver and Vehicle Standards Agency (DVSA), worked with AWS Advanced Consulting Partner, Kainos, to develop a system using ML and predictive analytics to identify fraud and inadequate standards at Ministry of Transport (MOT) testing sites. The ML tool enables DVSA to identify abnormal MOT testing behavioural patterns, effectively target enforcement and inspection activities, and ultimately improve Britain’s road safety.

“Thanks to AWS, we’ve discovered the art of the possible. Kainos has helped DVSA push its boundaries to find the best, most innovative ways to make UK roadways safer,” said Darren McIlveen, delivery manager for Kainos. The DVSA modelling tool created by Kainos was named AI and ML Project of the Year in 2018 by the UK IT Industry Awards, and as collaboration between Kainos and DVSA continues, so too does the innovation.8
2.2. Modernise and Innovate

Digital transformation requires innovative thinking. AWS sustains their pace of innovation through our economies of scale and commitment to delivering the products and services that matter most to PSBs. Roughly 90-95 percent of our product roadmap is driven by what customers tell us matters and we iterate our products continuously to assure the latest services are instantly available. AWS decentralised autonomous development teams who work directly with PSBs—and these teams are empowered to develop and launch new features requested by our customers. This continual innovation helps ensure that PSBs maintain state-of-the-art IT infrastructure without having to make recapitalisation investments.

AWS is at the forefront of disruptive technologies such as ML, AI, and Internet of things (IoT), with more organisations choosing AWS for ML than any other cloud provider. A recent comparative review of enterprise ML Operations (MLOps) platforms by independent analyst firm Omdia recognised AWS as “the outright leader,” with high scores across almost every measure. With AWS, PSBs can choose from a broad, deep set of services that match their business needs, supporting the vision of an eGovernment and the use of digital solutions to seamlessly deliver modern public services.

3. The Division of Responsibility

When considering cloud procurement and navigating the cloud adoption process in its entirety, the Cloud Advice Note recognises that security and compliance are shared responsibilities between the PSB and the CSP. This should be taken into account at the start of the decision-making process so PSBs can gain a clear understanding of expectations and obligations and migrate to cloud with ease. The division of responsibility is commonly referred to as security of the cloud (the CSP’s responsibility) versus security in the cloud (the PSB’s responsibility).

The AWS shared responsibility model relieves operational burdens as we are responsible for protecting the infrastructure that runs all of the services offered on the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities on which our cloud services run. PSBs, and in some cases, partners within the AWS Partner Network (APN) who work with them, assume responsibility and management of the guest operating system (including updates and security patches); other associated application software; configuration of the provided security group firewalls; and other security, change management, and logging features. Appendix C provides a detailed illustration of how this shared responsibility model works.

AWS provides a wide variety of best practices documents, encryption tools, blogs, and other guidance that PSBs can leverage in delivering application-level security measures.
4. Reliable Infrastructure

The most sophisticated and innovative applications demand reliable infrastructure on which to build. The infrastructure required to support new technologies is highlighted in the Cloud Advice Note as a factor that PSBs should consider to support the growing demand for digitalisation.

With the AWS global infrastructure, PSBs in Ireland have access to the most secure, extensive, and reliable cloud offering in the world today. With millions of active customers and tens of thousands of APN Partners globally, AWS offers a fully dynamic cloud while also enabling PSBs to retain control of the location of their data. We provide broad geographic coverage so customers can create a secure network connection from their on-premises environments to the AWS Cloud. These connections are already used by Irish Government Networks today to establish a dedicated network connection to the AWS Ireland Region.

As recommended in the Cloud Advice Note, PSBs should remain cognisant not only of geographic implications, but also operational effectiveness when considering the infrastructure of various CSPs. Outlined below are some of the key topics highlighted by the Cloud Advice Note which are inherent in AWS Cloud infrastructure.

4.1. Geographic Separation for High Availability

AWS data centres are situated in 81 geographic areas known as Availability Zones, which are grouped into 25 isolated and physically separate AWS Regions. We designed these both to ensure the resilience of the AWS Cloud.

The AWS Ireland Region is AWS’s longest tenured Region in Europe. With world-class infrastructure already built in Ireland, PSBs are well-positioned to leverage the benefits of high-bandwidth, high-quality, and low-latency networking. PSBs can quickly spin up resources as they need them, deploying hundreds or even thousands of servers in minutes.

PSBs in Ireland can achieve maximum availability and performance by deploying their applications across multiple Availability Zones within the Ireland Region for fault tolerance and low latency. Availability Zones are connected to each other with fast, private fibre-optic networking, enabling PSBs to easily architect applications that automatically failover between zones without interruption. Because each AWS Region, Availability Zone, and data centre is fully isolated from the others, we provision network capacity to tolerate multiple concurrent disruptions to enable traffic to be load balanced to the remaining sites—an approach unlike that provided by any other cloud provider.
4.2. Disaster Recovery (DR)

AWS enables PSBs to have their own DR site ready and on standby in the cloud without having to pay for the IT infrastructure. The AWS Cloud inherently improves DR because compute and storage—designed to deliver increased durability of 99.999999999 percent—is synchronously distributed across multiple facilities. Within the AWS Ireland Region, copies of an object can be distributed across at least three Availability Zones that are physically separate within a geographic area.

AWS is built for fault-tolerance and supports many DR architectures, from those built for smaller workloads to enterprise solutions that enable rapid failover at scale. These architectures include pilot light environments that are ready to scale up rapidly to hot standby environments that failover at a moment’s notice. PSBs have the flexibility to choose the right approach for their DR strategy.

4.3. Control Over Location

With AWS, PSBs define how and where they run their workloads, using the same network, control features, APIs, and AWS services that they already use in their current environments. The Cloud Advice Note explains that workloads can be run in other European Economic Area (EEA) member states. With AWS, PSBs can choose from five EEA AWS Regions, including Ireland, Frankfurt, Stockholm, Milan, and Paris. There is also an AWS Region located in London.

PSBs own their data, control who has access to it, and control its location. AWS is transparent about how our services process the personal data that PSBs upload to their AWS account (customer content). In addition, we provide capabilities that allow PSBs to encrypt, delete, and monitor the processing of their customer content. PSBs can use AWS services with confidence that their data will remain in the AWS Region they have selected. A small number of AWS services involve the transfer of PSB data to develop and improve those services—where PSBs can opt-out of the transfer—or because transfer is an essential part of the service (such as content delivery services like Amazon CloudFront).

Our highest priority at AWS is securing the AWS Cloud and the customer content that is uploaded to the AWS Cloud. We implement rigorous technical and organisational measures to protect the confidentiality, integrity, and availability of customer content—no matter which AWS Region a PSB selects to store its workloads. By providing these features, in addition to tools that help automate and monitor data storage location (such as Amazon CloudWatch, an observability service) we make it easier for PSBs to operate globally while retaining control over where their data is stored.
Wellola Uses AWS to Deliver a Secure Patient Communication Portal

Wellola, an Irish digital health software firm who provides secure video and patient portal services to healthcare providers, experienced a spike in users when the COVID-19 pandemic began. By using AWS, Wellola scaled quickly to meet demand and deliver a reliable, secure, and cost-effective platform that met regulatory standards and Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) requirements. Today, Wellola is providing over 600 general practitioners, governments, allied healthcare providers, charities, and Section 38 entities in Ireland, the UK, and Italy with secure video consultations, messaging, digital letters, record keeping, and payment facilities. These services help these organisations manage and mitigate the impact of the pandemic. Wellola is all-in on AWS and worked with APN Partner DNM to optimise the security and scalability of the software as a solution (SaaS) platform.

Although PSBs can replicate and back-up content in more than one AWS Region, they should remain cognisant of geographical data protection laws as referenced in the Cloud Advice Note, such as the GDPR, which is further discussed in Section 5.3.11

"Our data is hosted in Europe, which is crucial for us from a security perspective. With AWS, we have complete control over where and how data is stored, and who has access to it. This control, along with the extensive encryption, means we feel safe. We know the Trust’s data is protected."12

– Martin Brambley, Director of Sirocco Systems for the UK National Trust

5. Data Protection Made Simple

The Cloud Advice Note advises PSBs to consider their obligations concerning data protection. In the context of PSB content stored or processed using AWS services, the PSB performs the role of data controller, as the PSB controls their content and makes decisions about treatment of that content. AWS performs the role of data processor, as we only use customer content to provide the services selected by each customer and we do not use customer content for any other purpose. AWS personnel cannot log into PSB instances, which are also logically isolated from other customers by default.

The shared responsibility model makes data protection easier as PSBs retain complete control over how content is classified, stored, used, archived, and secured. AWS provides security tools and services in accordance with the guidance prepared by the Data Protection Commission (DPC) that is highlighted in the Cloud Advice Note that are designed to protect PSB data such as access controls, firewalls, antivirus, staff training, policy development, and publicly available best-practice guidance.
5.1. Data Sharing and Reuse

Improved hardware efficiency through resource sharing is a benefit of AWS’s multi-tenancy architecture. The AWS environment is a virtualised, multi-tenant environment with implemented security management processes, payment card industry (PCI) controls, and other security controls that are designed to isolate each customer from other customers. Services can be reused with no additional infrastructure setup or installation, leading to savings in infrastructure cost, energy costs, and human operational cost.

5.2. Data Classification

As acknowledged in the Cloud Advice Note, the vast majority of data processed by PSBs is suitable for location in or migration to the cloud.

The Cloud Safeguards Information at Nearly All Classification Levels

On 1 December 2021, the Flemish Government released Information Classification Flemish Government - Networking, Minimal Measures, a document that detailed five confidentiality classes for the classification of information. These include:

- Public: Public information
- Internal: Public information that has limited access based on organisational criteria
- Confidential: Information that is accessible to a limited group of users based on functional criteria that determine the need for access
- Secret: Information that is accessible to a limited group of users based on functional criteria that determine the demonstrated need for access
- Top Secret: Information that is accessible to a very limited group of users on the basis of explicit functional criteria with a motivated absolute need for access

Based on an analysis of the minimum measures required in the context of network security, the report suggests that cloud offers the tools and safeguards to maintain the confidentiality, integrity, and availability of data for at least four of the five classification levels.13

Per the shared responsibility model, PSBs control how they classify their data—and with the AWS Cloud, they can apply and enforce that classification in just a few clicks. This means PSBs can build a solution that protects information in accordance with the categories referred to in the Cloud Advice Note, as defined by the Council Decision on the Security Rules for Protecting European Union Classified Information (EUCI) and their respective mapping to equivalents across member states—including Ireland.

AWS offers several services and features that can facilitate implementation of a data classification scheme. For example, Amazon Macie can help PSBs inventory and classify sensitive and business-critical data stored in AWS. Macie uses ML to automate the process of discovering, classifying, labelling, and applying protection rules to data.
This helps PSBs better understand where sensitive information is stored and how it is being accessed, including user authentications and access patterns.

AWS services are content agnostic, in that they offer the same high level of security to all PSBs, regardless of the type of content being stored, with core infrastructure built to satisfy the security requirements for the military, global banks, and other high-sensitivity organisations. AWS is hyper-vigilant about security and has implemented sophisticated technical and physical measures against unauthorised access, alongside guidance such as the Data Classification: Secure Cloud Adoption whitepaper.

5.3. Data Privacy

In line with European Data Protection Board (EDPB) guidelines on determining the territorial scope of GDPR in relation to cloud services, AWS's Ireland Region is situated in the European Union (EU), and as such, the processing of any personal data related to EU individuals is subject to GDPR. All AWS services can be used in compliance with GDPR. In addition, AWS provides guidance to PSBs when they deploy AWS services including the GDPR Center and the AWS Security blog. AWS also provides a supplementary addendum to the AWS GDPR Data Processing Addendum, which offers strengthened contractual commitments that go beyond what is required by the Schrems II ruling and applies to all customer content subject to GDPR, whether it is transferred outside the EEA or not.

Under the shared responsibility model (and as the Cloud Advice Note points out), PSBs remain fully responsible for regulatory obligations including data protection. However, AWS continually monitors the evolving privacy, regulatory, and legislative landscape to identify changes and determine what tools our customers may need to meet their compliance needs. AWS strives to inform our customers of the privacy and data security policies, practices, and technologies that we have put in place, and we provide a wide variety of best practice documents that PSBs can leverage to protect the privacy of their data. Thousands of customers who are subject to GDPR, PCI, and/or HIPAA already use AWS for their workloads, and AWS is certified on numerous certification programs and rigorous international standards, such as International Organization for Standardization (ISO) 27017 for cloud security and ISO 27018 for cloud privacy.

AWS provides the means to closely manage the lifecycles of systems so that privacy can be maintained and security concerns can be addressed at all stages, as recommended by the Cloud Advice Note. AWS provides APIs for PSBs to integrate encryption and data protection with any of the services that they develop or deploy in an AWS environment. Most AWS services that store and manage PSB data support server-side encryption (SSE), where the service that stores and manages customer content also transparently encrypts and decrypts it for them. Additionally, AWS supports client-side encryption libraries that PSBs can include in their applications. These libraries make it easier to include best-practice encryption in PSB applications, even without cryptography expertise.
HSE uses AWS to Build a Scalable and Secure Contract Tracing App

To help reduce the spread of COVID-19 in Ireland, the HSE used AWS to build a scalable and reliable COVID-19 Tracker application. With AWS, HSE gained the agility needed to develop, test, and build the first prototype of the app, which was available in just two days, and received 1.54 million downloads by the fourth week—equivalent to 30 percent of Ireland’s population. Using AWS provided the HSE with a reliable solution that is hosted in Ireland and can be used in compliance with international regulations and standards including GDPR. The HSE uses AWS’s extensive portfolio of security services to ensure all data is encrypted when in transit and at rest.15

5.4. Data Control

The Cloud Advice Note highlights the importance of PSBs knowing who has access to their data and how this is controlled. With AWS, PSBs have complete control over their data including enabling governance, compliance, detection, and auditing. PSBs can assign rights and log access with tools and services such as AWS Identity Access Management (IAM). PSBs can manage access to their AWS services and resources securely through individual permissions for users, roles, and granular policy control. Additionally, if PSBs need to share specific data sets between agencies, AWS Organizations enables central management and governance of their environment as they grow and scale their AWS resources.

The Cloud Advice Note advises PSBs to ensure that they can access their data in a way they want (i.e., through APIs). As the logging and continuous monitoring of API calls are key components in cloud security and operational best practices, PSBs can migrate their data knowing that with the appropriate controls, AWS services can assist with access control and retention management. This interaction provides powerful visibility from a security perspective since all users must use an API to interact. With services like Amazon API Gateway, PSBs can easily create, publish, maintain, monitor, and secure APIs at any scale.

The Cloud Advice Note highlights data retention as a key requirement for PSBs. Retention can be harder and more expensive on premises. The AWS Cloud makes retention simple as critical system components, including audit evidence and logging records, are replicated across multiple Availability Zones and backups are maintained and monitored. PSBs can choose how they store and manage their data on AWS, and they have complete control and ownership of applicable retention policies and lifecycle rules. AWS provides services such as Amazon Simple Storage Service (Amazon S3), which provides industry-leading scalability, data availability, security, and performance, designed for 99.99 percent durability. With Amazon S3, PSBs can select from a range of storage classes based on how frequently they access their data, and they benefit from long-term archive and digital preservation at a lower cost. Additionally, PSBs can set an Amazon S3 Lifecycle policy to automatically transfer data to a different storage class without any changes to their application, enabling them to save valuable time and money.
5.5. Data Security

Security is our top priority at AWS, and our scale allows significantly more investment in security policing and countermeasures than almost any large organisation could afford on their own. Our core infrastructure is built to satisfy the security requirements for high-sensitivity organisations around the world and is monitored 24x7 to help protect the confidentiality, integrity, and availability of customers’ data. Although security responsibilities are shared between AWS and a PSB, we offer a deep set of cloud security tools, including 230 security, compliance, and governance services.

“We determined that security in AWS is superior to our on-premises data centre across several dimensions, including patching, encryption, auditing and logging, entitlements, and compliance.”

– John Brady, Chief Information Security Officer, Financial Industry Regulatory Authority (FINRA)

The Cloud Advice Note advises PSBs on enhancing their security practices when using cloud services. Under the shared responsibility model, PSBs assume responsibility of ensuring security management processes are in place. However, this is simplified through a wide range of data breach, response, and remediation tools provided by AWS, such as Amazon CloudWatch, which has more than one million active customers every week. PSBs can maintain and monitor a variety of logs files, collect and track metrics, set alarms, send notifications, and automatically react to changes in AWS resources. PSBs have the power to audit and monitor their own AWS environment.
6. Compliance and Standards

PSBs can look to a CSP’s compliance with certification schemes and frameworks for assurance that effective security controls are in place. Although the Cloud Advice Note highlights that there is no single certification for cloud computing, it currently recognises ISO 27001 as the most widely-adopted certification and points to the European Union Agency for Network and Information Security (ENISA) Cloud Certification Schemes List for additional guidance on relevant certification schemes. With AWS, PSBs can inherit the most comprehensive compliance controls—including ISO 27001 and those mapped by ENISA. We support more security standards and compliance certifications than any other offering—these include GDPR, the Payment Card Industry Data Security Standard (PCI-DSS), National Institute of Standards and Technology (NIST) 800-171, ISO 9001/27001/27017/27018, Cyber Essentials Plus, Cloud Security Alliance (CSA), and Service Organization Control (SOC) 1, 2, and 3.

The AWS Compliance Programs webpage provides a comprehensive list of IT standards we comply with broken out by certifications and attestations; laws, regulations, and privacy; and alignments and frameworks. We also publish reports and evidence of our compliance on the AWS Artifact webpage. Open access to compliance attestations enables PSBs to evaluate the effectiveness of AWS-managed controls and validates the operating effectiveness of AWS solutions. By leveraging AWS tools, PSBs can reduce the cost and time needed to run their own specific security assurance requirements, and can reduce risk while enabling scale by using AWS activity monitoring services that detect configuration changes and security events across a PSB’s system.

7. Solution Offering

The Cloud Advice Note recommends PSBs assess their technology stack when evaluating a cloud solution. With AWS, PSBs will have access to over 200 fully featured services—with a broad level of functionality within those services. AWS has launched over 11,000 new features and services since launch in 2006, including 2,757 in 2020 alone. AWS is trusted to power a wide variety of workloads including web and mobile applications; data processing and warehousing; storage, archive, serverless technologies; and technical requirements previously designated as unsuitable including large-scale online transaction processing (OLTP).
Irish tech startup Stripe chose to build their PCI-compliant payment platform entirely on AWS, relying on the security best practices and easy auditability of the AWS Cloud. Thanks to AWS, OLTP was not barrier to Stripe’s cloud adoption, and AWS’s scalability has been fundamental to the growth and cost-efficiency of Stripe. AWS empowered Stripe to automate away manual and time-consuming tasks—an infrastructure described by Jorge Ortiz, Manager of Infrastructure, as “unthinkable without AWS.” Today, Stripe handles hundreds of thousands of payments every day for some of the largest websites and companies in the world, including Salesforce, Spotify, Twitter, Reddit, Lyft, Fitbit, and more.17

7.1. Services

The AWS Cloud provides services globally on a one-to-many, self-service basis, and enables access to new and enhanced functionality as highlighted by the Cloud Advice Note. The economies of scale gained from providing hyperscale cloud computing to all customers translates into lower costs and cost-efficient support services focused on helping AWS customers with guidance driven by best practices. All of AWS’s service level agreements (SLAs), product information, and guides are publicly available and provide PSBs with simple and reliable access to any information they may need.

AWS understands that finding and deploying value-added software can be challenging. The AWS Marketplace is a digital catalogue that can connect PSBs to over 1,600 independent software vendors that run on AWS, with software across 50 categories, totaling more than 8,000 transactable listings. AWS Marketplace can simplify procurement, entitlement, and provisioning due to its flexible pricing options and multiple deployment methods. PSBs can select commercial software from well-known vendors, in addition to many widely-used open source offerings, enabling cloud users to rapidly and securely deploy solutions while reducing Total Cost of Ownership (TCO) and improving operational oversight.

Additionally, PSBs can leverage the APN for assistance with architecting, delivering, and managing AWS Cloud-based solutions. The APN consists of more than 100,000 partners, including 1,500 partners from the AWS Public Sector Partner (PSP) program, with solutions and experience in delivering on a combination of government, education, and non-profit customer missions around the world. According to research carried out by TechMarketView, APN Partners make up four of the top 10 suppliers to the Irish public sector software and IT services market (ranked by revenues), including Accenture, Version 1, Deloitte, and DXC.18 The APN allows a more diverse group of organisations to use AWS services by getting close to the customer’s needs at the ground level.

AWS keeps customers abreast of update release cycles and regularly announces new features on the What’s New with AWS webpage (the importance of such is highlighted in the Cloud Advice Note). AWS technical account managers (TAMs) and AWS Professional Services can also work with PSBs to take advantage of upcoming releases,
including support with monthly account plans. PSBs have the power to create product feature requests and directly influence AWS product roadmaps as AWS works with PSBs to identify the functionality they need and help them adopt it.

The West Java Provincial Government Innovates Faster and Reduces Development Time with AWS

West Java is the most populous province in Indonesia, and its government is committed to improving public services through technology. When looking at ideas to contribute to the province’s smart-city objectives, Setiaji, the head of the Communications and Informatics Agency for the West Java Provincial Government said, “We are actively looking to outsource some of our development work to AWS and its partners to move at an even faster pace when introducing new digital public services. This is very useful for public sector institutions, where budget and staffing are limited.” By building their apps on the AWS Cloud, the West Java Provincial Government has been able to innovate faster and reduce development time from 2-3 months to 16 days.

7.2. Supporting Sustainable Operations

AWS can help PSBs align with environmental initiatives included in the Cloud Advice Note, such as the Climate Action Plan, as well as government emissions targets as set out in the Climate Action and Low Carbon Development (Amendment) Act 2021. According to a report by global research and advisory firm 451 Research, businesses in Europe can reduce energy use by nearly 80 percent when they run their applications on the AWS Cloud instead of operating their own data centres. The report found that compared to the computing resources of the average European company, cloud servers are roughly three times more energy efficient, and AWS data centres are up to five times more energy efficient. Companies could potentially further reduce carbon emissions from an average workload—by up to 96 percent—once AWS meets its goal to be powered by 100 percent renewable energy, a target the company is on a path to achieve by 2025.

Economies of scale make the AWS Cloud inherently more sustainable than on-premises infrastructure. Meanwhile, PSBs are empowered to optimise their workloads using a wide range of AWS tools and resources. AWS provides guidance from teams that are knowledgeable about sustainability and can advise on best practices (including the AWS sustainability team). AWS works with customers to identify opportunities for optimisation, such as improved server utilisation, or using automation technologies to shut down underutilised or unused resources to help lower infrastructure costs and lower the environmental impact of workloads. Further information on the sustainability shared responsibility model is provided in Appendix D.

AWS is actively supporting Ireland in meeting its goal of becoming net zero carbon through the country’s first custom-built, sustainable solution to provide low-carbon heat to a growing Dublin suburb. The District Heating Scheme in Tallaght will provide heat recycled from an AWS data centre to public sector, residential, and commercial entities. Additionally, Amazon is a founding member of The Climate Pledge—a commitment to be net zero carbon across the business by 2040, 10 years ahead of the Paris Agreement.
8. Cost Management

Economies of scale allow AWS to pass on the savings to customers. As a result, AWS has reduced prices 111 times since launch in 2006. AWS enables PSBs to align with the Cloud Advice Note’s call to deliver services in the most cost-efficient way possible. We have been working with our customers continually to better understand their workloads so we can recommend best practices and services. Cloud costs are different than the costs associated with traditional IT purchasing—as there is little maintenance and no physical hardware. With AWS, customers pay only for the services needed, for as long as they use them, without requiring long-term contracts or complex licensing. AWS provides a suite of reports and specialised tools to estimate, monitor, plan, report on, and analyse spend so PSBs can take control of costs while building modern, scalable applications to meet public sector needs.

8.1. Budgeting and Forecasting

When starting the migration journey, building a business case and reviewing TCO (as advised by the Cloud Advice Note) can seem time consuming and may not always identify the most cost-effective options. AWS can simplify comparative TCO analysis by providing guidance when designing workloads, selecting services, and configuring and operating those services. PSBs can use the Migration Evaluator to gain access to insights and receive an assessment that includes a projected cost estimate (and potential savings) for running on-premises workloads in the AWS Cloud. Similarly, the AWS Pricing Calculator enables PSBs to configure a cost estimate that fits their unique business or personal needs with AWS products and services.

A survey by International Data Corporation (IDC), a global provider of market intelligence, found that developing, deploying, and managing workloads on AWS delivered a five-year TCO savings of 51 percent when compared to deployment of the same resources on-premises or in hosted environments. The findings also showed a 637 percent return on investment over five years.²¹

---

**CIHI Improves Agility, Performance, and TCO on AWS**

Before migrating to AWS, the Canadian Institute for Health Information (CIHI) was running costly data centres that were cumbersome to manage. To better serve their stakeholders, CIHI migrated key workloads to the cloud while maintaining strict data security and protection requirements. They achieved their cost optimisation savings goal by October 2020, months ahead of their March 2021 target. CIHI’s TCO showed a 10 percent reduction on AWS from the initial lift and shift, and once CIHI starts to modernise in the cloud, this reduction percentage is set to increase. CIHI can now determine the costs of developing new applications and run proofs of concept without having to buy infrastructure and capital assets, and by merging their time management system and their AWS billing system, they have the actual cost of all their business assets within their cloud infrastructure.²²
8.2. Cost Optimisation

AWS empowers PSBs to take control of cost and continuously optimise spend. To identify further areas for ongoing cost savings, PSBs can control workload variation and utilisation (highlighted by the Cloud Advice Note) through identifying instances with low utilisation and then reduce cost by stopping or rightsizing. Services such as AWS Cost Explorer and AWS Trusted Advisor provide recommendations to optimise spend and lower costs while AWS monitoring services can collect metrics, monitor log files, and set alarms based on usage. Taking advantage of these features not only allows PSBs to maintain optimal performance but also increases cost efficiencies as PSBs pay only for the resources they actually need.

In addition, PSBs can benefit from the elastic nature of cloud by utilising AWS Auto Scaling—a feature endorsed by the Cloud Advice Note—to monitor their applications and automatically adjust capacity to maintain steady performance at the lowest possible cost. To further drive down costs, AWS offers alternative pricing models to provide discounts based on capacity and utilisation needs—up to 72 percent with Savings Plans, up to 75 percent with Reserved Instances, and up to 90 percent with Spot Instances, in comparison to On-Demand pricing.

As the Cloud Advice Note highlights, it is important to understand both initial costs and ongoing costs (such as storage options). With AWS, PSBs can leverage the right storage class for cost efficiency based on how frequently or infrequently data is accessed. Amazon S3 Storage Classes offer six distinct storage classes that are designed to accommodate different access requirements at corresponding costs where PSBs have the flexibility to manage costs or have it storage automated to further optimise spend.

To view a full list of AWS services to help optimise and save costs, refer to the AWS Cost Management Services table.
9. Migration Support

The growing need for PSBs to review existing systems in order to evaluate which may be suitable for migration to the cloud is reflected in the Cloud Advice Note and recent government messaging around the wider use and adoption of cloud computing. A study carried out by Forrester into European government plans, priorities, and challenges regarding digital transformation also found the cloud to be the backbone of modernisation initiatives and improving citizen experiences. AWS and the APN Partner community is helping customers successfully migrate all types of workloads to AWS, including large-scale migrations of tens of thousands of servers. AWS can assist PSBs in this transition by providing a portfolio of migration tools and practical guidance that includes documented techniques based on years of experience (such the AWS Migration whitepaper).

9.1. Review and Planning

The Cloud Advice Note recognises that migration may require an iterative approach. At AWS, we can support PSBs by forming a cloud migration initiative, establishing cloud governance guardrails, and preparing PSBs to provide and consume new services. The AWS Public Sector Digital Transformation webpage provides a variety of checklists, tools, and inspiration through customer success stories. In addition, the AWS Government Transformation Team (GTT) can help government executives take control of their technology, change their business models, and build sustainable, world-class public services by leveraging the AWS Cloud.

AWS offers several programmes that can help PSBs assess their readiness and prepare their organisation for cloud adoption. The Cloud Advice Note encourages PSBs to balance the longer-term inefficiencies of migrating applications against modernising in advance—or replacing them altogether. Leveraging programmes like the AWS Cloud Adoption Framework (AWS CAF), which is designed to help organisations develop and execute efficient plans for their cloud adoption journey, can help with this. The AWS CAF enables PSBs to analyse their environment through six different perspectives: business, people, governance, platform, security, and operations. This gives PSBs a complete view of which areas to modernise and improve on before moving forward with a large migration effort.

The AWS Migration Acceleration Program (MAP) packages best practices, tools, expertise, and financial incentives to make cloud adoption easier by reducing migration complexity and costs. MAP for Windows also includes an AWS Optimization and Licensing Assessment (AWS OLA) so PSBs can make data-driven migration decisions based on actual resource utilisation, third-party licensing, and application dependencies.
9.2. Procuring Cloud

Cloud procurement is inherently different to traditional public sector procurement and contract approaches, but it need not be more complex. As the Cloud Advice Note points out, due diligence should be exercised when selecting a CSP and PSBs should seek guidance where necessary. AWS can engage with PSBs at all levels in order to provide guidance on procuring cloud and familiarize them with this process.

PSBs can work with AWS Professional Services and leverage the AWS CAF to help realise measurable benefits from cloud adoption faster and with less risk. AWS also offers digital courses (such as Getting Started with Cloud Acquisition) that help increase knowledge and comfort when discussing cloud procurement and related topics such as pricing, security, data sovereignty and residency, sustainability, and conditions. These courses cover all the fundamentals of how to buy cloud, including essential information that helps ease the process from the very start of cloud procurement.

As the Cloud Advice Note points out, the OGP has since released a separate Guidance Note on the procurement of cloud, bringing attention to contractual and commercial considerations. To assist PSBs in developing their knowledge of cloud procurement, the AWS Procuring Cloud Technology eBook provides in-depth guidance around these considerations and further information on purchasing cloud services through a competitive procurement process. For additional information and support, PSBs can look to the How to buy AWS Cloud for the public sector webpage, or the Cloud Infrastructure Services Providers in Europe (CISPE) Buying Cloud Services in Public Sector handbook, which includes sample request for proposals (RFP) language for a Cloud Framework Agreement.

The Cloud Advice Note recommends that PSBs fully understand contract terms and what they mean for service management. At AWS, we provide full visibility into AWS service terms, and we provide public access to over 100 SLAs that detail our general service commitment, including our monthly uptime percentage. Additionally, the AWS Marketplace offers standardised software license terms. Standard terms allow PSBs to alleviate lengthy negotiations, streamline software procurement, and speed innovation for their business.

In full support of the Cloud Advice Note’s inclusion of an exit strategy, AWS can help mitigate license lock-in as it allows PSBs to quickly move to another CSP. The AWS Cloud offers more flexibility in services and solutions than on-premises infrastructure and enables PSBs to architect for data portability from the beginning. Organisations only use the services when they see value, and they are able to use the technology of their choice. Pay-as-you-go pricing provides the ability to shut down an environment and export data and virtual machines (VMs). For further guidance on understanding and mitigating switching costs when changing CSPs, PSBs can refer to the Unpicking Vendor Lock-in whitepaper.

PSBs should avoid implementing commercial brokering services, suggested by the Cloud Advice Note, as this may lead to long-term contracts and paying support fees. Instead, PSBs can consider moving to a fully-managed, open-sourced, industry
standards-based solution such as Amazon MQ, which can reduce operational responsibilities by managing the provisioning, setup, and maintenance of message brokers. Alternatively, PSBs can establish a single endpoint to govern and monitor a cloud portfolio while being responsible for cloud strategy. The UK government’s guidance for organisations’ reliance on cloud technologies, *Managing Technical Lock-in in the Cloud*, describes this as a technical design authority (TDA). The TDA model can allow PSBs to coordinate a unified approach to governance and billing while still allowing individual departments to have flexibility in their consumption of cloud.

**AWS Helps DVLA Achieve Digital Excellence**
The Driver and Vehicle Licensing Agency (DVLA), a UK department for transport, wanted to pursue digital transformation in the cloud after 22 years of being locked into monolithic on-premises IT contracts. The DVLA cut costs, reduced application delivery time, and achieved self-sufficiency and digital excellence by working alongside AWS APN Partner, Mobilise. Over four years, they migrated their systems to Amazon Elastic Compute Cloud (Amazon EC2), built an award-winning Kubernetes-based solution, and upskilled their employees to adapt to the cloud. The DVLA is now a recognised cloud centre of excellence within the UK government.

**10. Summary**

The public sector in Ireland is well positioned to adopt the AWS Cloud in accordance with instruction provided by the government through the Cloud Advice Note. With AWS, PSBs can harness the technology that enables cost-effective, accessible public services to reach more people and drive positive change nationwide. Supported by AWS, the possibilities of digital transformation are growing by the day. With the power of open data, ML, and more, PSBs can align with the vision of an eGovernment and help improve the lives of people in Ireland.

If you would like to learn more about how the AWS Cloud can help your organisation innovate and digitally transform, please contact the Irish AWS Public Sector team via aws-publicsector-ireland@amazon.com.
Appendix A. Cloud Advice Note Mapping

The Cloud Advice Note sets out important considerations for PSBs to consider when making decisions in relation to the adoption of cloud services. As a helpful tool to aid understanding and assist with quick navigation of this document, Table 1 displays a chronological list of considerations found Section 7 of the Cloud Advice Note (Considerations) and the additional subjects listed under Section 9 (Other Matters). Each consideration has been broken down into its key concepts, which in turn, are mapped to specific sections of this eBook.

<table>
<thead>
<tr>
<th>Cloud Advice Note Section</th>
<th>Key Concept</th>
<th>eBook Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>7. Considerations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.1 Data Classification and Categorisation</td>
<td>Data categorisation</td>
<td>5.2 Data Classification</td>
</tr>
<tr>
<td></td>
<td>Data breach and response</td>
<td>5.5 Data Security</td>
</tr>
<tr>
<td></td>
<td>EUCI class rules</td>
<td>5.2 Data Classification</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
<td>5.3 Data Privacy</td>
</tr>
<tr>
<td></td>
<td>Access rights</td>
<td>5.4 Data Privacy</td>
</tr>
<tr>
<td></td>
<td>Logging access</td>
<td>5.4 Data Control</td>
</tr>
<tr>
<td></td>
<td>Data retention</td>
<td>5.4 Data Control</td>
</tr>
<tr>
<td>7.2 Product</td>
<td>Product roadmaps</td>
<td>7.1 Services</td>
</tr>
<tr>
<td></td>
<td>Core and configuration functionality</td>
<td>7 Solution Offering</td>
</tr>
<tr>
<td></td>
<td>Release cycles</td>
<td>7.1 Services</td>
</tr>
<tr>
<td></td>
<td>Workload variation and control</td>
<td>8.2 Cost Optimisation</td>
</tr>
<tr>
<td></td>
<td>Technical requirements</td>
<td>7 Solution Offering</td>
</tr>
<tr>
<td></td>
<td>Resilience of offering</td>
<td>4 Reliable Infrastructure</td>
</tr>
<tr>
<td></td>
<td>Online transaction processing (OLTP)</td>
<td>7 Solution Offering</td>
</tr>
<tr>
<td></td>
<td>Geo-separation</td>
<td>4.1 Geographic Separation for High Availability</td>
</tr>
<tr>
<td></td>
<td>Longer-term costs</td>
<td>8 Cost Management</td>
</tr>
<tr>
<td></td>
<td>Modernise or replace</td>
<td>9.1 Review and Planning</td>
</tr>
<tr>
<td>Cloud Advice Note Section</td>
<td>Key Concept</td>
<td>eBook Section</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td>---------------</td>
</tr>
<tr>
<td>7. Considerations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.3 Public or Private</td>
<td>Access to infrastructure</td>
<td>5.2 Data Classification</td>
</tr>
<tr>
<td></td>
<td>Private network access</td>
<td>5.5 Data Security</td>
</tr>
<tr>
<td></td>
<td>Data retention and obligations</td>
<td>5.2 Data Classification</td>
</tr>
<tr>
<td></td>
<td>Archive requirements</td>
<td>5.3 Data Privacy</td>
</tr>
<tr>
<td></td>
<td>Skills to use and maintain infrastructure</td>
<td>5.4 Data Control</td>
</tr>
<tr>
<td>7.4 Data-Sharing and Re-use</td>
<td>Secure exchange of data</td>
<td>5.1 Data Sharing and Reuse</td>
</tr>
<tr>
<td></td>
<td>Improved service delivery</td>
<td>5.1 Data Sharing and Reuse</td>
</tr>
<tr>
<td></td>
<td>Standardisation of system and practices</td>
<td>9.2 Review and Planning</td>
</tr>
<tr>
<td>7.5 Data Processing vs Storage vs In Transit</td>
<td>Encryption</td>
<td>5.3 Data Privacy</td>
</tr>
<tr>
<td></td>
<td>Lifecycle management</td>
<td>5.3 Data Privacy</td>
</tr>
<tr>
<td></td>
<td>Track record and maturity</td>
<td>Abstract 1 Introduction</td>
</tr>
<tr>
<td></td>
<td>Data in EEA</td>
<td>4.3 Control Over Location</td>
</tr>
<tr>
<td></td>
<td>Access through APIs</td>
<td>5.4 Data Control</td>
</tr>
<tr>
<td></td>
<td>Latency</td>
<td>4 Reliable Infrastructure</td>
</tr>
<tr>
<td>7.6 Timing</td>
<td>Iterative approach</td>
<td>9.2 Procuring Cloud</td>
</tr>
<tr>
<td></td>
<td>Skills for development</td>
<td>2.1 Supporting Skills Enablement</td>
</tr>
<tr>
<td>Cloud Advice Note Section</td>
<td>Key Concept</td>
<td>eBook Section</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>7. Considerations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.7 Governance</td>
<td>Security management process</td>
<td>5.5 Data Security</td>
</tr>
<tr>
<td></td>
<td>Standards</td>
<td>6 Compliance and Standards</td>
</tr>
<tr>
<td></td>
<td>Division of responsibility</td>
<td>3 The Division of Responsibility</td>
</tr>
<tr>
<td></td>
<td>Audits</td>
<td>5.5 Data Security</td>
</tr>
<tr>
<td></td>
<td>Exit strategy</td>
<td>9.2 Procuring Cloud</td>
</tr>
<tr>
<td></td>
<td>Data retention</td>
<td>5.4 Data Control</td>
</tr>
<tr>
<td></td>
<td>Cloud access security broker (CASB)</td>
<td>9.2 Procuring Cloud</td>
</tr>
<tr>
<td>7.8 Contractual Cover</td>
<td>Contract terms</td>
<td>9.2 Procuring Cloud</td>
</tr>
<tr>
<td></td>
<td>Service Level Agreement</td>
<td>9.2 Procuring Cloud</td>
</tr>
<tr>
<td></td>
<td>Technical support</td>
<td>7.1 Services</td>
</tr>
<tr>
<td></td>
<td>Avoidance of lock-in</td>
<td>9.2 Procuring Cloud</td>
</tr>
<tr>
<td></td>
<td>Multi-cloud approach</td>
<td>9.2 Procuring Cloud</td>
</tr>
<tr>
<td></td>
<td>Legal jurisdiction</td>
<td>4.3 Control Over Location</td>
</tr>
<tr>
<td></td>
<td>Office of Government Procurement guidance</td>
<td>Abstract / 1 Introduction</td>
</tr>
<tr>
<td></td>
<td>Procurement</td>
<td>9.2 Procuring Cloud</td>
</tr>
<tr>
<td></td>
<td>Procurement</td>
<td>9.2 Procuring Cloud</td>
</tr>
<tr>
<td></td>
<td>Costs</td>
<td>8 Cost Management</td>
</tr>
<tr>
<td></td>
<td>Skills</td>
<td>2.1 Supporting Skills Enablement</td>
</tr>
<tr>
<td></td>
<td>Technology stack</td>
<td>7 Solution Offering</td>
</tr>
<tr>
<td>Cloud Advice Note Section</td>
<td>Key Concept</td>
<td>eBook Section</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>9. Other Matters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.1 Data Protection</td>
<td>Data Protection Commission guidance (DPC)</td>
<td>5 Reliable Infrastructure</td>
</tr>
<tr>
<td></td>
<td>The European Data Protection Board (EDPB) territorial scope of the GDPR</td>
<td>5.3 Data Privacy</td>
</tr>
<tr>
<td></td>
<td>European Union Agency for Network and Information Security (ENISA)</td>
<td>6 Compliance and Standards</td>
</tr>
</tbody>
</table>
Appendix B. Additional Case Studies

The World Health Organisation (WHO)

The World Health Organization (WHO) worked with AWS to develop the WHO Academy (WHOA) app, which was designed to equip frontline health workers with extensive educational resources and continuously updated guidelines and tools for the coronavirus. It was developed based on a March 2020 survey of 20,000 WHO Academy global health workers in which the majority of respondents expressed a need for more on-demand virtual learning tools so they could be more prepared for coronavirus infection prevention and control.

Using the AWS Cloud, WHO developed a tool that enabled specific classifications of large volumes of COVID-19-related content from around the globe using ML. And when traffic to the WHO website increased almost eightfold, AWS provided WHO with increased computational capacity to help them scale rapidly and support the surge in demand, helping to ensure that users around the world could access the website at any time. AWS enables up-to-the-minute educational information and guidance on the coronavirus and by employing AWS’s data analytics prowess, systems can now retain a substantial amount of information—which WHO can distribute widely and rapidly to public health entities, WHO member states, and health organisations. To learn more about how AWS helped the WHO respond to COVID-19, view the Amazon News webpage.

The World Health Organisation (WHO)

The Cork Institute of Technology delivers cloud education by extending the classroom and increasing skillsets to include cloud education. Working with AWS, the Cork Institute of Technology was able to deliver cloud-based virtual classrooms, virtual desktops, and virtual lab environments to students in remote areas, removing disadvantages due to location. The learning management system (LMS) helped students feel less isolated and helped them communicate more effectively during lectures and with their peers. With these options, students could gain the theoretical and practical skills in cloud computing by using cloud technology.

Learn more by reviewing the AWS Summit London: Cloud Transformation in Education video on YouTube, where Pat McCarthy, lecturer and course coordinator of cloud computing, discusses how AWS is used to deliver virtual lectures as if the students were in the classroom.
The Health Service Executive

To help reduce the spread of COVID-19 in Ireland, the Irish Health Service Executive (HSE) used AWS to build a scalable and reliable COVID Tracker application. With AWS, HSE gained the agility and scalability needed to develop, test, and build the first prototype of the app. The first version of the app was available in just two days. Designed to improve the speed, accuracy, and effectiveness of contact tracing, the app received one million downloads in the first 36 hours and 1.54 million downloads by the fourth week, equivalent to 30 percent of Ireland’s population. Because of the cloud’s elasticity, the COVID Tracker app can seamlessly scale to meet fluctuating demands as pandemic activity changes.

Appendix C. Appendix C. AWS Shared Responsibility Model

Security and compliance responsibilities are shared between AWS and the customer. This shared responsibility model can help relieve customers’ operational burdens as 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 service operates.

Customers—and in some cases, the APN Partners who work with those customers—control how they architect and secure their applications and data in the AWS Cloud. AWS provides a wide array of security and compliance services—a customer’s responsibilities will vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations.

As shown in Figure 1 below, this differentiation of responsibility is commonly referred to as security of the cloud versus security in the cloud.

For more information on customer and AWS responsibilities under the shared responsibility model, view the AWS webpage.
Appendix D. AWS Shared Responsibility Model for Sustainability

As PSBs align their organisations with sustainable practices, it is important to review every functional area. If a PSB is building, deploying, and maintaining an IT stack, improving the environmental impact requires informed decision making.

At AWS, we are committed to running our business in the most environmentally friendly way possible. We also work to enable our customers to use the benefits of the cloud to better monitor and optimise their IT infrastructure.

That being said, sustainability is a shared responsibility between AWS and customers. As shown in Figure 2, AWS optimises for sustainability of the cloud, while customers are responsible for sustainability in the cloud, meaning they must optimise their workloads and resource utilisation.

For more information on AWS sustainability practices, please refer to the AWS sustainability in the cloud webpage, or the AWS architecture blog.
Appendix E. Additional Resources

For more support and information, please refer to the following resources:

- Adopting Cloud Technology - Guidance for Public Sector Organisations in Ireland
- Procuring Cloud Technology - Guidance for Public Sector Organisations in Ireland
- Hybrid Cloud with AWS
- Protecting Data Using Encryption
- AWS Security Best Practices
- Unpicking Vendor Lock-in
- Ten Considerations for a Cloud Procurement
- Cloud Computing Cloud Advice Note
- Cloud Services Procurement Guidance Note
- Irish Public Service Innovation Strategy

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. 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.

© 2021 Amazon Web Services, Inc. or its affiliates. All rights reserved.
Endnotes

4. https://twitter.com/IRLDeptPER/status/1360172728708452352
5. Information and Communications Technology, Dáil Éireann Debate, March 2021.
11. Wellolla, AWS Case Study.
14. On 16 July 2020, the Court of Justice of the European Union (CJEU) issued a ruling regarding the transfer of personal data of EU individuals outside the EEA (Schrems II). In Schrems II, the CJEU ruled that the EU-US Privacy Shield was no longer a valid mechanism to transfer personal data from the EEA to the US. However, in the same ruling, the CJEU confirmed that companies can (subject to implementing supplementary measures, if required) continue to use Standard Contractual Clauses as a valid mechanism for transferring personal data outside of the EEA. The European Data Protection Board (EDPB), a European body composed of representatives of the national data protection authorities, has since provided a non-exhaustive list of supplementary measures in its “Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data” (EDPB Recommendations).
15. The Health Service Executive, AWS Case Study.
25. DVLA Enlisted Mobilise to Create Cloud Center of Excellence on AWS, AWS Case Study.