Irish Public Sector Kickstart Whitepaper

December 2023

Table of Contents

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 and is subject to change. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services. 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. For current prices for AWS services, please refer to the AWS website at www.aws.amazon.com.

List of Figures

List of Tables

Abstract

This whitepaper is written for Irish public sector organisations and their technology partners, as part of the Amazon Web Services (AWS) Public Sector Kickstart program in Ireland (IE PS Kickstart). IE PS Kickstart offers prescriptive guidance on how Irish public sector bodies can quickly realise the value from AWS Cloud. The program provides funding options to offset the initial costs of cloud adoption and cloud skills support from AWS as you progress.

As part of the program, this whitepaper is intended to be a single go-to handbook introducing AWS Cloud in relation to the Irish public sector. The whitepaper:

- Details AWS's presence in Ireland.
- Introduces prescriptive technical guidance on AWS Cloud offerings.
- Describes how to work with AWS Partners in Ireland.
- Outlines guidance on how to procure AWS Cloud offerings.
- Provides information and contact details to enable the next stage of IE PS Kickstart.

The concepts are aimed at accelerating an organisation's cloud adoption. The customer examples include AWS customers in the Irish public sector that are using AWS Cloud to effectively accelerate innovation and digital transformation.

The technical offerings presented are solutions specific to Ireland. These include the AWS Direct Connect service via government networks and the AWS Landing Zone Accelerator solution that deploys a secure, compliant, scalable, and fully automated cloud foundation with industry and region-specific security and compliance blueprints.

The program provides guidance on architectures, and extensive security and compliance offerings that help public sector organisations meet strict standards.

1 Introduction

In 2006, AWS began offering IT infrastructure services to businesses as web services—now commonly known as cloud computing. Cloud computing allows organisations to access technology services, such as computing power, storage, and databases, as needed, instead of owning and maintaining their own physical data centres and servers. A key benefit of cloud computing is the opportunity to replace and supplement fixed upfront expenses such as infrastructure, hardware, software, data centre with ongoing variable costs that scale with your business needs.

Our parent company, Amazon, launched AWS so that other organisations could benefit from Amazon’s experience and investment in running a large-scale, distributed, and transactional IT infrastructure. Since its launch, AWS has been serving millions of active customers every month worldwide.

2 AWS in Ireland

The first AWS Region was launched in Ireland in 2007. AWS has significantly expanded operations in recent years. To establish the impact of that investment, AWS commissioned Indecon, an economic consultancy, to perform an independent analysis of AWS investments between 2012 and 2022. They found that:

- AWS investment increased the economic output in Ireland by more than €11.4 billion
- In 2022 alone, AWS investment supported €2.4 billion in additional economic output – a ten fold increase compared to the corresponding figure in 2011.
- AWS supported more than 10,000 jobs across the country

Indecon estimates that between initiatives funded by the AWS InCommunities program (€3.5 million) and the value of volunteering provided by AWS staff (€200,000), AWS has invested nearly €3.7 million in community engagement since 2018.

2.1 Region in Ireland

AWS maintains a global footprint to serve customers across the world. AWS maintains multiple Regions in North America, South American, Europe, Asia Pacific, and the Middle East. Each AWS Region is a separate geographic area. Each AWS Region has multiple, isolated locations known as Availability Zones.

The AWS **Europe (Ireland) Region** has three availability zones. An Availability Zone (AZ) consists of one or more discrete data centres with independent and redundant power infrastructure, networking, and connectivity in an AWS Region. AZs in a Region are meaningfully distant from each other, up to 60 miles (~100 km) to prevent correlated failures, but close enough to use synchronous replication with single-digit millisecond latency.

AWS has 6 Regions in the European Economic Area (EEA): Ireland, Frankfurt, Paris, Stockholm, Milan and Spain. Each of these Regions has 3 AZs.

2.2 Developing Local Tech Skills

Beyond investment in data centres, AWS made direct and focused investments into Irish communities to empower the next generation of tech practitioners and future builders.

In collaboration with the Technological University Dublin, AWS developed a bursary program called the Data Centre Technician program to help students learn the necessary skills for a career in cloud data centres. The program includes courses to train students on a range of technical tasks associated with data centre hardware and networking systems, such as software installation, configuration, maintenance, repair, and security. Students learn the skills of cloud computing and are offered a chance to the test their skills with paid work placements with AWS. Local people improve their skills, secure invaluable hands-on experience, and, in some cases, achieve full-time employment. As of 2023, the first 20 students graduated through the program, which is in its sixth year.

2.3 Commitment to Social Value in Ireland

Education has been a particular focus for AWS in Ireland, as shown in the following educational initiatives.

AWS GetIT. In 2020, AWS launched AWS GetIT in Ireland. This is a complementary program specially designed to introduce more 12–13 year old students—particularly girls—to cloud computing and digital skills to inspire them to pursue a career in technology. GetIT invites teams from different schools to participate in an app-building competition to solve real issues faced by their school or community.

AWS re/Start Ireland. In 2020, AWS launched AWS re/Start Ireland, a skills development and job training program that aims to build local talent by providing AWS Cloud skills development and job opportunities at no cost to learners from unemployed, under-employed, and under-represented members of Ireland’s communities.

AWS Think Big Space. Created together with South Dublin County Council and South Dublin Libraries, the AWS Think Big Space provides a place beyond the classroom for students to explore and cultivate an interest in science, technology, engineering, arts, and maths and their related careers. AWS Think Big Space provides access to high-quality resources for learning about cloud computing and technology.

2.4 Supporting Small and Medium Irish Enterprises

AWS is committed to supporting local Irish businesses through developing and growing the AWS Cloud infrastructure footprint in Ireland. Since 2018, AWS has spent more than €550 million with indigenous small and medium enterprises. Over €300 million of this was spent in the direct supply chain domestically and over €250 million was spent in the direct supply chain internationally.

3 AWS and the Irish Government

Tallaght University Hospital
Ospidéal Ollscoile Thamhlachta
An Academic Partner of Trinity College Dublin
Doctors on Call
Care Doc
Revenue
Comhairle Contae Mhuineacháin
Monaghan County Council
Swiftqueue
Dedalus group
CO-ORDINATED HEALTHCARE... EMPOWERED
NCBI
Working for People with Sight Loss
HSE
Leitrim County Council
Comhairle Chontae Liatroma
Hibernian HEALTHCARE
www.hibernianhealth.com
Comhairle Contae Chiarraí
Kerry County Council
FULLHEALTH MEDICAL
Realizeit
terminalfour
An Phríomh-Oifig Staidrimh
Central Statistics Office
ispcc
NBI
National Broadband Ireland
Irish Refugee Council 30 years
IRISH HORSERACING REGULATORY BOARD
wellola

Figure 1. Selection of Irish Public Sector AWS Customers

From 2011 to 2020, AWS invested over €4.4 billion in Ireland through direct and operational spend. With more than 5,000 direct employees, AWS is one of the largest private sector employers in the country. We work closely with the Irish public sector to support their digitalisation initiatives. For example, we provided the underlying cloud computing infrastructure for the COVID Tracker app, a digital contact tracing mobile app by the Irish Government and the Health Service Executive (HSE). AWS Cloud also hosts gov.ie, the Government of Ireland's public platform; our infrastructure is able to meet the ever-increasing demand for information concerning government services. Figure 1 displays examples of our public sector customers.

3.1 Office of Government Chief Information Office

The Office of Government Chief Information Office (OGCIO) set an ambitious target to provide EU Digital COVID Certificates to all Irish citizens who were vaccinated against, or have recovered from, the COVID-19 virus. More than two million certificates had to be created and distributed via email or print and post. To enable the deployment, the OGCIO utilised AWS Managed Services to collect, generate, and send the digital certificates. The solution consisted of an API-powered portal that allowed testing laboratories and pharmacies to upload data, as well as functionality to issue certificates via email or print and post. The solution is now running in the EU (Ireland) AWS Region.

As an example of the scale needed to accomplish this task, approximately one million emails were sent over a two-day period in July 2021. Gov.ie, developed by a team based at the OGCIO and hosted on AWS Cloud, expanded from 6 million visits in 2019 to 80 million in 2021.

3.2 Health Service Executive

To help reduce the spread of COVID-19 in Ireland, the Irish 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 by the fourth week, equivalent to 30 percent of Ireland's population. Because of the cloud's elasticity, the COVID Tracker app was able to seamlessly scale to meet fluctuating demands as pandemic activity changes.

3.3 National Broadband Ireland

National Broadband Ireland (NBI) was tasked with implementing Ireland’s National Broadband Plan (NBP), an Irish government initiative to deliver high-speed broadband services to all underserved premises in the country. This was the largest telecommunications project contracted by the Irish government and one of the largest telecommunications infrastructure projects globally. Rolling out broadband connectivity to more than 1.1 million people across 569,000 premises meant NBI needed to build a network spanning 96 percent of the country.

> NBI uses AWS as the foundation of its platform to provide high-speed internet to 1.1 million Irish people.

NBI used AWS as the foundation of its platform, which enabled Ireland’s entire market of internet service providers (ISPs) to connect to the NBI network seamlessly and start selling fiber broadband connections directly to end-customers. The organisation went live in 9 months after starting beta testing. NBI deployed more than 50 AWS services and now operates with high availability, robust fault tolerance, and scalability.

3.4 Irish Society for the Prevention of Cruelty to Children

The Irish Society for the Prevention of Cruelty to Children (ISPCC) supports, empowers, and helps children and young people to build their resilience so that they can live their best possible lives. The ISPCC needed to replace its existing websites, digital platform, and supporting databases to continue to support and protect children in Ireland. Using generous funding from the Vodafone Ireland Foundation, ISPCC worked with AWS Partner, Singlepoint (acquired by Version 1 in May 2020), to create a cost-effective, secure, and resilient solution. Using AWS, ISPCC developed a new platform for Childline—a no cost, anonymous, and confidential 24-hour national listening service for children in Ireland.

The platform brings together a contact centre, webchat, and SMS services into a single view and enables ISPCC volunteers to respond to children and young people more quickly and effectively. Since launch, the ISPCC’s live online chat service has recorded a 45 percent increase in online contacts. Additionally, the ISPCC has introduced more interactive content and self-help options for children and parents via the platform.

4 Amazon and AWS Approach for Sustainability

As a founding member of the Climate Pledge, Amazon—including AWS—is committed to reaching net-zero carbon emissions by 2040, 10 years ahead of the Paris Agreement. Amazon and Global Optimism co-founded the Climate Pledge to encourage organisations to work together to address the climate crisis and solve the challenges of decarbonising our economy.

To date, over 300 companies across 29 countries have joined the Climate Pledge. Amazon committed to the Science Based Targets initiative in 2020, and AWS is a founding signatory of the Climate Neutral Data Centre Pact.

4.1 Renewable Energy

To achieve the decarbonisation aim, Amazon is on a path to power its operations with 100 percent renewable energy by 2025, five years ahead of its original 2030 commitment. In April 2022, Amazon extended its position as the world's largest corporate buyer of renewable energy with 380 global renewable energy projects. As of 2021, Amazon had reached 85 percent renewable energy across corporate offices, fulfilment centres, and AWS data centres that support millions of customers globally. See Amazon's Renewable Energy Methodology documentation for more details on our approach.

4.1.1 Renewable Energy Strategy in Ireland

The renewable energy strategy is evident in Ireland, where, in Feb 2021, Amazon's first operational windfarm came online in County Cork. The project is Ireland's first-ever wind farm to be built without public subsidies and is the first of three utility-scale renewables projects invested in by Amazon. These projects will deliver clean energy to the Irish grid and support the country in meeting its 2030 renewable energy targets.

- Amazon's renewable energy portfolio includes 176 rooftop solar projects 134 wind and solar farms added to the grids where they operate.
- Amazon's total committed renewable electricity production capacity is 15.7 GW
- The amount of clean energy produced by these projects will avoid the equivalent of the annual emissions of 3.7 million cars in the U.S., or about 17.3 million metric tonnes of CO_2.
- Amazon's utility-scale renewables projects in Ireland are projected to add 229 MW of renewable energy to the Irish grid each year, reducing carbon emissions by 366,000 tonnes of CO_2 and producing enough renewable energy to power 185,000 Irish homes annually

In Cork, the wind farm project is expected to deliver 68,000 megawatt hours (MWh) of clean energy annually, reducing annual carbon emissions by 32,000 tonnes of CO_2 and producing enough renewable energy to power 17,000 Irish homes per year. The company has also invested in wind farm projects in County Galway and County Donegal, both of which are due to become operational in 2023.

4.2 Energy Efficiency

Moving workloads to the cloud presents public sector organisations with the opportunity to reduce the environmental footprint of their IT operations. AWS Cloud infrastructure is up to five times more energy efficient than typical EU enterprise infrastructure. A report by 451 consulting, shows that companies in Europe can reduce their energy use by almost 80 percent by moving their compute workloads out of on-premises data centres to AWS.

Businesses could potentially reduce carbon emissions of an average workload by up to 96 percent when AWS reaches its goal of purchasing 100 percent of its energy from renewable sources, which we are on the path to do by 2025. This is because AWS's scale allows for energy efficiencies, and efficient resource usage.

> In 2022, AWS announced a Water Positivity commitment, which means that the organisation will return more water to communities than it uses in its direct operations by 2030.

4.3 Energy Efficiency in the Irish Community

AWS helps implement sustainability initiatives in the communities in which they operate.

In February 2023, the first phase of the EnergyCloud project was launched in Ireland. Supported by AWS, and running on the AWS Cloud, EnergyCloud uses technology solutions to take excess renewable energy from the Irish grid and provide it to an initial pilot of 50 Clúid properties in the form of a tank of hot water at zero cost, diverting energy from wind farms that would otherwise be wasted. Clúid are a not-for-profit charity who provide affordable homes to people in housing need. The goal of this initial phase is to reduce renewable energy wastage and instead divert it for social good to heat water in fuel-poor homes. The plan is for the project to expand over time to the entire Clúid Housing property portfolio of over 8,300 homes, thereby working to reduce fuel poverty for Clúid's more than 21,600 residents.

In April 2023, the Minister for Environment and Climate in Ireland, Mr. Eamon Ryan launched one of Ireland's first district heating programs with South Dublin County Council in collaboration with AWS. The Tallaght District Heating Scheme takes waste heat from our AWS data centre and uses it to heat South Dublin County Council offices and the local library. The heat is carried by hot water pumped through a network of insulated pipes. The scheme will also serve 133 affordable apartments to be built on public land in Tallaght and 3,500 sq./m innovation centre hosting tech start-ups on the same site. The council says that over the lifetime of the scheme it could also heat 2,000 to 3,000 apartments. It is expected to save 1,500 tonnes of carbon emissions per year in its current phase.

The Minister Mr. Eamon Ryan described the Tallaght scheme as "an example of the future being delivered today". He added: "Managing how we use heat and how we keep heat in is probably the biggest change we need to make to keep our climate targets".

5 AWS Partners

The AWS Partner Network (APN) is a global community of partners that uses programs, expertise, and resources to build, market, and manage AWS Cloud-based offerings.

5.1 AWS Partner Network

The APN has more than 100,000 partners with experience delivering for government, education, and non-profits located in more than 150 countries, with over 100 partners with offices in Ireland. We recommend that customers use the APN for support with architecting, delivering, and managing AWS Cloud–based solutions. For more information, and a complete list of AWS Partners, refer to the AWS Partner Network page.

5.2 AWS Public Sector Partner Program

The AWS Public Sector Partner Program distinguishes partners that have a public sector focus. Members of the program:

- Align closely with our public sector sales, marketing, partner, and bid teams
- Are designated as public sector partners in AWS Partner Solutions Finder
- Are eligibile for further unique benefits and differentiation programs, such as the AWS Channel Reseller Program, AWS Managed Service Program, AWS Competency Program, and AWS SaaS Partner Program (to name only a few).

5.3 Why Choose an AWS Partner?

Customers who work with the APN can be confident that the support they receive is informed by our best practices, technical expertise, and proven methodologies. This is because AWS Partners receive a variety of benefits that distinguish them from other vendors. AWS provides them with resources to assist their customers, including the following:

- **Training and Certifications:** AWS Partners have access to training, service information, certifications, and other AWS resources that help them become experts in the AWS Cloud. These resources help AWS Partners be more competent and effective in the solutions they offer to customers.
- **Corporate Resources:** AWS Partners have direct access to AWS corporate resources (such as business developers, engineers, and solutions architects) to help build and enhance solutions that work best for their customers. This level of cloud support is not normally available to vendors and companies that do not participate in the APN.

Customers seeking AWS solutions or wishing to use AWS as a cloud service provider can do so by engaging with a member of the APN. AWS Partners have the expertise to help customers deliver greater business value, become more agile, and lower costs. While AWS maintains, develops, and expands the AWS Cloud environment and the services available in it, our AWS Partners can architect, deliver, or manage additional solutions for customers, which they can use to undertake a variety of workloads.

5.4 AWS Competencies

AWS Partners can achieve AWS Competencies based on their expertise in AWS solution areas and proven customer success. Achieving any of the AWS Competencies—which requires meeting or exceeding several requirements and passing a third-party audit of capabilities—is a public indication of the AWS Partner's ability to excel in a specific area of expertise. See Table 1 for a selection of available competencies.

Table 1 Selection of Available AWS Competencies

Competency	Description
Education	AWS Education Competency Partners offer solutions that align with AWS architectural best practices to build mission-critical applications for educational institutions on the AWS Cloud.
Energy	This competency will introduce AWS Partners who completed a technical validation with AWS and demonstrated repeat success supporting energy customers worldwide.

Competency	Description
Government	AWS Government Competency Partners have demonstrated experience delivering solutions to help agencies meet mandates, reduce costs, drive efficiencies, and increase innovation at national and local government level.
Healthcare	AWS Healthcare Competency Partners have demonstrated technical expertise and success in building healthcare solutions on AWS that securely store, process, transmit, and analyse clinical information.
Migration	Migration Competency Partners help customers move applications to the AWS Cloud to reduce cost, increase agility, and improve security. AWS Partners with this competency have successfully demonstrated how they can help enterprise customers migrate applications and legacy infrastructure to AWS.
Non-profit	AWS recognises that non-profit customers must work with tight budgets and juggle the day-to-day of IT operations with their mission-critical workloads. With the help of AWS Non-profit Competency Partners, they can quickly and securely employ technology to support fundraising and program management.
Machine Learning	These partners offer a range of services and technologies to help customers create intelligent solutions for their business, from enabling data science workflows to enhancing applications with artificial intelligence and machine learning.

For more information, see https://aws.amazon.com/partners/programs/competencies/. You can also visit the Engage with AWS Partners page to read customer success stories, learn more about AWS Competencies, and search for AWS Partners by service, industry, workload, or solution. The Customer Success page provides additional information on how AWS Partners are helping customers achieve success in the AWS Cloud.

5.5 Choosing the Correct AWS Partner

AWS Account Managers can help customers find a suitable partner. There are many considerations when choosing the right type of partner, including their location, skill set, references, access to AWS support such as training and funding, and whether the partner is trained on Landing Zone Accelerator. Customers can use the AWS Partner Finder webpage to shortlist partners and discuss with the AWS Account team.

6 Procurement Landscape in Ireland for Public Sector

In Ireland, as of 2023, the Office of Government Procurement (OGP) does not have a cloud-specific procurement framework for public sector bodies (PSBs) to purchase cloud services. PSBs have two options to procure cloud: use an existing framework or a one-off cloud procurement.

6.1 Use an Existing Framework

While there is no cloud-specific framework available, PSBs can use various OGP frameworks to procure elements of the cloud. These frameworks have a defined scope and would need to be reviewed in terms of suitability on a case by case basis.

All member institutions of HEAnet (see https://www.heanet.ie/who-we-are/our-clients) can use the Open Clouds for Research Environments (OCRE) framework. Although AWS is not on the framework directly, Rackspace Technology, an AWS Partner, is the single supplier appointed for AWS services in Ireland. HEAnet members can procure all AWS services using the OCRE framework through Rackspace.

For any questions or queries relating to public sector frameworks in Ireland, please reach out to the AWS Capture Manager or AWS Proposal Manager via email at wwps-cpt-ie@amazon.com.

6.2 One-Off Procurement Exercise

In the absence of a cloud procurement framework, PSBs can conduct a one-off procurement exercise. A shift from the traditional ICT procurement to the cloud requires a new approach to drafting tender documents. For example: terms and conditions, pricing, evaluation criteria, and contracting terms differ when procuring cloud as opposed to traditional IT.

To assist with performing a one-off cloud procurement, there are a number of resources available, including:

- The OGP Cloud Services Procurement Guidance Note
- Procuring Cloud Technology—Guidance for Public Sector Organisations in Ireland (AWS's supplementary response to the OGP Guidance Note)
- Cloud Services RFT Templates (Contact Centre as a Service) (industry templates from Ireland)
- The CISPE Buying Cloud Services in Public Sector handbook.

For any questions or queries related to a one-off cloud procurement exercise, reach out to the AWS Capture Manager or AWS Proposal Manager via email at wwps-cpt-ie@amazon.com.

7 Irish Government Network

The Irish Government Network is a wide area network offering carrier-grade, resilient, high-capacity private voice, video, and data network services across the public sector, nationwide. It is operated by the OGCIO in the Department of Public Expenditure and Reform.

The Irish Government Network uses AWS Direct Connect to provide a dedicated, redundant, high bandwidth, low latency connection to the AWS Europe (Ireland) Region. AWS Direct Connect is a networking service that provides an alternative to using the internet to connect to AWS. Using Direct Connect, data that would have previously been transported over the internet is delivered through a private network connection between your facilities and AWS. This allows government networks customers to securely access their AWS workloads without traversing the public internet.

This is the recommended way to get access to dedicated connection if you are a public sector body connected to Government Networks in Ireland.

7.1 Direct Connect

Use cases that benefit from Direct Connect include:

- **Hybrid Connectivity.** AWS Direct Connect helps you satisfy regulatory requirements that require private connectivity. These types of hybrid environments allow you to combine the elasticity and economic benefits of AWS while continuing to use your existing infrastructure.
- **Real-Time Applications.** For applications that use real-time data feeds, network latency is an issue because the internet is constantly changing how data gets from point A to B. With AWS Direct Connect, you control how your data is routed, for a more consistent network experience compared to internet-based connections.

- **Working With Large Datasets.** Transferring large datasets over the internet can be slow when your critical network traffic must compete for bandwidth with other network traffic. To decrease the time required to transfer your data, you could increase the bandwidth to your internet service provider, but this frequently requires a costly contract renewal and a minimum commitment. With AWS Direct Connect, you can transfer your business-critical data directly from your data centre, office, or co-location environment into and from AWS, bypassing your internet service provider and removing network congestion.

As part of the AWS Public Sector Kickstart program, AWS can help facilitate an AWS Direct Connect connection, via the Government Network, to your workloads running in the EU (Ireland) Region. The Direct Connect connection will terminate in your landing zone, allowing use by all of your workloads running on the AWS Cloud. You can choose your required bandwidth, and whether you want a single or a redundant connection. For more information, see the Connecting to AWS via Irish Government Networks whitepaper.

8 Well-Architected Framework

The AWS Well-Architected Framework provides a way to consistently measure your architectures against AWS best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the cloud. It describes strategies to use when operating a cloud workload, and provides links to further implementation details and architectural patterns. It is not an audit mechanism. Rather, the process for a constructive conversation about architectural decisions. The framework is intended for those in technology roles, such as chief technology officers, architects, developers, and operations team members.

The AWS Well-Architected Framework helps you understand the pros and cons of decisions you make while building systems on AWS, and identify areas for improvement. The framework involves a set of foundational questions that allow you to understand if a specific architecture aligns well with cloud best practices. The framework provides a consistent approach to evaluating systems against the qualities you expect from modern cloud-based systems, and the remediation that would be required to achieve those qualities.

AWS solutions architects have years of experience architecting solutions across a wide variety of business verticals and use cases. As AWS continues to evolve, and we continue to learn more from working with our customers, we will continue to refine the definition of well-architected. We believe that having well-architected systems greatly increases the likelihood of business success. We have helped design and review thousands of customers' architectures on AWS. From this experience, we have identified successful practices and strategies for architecting systems in the cloud.

We also provide a no-charge service for reviewing your workloads. The AWS Well-Architected Tool (AWS WA Tool) is a service in the cloud that provides a consistent process for you to review and measure your architecture using the AWS Well-Architected Framework. The AWS WA Tool recommends ways to make your workloads more reliable, secure, efficient, and cost-effective.

To help you apply best practices, we have created AWS Well-Architected Labs. These are repositories of code and documentation to give you hands-on experience implementing best practices. We also have teamed up with select AWS Partners, who are members of the AWS Well-Architected Partner program. These AWS Partners have deep AWS knowledge, and can help to review and improve your workloads. For more information, see https://aws.amazon.com/architecture/well-architected/.

The AWS Well-Architected Framework is based on six pillars — operational excellence, security, reliability, performance efficiency, sustainability, and cost optimisation, described in Table 2.

Table 2. Pillars of the Well-Architected Framework

Pillar	Narrative
Operational excellence	The ability to support development and run workloads effectively, gain insight into their operations, and to continuously improve supporting processes and procedures to deliver business value.
Security	Describes how to take advantage of cloud technologies to protect data, systems, and assets in a way that can improve your security posture.
Reliability	Encompasses the ability of a workload to perform its intended function correctly and consistently when expected. This includes the ability to operate and test the workload through its total lifecycle.
Performance efficiency	The ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.
Cost optimisation	The ability to run systems to deliver business value at the lowest price point.
Sustainability	The ability to continually improve sustainability impacts by reducing energy consumption and increasing efficiency across all components of a workload by maximising the benefits from the provisioned resources and minimising the total resources required.

When architecting workloads, you make trade-offs between pillars based on your business context. These business decisions can drive your engineering priorities. You might optimise to improve sustainability impact and reduce cost at the expense of reliability in development environments. For mission-critical solutions, you might optimise reliability with increased costs and sustainability impact. In ecommerce solutions, performance can affect revenue and customer propensity to buy. Security and operational excellence are generally not traded-off against the other pillars.

9 Security

Cloud security is our top priority. As an AWS customer, you benefit from data centres and network architectures that are built to meet the requirements of the most security-sensitive organisations.

9.1 The Shared Responsibility Model

Security and compliance are shared responsibilities between AWS and the customer. This is because AWS operates, manages, and controls the components from the host operating system and virtualisation layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches) and other associated application software, in addition to the configuration of the AWS-provided security group firewall. Depending on the services deployed, this shared model can help relieve the customer's operational burden. The nature of this shared responsibility also provides the flexibility and customer control that permits customers to deploy solutions that meet industry-specific certification requirements.

The shared responsibility model, described in Figure 2, involves security of the cloud and security in the cloud:

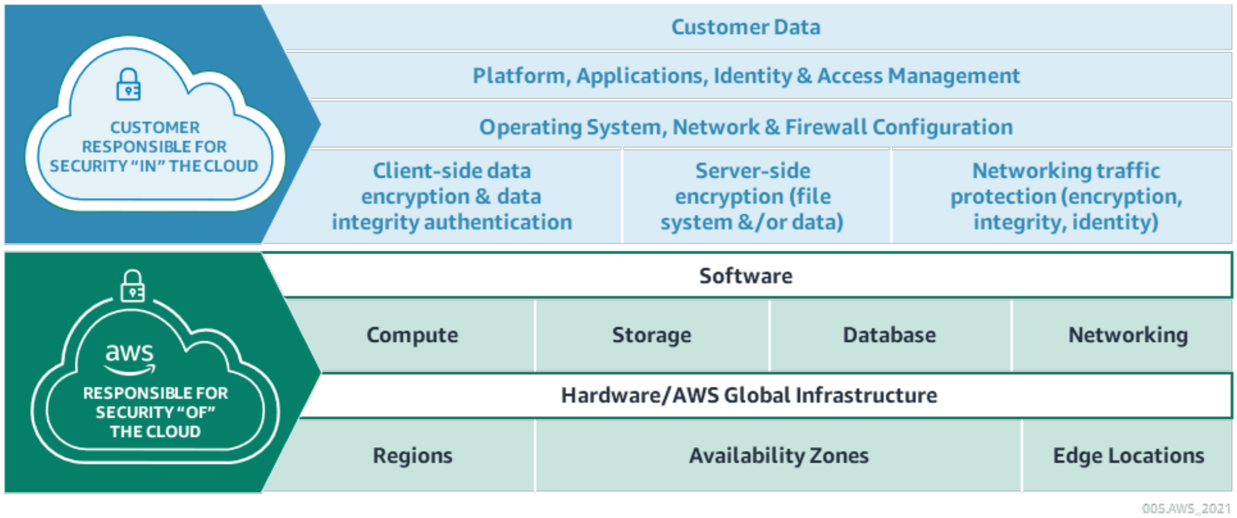
CUSTOMER RESPONSIBLE FOR SECURITY "IN" THE CLOUD
Customer Data
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-side data encryption & data integrity authentication
Server-side encryption (file system &/or data)
Networking traffic protection (encryption, integrity, identity)
aws
RESPONSIBLE FOR SECURITY "OF" THE CLOUD
Software
Compute
Storage
Database
Networking
Hardware/AWS Global Infrastructure
Regions
Availability Zones
Edge Locations
005.AWS_2021

Figure 2. AWS Shared Responsibility Model for Security

- **Security of the Cloud.** We are responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. We also provide you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to AWS Identity and Access Management (IAM), see AWS Services in Scope by Compliance Program.
- **Security in the Cloud.** Your responsibility is determined by the AWS service that you use. You are responsible for the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, the management, operation, and verification of IT controls is also a shared responsibility. AWS can help customers by managing those controls associated with the physical infrastructure deployed in the AWS environment. Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required.

We recommend that customers carefully consider the services they choose because their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. It is possible for customers to enhance their security or meet their more stringent compliance requirements by using technology such as host-based firewalls, host-based intrusion detection and prevention, encryption, and key management. For more information, see https://aws.amazon.com/compliance/shared-responsibility-model/.

9.2 Data Protection and Privacy

Storage of content presents all organisations with a number of common practical matters to consider, including:

- Will the content be secure?
- Where will content be stored?
- Who will have access to content?
- What laws and regulations apply to the content and what is needed to comply with these?

These considerations are not new and are not cloud-specific. They are relevant to internally hosted and operated systems and traditional third-party hosted services. Each may involve storage of content on third-party equipment or on third-party premises, with that content managed, accessed, or used by third-party personnel. When using AWS services, each AWS customer maintains ownership and control of their content, including control over:

- What content they choose to store or process using AWS services
- Which AWS services they use with their content
- The Regions where their content is stored
- The format, structure, and security of their content, including whether it is masked, anonymised, or encrypted
- Who has access to their AWS accounts and content, and how those access rights are granted, managed, and revoked.

Because AWS customers retain ownership and control over their content within the AWS environment, they also retain responsibilities relating to the security of 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 privacy and data protection requirements that may apply to content that customers choose to store or process using AWS services. Read more at, Using AWS in the Context of Common Privacy and Data Protection Considerations.

9.3 Security Certifications

Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS System and Organisation Control (SOC) 1, 2, and 3 reports; ISO 27001, 27017, 27018, and 9001 certifications; and PCI DSS Attestation of Compliance.

The AWS ISO 27018 certification demonstrates that AWS has a system of controls in place that specifically addresses the privacy protection of customer content. These reports and certifications are produced by independent third-party auditors, and attest to the design and operating effectiveness of AWS security controls.

9.4 AWS Certifications, Programs, Reports, and Third-Party Attestations

We regularly undertake independent third-party attestation audits to assure our control activities are operating as intended. We are audited against a variety of global and regional security frameworks dependent on location and industry. We participate in over 50 different audit programs.

Audit results are documented by the assessing body and made available for all AWS customers through AWS Artifact, a no-cost self-service portal for on-demand access to AWS compliance reports. New reports are available in AWS Artifact once they are released, allowing customers to continuously monitor the security and compliance of AWS with immediate access to new reports. See Figure 3 for a selection of AWS international certifications and accreditations.

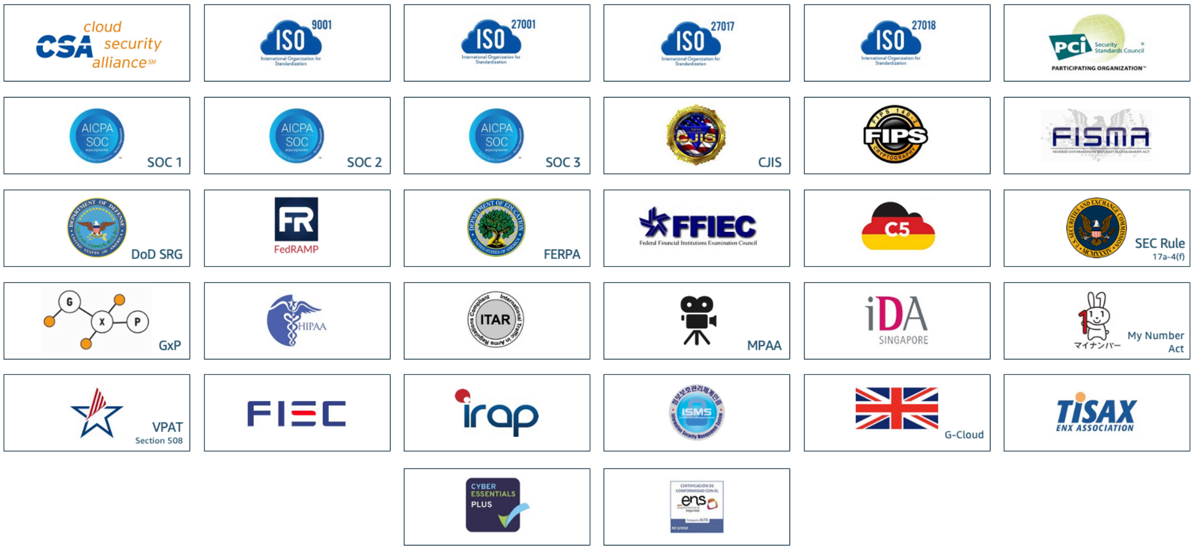

Figure 3. Selection of AWS Certifications and Accreditations

Depending on a country's or industry's local regulatory or contractual requirements, AWS may also undergo audits directly with customers or governmental auditors. These audits provide additional oversight of the AWS control environment so that customers have the tools to help themselves operate confidently, compliantly, and in a risk-based manner using AWS services.

For more detailed information about the AWS certification programs, reports, and third-party attestations, visit the AWS Compliance Program webpage. You can also visit the AWS Services in Scope webpage for service-specific information.

10 AWS Landing Zone

A landing zone is a well-architected, multi-account AWS environment that is scalable and secure. This is a starting point from which your organisation can quickly launch and deploy workloads and applications with confidence in your security and infrastructure environment. Building a landing zone involves technical and business decisions to be made across account structure, networking, security, and access management in accordance with your organisation's growth and business goals for the future.

10.1 Landing Zone Accelerator

Landing Zone Accelerator on AWS is an open-source solution that will help customers quickly deploy a secure, compliant, scalable, and fully automated cloud foundation. Landing Zone Accelerator is architected to align with AWS best practices, and, when used in coordination with services such as AWS Control Tower, it provides a simplified no-code solution to manage and govern a multi-account environment built to support customers with complex compliance requirements. This is the recommended way of setting up your infrastructure with prescriptive guidance on security and governance.

AWS Control Tower offers the easiest way to set up and govern a secure, compliant, multi-account AWS environment based on prescriptive best practices. Using AWS Control Tower, customers can provision their accounts and infrastructure while complying with corporate standards and regulations.

10.2 Benefits of Landing Zone Accelerator

With Landing Zone Accelerator on AWS, customers can more quickly deploy their AWS infrastructure, meet compliance requirements, and focus their energy on serving their own customers and citizens.

Improve Security. Having a single, managed codebase improves quality and security for customers. Security and compliance are baked in, and any new features or improvements made to the Landing Zone Accelerator during an engagement can be captured and merged with the open-source solution, allowing for continuous improvement and tight engagement security.

Drive Velocity. Landing Zone Accelerator speeds the customer's time to value, reduces their cost to implement, facilitates use of security best practices, and focuses their resources on high-value opportunities for mass migration, next-generation serverless application development, and reinvention in the cloud.

Increase Simplicity. Landing Zone Accelerator simplifies the complex approaches taken to building multi-account AWS environments for customers, and reduces the probability of defects, as much of the engineering, code development, and testing has been done before the engagement.

Reduce Technical Debt. With a modular design, customers and AWS only use the components necessary for the engagement. Customers can self-support after an engagement, with no-charge access to improvements or new features when released into open-source.

Cost. There are no additional charges or upfront commitments required to use Landing Zone Accelerator on AWS. You pay only for AWS services enabled to set up your platform and operate your guardrails.

10.3 Landing Zone Accelerator Within Specific Industries

To help various industries better manage the risks they confront, Landing Zone Accelerator solutions are created with a specific configuration. The setup employs controls from the following frameworks to support these organisations.

10.3.1 Education

- International Traffic in Arms Regulations (ITAR)
- National Institute of Standards and Technology (NIST) 800-171
- NIST 800-53
- Cybersecurity Maturity Model Certification (CMMC)
- International Organization for Standardization (ISO) 27001 and ISO 27002.

10.3.2 Health

- Health Insurance Portability and Accountability Act (HIPAA)
- National Cyber Security Centre (NCSC)
- Esquema Nacional de Seguridad High

- Cloud Computing Compliance Controls Catalog (C5)
- Fascicolo Sanitario Elettronico.

10.3.3 National Security, Defence, and Law Enforcement (Outside US)

- National Institute of Standards and Technology (NIST)
- Information Technology Standards Guidance (ITSG)-33
- Federal Risk and Authorization Management Program (FedRAMP)
- Information Security Registered Assessors Program.

The Trusted Secure Enclaves Sensitive Edition (TSE-SE) for National Security, Defence, and National Law Enforcement reference architectures for national security, defence, and national law organisations, guide the creation of multi-account AWS Cloud architecture for mission-critical and sensitive workloads on AWS with unique security. TSE-SE is designed to address customer concerns such as scalability, agility, high availability, cost, data security, network security and segmentation, and central identity access.

10.4 Where Can Customers Access the Landing Zone Accelerator?

- The Landing Zone Accelerator is published on the AWS Solution Library at https://aws.amazon.com/solutions/.
- The implementation guide, documentation, and necessary information are publicly accessible at https://github.com/awslabs/landing-zone-accelerator-on-aws.
- You can find industry based configurations and source code at https://github.com/awslabs/landing-zone-accelerator-on-aws/tree/main/reference/sample-configurations.

For further questions, reach out to your point of contact at AWS.

10.5 Funding Available for AWS Landing Zone Accelerator Solution

AWS Partners can integrate AWS services into offerings and launch solutions built on AWS, faster and more efficiently. To help eligible AWS Partners offset costs for deploying the Landing Zone Accelerator on AWS solution, AWS offers Partner programs that offer funding benefits. Eligible partners receive funding benefits if the necessary conditions and requirements are met. The funding amount depends on the size of the initial workload and the annual revenue rate it generates. To inform a potential funding amount, reach out to your AWS Account Manager. For information on wider partner funding options, see https://aws.amazon.com/partners/funding/.

Funding depends on the size of your initial workload's Annual Recurring Revenue (ARR). For workloads scoped at $300K ARR or lower, the Landing Zone Accelerator engagement is eligible for up to 45 percent of the workload’s ARR, paid at the end of the engagement. Often this amount will offset most, if not all of, Landing Zone Accelerator and the first workload project delivered by AWS Partners.

11 Conclusion

As part of the AWS IE PS Kickstart initiative in Ireland, this whitepaper helps to inform decisions on how to quickly realise value from AWS Cloud. The information, resources, and funding options that are specific to Ireland, accelerates the time to value for your organisation’s digital transformation. To discuss the available cloud offerings and solutions that are specific to your organisation, get in touch with the AWS public sector team in Ireland through https://aws.amazon.com/government-education/contact/. The AWS team works collaboratively to review use cases that are specific to your organisation's needs and presents offerings that are available as part of IE PS Kickstart initiative. This includes a guided plan for assessing and onboarding your organisation to the AWS Cloud.

12 Appendix

Appendix 1 : Security and Protection Guidance

1. Detection

1.1 AWS Security Hub

AWS Security Hub is a cloud security posture management service that checks security practices, aggregates alerts, and enables automated remediation. It collects security data from across AWS accounts, services, and supported third-party products and helps you analyse your security trends and identify the highest priority security issues. Security Hub provides you with a comprehensive view of your security state in AWS and helps you check your environment against industry standards and practices.

1.2 AWS Foundational Security Best Practices Standard

The AWS Foundational Security Best Practices standard is a set of controls that detect when your AWS accounts and resources deviate from security best practices. The standard lets you continuously evaluate all of your AWS accounts and workloads. It provides actionable and prescriptive guidance about how to improve and maintain your organisation’s security posture.

The controls include security best practices for resources from multiple AWS services. Each control is also assigned a category that reflects the security function that it applies to. For more information, see https://docs.aws.amazon.com/securityhub/latest/userguide/control-categories.html.

1.3 Center for Internet Security AWS Foundations Benchmark v1.2.0 and v1.4.0

The Center for Internet Security (CIS) AWS Foundations Benchmark serves as a set of security configuration best practices for AWS. These industry-accepted best practices provide you with clear, step-by-step implementation and assessment procedures. Ranging from operating systems to cloud services and network devices, the controls in this benchmark help you protect the specific systems that your organisation uses. AWS Security Hub supports CIS AWS Foundations Benchmark v1.2.0 and v1.4.0.

For more information, see https://docs.aws.amazon.com/securityhub/latest/userguide/cis-aws-foundations-benchmark.html.

2. Infrastructure Protection

2.1 AWS Best Practices for DDoS Resiliency

It’s important to protect your business from the impact of distributed denial of service (DDoS) attacks, as well as other cyberattacks. Maintaining customer trust in your service by maintaining the availability and responsiveness of your application is a high priority. You also want to avoid unnecessary direct costs when your infrastructure must scale in response to an attack.

The AWS Best Practices for DDoS Resiliency whitepaper gives prescriptive DDoS guidance to improve the resiliency of applications running on AWS. This includes a DDoS-resilient reference architecture that can be used as a guide to help protect application availability. The whitepaper also describes different attack types, such as infrastructure layer attacks and application layer attacks. We explore practices to effectively manage each attack type. In addition, it outlines the services and features that fit into a DDoS mitigation strategy, along with how each one can be used to help protect your applications.

2.2 Security Automations for AWS WAF

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to a number of AWS services. AWS WAF also lets you control access to your content to protect the AWS resource AWS WAF is monitoring. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, the protected resource responds to requests with either the requested content, an HTTP 403 status code (Forbidden), or with a custom response.

You can use AWS WAF to create custom, application-specific rules that block attack patterns to provide application availability, secure resources, and prevent excessive resource consumption.

The Security Automations for AWS WAF solution supports the latest version of AWS WAF (AWS WAFV2) service API.

Appendix 2 : AWS Risk and Compliance

AWS serves a variety of customers, including those in regulated industries. Through the AWS shared responsibility model, we enable customers to manage risk effectively and efficiently in the IT environment, and provide assurance of effective risk management through our compliance with established and widely recognised frameworks and programs. The Amazon Web Services: Risk and Compliance whitepaper outlines the mechanisms that we've implemented to manage risk on the AWS side of the shared responsibility model and the tools that customers can use to gain assurance that these mechanisms are being implemented effectively.

Appendix 3 : Identity and Access Management

AWS IAM is a web service that helps you securely control access to AWS resources. When a principal makes a request in AWS, the AWS enforcement code checks whether the principal is authenticated (signed in) and authorised (has permissions). You manage access in AWS by creating policies and attaching them to IAM identities or AWS resources. Policies are JSON documents in AWS that, when attached to an identity or resource, define their permissions. For more information about policy types and uses, see Policies and Permissions in IAM. For details about the rest of the authentication and authorisation process, see How IAM Works.