AWS Well-Architected Framework

Government Lens

Government Lens: AWS Well-Architected Framework

Table of Contents

Government Lens

Publication date: **January 10, 2024** (*Document history*)

This whitepaper describes the Government Lens for the AWS Well-Architected Framework including general design principles, best practices, government-specific guidance for the pillars of the Framework, and an additional chapter for government service outcomes. The Government Lens is based on other domain lenses, such as the Financial Services Industry Lens. This whitepaper is designed to be used by anyone responsible for, or involved in the design and delivery of government services, including service and product owners, architects, engineers, policy staff, and program managers. A government service might include multiple workloads.

Introduction

Government customers have a special set of legal, legislative, accountability, and trust requirements. These requirements need to inform architectural and delivery considerations for solutions that support government services. Government policies and services often have a significant impact on society, which creates a strong but understandable culture around responsible risk management. Governments everywhere are prioritizing and investing in high veracity, modern, and omni-channel citizen-centric services that meet the special requirements of government. To improve agility in a rapidly changing world, they also are creating reusable and modular architectures.

The Government Lens helps people understand the special context and requirements of government and how to best deliver meaningful outcomes on AWS. This lens drives architectural qualities that layer government-specific best practices for progressive enhancement as a service design assurance function. For example, government customers can use the new service outcomes chapter as an indicator of readiness for government service launches, and to inform AWS Enterprise Support event management.

The Government Lens should be applied as an expansion to the AWS Well-Architected Framework. The output of both the AWS Well-Architected Framework review process and this Government Lens is a report containing applicable best practices and if they are in use at the time of review. Government customers can use these outputs to improve the impact and outcomes of their services, and to engage with their own governance mechanisms in a meaningful way.

It is important to note that every government operates in a unique cultural and historical context, which means different expectations, needs, mandates and even a different perspective about the

role of government in that society. Anyone responsible for delivering services in government must make sure to learn and understand the special context of that government customer to apply what is appropriate from this Lens. The Government Lens is informed by frameworks from the AWS global experience working with government customers.

Lens availability

The Government Lens is available as an AWS-official lens in the Lens Catalog of the AWS Well-Architected Tool.

To get started, follow the steps in Adding a lens to a workload and select the **Government Lens**.

Service context checklist

We recommend that you work through this checklist to prepare the service context prior to running your Government Lens review in AWS Well-Architected Tool. The review is performed in your AWS account so that you can record it as a milestone, save it, and use it to track your remediations and progress after the review. The completion of the review produces a detailed report and it's up to you to assess and perform risk remediation activities.

	ID	Priority	Service Context
☐	C1	Required	Clearly identify the service or system you want to review, which might include one or more end-user facing process flows. **Note** The term *service* is used in this context throughout the Government Lens review.
☐	C2	Recommended	AWS recommends that all individual process flows have a review using the Well-Architected Framework lens prior to running a Government Lens review of the *service*

	ID	Priority	Service Context
			as a whole. This helps verify that the individual flows meet the AWS best technical practices , which are then complemented by the service review done against the government context.
☐	C3	Required	Schedule at least three hours for the Gov Lens review (which could be spread over 2–3 shorter sessions, if desired). Invite the relevant AWS account executive and the customer product owners to participate in the entire Government Lens review session.

	ID	Priority	Service Context
☐	C4	Recommended	• Enterprise risk representatives —for the last operational excellence pillar question, and the security and reliability pillar questions. • Security personnel —for the security and reliability pillar questions. • Relevant policy and program owners, frontline staff representatives (who understan d the context of end users), and business and policy owners —for the reliability pillar and service outcomes for government questions.

Using the Government Lens in AWS WA Tool

A common request from our customers has been to enable them to run a *self service* Government Lens review in the AWS Well-Architected Tool (AWS WA Tool).

The Government Lens is available as a custom lens for the AWS Well-Architected Tool in the AWS Management Console. Custom lenses, such as the Government Lens, are defined in a JSON file and

allow you to tailor your workload reviews to particular technologies, help you meet governance needs, and extend the guidance already provided by the Well-Architected Framework and the AWS lenses.

To add the Government Lens to the AWS Well-Architected Tool:

1. Download the Government Lens JSON file provided by your Technical Account Manager (TAM), Solutions Architect (SA), or Support. This file is used in Step 5.
2. Sign in to the AWS Management Console and open the AWS Well-Architected Tool console at https://console.aws.amazon.com/wellarchitected/.
3. In the left navigation pane, choose **Custom lenses**.
4. Choose **Create custom lens**.
5. Choose **Choose file** and select the JSON file you downloaded in Step 1.
6. (Optional) In the **Tags** section, add any tags you want to associate with the Government Lens.
7. Choose **Submit & Preview** to preview the Government Lens, or **Submit** to create the lens without previewing.

   If you choose to **Submit & Preview**, you can select **Next** to navigate through the Government Lens preview, or select **Exit Preview** to go back to **Custom lenses**.
8. Select the Government Lens and choose **Publish lens**.
9. In the **Version name** box, enter a unique identifier for the version change. This value can be up to 32 characters and must only contain alphanumeric characters and periods (".").
10. Choose **Publish custom lens**.

    After the Government Lens has been published, it's in **PUBLISHED** status.

The Government Lens can now be applied to workloads in your AWS account, and shared with other AWS accounts and users. If your account is managed by AWS Organizations, you can share the lens with all accounts in the organization or in an OU without having to enumerate each account.

As you work through the service context checklist, risks can be identified and comments can be captured. A workload report is available in PDF format for sharing with stakeholders to document risks and future recommendations. Open risks can be managed and assigned in the tool and periodic milestone reviews can be performed.

For more information on using the AWS WA Tool, custom lenses, reports, and the risk dashboard, see the AWS Well-Architected Tool User Guide.

Definitions

These definitions mean to provide AWS builders, architects, and technologists with a starting point for commonly used terms and phrases used within the government sector. Specifics of the terms and how they are applied can vary by jurisdiction.

Public Sector: The portion of the economy composed of all levels of government and government-controlled entities, usually defined in legislation or by Administrative Orders.

Digital Nations: A collection of ten governments committed to digital reform and best practices. Usually led the by the national digital government unit or Chief Digital Officer for the jurisdiction.

Government versus government: Government (with a capital G) refers to the political system or form by which a country or community is administered and regulated. The Government is supported by the public sector to fulfill the obligations of that jurisdiction and to represent the best interests of the people served. The public sector is often referred to as the government (lower case g).

Open Government: The governing doctrine which maintains that citizens have the right to access the documents and proceedings of government to allow for effective public oversight. This doctrine includes transparency, public reporting, and accountability mechanisms, and is often inclusive of public participation in improving public services and policies.

Open Government Partnership: A collection of over 75 countries committed to open government measures. Usually led by a central government department responsible for transparency and accountability, such as a Department for the Attorney General, although it's sometimes led by the head of state.

Protection of Civil Rights and Privacy: The degree to which government entities are required to verify that information relating to citizens collected and held by Government is secure and confidential, that the privacy rights of individuals are not breached by governments or non-governmental actors, and that a range of civil rights are protected.

Accountability: Enabling public, parliamentary, independent, and internal oversight of government activities.

Access to information: Mechanisms that govern the release of government-held information into the public domain.

Open Information or Data: Data (or information) that is provided publicly to be freely accessed, used, or shared. Includes mechanisms to encourage non-government actors and other governments to reuse government information and data.

Jurisdiction: A jurisdiction is an area with a set of laws under the control of a system of courts or government entity that are different from neighboring areas. A jurisdiction might be at a national/federal level, a provincial/state/territory level, or a local level. Countries such as Australia, Canada, and the United States have three levels of government. Other countries, such as New Zealand, have two levels. It's important to be aware of the jurisdictional context of the government customer.

Public or government services: The services provided by the government or public sector to the public. Programs intended to improve public services usually refer to raising the quality of services to the public, making them more accessible, end user friendly, inclusive, and effective at driving policy outcomes.

Transparency: Promote corporate and operational accountability, including programs that encourage transparency and ethical conduct, while tackling corruption.

General design principles

This Government Lens lists high level design principles that government customers expect to be applied to services being developed with and for them. A version of these principles is found in most governments today and in some jurisdictions. Services can be audited to verify that they comply with service standards. Each principle has one or more questions to consider that support the pillar assessment. The principles outlined in this whitepaper draw from the Australian Digital Service Standard, the Canadian Digital Standards, the New Zealand Digital Service Standard, the UK Government Service Standard, and the US Government Digital Services Playbook. It's important that builders are aware of the standards for their jurisdiction. It is also worth being aware of the Digital Nations Charter, first signed in 2014 by the Digital Nations cohort, including leading digital government from around the world.

The general design principles are:

- Design with purpose
- Design with end users (citizens, residents, businesses)
- Make the service simple and intuitive
- Iterate and improve frequently (with end user and staff feedback)
- Collaborate and work in the open by default
- Address security and privacy risks
- Build inclusive services
- Design trustworthy services
- Measure, report, and take data-driven decisions
- Consider composable architecture and reusability
- Maintain service continuity

Design with purpose

All government systems, programs, services, and policies are meant to deliver an outcome. Whether it is for the department mission, legislative responsibilities, a policy objective, or something else, it's important that those designing and delivering government solutions understand the purpose and intent behind the service, as well as how it's meant to impact the

public. These factors should inform the design, success criteria, end-user research, engagement strategy, architectural design, and the measurement framework for the system.

Questions to ask:

- Do you understand the mission, mandate, and policy objectives of the government customers? How will you measure success?
- What is the intended impact of the system or service? Are you measuring or tracking that impact from the beginning?
- Does the measurement framework include customer and end-user feedback and satisfaction? Does it include staff feedback the intended policy impacts and monitoring for unintended human impacts?
- Have you considered the potential risks of this service to the community?

Design with end users (citizens, residents, businesses)

Service design provides a good framework for a multi-disciplinary team to deliver a design-led and end-user engaged service. People responsible for service delivery must engage end users early in the design and iteration process, and consider their feedback for validating the best potential design, governance, and the continuous improvement process for a service. Concept testing should be conducted well before a solution is decided upon or anything is built. It's important to keep in mind that public-facing services might include third parties delivering services on behalf of Government, suppliers, and business end users in addition to citizens.

Questions to ask:

- Who is the service design lead on your project or product team?
- Have you clearly defined who your end users are?
- Have you included end users in the research, design, concept testing, user testing, and continuous improvement of the service?
- How many potential solution concepts have you tested with end users? (This should be more than just one.)
- How can a user provide feedback, either positive or negative, that directly goes into the continuous improvement of the system or service?

Make the service simple and intuitive

Most government service standards talk about making it simple for people to get what they need from the government service. Designing with users will help facilitate this goal, but it's a good additional design principle to purposefully do the hard work to make it simpler to use. Try to integrate or incorporate functionality rather than redirecting to an existing service. Take a whole of experience approach rather than just a transactional step improvement. Use simple and clear language. Use and contribute to common design services to maintain a common look and feel for government services.

Questions to ask:

- How are you measuring and designing for simplicity and intuitive services?
- How are you engaging with a diverse group of users through the product design and development?
- What customer experience (CX) and user satisfaction measures are you implementing?
- How readable and simple to understand is the language used across the service?
- How consistent and intuitive is the design of the service?

Iterate and improve frequently (with end user and staff feedback)

Continuous improvement of services in response to events or initiatives impacting society, citizens, end users, and public sector employees is vital to maintain trust and verifies that service delivery can evolve in a timely manner. Therefore, mechanisms for collecting and responding to requirements need to be established. People responsible for service delivery can ask themselves how the service will be managed after launch, and if there is a supporting operating model with continuous improvement mechanisms in place. This approach also could include automation of testing and deployment, load testing at scale, and other ways to improve consistency of continuous change deployment to reduce unexpected issues or unnecessary human error.

Questions to ask:

- How will the product management team identify, escalate, prioritize, and implement change from user and staff feedback?
- How often can product improvements happen? Daily, weekly, monthly, quarterly?

- How long does it take and how much effort is needed to push iterations or improvements to the service?
- Does the service have funding and the necessary resources to manage it past the initial launch?
- Who is the product owner and how will they engage with the development and design teams through the lifecycle of the service?

Collaborate and work in the open by default

Open Government is a concept that can not only improve public trust, but also improve services and policy outcomes. In addition, some governments have a legal requirement to consider or publish service reporting or open source code. People working with government directly or as a third party must consider how government can share the service's non-sensitive data, code, evidence, research, and decision making openly. This includes using open standards where possible and open-source licensing where required. The Digital Nations Charter recommends that government prioritize open government, open data, open source, open standards, and open markets to maintain sustainable digital transformation of governments.

Questions to ask:

- How will the general public find out information about the service, such as its compliance or performance?
- How will citizens participate in the design or ongoing improvements to the system or service?
- Have you explored how other governments might have solved this problem, including the use of reusable tools?
- How might the government customer share information across their own organization and jurisdiction?
- How does the government customer want to share this work so that other governments can reuse it?
- Can you share your outputs with appropriate open source licenses and channels?

Address security and privacy risks

The privacy requirements of government services can be extremely strict. Take a balanced approach to managing risk by implementing appropriate privacy and security measures, and by understanding the real impact of the system on the people, communities, and businesses affected.

Support a security culture where security measures are frictionless for service operations, and do not place additional burden on users. This includes responsible, accountable and auditable stewardship of government data and systems.

Questions to ask:

- How can you demonstrate and monitor for security in your system or service?
- How can you demonstrate compliance to and stewardship of privacy for all data and systems?
- What are the jurisdictional requirements around identity, including identity frameworks, data sharing legislation, privacy impact assessments, and so on?

Build inclusive services

Government services are not usually optional for people, so they often need to be accessible to everyone. Services should meet or exceed accessibility standards and be inclusive by design. No person should be excluded by service, which means there will always be a need for offline options to complement online channels. Design omni-channel services, and verify that needs have a pathway to the service. Users with distinct needs should be engaged from the outset to verify what is delivered will work for them. In any project that you do with the government, even if they aren't asking for it, you need an answer to the question "Is this an inclusive service?" and if not, then what are the alternative options.

Questions to ask:

- Do you know who all the potential users of the service are? Is this system or service inclusive for all those users?
- Have you taken into account different language and literacy requirements for end users?
- Have you involved diverse representation of your users in the design and testing of your system or service?
- Can users get access to an assisted version of the service (such as in person, or over the phone) as well as by self-service online?
- Are there minimum legal requirements around accessibility or access for this government customer?

Design trustworthy services

Government services can become contentious if they don't verify that everyone receives fair and equitable treatment, and governments are expected to deliver value and benefits to the community. It's critical that government services are explainable so they can be audited and appealed (as per administrative law and other requirements). It is important to verify that ethical considerations are part of the design, implementation and governance models for the service.

Government services also need to comply with relevant ethical guidelines in the design and use of all systems, especially for automated decision making (such as the use of artificial intelligence).

Questions to ask:

- Do you know the relevant ethics frameworks and requirements for the jurisdictions?
- Is your system designed to have privacy, dignity, legitimacy, and accountability by design?
- Can an end user understand and challenge the output from the system?
- How do you audit and monitor decisions, accuracy, and legal authority or compliance, in real time?
- How do you know whether your service is having a fair, positive, or negative impact on people?
- How have you verified that independent oversight and effective governance?
- How could you earn social license and operate this service in a way that the public will consider trustworthy?
- What are the jurisdictional requirements around transparency? For example, do you need to publish algorithms, or apply a special risk assessment?

Measure, report, and take data-driven decisions

Work out what success looks like for the government service or system and identify metrics that will tell the end user and the government itself what's working and what can be improved. Combine this effort with user research. Support the government to build measurement capabilities from the beginning, so that they can baseline and measure the impact of their service, taking into account the service performance, user experience, intended policy impact, and measurable impact. Use testing and actual data to drive decision making, so that changes and improvements have a higher chance of success.

Questions to ask:

- Have you established the measurement and monitoring systems to enable data-driven decision making?
- Are threats or anti-patterns identified and escalated in close to real time?
- How is the system performance, user experience, policy impact, and human impact measured and monitored?
- What do you need to measure in order to determine performance success outcomes and impact?

Consider composable architecture and reusability

Designing composable, modular architecture allows the government customer to identify repeatable architectural patterns to inform product design, development, and procurement. Many jurisdictions have established design systems or component catalogs that can be used to simplify and standardize the end-user experience, to accelerate service delivery, reduce operations overheads and improve consistency so users do not have to constantly relearn how to interact with a jurisdiction's digital services. To promote reuse and reduce complexity, some jurisdictions might have defined core environments or components to be used as part of new services. These elements are usually defined as part of a jurisdiction's enterprise architecture.

Leveraging government environments and procurement agreements allow builders to take advantage of particular terms and standards already agreed upon between the vendor and the government, which improves and speeds up delivery and helps make compliance with government standards simpler. Builders should identify and engage with Government architectural standards and groups where a service they are building might deliver services across multiple departments of agencies, and should be aware of whole government patterns that can be leveraged.

Questions to ask:

- Have you considered a modular, extendable, and composable architecture for this service?
- What platforms, frameworks, agreements, and patterns exist that you can leverage (for example, from this jurisdiction and others)?
- How difficult is it to reuse an existing agreement, environment, or pattern, and what ongoing effort is required to maintain it?

Maintain service continuity

Particular government services must not have unexpected downtime due to the risk of immediate dangers to the quality of life for citizens, for example, emergency services, social welfare payments, policing systems, and healthcare services. Resilient architectures are key to support this design principle, and the people responsible for service delivery must take a risk-based approach to architectural decisions to support critical government services. Make deliberate use of the AWS Well-Architected Framework Reliability Pillar to inform your decision making.

Questions to ask:

- How will your system or service handle an attack or disruption? What backup options exist for users?
- How will a disruption to service be detected and escalated proportionately to the risk and impact of the service?

Scenarios

In this section, we provide common government scenarios with guidance to inform your architectural design. Each scenario includes best practices, characteristics, considerations, and reference architectures where applicable.

Scenarios

Artificial intelligence in the public sector

Artificial intelligence (AI) provides significant opportunities for better public policy and services that deliver more equitable and scalable support for the community. But poorly designed AI systems can similarly create difficulty at a scale not possible in other sectors due to the special context of government. For this reason, careful design and governance of AI in government, including in the context of usage patterns and public impact, is critical for maintaining responsible and trustworthy AI systems in government.

Understanding the broad categories of how, and in which context you can use AI helps to establish the right controls and approaches to appropriately govern, design, manage, and mitigate risks with your AI systems. In this scenario, we explore common patterns for how AI is broadly used with pragmatic guidance and recommendations to maintain responsible, ethical, and high integrity outcomes from AI in the special context of government.

Characteristics of a good AI architecture in government include:

- Clear delineation between systems that require explainability (such as deciding eligibility to social services) and systems that don't (such as general research or patterns analysis). Explainability is the ability to describe why a machine learning (ML) model makes a specific prediction.
- Good practice approaches to identifying, addressing, and ongoing monitoring for bias in data for training AI models and the AI models themselves.

- Monitoring for the measurable intended and unintended impact on people, communities and the environment.
- Support for ongoing end user and staff feedback to inform continuous improvement and quantitative impact analysis.
- Demonstrable lawfulness of the outcome (particularly in the case of decision making systems).
- Transparency for when and how AI is used.
- Augmentation that improves policy and community outcomes, rather than just efficiency through automation.
- The system is perceived as lawful, fair, and trustworthy by the public.

The following patterns of AI usage can stand alone or be combined with others. This makes it simpler to verify that standalone use cases are not over governed, but also that combinations of usage patterns into a solution can address the relevant aspects of good governance. Each usage category includes analysis on the suitability of the two mainstream types of AI, rules based (RB), and machine learning (ML), and some ideas on risk profile and remediations.

Usage patterns	Description	Suitability of AI types	Risk profile	Risk management tools
Analytical	AI systems that perform analysis, identify patterns, produce trends and insights. Examples include risk assessment systems, patterns analysis in helpdesk data to identify	RB: Low, as it doesn't scale and only useful for pre-determined inquiry. ML: High, both for scalability and to explore unknown unknowns in data.	Both RB and ML based systems run the risk of perpetuating bias and inaccuracies from past systems. However, if the outputs from such systems are treated as indicators, and supplemented by robust	• The assessed level of impact should inform governance. • Either use AI to find and mitigate bias, or make sure that data bias is addressed. • Verify that analysis outcomes are supplemen

Usage patterns	Description	Suitability of AI types	Risk profile	Risk management tools
	bias, and trends projection.		information, they can be extremely useful.	ted with other inputs. • Transparency on use of AI for all use cases. • Provenance of sources will help make sure that outputs are not manipulated.

Usage patterns	Description	Suitability of AI types	Risk profile	Risk management tools
Process Automation	AI systems that automate a process, whether it be an existing, pre-defined, or an inferred process created from data or model training. Examples include automatic triaging of calls or email based on rules or data, application sorting, and digitizing PDF files.	RB: Medium, provides consistency of processes automated, but doesn't scale or learn. ML: High, scales and can improve processes over time.	Depends on the process, who is impacted by the process, and the worst possible likely impact. If the impact is considered low and the output is not something that needs to be appealable, then risk is likely low. If explanation is needed or if the worst likely impact is high, then risk is high.	• The assessed level of impact should inform governance. • Make sure that data bias is addressed. • If process automation informs a decision or action, include risk mitigations for that category. • Transparency on use of AI for all use cases. • Make sure that unintended impacts are monitored for and addressed.

Usage patterns	Description	Suitability of AI types	Risk profile	Risk management tools
Automated Decision Making (ADM)	AI systems that generate a specific decision or action, either from rules or data. Examples include social service eligibility decision systems, autonomous cars, and chess and game playing engines.	RB: Medium to High, rules-based ADM systems provide consistent and traceable outputs. ML: Low to medium, ML ADM systems are currently not traceable to legal authority, nor do they provide consistent outputs over time.	Risk is based on the worst likely impact on the end-user, citizen, or company. If the decision or action being automated is subject to administrative law, then the risk of ML based systems is much higher to mitigate.	• The assessed level of impact should inform governance. • Make sure that data bias is addressed up front and monitored over time. • Make sure that ADM outputs are explainable or at least testable against their legal authorities to help verify legislative compliance. • Transparency on use of AI to end users. • Ease of appeal available to end users. • Continuous service design, monitoring, and

Usage patterns	Description	Suitability of AI types	Risk profile	Risk management tools
				improvements based on public feedback. • Provenance of sources will help make sure that outputs are not manipulated.

Usage patterns	Description	Suitability of AI types	Risk profile	Risk management tools
Generative	AI systems that produce some form of consumable content, such as video, text, audio, images, code, or recommendations.	RB: Low. RB systems don't tend to deliver quality new artefacts. ML: High. ML-based systems can use enormous quantities of inputs and dramatically improve generated outputs over time.	If the artefact being generated is considered representing government, the risk could be high due to reputational risk, misdirected efforts in an emergency, or electoral or policy distrust. Public trust and confidence can be undermined if they can't validate authenticity.	• The assessed level of impact should inform governance. • Transparency on use of AI for all use cases. • Human review is critical for all decision making and public facing usage. • Provenance of sources will help make sure that outputs are not manipulated.

Usage patterns	Description	Suitability of AI types	Risk profile	Risk management tools
Virtual assistance	AI systems that provide assistance or augment the experience of a person in the moment. Examples include chatbots (either rules- or data-based), augmented and mixed reality (for example, applications for emergency response support), or personal assistant technologies (such as Amazon Alexa.)	RB: Low. RB assistants and chatbots work for very limited use cases, but are at least consistent. ML: High. ML will drive improvement in service and functionality of virtual assistants over time, responding to changing use cases and user needs.	High: Government use of this category can be high risk, because the information or service an individual or business receives from this application is likely subject to the same requirements as ADM (namely, explainable traceability, appealability) and directly influences the public perception of public institutions and government.	• The assessed level of impact should inform governance. • Make sure that ADM risk mitigations are implemented if solution makes decisions or provides advice. • Continuous service design, monitoring, and improvements based on public feedback. • Provenance of sources will help make sure that outputs are not manipulated.

This reference architecture illustrates a secure, self-service, data science environment using Amazon SageMaker AI Studio. It provides data scientists with access to a secure and persistent experimentation environment as well as continuous integration and continuous deployment (CI/CD) pipelines to perform data science and machine learning at scale.

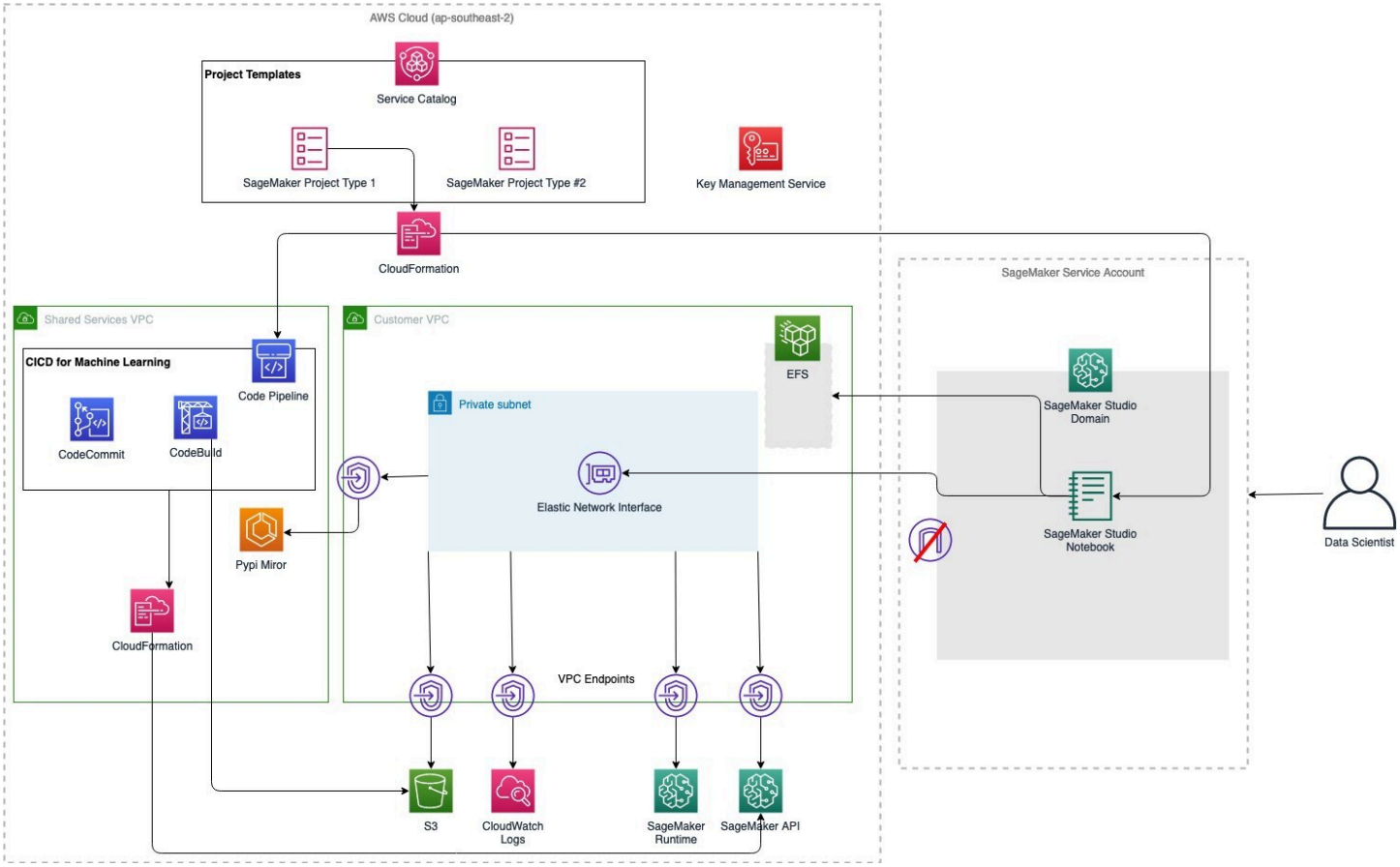

Figure 1: A sample reference architecture to enable public sector customers with AI

This architecture demonstrates a self-service model for enabling multiple project teams to create environments and details the design choices and security controls that your organization can rely on in these environments. Organizations should modify these controls to verify that they meet their specific requirements.

This architecture is capable of supporting some of the hardest challenges for the public sector when implementing ML programs such as:

- **Management and governance:** Public sector organizations need to provide increased visibility into monitoring and auditing ML workloads. Changes need to be tracked in several places, including data sources, data models, data transfer, transformation mechanisms, deployments, and inference endpoints.

- **Bias and explainability:** Given the impact of public sector organizations on citizens, the ability to understand why a ML model makes a specific prediction becomes paramount—this is also known as ML explainability. Organizations are under pressure from policymakers and regulators to verify that ML- and data-driven systems do not violate ethics and policies, and do not result in potentially discriminatory behavior.
- **ML Operations (MLOps):** Integrating ML into business operations, referred to as MLOps, requires significant planning and preparation. One of the major hurdles facing government organizations is the need to create a repeatable process for deployment that is consistent with their organizational best practices. Mechanisms must be put in place to maintain scalability and availability, as well as ensuring recovery of the models in case of disasters. Another challenge is to effectively monitor the model in production to verify that ML models do not lose their effectiveness due to the introduction of new variables, changes in source data, or issues with source data.

The following list provides some examples of public sector use cases for AI and ML in AWS. For a more comprehensive list, refer to the AWS Blog.

- The AWS toolkit for responsible use of artificial intelligence and machine learning
- Improve governance of your machine learning models with Amazon SageMaker AI
- Protecting Consumers and Promoting Innovation – AI Regulation and Building Trust in Responsible AI
- How NASA uses AWS to Protect Life and Infrastructure
- Paper on Forecasting Spread of COVID-19 Wins Best Paper Award
- Amazon Supports NSF Research in Human/AI Interaction Collaboration
- Using AI to rethink document automation and extract insights
- Chesterfield County Public Schools uses machine learning to predict county's chronic absenteeism
- Using advanced analytics to accelerate problem solving in the public sector
- How AI and ML are helping tackle the global teacher shortage
- Improving school safety: How the cloud is helping K12 students in the wake of violent incidents in schools
- Heading into Hurricane Season

Classified information systems

Classified information is information that a government or agency deems sensitive enough to national security that access must be controlled and restricted. Every government has differing levels of classification that are specific to their own context. For example, the U.S. Government uses three levels of classification to designate how sensitive certain information is: confidential, secret, and top secret. The lowest level, confidential, designates information that, if released, could damage U.S. national security. The other designations refer to information, the disclosure of which, could cause *serious* (secret) or *exceptionally grave* (top secret) damage to national security. Some data and information is considered unclassified and low risk, but this scenario is for higher risk and classified information systems.

The decisions concerning the level of data classification are often based on a risk approach and are often dependent on regulatory and compliance requirements. These requirements are often reflective of the data types. for example, personally identifiable information (PII) or personal health information (PHI), or information related to ITAR, HIPAA, IRAP, GDPR, or other compliance and regulatory requirements.

Often, the standards do not prescribe how agencies should meet the requirements, as agencies vary in size and complexity. Every agency has a unique information management environment with varying culture, risk tolerance, legacy systems, and resources. Agencies should implement the principles and characteristics to meet their specific circumstances.

Characteristics and principles of classified information systems architectures include:

- Business information is systematically and holistically governed throughout its lifecycle.
- Only necessary business information is created.
- Business information is adequately described.
- Business information is suitably stored and preserved.
- It is known how long business information should be kept.
- Business information is accountably destroyed or transferred.
- Business information is saved in systems where it can be appropriately managed and monitored.
- Business information is available for use and reuse.

Citizen engagement reference architecture

Governments are increasingly investing in citizen facing channels: mobile applications, web portals, call center agents, and chatbots to enhance the overall citizen experience. In a regulated industry space, user engagement architectures challenge the segregation often recommended for classified workloads and in some cases with citizen engagement it's based on verifiable identity along with:

- High volumes of real-time ingestion from public and private sources.
- The requirement for different data protection based on data classification.
- Use of event-driven architectures to leverage on-demand scalability and pay-per-use model.
- Inclusion of real-time and archival flows.

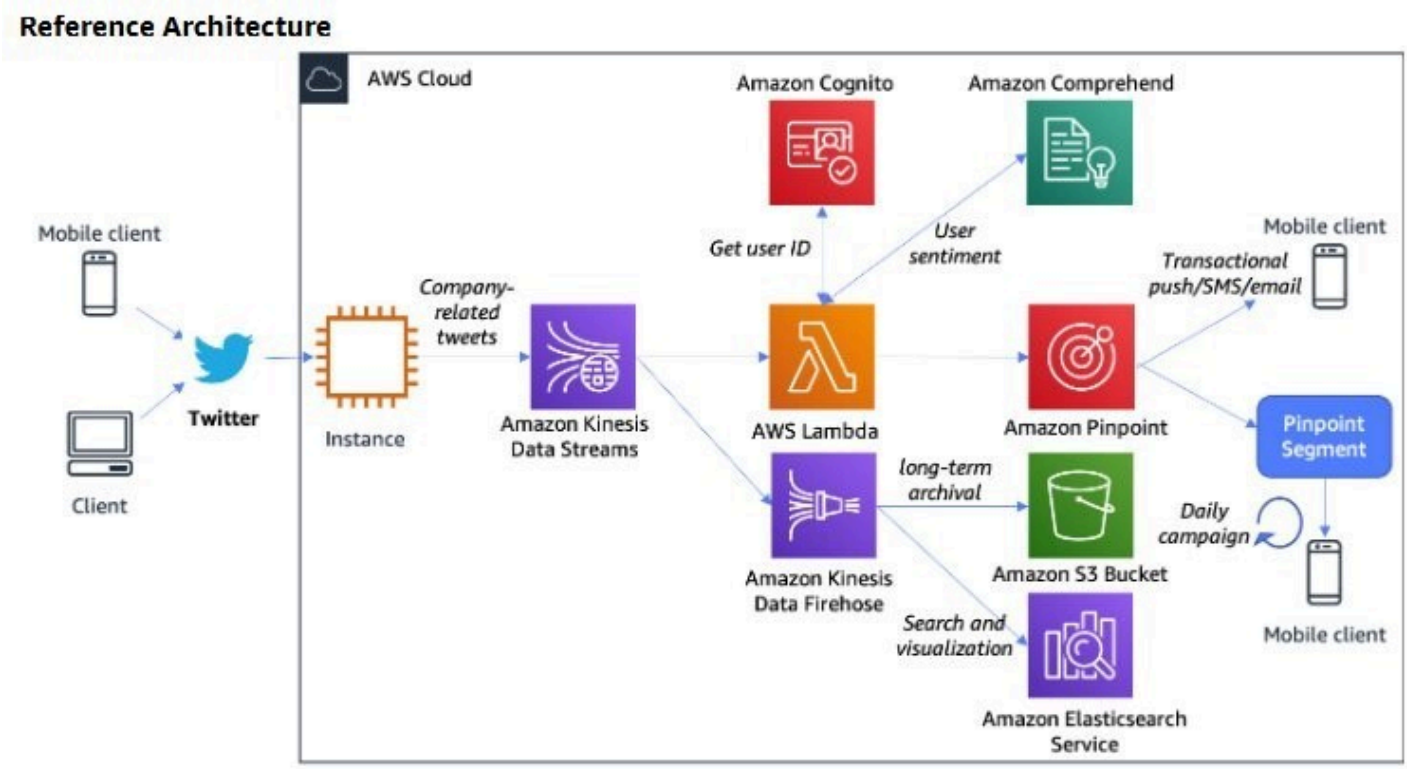

Figure 2: Reference architecture for a citizen engagement solution

Regulatory reporting reference architecture

Every government institution deals with volumes of information for legislative or regulatory reporting. Static legacy infrastructure and inefficient reporting processes can make reporting

costly and prevent customers from responding quickly to regulatory changes. Building a reporting data lake on AWS and using the rich set of services available can address many of the issues that complicate regulatory reporting, such as data residing in disconnected silos and distributed ETL processes. After customers integrate reporting data into a consistent dataset or data pipeline, they can use that data to gain additional insights through advanced analytics and machine learning.

Data lake architectures supporting these government services use cases share the following characteristics:

- They implement data quality, integrity, and lineage into the ingest and processing pipelines.
- They require that data is encrypted at rest and in transit.
- They mask or tokenize personally identifiable information (PII) data to help align with regulatory requirements (for example, EU General Data Protection Regulation).
- They use data catalogs with fine-grained access control and entitlements.

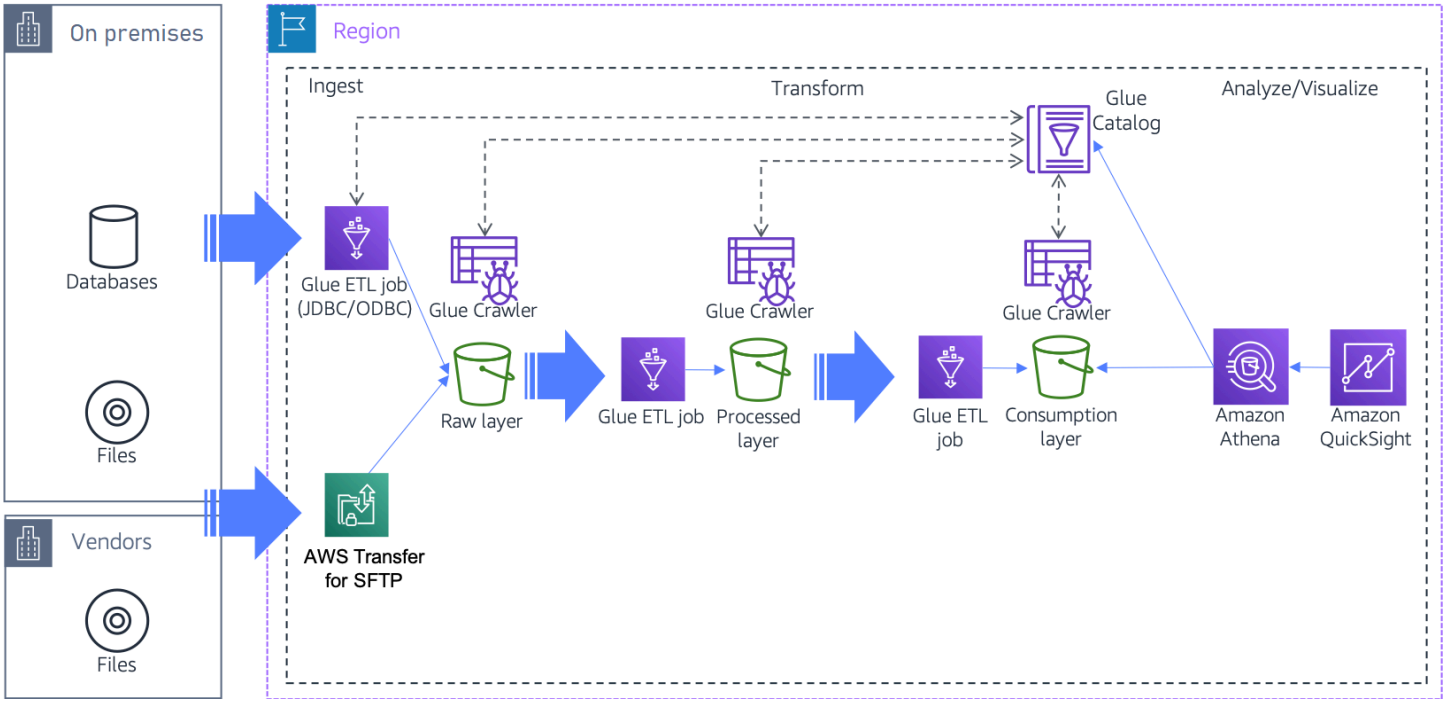

Figure 3: Reference architecture for a regulatory reporting solution

Distributed processing of sensitive documents reference architecture

Governments often need to separate their processing in segmented ways to heighten the level of security. This often occurs when the information is classified as confidential. However, there is still

a need to effectively process the data in segregated environments. In this scenario, the processing of sensitive documents might involve distributed and separated systems.

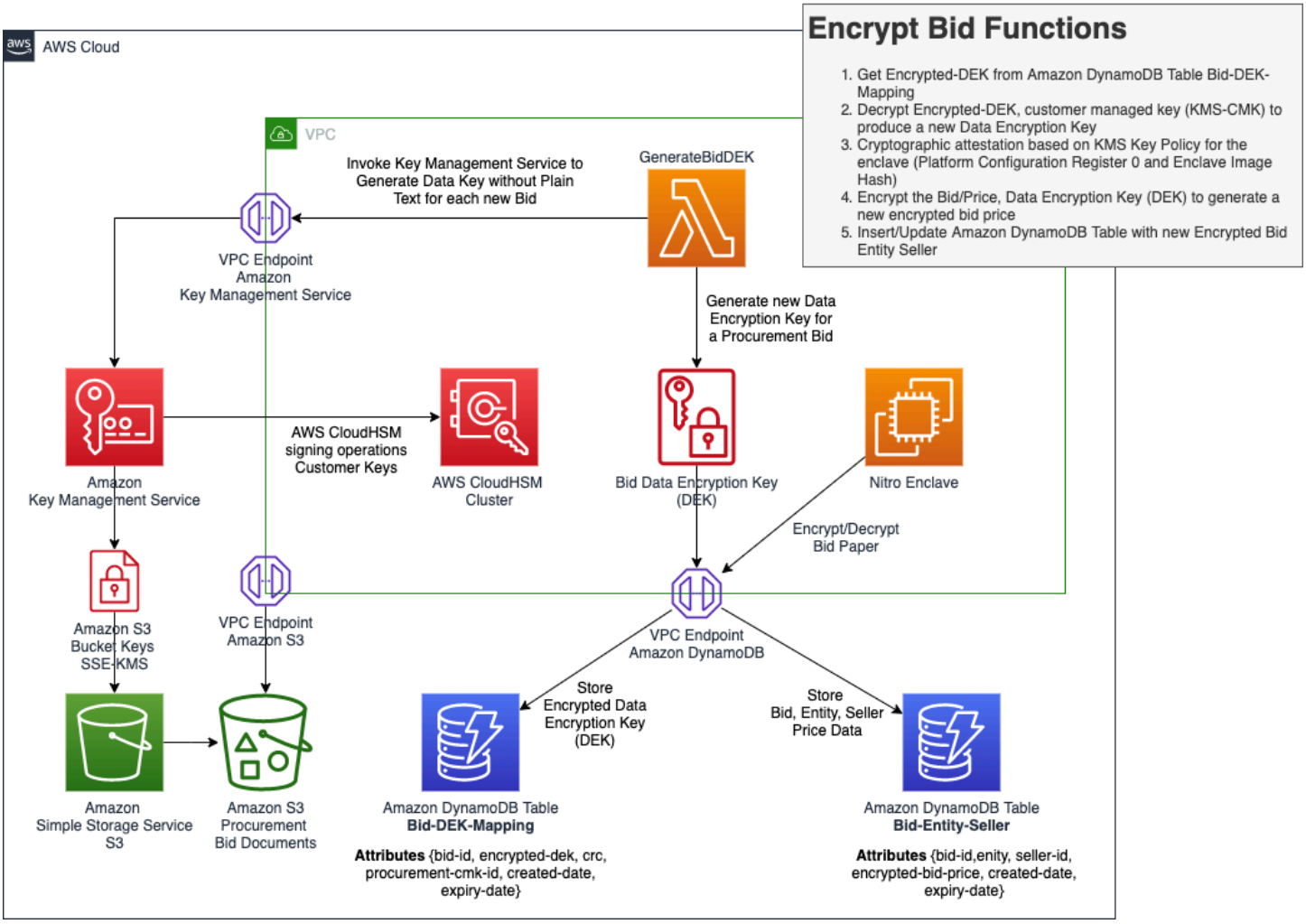

Figure 4: Reference architecture for the distributed processing of sensitive data

Omni-channel public services

Public-facing government services should have online and offline options to verify that they are inclusive and accessible by all. In many cases, this requirement will be legislated. If a digital service is built in isolation to a phone or in-person channel, then you might have a duplication of functions and increased management costs, as well as potential inconsistency across channels. Inconsistency can lead to inequities, especially given the reality of many government services being either mandatory (such as submitting a tax return) or a last resort for people at their most vulnerable (such as emergency payments or social services).

Omni-channel public services help provide a consistent experience for users, including staff, by providing a virtualized presentation layer. This approach makes reusable service components and capabilities available to channels through an integration layer. This means that the backend and business systems can be consumed across all channels in a consistent way, while still providing flexibility to the public-facing services to optimize interactions for different channels.

Through this integration layer, governments should also consider providing a set of highly reusable modular components for the most commonly needed functions within digital services, such as taking payments, sending notifications, verifying identity, and collecting form data. This approach is often referred to as Government as a Platform (GaaP), where collectively these modular commodity service components provide a platform for services to be built upon. GaaP allows service teams to consume existing commodities so that they can spend more time on what is unique to their service and users.

Characteristics of a good omni-channel architecture:

- Consistency of functionality and features across channels.
- A virtualized presentation layer, where all channels draw on common business functions through a common integration layer.
- An integration layer that provides secure, consistent, and common management of data, content, rules, and transactional functions across all channels.
- Channel agility, where channels can rapidly evolve and change according to new technologies, devices, and user needs as they emerge, decoupled from the management of business systems.
- Policy and program teams can use the same infrastructure to measure, monitor, and model the intended and unintended impacts of government services.

Conceptual architecture for omni-channel public services

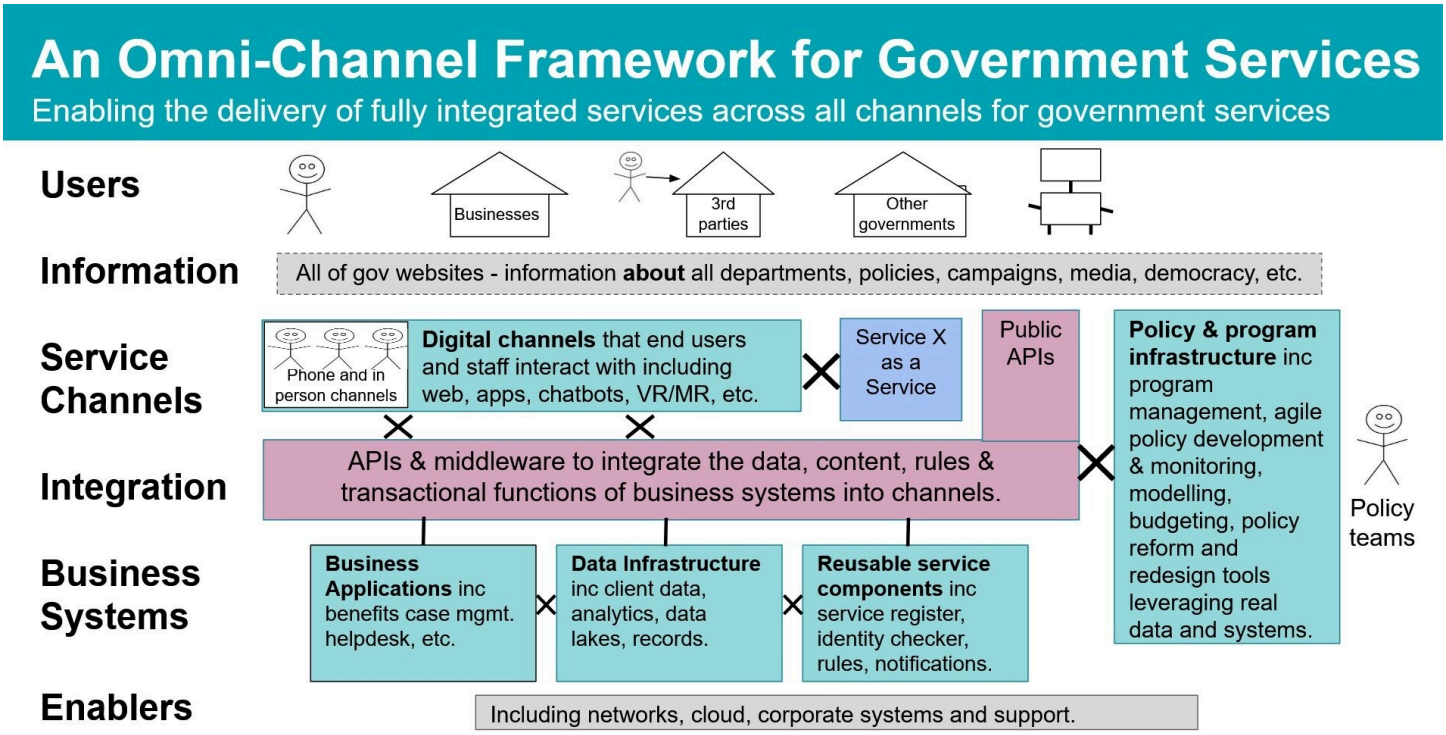

Figure 5: The omni-channel architectural framework for government services

Open government methods, infrastructure, and tools

To maintain the trust of the people they serve, governments need to be transparent, accountable, and truthful. This covers many different aspects of government operations such as how and with whom taxpayer money is spent, how effective policy initiatives are, what the laws are and the penalties for breaking them, and how decisions are taken. Being open is essential to help avoid perceptions of corruption or unfairness in society. There are a number of open government tools and approaches that can be used by governments as they develop public services that can increase trust, improve outcomes and, in some cases, help verify that legal or regulatory obligations are met.

Characteristics and principles of open government system architectures include:

- High public trust and confidence in government systems and services
- Clear accountability and reporting measures
- Public visibility and participation of programs, projects, services, and policies
- Open feedback mechanisms for the public

Working in the open

Working in the open has benefits to both government and society. It provides a scalable mechanism for peer review, partnerships, and public participation as well as greater opportunities for collaboration and reuse between government teams, departments, and jurisdictions. Blogging, sharing tools and code, showcases, feedback opportunities, open prototyping, and visible product management can all benefit the quality of delivery. AWS architecture and delivery practices exemplify many of these open ways of working.

Open-source software publication and reuse

Many governments have a policy of publishing code repositories that they have developed under an open source license to increase transparency and allow for reuse by others. This approach can also extend to infrastructure as code (IaC) configurations. It's important to understand if the government systems and services you work on will be published as open source so that information not intended for the public domain isn't published in the code repository, and that no proprietary code is included. Increasingly, governments have open-source software policies that encourage or require teams delivering new systems or services to explore the reuse of existing open-source solutions before investing time or money into building new ones. In some countries, these requirements are legislated. It is therefore important to understand any open-source software policies when designing and architecting new government systems and services, and to support government organizations to evaluate open source offerings as part of these processes. AWS provides an open source repository and guidance to help.

Algorithmic transparency

To maintain trust and fairness when using algorithms for automated or semi-automated decision making, it's important to consider whether the algorithms used can be published. A number of government organizations maintain a public register of algorithms used within their systems for this purpose. Not all algorithms will be appropriate for publication, for example, some fraud detection measures, however, where automated decisions are taken that directly affect people's lives and livelihoods, consideration should be made around publication of the algorithm and what mechanism is most appropriate for doing so. Algorithmic transparency could also mean traceable explainability to the legislation or rules used to make a decision, or providing transparency to end users on when they are interacting with algorithms. Finally, it can be useful to test inputs/outputs of algorithmic decision making against the relevant legislation/regulation as code, to work toward compliance.

Performance reporting

A key tool for government accountability is monitoring, measuring, and publishing performance data of public services and policy initiatives through public facing dashboards. Dashboards provide a simple way for the public and policymakers to visualize, and access the data and insights around the performance of important government operations. Considerations should be made around what metrics are useful indicators for performance, what mechanisms are required to derive those metrics, and how this data can be published.

Open government data

Government organizations generate and manage a wide array of data and information for which they are the canonical source. While much of this data contains private information, such as personal, confidential, or classified, there is a large amount of non-private data and information that can provide significant value to society if openly shared and licensed for reuse. This sharing allows others to build on this data to create innovative solutions. Common examples of open data range from the large scale, such as geospatial information, population statistics or weather data, to the smaller scale, such as locations of public toilets, lists of local authorities, and academic institutions. You should consider if your service holds data that is appropriate for open publication. If it does, you should explore mechanisms for publishing and providing both programmatic and manual access to the data, and that the data is licensed for reuse.

Verifiable credentials (claims) for government

There are several scenarios where verifiable credentials (VCs) make sense in a government context. Verifiable credentials provide a repeatable pattern in scenarios where assertions about the state of something is useful and those assertions are valuable outside the four walls of government or a specific department. Examples include trade, identity, technology bill of materials, inspections, and certifications. The key concept for government is that they are in a unique position in society to be a *trust anchor* for specific types of claims that become a tether for *chains of claims*.

In most economies, the trust anchors are government agencies and accreditation authorities. The role of trust anchors is to issue digital credentials to their community members, which the members can use to make their own credentials more trustworthy. For example, a national company's register that traditionally issues company registration certificates as paper or a PDF file, can now issue them as VCs so that the company can prove its identity to any verifier. A fundamentally important advantage of the decentralized architecture of VCs and Digital Identities

(DIDs) is that there is no need for a direct relationship between the issuer (for example, the company's register) and the verifier who, for cross border trade scenarios, is most likely in another country.

Here's how it works:

- A member of a regulated community (such as a company director) creates a DID and associated public and private key pair using the software of their choice.
- The member authenticates to the trust anchor service (such as the company's register) as they would normally do when interacting with the regulator or trust anchor.
- The member presents evidence that they are the owner of the DID (a digital signature using the DID private key) that the trust anchor can verify using the public key.
- The trust anchor issues a VC with the member DID as subject that contains relevant claims (for example, that the DID subject is indeed an authorized officer of the company).
- The member (that is, the company) can now leverage this regulator-attested digital identity as part of its normal business. For example, the company issues a commercial invoice with their DID as the issuer. The invoice VC includes a link to the company registration VC.
- The invoice recipient can now verify that the invoice VC was issued by the company DID and hasn't been tampered with, and that the registration VC was issued by the authorized government regulator and confirms that the same DID is for the same company.
- If the company is de-registered, the regulator can revoke the registration VC. Immediately after revocation, any verification of the original VC will result in failure.

It's important to re-emphasize that the trust anchor is still doing their normal business of issuing certificates, permits, registrations, and licenses to their members—they are just doing it digitally. There is no relationship between the trust anchor and verifiers. The digital credentials are also paper-compatible, for example, they can be made available as a QR link on a paper or PDF certificate. Whether the member makes use of the digital credential for downstream proofs is up to the member.

When well-implemented, a VC architecture has the following characteristics:

- Claims and credentials are able to be quickly and programmatically verified in real time by relevant authorities.
- The claims and credentials are considered trustworthy for major stakeholders.
- An end user gets a more personalized service without having to over share personal information.

- VC is made available as a utility to serve multiple use cases.
- VCs are signed from a central, reliable, and trustable source – that is, at the organizations domain (that is, from `did=trade.govx`) so that people, systems, and organizations can rely on the claim issued by the trust anchor.
- VCs issued from the organization are within the legislative or administrative scope of the department.
- VCs issued have a human understandable description that maps back to the organization's scope or legislation.
- VC domains map to legislative, international agreements, or both so that claims are understandable beyond just the scope of the department.
- VC domains are validated against the organizations legislative or administrative scope.
- Test architectures, methodologies, and infrastructure are in place to verify that only quality claims are issued.

Conceptual architecture

The following diagram represents a *trust graph* combining several claims from various departments for the benefit of the community.

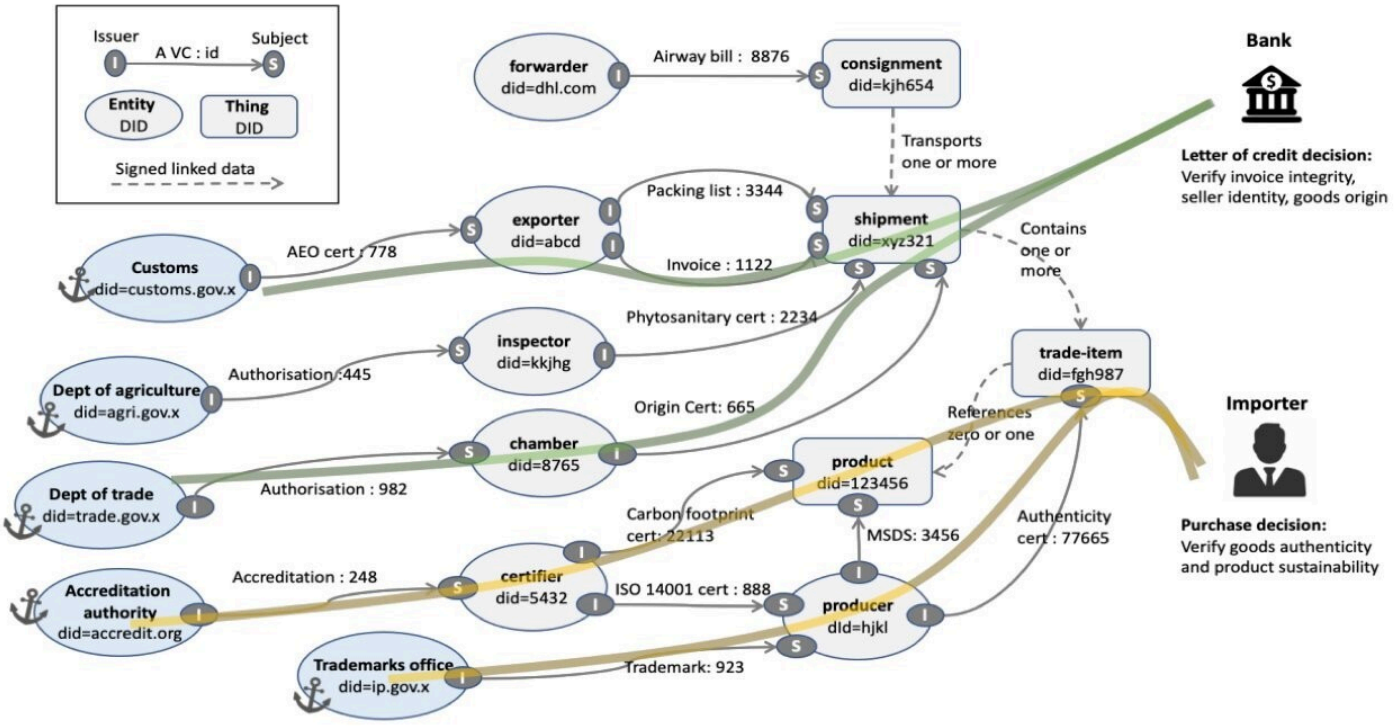

Figure 6: Illustration of the range of government digital identity proofs

Figure 6 shows a range of government digital identity proofs examples (Customs, Department of Agriculture, Department of Trade, Accreditation Authority, and Trademarks office), each of which can issue a verifiable identity of an entity (exporter, inspector, chamber, certifier and producer, respectively) or a verifiable piece of information that relates to a consignment, shipment, product, or producer (such as source, supply chain, or ingredients). This leads to a bank being able to issue a Letter of Credit decision which can automatically verify the invoice integrity, seller integrity, and goods origin from each of the relevant authorities through the verifiable credentials system. It also enables an importer to make a purchase decision by being able to automatically verify the goods authenticity and product sustainability through relevant verifiable credentials.

A single verifiable credential allows an issuer to make one or more verifiable claims about a subject. For example, an exporter might issue a commercial invoice for a given shipment of goods as a VC. A verifier can be confident that the invoice was issued by the identified exporter and hasn't been tampered with. Similarly, a certifier can issue an ISO-14000 environment certificate to an identified producer that can be presented to a party for digital verification of ISO certification.

These uses are valuable in themselves, but credentials can be chained together to create *trust graphs* that release much greater value. The connections that make up the graph can be explicit (for example, a credential includes a link to another credential) or implicit (for example, the same DID appears in two separate credentials). Consider the previous example, in which nodes represent DIDs and links are VCs.

References

- Section 3.4 of UN/CEFAFT White Paper on eDATA Verifiable Credentials for Cross Border Trade

Pillars of the Well-Architected Framework

This section maps the six pillars of the Well-Architected Framework to government environments.

Pillars

Operational excellence pillar

In the Government Lens, the operational excellence pillar describes the ability to support the departmental mandate and government priorities to run services effectively, gain insight into operations, and to continually improve supporting processes and procedures to deliver policy outcomes and public value.

The following questions and best practices complement the best practices in the Operational Excellence Pillar whitepaper.

Reshape the operating model

As governments seek to digitally transform, technology expertise and experience is essential to achieving strategic policy outcomes. To verify that digital delivery of mission objectives can consistently evolve and be delivered successfully, organizational structures must be reshaped and be inclusive of both business and technology experts.

Many government departments have functionally segmented structures that create a challenge for modern delivery of portfolio objectives. These departments often have technology in a corporate silo or have outsourced their technology entirely. This structure has left many governments with an operational divide between their business and technology staff that slows or prevents the realization of new strategic intent. Meanwhile, in the context of a rapidly changing world, many government organizations are actively seeking solution and service agility.

GL-OPS-01: How do you adjust the organizational structure to better realize strategic policy outcomes?

- **Support the establishment of persistent and multi-disciplinary team structures:** When services are developed as projects, and teams assembled for the project are disbanded at the end of the project, the service is left without persistent product management. Establish team structures and governance models that can persist beyond the end of project.
  - **Improvement plan** – Encourage the organization to consider persistent team structures that span policy and delivery in their forward planning for the service. Consider running a Cloud Adoption Framework assessment to support operational assessment and planning.
- **Enable team structures and appropriate governance to delegate delivery decision making:** Delivery and innovation happen at the speed of trust. Service and product owners require a reasonable amount of decision-making autonomy to realize continuous improvement and operational reform in a timely manner. This autonomy has the benefit of streamlining escalation, unblocking slow and laborious go-live protocols, and minimizing decision gaps between business owners and technology people, and can be complemented by oversight mechanisms without slowing or impeding good service delivery.
  - **Improvement plan** – Encourage the organization to consider delegation of two-door decision making, including continuous improvement and operational reforms in their forward planning for the service.
- **Support the creation of a Concept of Operations for the service:** Create a *Concept of Operations document* that explicitly describes how the service will continually improve over time, with supported and authorized product management and team. Its contents might include delegated decision-making mechanisms, product management in government, outcomes or product-based funding, and how to bring multi-disciplinary teams together to manage aspects of the service.
  - **Improvement plan** – If the organization does not have a Concept of Operations document, or equivalent documentation, encourage the organization to consider it in their forward planning for the service.
- **Consider all relevant feedback loops:** Consider what additional feedback loops might complement the feedback loops defined in the Operational Excellence Pillar in the special context of the department and jurisdiction. For example, how might staff or the public report legal or impact concerns.

    - **Improvement plan** – Identify and document additional feedback loops, and build these into the service architecture, escalation mechanisms and operating model as appropriate.
- **Consider a minimum viable product (MVP) deployment model where viable:** Many government projects take a *big bang* deployment model approach, attempting to develop all features and then launch a fully formed product. This approach can create substantial risk, which can be minimized through iterative and MVP-based deployment. An MVP deployment model identifies the minimum features needed for a functional product to launch, often initially to a subset of end users, and then scales and adds features in a test-driven way. This method accelerates early identification of and validation of product goals, while minimizing risk, delivering early value, and ensuring that all product features are tested for effectiveness with end users.
    - **Improvement plan** – If the organization does not want to adopt an MVP-based deployment model, advise on the risk and encourage the organization to consider it in their forward planning for the service. Provide use cases where appropriate.
- **Document and engage with cultural context:** Understand the cultural context, including indigenous or First Nations needs. Ensure culturally diverse needs are included in user research, user testing, and other service engagements, and where possible diverse representation in product teams and governance can be applied.
    - **Improvement plan** – Encourage the organization to consider cultural context in their forward planning for the service.

GL-OPS-02: How do you verify that digital experiences remain operational and relevant over time?

Some government departments can only fund changes to a service through a new funding application, which can make change slow and expensive. This funding model can lead to a great product becoming less than great over time.

- **Ensure that government and other staff are well supported to operate the service:** The more empowered public servants are to understand, manage, and improve their services, the more they are positioned to be proactive and effective in delivering great services, both directly and with vendors.

    - **Improvement plan** – Provide information and access to relevant AWS skills and capabilities training for the service, and support the organization to identify gaps throughout the process, with AWS digital transformation guides, whitepapers, and case studies.
- **Embed continuous improvement into the operating model:** Continuous improvement helps make sure that public-facing government digital experiences don't deteriorate over time. Investment must be made to maintain the continuous evolution and maintenance of the service to match the expectations and feedback of consumers. If you have a fixed or scheduled approach to improvement, support the best practices possible.
    - **Improvement plan** – Run change scenarios with the organization, including small and significant changes to the service, to identify and document how continuous improvements will be enabled, and with what oversight and decision making.
- **Implement a design-led agile development and funding framework:** Ensure that the operating and funding model supports a design-led agile approach that incorporates:
    - Early feedback on requirements from citizens, industry, and government
    - Testing and evolving of non-technical go-live processes the government might need to conduct
    - Consistently and continuously evolve functionality as the service feedback and requirements mature over time
    - Align with the concept of operations document to make sure that expectations are met during service development.
    - **Improvement plan** – Support the need for an agile development framework, providing use cases where helpful, and AWS digital transformation guides, whitepapers, and case studies.

GL-OPS-03: How do you verify that the service meets operational transparency requirements?

- **Document how the service delivers operational accountability requirements:** Many governments have strong requirements around operational accountability through various audit and reporting mechanisms. In some jurisdictions, there are public reporting requirements for public facing services.
    - **Improvement plan** – Include any reporting requirements in the concept of operations document, along with the chain of those responsible.

- **Document how citizens and companies will be kept informed:** To manage expectations and make it simple for consumers to use the service, create high quality communications (both marketing and transactional), supporting information, and technical documentation for the service.
  - **Improvement plan** – Include the public communications approach in the concept of operations document, including who is responsible.

GL-OPS-04: How can you improve solution definition criteria?

Taking time to ensure the right solution is defined from the start can save money, time, and effort down the line. This best practice encourages ways to validate and likely iterate the solution definition through policy, problem, and opportunity validation, and testing with end users.

- **Ensure that multiple concepts are tested with end users prior to deciding on a solution:** Testing concepts provides the opportunity to validate assumptions about what might work, and to proceed only with tested policy interventions. Sometimes the best solution is no solution at all, a regulation, or a change to an existing service.
  - **Improvement plan** – Encourage the use of the AWS Digital Innovation program, including Working Backwards workshops, to explore and identify the purpose and goals for the service. Leverage service and system design, as is helpful.
- **Identify patterns in the desired service capabilities and intended service usage:** Patterns might appear as emergent (such as self-sovereign digital identity), or common (such as a notification service, or application of government legislation and rules in a desired service capability). Patterns should have broad use case applicability with high volumes of reuse and could be candidates for whole of government reusable capabilities.
  - **Improvement plan** – Identify and recommend potential reusable patterns for consideration in the solution architecture.
- **Define foundational reusable components:** Informed by the previous pattern identification, look for opportunities to standardize people, processes, and technology solutions to optimize delivery, implementation, and operation of one or many components that support a service capability.
  - **Improvement plan** – Consider relevant government architectural frameworks, including from the Scenarios section of this whitepaper.

GL-OPS-05: How can you improve solution acquisition criteria?

When considering technology acquisition for a service, you'll need a business or organization level understanding of the government mission and policy objectives, government process, standards, and how these map to service capabilities, which then inform solution requirements. For more information, see Enabling services outcomes for government.

Not all components have the same business and technical requirements. Consider the following best practices when designing, evaluating, or acquiring solutions and technologies:

- **Consider and prioritize reuse where appropriate:** Leverage modular architecture and use existing design systems, tools, environments, and open-source government solutions, where feasible, to minimize duplication of systems and efforts, and to enable future system agility and extendability of the solution. Provide relevant AWS reference architectures to support modular, virtualized, and utility based approaches, enabling greatest extendibility and scalability of the service, ideally with an omni-channel approach if public facing.
  - **Improvement plan** – Look for relevant existing tools, solutions, or capabilities available in the jurisdiction or globally, and consider the AWS open source catalog.
- **Consider build versus buy/acquire strategically:** If an existing solution can be used with minor modification, you might prefer an off the shelf (proprietary or open source) tool. If you require system agility, if a solution does not yet exist, or if you want to integrate multiple systems into a channel, consider the benefits of building it yourself. The capabilities and strengths of the customer's team should be considered and planned for to ensure service viability, both technically and financially.
  - **Improvement plan** – Consider an AWS Digital Innovation program to work backwards from the problem and identify the requirements and capabilities needed for a new solution. Support the customer to take a strategic approach to designing the architecture and sourcing of the service components. Where minimal customization is required and the solution is mission-aligned, consider purchasing a solution to meet a particular need, noting most modern services will require a blend of solutions.
- **Consider where code, research, and efforts can be shared:** Reusable foundational components and solutions could be shared back to the open government community through open-source licensing.

    - **Improvement plan** – Provide guidance on sharing and contributing back to projects or to government.
- **Consider a sustainable and delivery focused approach to sourcing:** Outsourcing might be suitable in the short term if there is a staffing constraint for design, implementation, and ongoing operations. Customers are encouraged to develop and maintain a minimum viable internal expertise and delivery capability, to maintain control over the strategic direction, product management, continuous improvement, and the selection criteria as above. These competencies can support and leverage vendors, while maintaining the necessary internal agility for operational excellence. Explore flexible procurement arrangements, such as sprint or outcome-based procurement.
    - **Improvement plan** – Provide guidance, support, and training materials to support capability uplift.
- **Consider the suitability of solution licensing:** Licensing conditions can sometimes constrain the effectiveness or financial viability of a service in several ways, such as:
    - If a user-based license model is used for a government service with significant citizen uptake.
    - License terms that are bound by hardware configurations can have an impact on service agility with financial consequences to scaling the government service as demand evolves.
    - Creating a preferential technology ecosystem that inhibits the government's use of other technologies can limit the ability to innovate and scale.
    - **Improvement plan** – Organizations will have their own capabilities for this domain.

Organizational risk

Every service should have a risk management plan to assess and manage risk. Risk management should be comprehensive to consider all hazards, including how the cloud service supports risk mitigation by design. This assessment is essential to make informed design decisions. Service risk must be contextualized as part of the broader organization risk strategy.

GL-OPS-6: Do you have adequate people and process risk management systems in place covering a broad risk spectrum?

- **Take an all-hazards approach:** Include consideration of personnel, supply chain, cyber security, information security, and natural risks.

  - Have a strong understanding of controls that can be inherited from the cloud service provider, for example, the physical security of data centers.
  - Consider sovereign resilience requirements, which can aid in the survival of government in extreme circumstances.
  - **Improvement plan** – Document the preceding items into the relevant security documentation or concept of operations document.
- **Develop a risk management plan:** Have a plan that supports ongoing risk assessment and treatment, and verifies that the service risk is contextualized as part of the organization's risk profile.
  - Decide what matters most to your organization, and to your service. Considerations include social, cultural, political or regional issues, economic and technology trends, policy and law, and your organizations aims, policies and strategies.
  - Identify, analyze, and evaluate risks to help make sure that adequate treatments are identified so that your service is resilient.
  - When considering the risk of a service, consider whether the risk is acceptable for the associated service outcome it achieves.
  - **Improvement plan** – Document these items into the relevant security documentation or concept of operations document.
- **Align with required compliance frameworks:** When implementing compliance frameworks such as CSA, NIST, CISPE, ISM, and ISO, verify that the framework is appropriate for the risks requiring mitigation and that it is considered as part of the broader organizations risk strategy and risk appetite statement.
  - **Improvement plan** – Document the preceding items into the relevant security documentation or concept of operations document, and provide relevant AWS certifications and risk management guides and case studies.
- **Determine the necessary conditions of engagement:** Consider the Business Impact Level (BIL) of the service to determine personnel requirements, such as security clearances, vetting, data handling, and risk training.
  - **Improvement plan** – Document the preceding items into the relevant security documentation or concept of operations document, and provide the AWS certification programs as required.

Resources

- AWS Compliance Programs

- Open source at AWS
- The AWS Cloud Adoption Framework (AWS CAF)
  - AWS Cloud Adoption Framework whitepaper
  - Risk Management in the AWS Cloud Adoption Framework
  - AWS risk and compliance program
- Building your Cloud Operating Model
- How governments can transform services securely in the cloud
- AWS digital and operational transformation guidance
  - Digital Transformation: The Why, Who, How, and What – Part 1, "The Why"
  - Digital Transformation: The Why, Who, How, and What – Part 2, "The Who"
  - Four Steps Toward Digital Government
- AWS digital and data controls
  - AWS Digital Sovereignty Pledge: Control without compromise

Security pillar

The security pillar encompasses the ability to protect data, services, and systems by taking advantage of cloud technologies to improve your security, including practices for understanding the threat and risks, empowering end users to control how their data is used, and shifting to real time monitoring and escalation models for security.

The following questions and best practices are designed to complement the best practices in the Security Pillar whitepaper.

> **Note**
>
> Governments have different security, risk, and compliance requirements, which might be enforced through rules, regulations, and laws. It's important for you to understand your obligations as a person involved with a government service. This topic is also covered in the services outcomes pillar.

Verifying privacy-by-design

GL-SEC-01: What privacy practices have you adopted relating to the use of data?

- **Elevate encryption beyond the basics:** Cloud technologies make it simpler and cost effective to encrypt data. Government jurisdictions have specific compliance and data classification requirements. For example, they might have hardware or software certification requirements, or require that cryptographic controls be managed independently of the cloud service provider's managed encryption services.
  - **Improvement plan** – Leverage encryption to protect data at transport and at rest. See the AWS Digital Sovereignty Pledge and guidance.
- **Document how privacy and end user control has been considered:** The possibilities for a personalized government service delivery must be balanced with maintaining end user control and privacy to maintain public trust. Government services should be designed to be as private as possible. Architects can link to data in place, use verifiable claims and credentials where possible, to maintain strong privacy controls and minimize any requirement to create new copies of data. Validate that sensitive data is protected, removed, or obfuscated to limit exposure. Use detection controls so that the operations team knows where sensitive data exists in the service. Access to data should require users and systems to demonstrate a strong security posture assessment, enforced with fine-grained authorization rules and multiple authentication controls.
  - **Improvement plan** – Encourage the organization to consider privacy in the design and management of the service.
- **Give end users appropriate control:** To help alleviate privacy concerns, provide end users as much control over their experience as possible. This control can include the ability to dial up or down the helpfulness of the service, for example, the level of prompting, proactive delivery, or other forms of personalization. Be transparent about data storage, use, transmission, and access. Modern technologies must allow for continuous and informed consent mechanisms where users can be involved in the decision to share their data. Make it simple for end users to understand what has been shared, with whom, and for what purpose. Enable them to revoke consent at will, and verify that access to the data is immediately restricted.
  - **Improvement plan** – Encourage the organization to consider personal agency in the design and management of the service.

- **Minimize data copies where avoidable:** In some circumstances, the ability to link to existing data might not be possible. Make use of aggregated data, synthetic data, or both. Use techniques such as verifiable claims or confidential computing to verify that the service can be operated with similar data to what is expected, while minimizing the risk of exposure or re-identification of personally identifiable information (PII).
  - **Improvement plan** – Identify ways to use data that leverages verifiable claims, credentials, anonymization, and APIs for consideration by the organization.
- **Enforcing exposure consequences:** Verify that vendor contracts inherit these obligations, and use legal and contractual means to prohibit the sharing, reuse, or storing of the data for any purpose other than delivering the government service.
  - **Improvement plan** – Support the organization to assess exposure consequences.

Shifting to a real time security model

When security is compliance-led or reactive, it can miss opportunities to be proactive in real time.

GL-SEC-02: How do you handle real time responsiveness to security (including national security) threats?

- **Do threat modelling and scenario planning** to assess and inform business continuity planning, including an incident response plan within your ecosystem, taking into consideration critical infrastructure, outside interference, disaster preparedness, and national resilience.
  - **Improvement plan** – Use scenario planning, and conduct an AWS security audit to help identify areas to improve.
- **Test and document how security threats are detected and disrupted in real time**, including the escalation plan and mechanisms to relevant security and intelligence agencies for that jurisdiction.
  - **Improvement plan** – Run threat scenarios with the organization to identify and document how threats are detected and disrupted in real time with clear lines of accountability. Provide AWS guidance and tools, such as AWS Shield Advanced, and consider an AWS security workshop.
- **Document the critical infrastructure considerations**, as this is of particular importance for national critical infrastructure.

- **Improvement plan** – Support the organization to identify critical dependencies and likely impacts of service disruption.

> **Note**
>
> The operational excellence pillar addresses agile operating models which support this outcome.

Resources

- AWS Shield Advanced Developer Guide
- AWS Digital Sovereignty Pledge
- Security, Identity, and Compliance on AWS
- AWS Risk and Compliance whitepaper
- AWS Clean Rooms
- Why AWS Data Exchange?

Reliability pillar

The reliability pillar encompasses the ability of a service to perform its intended function correctly and consistently when it's expected to. This includes the ability to operate and test the service through its total lifecycle and includes a high level of planning around service continuity and perceived reliability by the public.

The following questions and best practices are designed to complement the best practices in the Reliability Pillar whitepaper.

GL-REL-01: How do you test the service and demonstrate resilience?

- **Establish and document test-driven design and implementation, including scenario testing and mitigation planning:** Establish system and process test environments, including scaled functional testing, user testing with the public, war gaming for procedural and scenario testing, and the potential for regulatory sandboxes for policy testing.

  - **Improvement plan** – Consider running regular AWS Well-Architected *game days* in the lead up to launching a new product to identify areas for improvement and end to end system/service reliability. Encourage the organization to consider persistent team structures that span policy and delivery in their forward planning for the service, design and run scenarios and mitigation planning sessions with the customer and scaled test processes and planning.
- **Seek peer review of reliability planning:** Run and document feedback and recommendations from peer review sessions for the service and reliability planning.
  - **Improvement plan** – Support the customer to engage with relevant peers to review, share, and help assure the best possible reliability of the service.

GL-REL-02: How do you plan for service continuity?

Continuity of service is one of the highest priorities for government services. Many government services are not optional for people. These services are relied upon when we are at our most vulnerable. Business continuity is especially important to verify that end users are not put at risk from a lack of access to critical government services and systems.

- **Assess the impact of downtime and service deadlines:** Test and document the assumptions about the likely impacts of service downtime, especially on vulnerable people and communities, and around anticipated deadlines such as elections, seasonal emergencies (such as fire season), and waiting times at medical care facilities. Capture these assumptions in user journey maps and document remediations and strategies in the concept of operations document.
  - **Improvement plan** – Analyze and document the full impacts of downtime on end users, stakeholders, and others who depend on the service, using a variety of relevant planned and unplanned scenarios.
- **Plan for a graceful degradation of service, with appropriate fail-overs and alternative service pathways:** Verify that the service has appropriate fail-over strategies proportionate to the risk, and that users can identify alternative pathways to the service, including offline and phone-based user journeys. Verify that alternative service pathways are quickly discoverable by end users, even if the digital services are down. Have a stakeholder list, FAQs, and a communications plan prepared.

  - **Improvement plan** – Use scenario planning, user journey maps, and support the organization to resource and plan for service degradation, failovers, and alternative pathways for the service.
- **Verify and document the processes and public reporting of post-incident reviews:** Government departments often have specific requirements to report incidents publicly, and even when there isn't a requirement, it is often good practice to help maintain high public trust and confidence in the public institution. Identifying any requirements and ensuring the processes and expectations are clear and documented can assist in future incident management.
  - **Improvement plan** – Work with the organization to document any specific or legislative requirements to report incidents publicly, and document relevant processes.

Resources

- Protect critical services with new Continuity of Government IT on AWS solution guide
- Leverage the latest cloud technologies to build a resilient organization
- Modernizing government for the new normal: Advice for building resilience
- AWS Well-Architected game days

Performance efficiency pillar

The performance efficiency pillar includes the ability to efficiently adhere to policy and mandate requirements, and to maintain that efficiency as demand or policy changes and technologies evolve.

The following questions and best practices are designed to complement the best practices in the Performance Efficiency Pillar whitepaper.

GL-PERF-01: How do you report outcomes performance of this solution?

- **Document the public and governmental reporting mechanisms:** Government services are expected to be reliable. Demonstrate how the public would have visibility to the reliability of the service through public dashboards, reporting, performance metrics, or annual reports. In some jurisdictions, this public reporting might include program reviews, where funds to deliver the service were allocated in the budget process.

  - **Improvement plan** – Encourage the organization to consider public performance reporting in their forward planning for the service.
- **Document the measurement and monitoring approach:** Service and product owners must verify that government services are measuring and monitoring in a way that aligns with an agency's key performance indicators (KPIs), as well as to monitor for service performance and user satisfaction.
  - **Improvement plan** – Encourage the organization to include agency, policy, and mandate measures in the monitoring for the service.
- **Document the compliance foundations and the cost or effort for ongoing compliance and audit:** Identify opportunities to keep the duplication of efforts to a minimum, and maximize opportunities to automate and streamline compliance where possible.
  - **Improvement plan** – Encourage the organization to demonstrate and measure efforts to streamline and automate compliance, and to demonstrate and report costs avoided throughout the delivery of the service. Support the customer to build the foundations for compliance from the beginning.

GL-PERF-02: How do you manage continuous change and improvements for service reliability?

Document the process, cost, and resourcing for change using a range of likely change scenarios: These scenarios include changes to load (for example, major expected changes, unexpected public usage, or malicious events) and changes to service ranging from simple changes (such as updating content and minor feature changes), to new functionality and major changes. This can help to identify and manage performance efficiency as demand changes and technologies evolve, and can help identify structural or operational challenges for change agility.

- • **Improvement plan** – Use common change scenario planning to support the organization to resource for continuous change in operational planning for the service.

Resources

- New Performance Dashboard on AWS makes delivering open, responsive government simple
- Four steps to build a data strategy for managing performance in the public sector

- Raising the bar on accessibility for open-source public sector solutions

Cost optimization pillar

The cost optimization pillar includes the ability to run services which deliver policy intent and user outcome at the best value.

The following question and best practices are designed to complement the best practices in the Cost Optimization Pillar whitepaper.

GL-COST-01: How do you demonstrate an understanding of "value for money" in the customer's context?

Most government entities have clear rules around how they assess *value for money*, but this can be subtly different across jurisdictions. For some countries, value for money is considered whatever is the best functionality for the cost to deliver the desired policy outcome. Other countries take into account the best balance of social, public, and environmental benefits along with cost.

These procurement rules translate to how cost optimization is perceived, with broader analysis of the public value or policy realization sometimes considered as pure cost efficiencies. For this reason, running services at the lowest price point to deliver policy outcomes may or may not be considered cost optimization for the government department, although it's still a generally useful goal.

The following is a list of considerations and good practices to explore with the customer and to document to make sure that value for money is achieved in a government context.

- **Document the definition of *value for money*** for the jurisdictional and portfolio context, and how this service meets that definition.
  - **Improvement plan** – Engage with the government organization to understand and document their value for money definition. Work with your AWS account team to optimise costs. If you're on AWS Enterprise Support, your Technical Account Manager (TAM) can help with this. The AWS Tools for Reporting and Cost Optimization whitepaper can provide guidance.
- **Define how the cost and value is reported** to oversight and governance bodies (for example, parliament, and public scrutiny).

  - **Improvement plan** – Encourage the organization to automate and provide ease of cost/value reporting for the service. AWS provides several reporting and cost-optimization tools, including AWS Cost Explorer Service, AWS Budgets, and AWS Cost and Usage Report. Serverless applications running on services like AWS Lambda and Amazon DynamoDB can help by providing insight into costs per event.
- **Build in-house capability manage costs** through training, tools, and equipping teams.
  - **Improvement plan** – Provide delivery teams with the services and tools that they need to be able to actively understand and manage their costs.
- **Leverage existing solutions and capabilities where possible.** Support the reuse of platforms, panels, marketplaces, research, design systems, and existing solutions or components where possible.
  - **Improvement plan** – Encourage the organization to identify and leverage reusable tools, solutions, research and methods for the service. See the AWS Solutions Library.
- **Leverage professional networks and user groups.** Identify and engage with cross-governmental networks, professional networks and relevant user groups to engage peer review and feedback on the solution.
  - **Improvement plan** – Encourage the organization to identify and leverage networks and communities of practice, and establish peer review sessions.
- **Optimize for speed of change.**. It's sometimes necessary to optimize for speed to respond to a citizen need or department mandate rapidly. Government solutions might need to initially overcompensate on capacity to maintain service reliability during peak popularity, for example, at the time of a press release, to avoid breaking citizen trust. Fortunately, this necessary choice is temporary and works well with cloud economics. Service delivery teams can cost optimize and consider automatic scaling after release events, when utilization and popularity have normalized.
  - **Improvement plan** – Provide guidance and support on automated resource optimization.
- **Optimize for budget planning processes in the jurisdiction.** Provide decision makers with the key metrics that they need to balance citizen needs with service costs. Support the organization to take into account funding cycles and ensure continuity of service. Often, there is low flexibility in these cycles, however, government customers can be supported to build more flexibility into the program, project, or product-based funding mechanisms.
  - **Improvement plan** – Encourage the organization to automate and provide ease of cost/value reporting for the service, especially for delivery teams and decision makers.

Resources

- AWS Tools for Reporting and Cost Optimization whitepaper
- AWS reusable solutions, patterns, and applications:
  - AWS Solutions Library
  - AWS Construct Library
  - AWS Serverless Application Repository
- How cloud can help agencies enhance security, save costs, and improve mission delivery through the Technology Modernization Fund (TMF)
- For Small Governments – The Cloud is Only as Big as You Want it to Be
- Optimizing nonprofits' costs in the cloud

Sustainability pillar

The sustainability pillar focuses on environmental impacts from government systems, services, and policies, especially energy consumption and efficiency. The government typically has the largest information and communications technology (ICT) expenditure in a jurisdiction, so environmentally sustainable practices in government is key to driving a national sustainability agenda.

The following questions and best practices are designed to complement the best practices in the Sustainability Pillar whitepaper.

Climate action and technology

Many governments around the world have made commitments to introduce measures to reduce their impact on the climate, and have become signatories to the Paris Agreement committing to introduce specific emission reductions by 2050. The sustainability pillar supports this action by exploring how a government might reduce the environmental impact of its own services. Many jurisdictions have introduced sustainable procurement rules that provide broad guidance of the considerations an entity should undertake when considering the procurement of a new product or service.

Exploring the digitization of other government functions will contribute to how a government might reduce the climate impacts of its operations. The government will need to review existing digitized services and identifying opportunities for optimization, while also exploring how digital technologies might be deployed to accelerate sustainability outcomes.

Sustainable digital services are designed, developed, and operated in a way that minimizes their impact on the environment while still meeting business goals and user needs. These services are designed to support sustainability goals by reducing energy consumption, reducing carbon emissions, minimizing waste, and promoting resource efficiency. In some jurisdictions, there are specific targets to meet.

GL-SUS-01: What are the sustainability policies for the jurisdiction that your service operates within?

- **Document the public and governmental sustainability reporting mechanisms.** Identify relevant sustainability metrics, reporting, targets, and policies that not only reduce resource usage for the government customer, but also across the sector and nationally.
  - **Improvement plan** – Encourage the organization to consider public sustainability performance reporting in their forward planning for the service.
- **Minimize duplication of computing power where possible.** Leverage and enable reusable environments, patterns, and marketplaces as a way to minimize duplication of computing power.
  - **Improvement plan** – Encourage the organization to minimize computing power where possible in the service.
- **Share best sustainability practice across the jurisdiction or sector.** Use cross-agency, cross-jurisdiction, and cross-sector collaboration to identify and learn from examples of similar problems in other areas.
  - **Improvement plan** – Encourage the organization to engage with jurisdictional sustainability best practice throughout the delivery of the service.
- **Identify sharable data where appropriate, internal and external.** Sharing data proactively can reduce system inefficiencies. Explore the data, APIs, and tools that could be leveraged by other government departments, the broader economy, and the community to spur the scaling of digital government applications.
  - **Improvement plan** – Support the organization to include data, insights, or both in the architectural design.
- **Identify sustainability policies relevant to the organization.** Identify any sustainable procurement guidelines or policies that a jurisdiction might have to adopt, such as the Green Public Procurement in the EU.

- **Improvement plan** – Encourage the organization to understand and adopt relevant sustainability policies in the design, delivery, and management of the service.

GL-SUS-02: What design choices have been made in the service definition that is inclusive of sustainability policy outcomes and reporting requirements?

- **Identify and design or deliver inclusively of jurisdictional sustainability goals.** Verify that national sustainability goals and reporting are built in from the beginning, or have a funded plan to have them created over time.
  - **Improvement plan** – Identify if broader sustainability goals are relevant to the service and how.
- **Leverage contextual design methods, like life journey based service design.** Take a more holistic view using modes, such as life events or user journeys, to produce an improved customer experience as well as better sustainability outcomes by reducing duplication and consolidating services.
  - **Improvement plan** – Identify the end user context or journey as a means to identifying opportunities to consolidate or reduce duplication of resourcing.
- **Minimize physical impact of services, such as printing.** Design services so that they can be completed entirely digitally by reducing the need for printing documents, such as eliminating the need for physical signatures or documents.
  - **Improvement plan** – Use end-to-end service design to minimize physical printing and environmental impacts of the service.

GL-SUS-03: How might this solution be built to be extendable to other opportunities in the future?

- **Leverage automation and virtualization where possible.** Explore the opportunity to deploy digital technologies by rethinking existing processes that might improve operational efficiencies, for example, using smart technologies to manage built environments.

    - **Improvement plan** – Plan around maximum virtualization of services and where components might be made available as a utility for ease of reuse.
- **Leverage low energy sensor technologies for early detection and modelling opportunities.** Leverage new technologies, such as IoT, digital twins, and AI analysis and modelling to support more sustainable systems, decision making, and services.
    - **Improvement plan** – Support the organization to identify opportunities to leverage sensor and modelling technologies in the service, where appropriate.

Resources

- General guidance on implementation can be found in the Well-Architected Sustainability Pillar whitepaper.
- AWS Customer Carbon Footprint Tool

Enabling services outcomes for government

An additional and necessary set of considerations for government services covers best practices to verify that services measurably meet the intended policy or service outcomes, whether for public facing services (online or offline), grants management, budgeting, law enforcement or any other function of government. Service effectiveness is a responsibility of the government, but understanding the intended purpose and context of a service helps all parties involved to develop effective services with, or for, government customers. As such, this chapter should be considered for government services to maintain appropriate outcomes.

Identify the policy or purpose of this service with measurable success criteria

Most systems and services traditionally only measure operational performance (such as uptime, and the number of concurrent users) and efficiency (such as cost per transaction, staying within budget, and revenue). In the case of government systems and services, it's increasingly important to understand how *effective* a system is regardless of its performance or efficiency. Service effectiveness measurement could include both the policy and purpose measures, and the ongoing human impact measures.

- **Policy outcomes:** Every service is meant to deliver on some form of policy outcome. The purpose or intention of a system or service might be found in government policy, legislation, regulation, the mission or mandate of a department or ministry, or perhaps even in the constitutional foundations of that government. Whatever the intended policy outcome, relevant metrics and indicators should be identified which the system or service needs to measure and monitor in order to demonstrate the policy effectiveness of the system or service.
- **Human outcomes and impact:** Because government services can affect a large percentage of the population, and because these services are often either unavoidable or required, it's important to identify some baseline quality of life measurements to measure and monitor for unintended impacts on people and communities. For example, monitoring known quality of life measures, such as health indicators, employment, homelessness, and household debt, and constantly seeking unknown patterns of impacts of specific cohorts. This helps grow and maintain public trust and confidence in government systems and services, and also helps verify that any unintended harm from a system or service is able to be quickly identified and mitigated.

- **Establish mechanisms to measure, monitor, and escalate trends or patterns of policy or human impacts:** Verify that your service measurement infrastructure includes policy and human outcomes measurement and monitoring, with deviations or divergent trends being escalated in the same way that security or performance issues are escalated, and enable real-time response to change and unintended impacts. Policy impacts might include the target measures and metrics of the relevant policy. Intended human impacts might include quality of life measures like positive housing, health, or well-being outcomes for that person and their family as a result of the service.

Identify and test multiple ways to meet the desired outcome

- **Produce a discovery report with concept testing outcomes:** Verify that each service includes a *discovery phase* to describe the problem or opportunity space, and explore and test with end users a variety of concepts before heading into prototyping or solution design and architecture. Document the concepts, the results of user testing, and the resulting preferred solutions with rationale.

Identify the user needs and measures for success

- **Document the user needs and measures for success:** Government services that a person or business interact with should also measure the user outcomes and satisfaction of the service.
  - **User outcomes:** Identify what *done* is for a user, and measure it to verify that the service is delivering as expected outcomes for users. For example, a service might intend to support people to live at home longer, reducing the pressure on aged care services. Or a service might be intended to alleviate the costs of living.
  - **User satisfaction:** A combination of measures should be used to monitor and measure the end-user experience of the service, whether that user is a citizen, resident, refugee, a business, or even an internal team. Customer experience (CX) measures expectations using polling and other tools to verify that the user experience of the system or service is good. Government services are different from those in the private sector as the end user might not have a choice and must interact with the service (for example, tax, social support, and emergency services).

User satisfaction isn't just about CX, it's also about whether the service meets the public expectations for that government system or service.

- **Document how the service has been designed inclusively:** Demonstrate and document how the service was designed and tested with a diverse variety of users that represent the needs of the population, and that there are multiple channels supported that take into account different access requirements.
- **Document how the public have been engaged:** Ideally, the government customer would be engaging with the general public on the reporting, design, delivery, and operational transparency of the service to grow and maintain public trust, confidence, and perceived legitimacy of the system or service, and AWS can encourage and support this approach. Engagement with the public is also useful to design and test a range of public feedback mechanisms to verify that the continuous improvement of the service over time aligns with changing public needs. Citizen participation is increasingly expected through novel forms of public engagement and participation in the design, delivery, and governance of policies and services.
- **Identify and document the cultural context:** Every government organization serves the public, so understanding the cultural context of the service is important to inform the architecture, design, needs, and what it would take for the service to be considered welcoming and dignified. As part of this, it's helpful to consider both the demographic range of cultural needs, as well as the Indigenous and First Nations cultural context and needs, which will be different in every country.

Identify the special requirements of the government customer for this service

- **Document and understand the portfolio and jurisdictional policy context of the government customer:** All systems administered by public institutions need to be compliant with and supportive of the jurisdictional context (the constitutional and whole of government framework of that government) and of the portfolio context (the specific legislative or regulatory responsibilities of that department). Building in or documenting this context should be done in early stages to inform and influence design, architecture, and delivery. Understanding these can help you to hone in on the special obligations, responsibilities, and mission of your government customer, and to engage in conversations about what *success* looks like, so you can demonstrably and measurably design and deliver in accordance with the jurisdictional and portfolio context of your customer. A portfolio mandate might include things such as the

Social Security Act. A jurisdictional mandate might include the Constitution, or legislation that applies to the whole jurisdiction of a government customer, at a federal, state, or local level, like the Privacy Act. This might also include policy requirements like whether the service must consider open source options first (a requirement in the UK Government), or whether there are architectural standards or Indigenous engagement or procurement requirements (a requirement in the New Zealand Government).

- **Document how the service will meet public transparency and appeal-ability requirements:** How will your service provide ease of citizens' and Parliamentary access to information on service delivery, performance, reporting, explanations, and ease of avenues to appeal? Most governments have transparency requirements, such as publishing certain types of data, public reporting of metrics, and annual reports, so identifying the transparency and open government requirements for the customer is also important.
- **Align with compliance to the jurisdictional equivalent of Administrative Law:** In all governments, there are rules that govern how the public sector has to operate. For example, in Westminster-based governments, all systems and processes need to comply with the principles of Administrative Law and Rule of Law, which requires among other things, that decision making is explainable, accountable, appealable, consistent with the law, and consistently applied.

  Alternatively, if you can't explain a decision, you should at least be able to validate that it's legally compliant. High-integrity records keeping is also critical. A service can be beautifully designed, architected, delivered, and operating perfectly, but if it isn't demonstrably lawful or considered legitimate in the context of government, then it creates significant issues for the government organization and for the public, resulting in public distrust. Ideally, a modern government service should be *auditable in real time*, and have *governance* that assures oversight and escalation of issues as they emerge.

Conclusion

The goal of the Government Lens for the Well-Architected Framework is to provide architectural and operational best practices for designing and operating reliable, secure, efficient, effective, sustainable, and compliant government services on AWS. The considerations for the traditional Well-Architected pillars, combined with an additional section on enabling service outcomes for government, provides a well-rounded framework for verifying that government services built on AWS are best able to meet the special needs, context, and purpose of government customers. This approach is repeatable, extendable, and able to support meaningful discussions with government customers about the mission, purpose, and intended outcomes of their systems and services.

Architectures for government workloads need to incorporate policy considerations along with high privacy, security, and evidence-based compliance design patterns, effective measurement and feedback loops for continuous improvement, and strong governance to help maintain compliant, legitimate services and systems that can withstand the necessary accountability and scrutiny of government. Government customers need to continually monitor, measure, and detect changes or unintended impacts to meet their policy and legislative requirements.

Business continuity is critical not only to achieve business resiliency and performance objectives, but also to verify that people and communities are supported in times of high stress or emergencies. This lens was designed to support AWS builders and architects to take government needs and context into account in the design, delivery, and operation of government systems and services.

Contributors

Contributors to this document include:

- Pia Andrews, Strategic Advisor (Public Sector), Strategic Development, APAC
- Jithma Beneragama, Strategic Advisor (Public Sector), Strategic Development, APAC AWS
- Bruce Haefele, Head of Strategic Development, APAC
- Pete Herlihy, Senior Tech Product Manager, GTT, AWS WWPS
- Andrew Hodges, Senior Security Advisor, WWPS APJ
- Peter James, Principal Solutions Architect, AWS WWPS Geo APAC SA
- Jess Modini, Advisory Solutions Architect, AWS WWPS Geo APAC SA
- Ash Wallace, Senior Solutions Architect, APAC
- Emma Whitty, Senior Customer Solutions Manager, AWS WWPS
- Bruce Ross, Global Lens Lead for the Well-Architected Framework

Document history

To be notified about updates to this whitepaper, subscribe to the RSS feed.

Change	Description	Date
Minor update	Updated to reflect availabil ity of custom lens, added improvement plans for best practices, and numerous editorial changes throughout.	January 10, 2024
Minor update	Corrected broken link.	August 29, 2023
Initial publication	Government Lens first published.	August 18, 2023

Note

To subscribe to RSS updates, you must have an RSS plug-in enabled for the browser that you are using.

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.

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.