GovStack

GovSpecs 2.0

GovStack specifications vision and strategy for 2025-2027

estdev
From the people of Estonia

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

ITU

digital impact alliance

Table of Contents

1. The Big Picture: three phases of the evolution of internet

The internet began as a research network linking four US universities in 1969. Its real power emerged on 1 January 1983 when every connected node adopted the TCP/IP protocol suite, allowing any compliant network to join the growing web of links. By 1991 Tim Berners-Lee had added the World Wide Web, publishing open drafts for HTTP, HTML and URI and founding the World Wide Web Consortium to keep these formats vendor neutral. An open standards process, run by the newly formed Internet Engineering Task Force, ensured that anyone, anywhere, could implement the same protocols and achieve instant interoperability. This phase fixed the language of internetworking and proved that global reach depends on transparent specifications. This can be considered the **first phase** of evolution of the internet.

The **second phase** focused on platforms that host and deliver services. Apache HTTP Server dominated website runtimes after 1995, VMware commercialised virtual machines in 1999, and Amazon Web Services turned elastic infrastructure into a commodity in 2006. Apple's release of WebKit gave browsers a shared rendering engine across desktop and mobile, which Google later adopted and its use exploded to become a de-facto standard. Containers followed: Docker's 2013 launch popularised layered images, the Open Container Initiative froze the image and runtime format in 2015, and Kubernetes reached production-ready status under the Cloud Native Computing Foundation in 2018. Together these projects created a uniform execution environment where a workload can run unchanged from a laptop to a global cloud region. Platform standardisation brought speed, scale, and predictable deployment models for everyone building on the internet. This can be considered the second phase of the evolution of the internet.

A **third phase** is starting to unfold. Attention is moving above infrastructure to the behaviour of the applications themselves. Citizens now expect seamless services that cross agency and national borders. Developers need confidence that a data-exchange layer, a digital identity wallet, or a workflow engine from one vendor will interoperate with components from another. This is the realm where GovStack operates. By defining open, testable contracts for registries, messaging, security, and user experience, and by backing those contracts with reference implementations, GovStack sets the stage for application-level plug and play. GovSpecs will provide the rulebook that turns these ambitions into repeatable engineering practice. If the first phase connected machines and the second phase standardised how we

run code, the third phase will standardise the services themselves, unlocking a truly interoperable digital society.

The public sector is likely to lead this third phase. Core government functions – identity, registries, payments, case management – are strikingly similar in every country, and cross-border collaboration relies on these foundations lining up. Unlike private firms, which compete on proprietary features, administrations gain more from shared blueprints that slash integration cost and time. Standardised application building blocks therefore answer an immediate, common need for governments, positioning initiatives such as GovStack to drive the next wave of internet evolution.

2. Introduction to GovSpecs

GovStack is a multistakeholder, community-driven initiative, focused on accelerating national digital transformation worldwide, and drawing on expertise from contributors across the private sector, civil society, and governments all over the world. The initiative was founded by the International Telecommunication Union (ITU), Estonia, Germany, and the Digital Impact Alliance at the United Nations Foundation in 2020.

The goal of this strategy is to lay out the strategic principles, scope and targets for GovSpecs offering under the GovStack initiative for the next two years.

This document focuses primarily on GovSpecs, which is an offering within the broader GovStack initiative, aiming to establish a global de facto standard for interoperable digital government specifications. GovSpecs focus is the delivery and quality of digital government oriented building block specifications meant to be used in the design and development phase of digital government solutions, for validating solutions made available on both the GovMarket as well as for use in public tenders.

This strategy directly addresses evolving challenges in digital governance, including the necessity for AI-readiness, interoperability, and vendor-neutral architectures, drawing on international best practices.

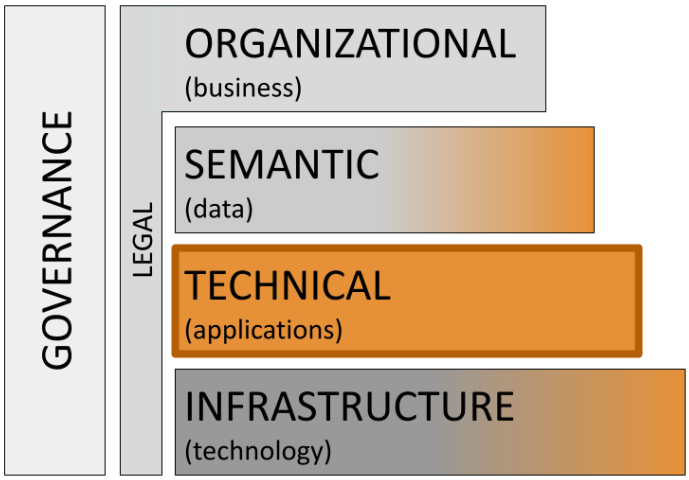
The strategy is grounded in explicit principles and a clearly defined scope, structured around three strategic pillars: enabling AI-ready government stacks, prioritizing practical and implementation-centric specification lifecycles, and applying rigorous approaches to specification modernization and quality management. These pillars collectively ensure specifications remain relevant, adaptable, and readily implementable.

A phased two-year roadmap outlines the planned progression of GovSpecs from foundational improvements to the comprehensive integration of AI capabilities and expanded global engagement. An organized governance framework clarifies roles, responsibilities, and collaborative mechanisms, reinforcing effective specification adoption.

The strategy also addresses known risks such as adoption barriers, fragmentation potential, vendor resistance, and capability gaps, with targeted mitigation approaches embedded into the execution plan.

2.1 GovSpecs architectural focus

In terms of TOGAF architecture applied to digital government interoperability and govtech, GovSpecs primarily focuses on the technical level of government digital architecture, with slight overlap with the semantic (*due to specification data requirements*) and infrastructure (due to expectations for infrastructure compatibility) layers.



The other aspects of digital government, such as legal and business architecture requirements are covered in part in other aspects of GovStack initiative, such as GovLearn (and its PAERA). *GovSpecs may also include implementation guides that impact organizational, regional and legal aspects (see 7.2.2), but they apply only when required.*

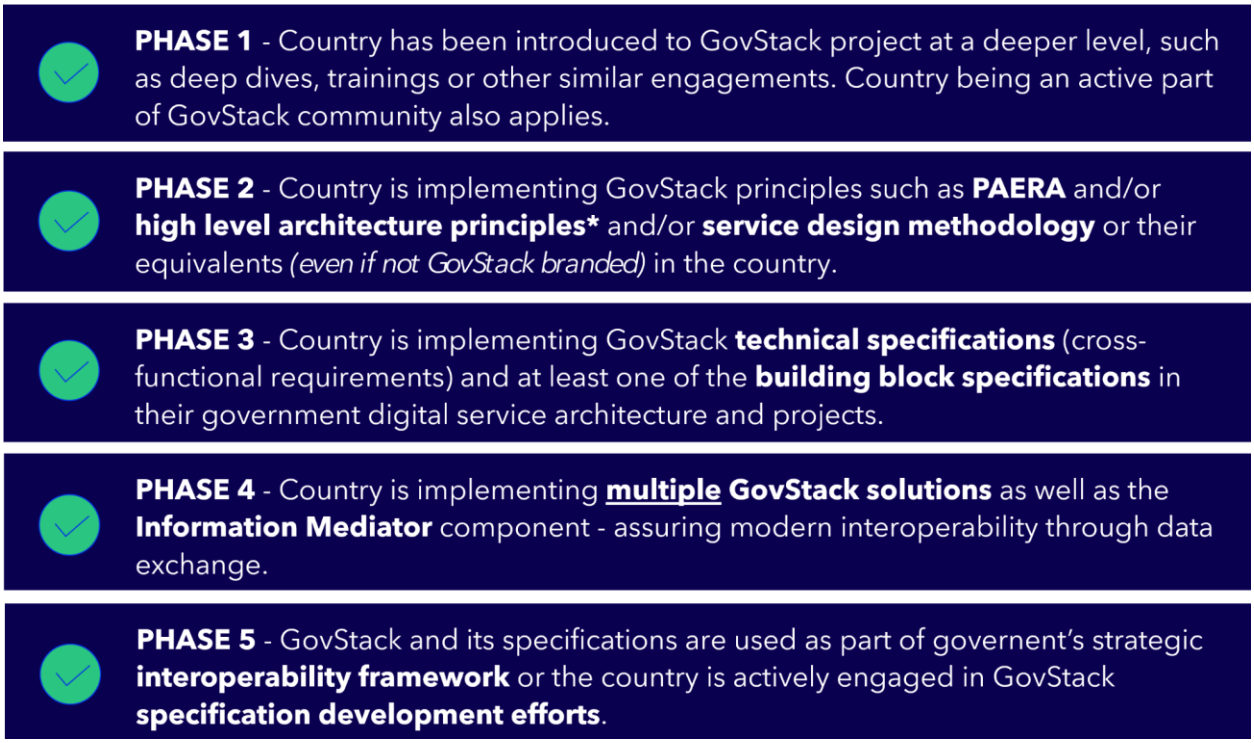
2.2 Value proposition of GovSpecs implementation

One of GovStack's goals is to help build more sustainable digital governments and related organizations. GovStack is however a big initiative and its integration in parts or in whole into digital government transformation efforts can be complicated.

Government and related organizations can also participate in specifications development work of GovSpecs directly or contributing to development of GovSpecs specifications once they have experience with GovStack.

It is recommended to consider approaching GovStack implementation in phases, with separate maturity levels defined below, each with its own benefits. Phases are covered in

more detail in further sections, but the five high level of maturity phases are the following:



IMPORTANT! For classification, each phase assumes that the criteria of the previous phases have also been met.

GovStack countries and their related phases will be published as part of country engagement work and updated when phases change.

2.2.1 Phase 1

Country has been introduced to GovStack project at a deeper level, such as deep dives, trainings or other similar engagements. Country being an active part of the GovStack community also applies.

This is the usual starting point of introducing GovStack to a new organization. This means that the organization has gone through GovStack related introduction projects (deep dive, training etc.) and is aware at the high level of what GovStack is about and what value it may bring to the country. It is able to implement high level principles[1] of GovStack in its

[1] https://www.govstack.global/about/govstack-principles/

government initiatives. Alternatively a country may already be involved with GovStack activities and the community through other collaboration projects, which also applies.

CRITERIA (1 of 2 required)
Country has gone through GovStack deep-dive, training or another equivalent project.
Country is part of the GovStack community and is aware of the GovStack project and its value.

2.2.2 Phase 2

Country is implementing GovStack principles such as PAERA and/or high level architecture principles* and/or service design methodology or their equivalents (even if not GovStack branded) in the country.

This means that the organization is implementing the high level principles of GovStack in their digital government efforts. Organization is implementing PAERA and/or architecture principles[2] and/or service design methodology[3] of GovStack in at least one of their projects. This is the usual starting point of implementing GovStack in the organization. The government benefits from this as GovStack service and technical principles have been defined by a vendor-neutral international community of experts, saving time on not having to figure out all of the principles again. *Alternatively a country may already have established equivalent mechanisms in their country that are compatible with GovStack principles and are thus considered a phase 2 country.*

CRITERIA (1 of 4 required) + needs to apply with the Phase 1 criteria
Country is implementing PAERA principles in their digital government architecture planning.
Country is implementing high level GovStack Architecture Requirements (minimally Architecture Principles) in their digital government projects.
Country is implementing the GovStack service design methodology in their digital government projects.

[2] in progress, not available at the time of strategy

[3] https://govstack.gitbook.io/sandbox/follow-methodology/best-practice-example-design-of-the-sandbox-building-permit-use-case

Country is already implementing other equivalents to PAERA, architecture principles or service design methodology that are compatible with GovStack.

2.2.3 Phase 3

Country is implementing GovStack technical specifications (cross-functional requirements) and at least one of the building block specifications in their government digital service architecture and projects.

Government and related organizations are implementing a GovSpecs compliant solution and/or technical architecture specifications[4] (architecture and security non-functional requirements) in their projects. Implementing GovStack compatible software gives assurances that the solution is more sustainable and follows international best practices and experiences. It also mitigates the risks of vendor lock-in. This level means that an organization has implemented either one of the solutions from GovMarket or has developed a digital government component based on GovSpecs specifications (such as using it in a tender as a base requirement).

CRITERIA (1 of 3 required) + needs to apply with the Phase 1 and 2 criterias
Country is using GovStack technical Architecture Requirements (including cross-functional requirements) in their government development projects when developing new digital services.
Country is implementing at least one of the GovStack compliant solutions from the GovMarket.
Country is using at least one of the GovStack building block specifications as part of their government development/tender projects.

2.2.4 Phase 4

Country is implementing multiple GovStack solutions as well as the Information Mediator component – assuring modern interoperability through data exchange.

[4] https://govstack.gitbook.io/specification/architecture-and-nonfunctional-requirements

Government and related organizations are implementing multiple GovSpecs compliant solutions. Implementing further GovStack compatible solutions enables interoperability between already existing GovStack solutions and the new services. Common technical language allows also for faster implementations of new services. Information Mediator building block is implemented to assure interoperable data exchange in the organization.

CRITERIA (2 of 2 required) + needs to apply with the Phase 1, 2 and 3 criterias
Country is using a GovStack Information Mediator compliant solution (either from GovMarket or developing a solution which is compliant with GovStack IM specification) in their government.
Country is implementing at least one *other* GovStack compliant solution from the GovMarket or one of the *other* GovStack building block specifications as part of their government development projects.

2.2.5 Phase 5

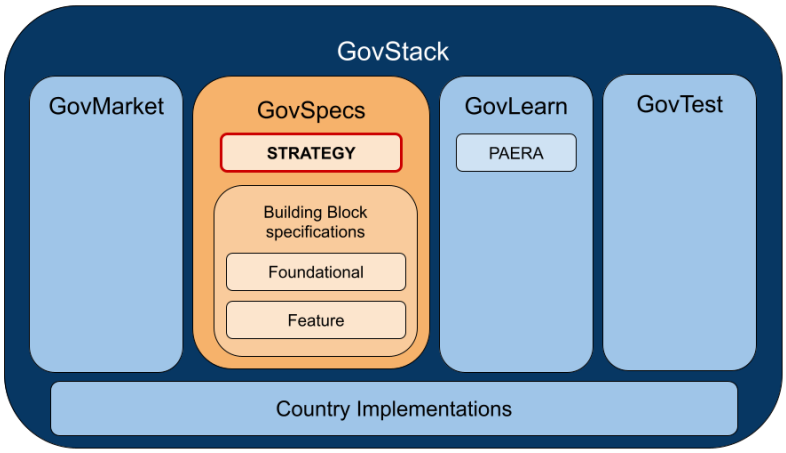
GovStack and its specifications are used as part of the government's strategic interoperability framework or the country is actively engaged in GovStack specification development efforts.

Government and related organizations have integrated GovStack architecture principles, cross-cutting requirements and building block specifications as part of their strategic government interoperability framework. They are using multiple GovStack building blocks either from GovMarket or developing based on specifications. They are also involved in the evolution of GovStack specifications by partnering with GovStack working groups, enhancing the quality of GovStack based on their experience.

CRITERIA (1 of 2 required) + needs to apply with the Phase 1, 2, 3 and 4 criterias
The country is using GovStack Architecture Requirements as part of their own country's Interoperability Framework.
Country is actively engaged with GovStack specification development efforts as part of the workgroups, bringing their experience into enhancing GovStack.

2.3 Strategy Scope and Boundaries

GovStack is a major initiative with a very broad scope affecting the digital government and e-governance and govtech space. GovSpecs is one of the offerings under the wider GovStack initiative.



GovStack as an initiative extends beyond specifications, but its effectiveness depends directly on the quality of GovSpecs specifications. Without clearly defined building block specifications, the practical implementation of GovStack's broader goals is compromised.

GovSpecs specifications serve and are used in several key areas: for validating solutions published on GovMarket, guiding the development of new digital solutions that governments and vendors might later share on GovMarket, and enabling countries to implement digital transformation efforts without duplicating existing work.

2.3.1 Relation to GovMarket

GovSpecs building block specifications are fundamental for solutions published on GovMarket. Each solution published has a link to a specific specification of GovSpecs, including its version number and compliance (see 7.3). Only the solutions that are compliant with GovSpecs published specifications are published on GovMarket.

2.3.2 Relation to GovLearn

GovLearn provides a global knowledge hub for digital e-government, supporting countries on their digital transformation journeys by offering tools, support, strategic guidance and communities of practice.

GovLearn includes the Implementation Playbook[5] and PAERA[6] (Public Administration Ecosystem Reference Architecture), a document that aims to guide public sector organizations and governments undergoing digital transformation. PAERA outlines building blocks for implementing Enterprise Architecture practices in Digital Government and establishes a Reference Architecture for the target ecosystem utilizing GovSpecs building block specifications.

2.3.3 Relation to GovTest and the Sandbox

The GovStack Sandbox provides an open demonstration environment for developers to learn about and test the GovStack building block approach. This isolated, safe environment simulates a small governmental e-service system where experts can learn more and test an example implementation of the GovStack architecture and the Building Block approach. Solutions demonstrated on GovTest are compliant with GovSpecs specifications.

2.3.4 Relation to Country Implementations

Country implementations of GovStack are varied. Countries are implementing GovStack at high level principles (including using PAERA), implementing solutions from GovMarket as well as implementing specifications from GovSpecs - both in parts and in whole. Country implementations are critical for the success of GovSpecs initiative under GovStack since it is the direct value output for the specifications developed within GovSpecs.

[5] https://govstack.gitbook.io/implementation-playbook
[6] https://govstack.gitbook.io/paera-doc

3. The Gold Standard for Interoperability

The goal of GovStack is threefold: to help countries in their digitalization efforts, to reduce the reinvention of the wheel in technology development and implementation, to break apart vendor locked IT - thus enabling new innovations - and to enable national and also support international digital interoperability. GovStack's specifications - direct result of this GovSpecs strategy - aim to be a de facto gold standard of digital government architecture specifications in the world.

This strategy does not aim to give an overarching strategy and cover the whole scope of GovStack itself, however the following four domains and their goals directly impact and are impacted by this strategy and which are what GovStack has originally been built around.

3.1 Building Blocks

GovStack community has defined building blocks as *"software modules that can be deployed and combined in a standardized manner. Each building block is capable of working independently, but they can be combined to do much more. Building blocks are composable, interoperable software modules that can be used in various use cases. They are standards-based, preferably open-source, and designed for scale. Each building block exposes a set of services in the form of REST APIs that can be consumed by other building blocks or applications."*[7]

Building blocks are meant to be:

- **autonomous** - meaning that each building block must not fail outside defined business processes when its dependencies to other building blocks fail
- **scalable** - meaning that each building block must be possible to be scaled based on demand, ideally its use directly impacting its cost (when in low use, low cost and vice versa)
- **consist of code and/or containers**
- **have applied functional and environmental requirements** (specifications, see 3.2)
- may provide **blueprints, templates, guidelines and documentation** for its use

[7] https://govstack.gitbook.io/specification/building-blocks/about-building-blocks

- **interoperable** - different building blocks are expected to be compatible with one another (through following core GovStack specifications)
- are *preferably* open source
    - Software as a Service is an option - this includes both for vendor locked and open source solutions which may be provided as SaaS
    - Vendor locked solutions require separate audits by GovSpecs team to validate compliance to specifications

The relevance of building blocks to GovSpecs strategy is that the specifications are the core focus of GovSpecs efforts and the direct output of this strategy once implemented.

3.2 Specifications (GovSpecs)

GovStack specifications are the core product focus of GovSpecs initiative within the initiative. Specifications are quality requirements and principles for the building blocks (3.1). Specifications are meant to be applied for public tenders for new digital service component developments as well as for validating digital government oriented solutions made available on the market.

A specification is:

- **requirements / principles / standards**
    - for the quality of building blocks themselves
    - for the process of developing related building block solutions
    - guidelines for implementation of said specifications to building blocks
- **interoperable**
    - **ideally** supporting asynchronous decoupling through event driven architecture and message rooms
    - **minimally** supporting API-based decoupling for data exchange
- **sustainable**
    - each specification lists a date for its last validation by the related working group
    - flexible (supporting low-code approaches or dynamic configurations for applicability in wide variety of use cases)
    - a link to its workgroup and related communication

- a reference to real life use in regions/countries

supports cloud native building blocks - specifications are universally expected to enable creation of building blocks that can be deployed in the cloud

3.3 Market (GovMarket)

Market is necessary for making the building blocks available for countries that are interested in a trusted source of software components where these principles and specifications have been applied.

A market is:

- **a gateway to building blocks and related solutions**
- **hub for certified blocks** (enforcing standards)
  - only building blocks that are compliant 100% to GovStack required-requirements.
  - showing compliance percentage to recommended-requirements
- **showing additional qualifications and audit results**
  - compliance with security audits
  - real life use in regions/countries
  - Tags and filters for local relevance (e.g., language, bandwidth constraints, offline capabilities).
- **recommendations and reviews from the community**
- User feedback, ratings, and testimonials from governments or organizations that have implemented the solutions. Community-driven insights on scalability, support, and adaptability.
- **contacts for experts and companies** with experience with said solutions

3.4 Support (inc. GovLearn)

Specifications and building blocks require a wider framework and support to be successful long-term.

Support consists of:

- **clear leadership and support** - GovSpec team is staffed with high quality experts who are responsible for the quality and delivery of specifications and supporting issues when they arise regarding specifications implementation and quality.
- **public documentation** (Confluence, Gitbook etc.) - GovStack specifications and documentation is public.
    - GovSpecs building block specifications are published.
    - Meta specifications - covering all aspects of GovStack Specification lifecycle, including the operating procedures for the Working Groups that create specifications. Its objective is to ensure there are clear processes for the different participants and stakeholders using, building and implementing the GovStack framework.
- **public communication** (Slack) - GovSpecs related working groups have communication networks established on GovStack Slack.
- **code and artifact repository** (Git/Artifactory etc.) - GovStack building block solutions are optionally published on GovStack supported code or artifact repository.
- **learning materials and implementation support documentation** (GovLearn inc. PAERA) are made available and kept up to date where relevant.

4. Context and Drivers

GovSpecs plays a key role in the broader GovStack initiative by defining interoperable specifications crucial for digital government solutions globally. This section explores the rationale behind the strategy, drawing on insights from leading international practices in digital governance, particularly emphasizing emerging trends such as AI-readiness, interoperability, and vendor-neutral architectures. It identifies challenges GovSpecs specifically addresses, providing clarity on strategic priorities and justifying the initiative's approach within the larger context of digital transformation in government sectors worldwide.

GovSpecs specifications cannot exist independently. They must account for global technological trends, interoperability challenges, and vendor-driven complexities. Specifications therefore must actively solve practical problems rather than introducing new complexities, supporting long-term, sustainable digital transformation.

4.1 Lessons from Global Digital Government Best Practices

Global digital government initiatives reveal several critical lessons shaping the design and implementation of GovSpecs. The following topics are themes internationally covered and discussed that are impacting the digital transformations of tomorrow's digital services.

4.1.1 AI-driven conversational services

Governments that lead in digitalisation are replacing menu-based portals with conversational interfaces. Estonia's Bürokratt demonstrates the shift: a network of virtual assistants will let citizens renew documents, check benefits, and sign contracts through voice or chat in a single dialogue as well as play a role of a supportive citizen consultant (helping citizens figure out how to use government provided services the best). Finland pilots the same life-event approach with AuroraAI, aiming to route a request - such as "I am starting a business" - to every relevant agency without the user touching a form. U.S. federal agencies and state unemployment offices report similar gains after deploying chatbots that handled millions of queries during peak demand.

Conversational delivery changes the engineering baseline. Every building block must expose machine-readable, self-describing APIs that an AI agent can discover and orchestrate via workflow engines. Event streams need consistent life-event vocabularies so an assistant can chain services without human intervention. Strong identity, consent, and logging hooks are mandatory for secure automation. Specifications that fail to meet these conditions risk locking governments into yesterday's portal model while citizens migrate to voice and chat channels.

Further exploration:

1. https://oecd-opsi.org/innovations/auroraai/
2. https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2024/finland/trends-and-developments
3. https://botpress.com/blog/chatbots-for-government
4. https://highlighttech.com/chatbots-gain-favor-by-government-agencies/
5. https://www.gupshup.io/resources/blog/how-is-conversational-ai-personalizing-public-services-in-2024
6. https://complexdiscovery.com/beyond-the-baby-a-vision-for-next-generation-government-technology/

4.1.1.1 Data governance and ethical AI

Trust in automated decision making depends on strong data governance and transparent model behaviour. The EU AI Act applies risk-based obligations, including mandatory impact assessments, public registers for high-risk systems, and human oversight measures. OECD AI Principles and UNESCO's Recommendation on the Ethics of AI provide accompanying guidance for fairness, transparency, and accountability. Canada's Algorithmic Impact Assessment, New Zealand's Algorithm Charter, and the United States Blueprint for an AI Bill of Rights translate those principles into practical checklists that public bodies must complete before deploying algorithms. Each framework stresses quality metadata, audit trails, and accessible explanations. GovSpecs could therefore require standard audit APIs and logging so that any building block can pass compliance reviews and maintain public trust.

4.1.2 Layered interoperability frameworks

Many governments now frame interoperability across distinct, stacked layers to avoid piecemeal integration failures. The European Interoperability Framework formalised legal, organisational, semantic, and technical layers, giving each its own principles and artefacts. The 2024 Interoperable Europe Act turned that model into binding regulation, forcing public bodies and vendors to publish reusable data models, interface contracts, and governance

workflows for cross-border services. Several member states already map legacy registers to the semantic layer to enable one-time data provision in social-security and customs exchanges.

Outside Europe, India Stack packages open APIs for identity, data, and payments at national scale, proving that a public-good interface layer can support billions of daily transactions. Singapore's Digital Economy Agreements extend the layered idea to trade partners, aligning rules on data flows, digital identities, AI governance, and cybersecurity so systems interoperate by default. These examples show why GovSpecs must embed clear artefacts for each layer - legal clauses, process handbooks, canonical vocabularies, and technical interface profiles - while supporting development and existence of adapters/connectors that wrap legacy platforms until they can be replaced.

Further exploration:

1. https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/3-interoperability-layers
2. https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf
3. https://www.capgemini.com/insights/expert-perspectives/the-interoperable-europe-act-what-should-public-sector-leaders-know/
4. https://www.imf.org/external/pubs/ft/fandd/2021/07/india-stack-financial-access-and-digital-inclusion.htm
5. https://www.mti.gov.sg/Trade/Digital-Economy-Agreements

4.1.3 Vendor lock-in and open standard APIs

Long outsourcing cycles have tied many administrations to proprietary platforms that stall reform. Governments now put exit clauses and interface obligations into contracts to avoid repeat lock-in. When legacy systems cannot be replaced immediately, adapter middleware with open, versioned APIs lets agencies swap proprietary components without rewriting upstream services. The Open Standard Identity APIs (OSIA), recently adopted as an ITU standard, show how a thin contract layer allows biometric or credential modules from different suppliers to interoperate. The UK Technology Code of Practice and similar procurement guides in Canada require departments to publish interface specifications early in a project, enforcing competition at every upgrade. By codifying adapter patterns and open interfaces, GovSpecs ensures each building block can evolve or be replaced as policy and technology move on.

Further exploration:

1. https://www.gov.uk/guidance/the-technology-code-of-practice
2. https://osia.readthedocs.io/en/stable/01%20-%20intro.html

4.1.4 Regulatory and security mandates

Cloud portability, zero trust, and sector-wide resilience are no longer optional goals. For example the EU Data Act forces cloud providers to let customers switch without exit fees and requires standardised migration playbooks that come into force from 2025, removing economic barriers to interoperability. In parallel, the NIS2 Directive and the Digital Operational Resilience Act push public administrations and financial entities to adopt structured risk management, supply-chain security, and incident reporting. Across the Atlantic every US agency is ordered to build identity-centric access control, continuous telemetry, and tamper-proof logs into all components. These instruments converge on one expectation: interface contracts, audit trails, and security controls must be baked into specifications. GovSpecs therefore needs clauses for data portability, identity assertions, policy enforcement points, and evidence logging, ensuring each building block can pass legal scrutiny and integrate with national security frameworks.

Further exploration:

1. https://www.lexology.com/library/detail.aspx?g=9b52d8d4-0e16-44df-9cc3-8b589802e229
2. https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained
3. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
4. https://www.dlapiper.com/en-us/insights/publications/2025/02/application-of-the-digital-operational-resilience-act---dora
5. https://www.gsa.gov/technology/government-it-initiatives/cybersecurity/executive-order-14028

4.1.5 Data governance and privacy-by-design

Personal data use now sits under strict legal controls in most jurisdictions. The EU General Data Protection Regulation and the 2024 Data Governance Act require purpose limitation, explicit consent, and traceability for any cross-agency data exchange. Brazil's LGPD, California's CPRA, and India's Digital Personal Data Protection Act follow similar patterns, making privacy audits a routine part of public service rollouts. At the same time, the rise of health and mobility data sharing during the pandemic exposed gaps in metadata, retention rules, and citizen oversight. Modern practice answers with privacy-enhancing techniques such as differential privacy and federated learning, letting agencies share insights without exposing raw records. For GovSpecs this means embedding consistent data-classification

tags, consent receipts, audit trails, and retention policies into interface definitions, ensuring that every building block can pass local privacy reviews and operate across borders.

4.1.6 Sustainability and green ICT

Environmental targets now shape digital government decisions. For example the EU Digital Decade sets a 2030 goal for climate neutral, energy efficient data centres and electronic communications networks. National regulators track ICT greenhouse-gas baselines and require public agencies to include carbon criteria in procurement. Reports from BEREC and the World Benchmarking Alliance recommend standard metrics for ICT emissions and energy use, pushing governments to publish annual footprints. UN e-government surveys add resilience goals, linking low-carbon cloud strategies with disaster readiness. Specifications therefore may need power-efficiency indicators for every component, reference patterns for workload placement in certified green data centres, and life-cycle data to support circular-economy requirements. By codifying these artefacts, GovSpecs aligns building blocks with emerging legal mandates and budget pressures for sustainable IT.

Further exploration:

1. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en
2. https://publicadministration.un.org/egovkb

4.1.7 Digital inclusion and resilience

Broadband access underpins both economic growth and equal participation in digital public services. World Bank studies link a ten-point rise in mobile broadband penetration with about a third of a percentage point in GDP growth. Research from the US Federal Reserve and national digital-inclusion groups shows households without reliable internet face higher unemployment and limited access to essential services. Governments respond with universal-service funds and targets such as the EU's Gigabit Society goals and the United States Broadband Equity, Access, and Deployment program.

Resilience requirements follow directly. Specifications must permit low-bandwidth channels, tolerate intermittent connectivity, and support asynchronous catch-up once a device reconnects. Offline-first design patterns, compressed data formats, and fallback SMS or USSD channels remain critical where last-mile connectivity is unreliable. By embedding

these patterns, GovSpecs can ensure that digital services stay available during network outages and that citizens in rural or low-income areas are not excluded.

4.1.8 Open-source ecosystems and community stewardship

Open-source software now underpins most national digital platforms. For example the EU's Open Source Observatory tracks more than seven hundred public-sector codebases, while the Interoperable Europe programme funds bug bounties and long-term maintenance for critical libraries. France's "BlueHats" movement embeds developers inside ministries to contribute upstream fixes and win faster security updates. The United States Defense Department's "Iron Bank" requires source availability and automated supply-chain scans before any container enters production, showing that transparent code and reproducible builds are treated as security controls, not cost savers.

For GovSpecs this trend has two consequences. First, every specification benefits from a reference implementation released (perhaps under an OSI-approved licence) so adopters can verify semantics and performance. Second, community governance - issue trackers, continuous integration pipelines, security disclosure policies - must be specified alongside technical requirements. This ensures building block specifications evolve in the open and receive updates when vulnerabilities emerge, reducing total lifecycle risk and supporting vendor diversity.

4.1.9 Agile and modular procurement

Long, one-shot IT contracts fail when technology or policy shifts mid-project. Leading administrations now break work into small increments, buying outcomes that fit two-to-six-month delivery windows. The US Digital Services Playbook and its companion TechFAR handbook show agencies how to run short sprints, release code continuously, and add suppliers through rolling competitions. The United Kingdom's Digital Marketplace applies the same logic at framework scale: pre-approved vendors list cloud services, buyers compare prices in days, and contract extensions hinge on delivered value rather than sunk cost. Open-contracting reforms add transparency by publishing tenders and spending data as JSON feeds, letting civil-society groups and auditors track delivery against promises.

Modular procurement changes specification design. Interface standards and compliance checkpoints must align with sprint boundaries so suppliers can demonstrate conformance as they ship. Versioned APIs, automated test suites, and open documentation become contractual artefacts. GovSpecs therefore needs reference contract language, outcome metrics, and open-data publishing formats that match agile delivery rhythms while preserving competition and accountability.

Further exploration:

1. https://playbook.usds.gov/
2. https://www.open-contracting.org/resources/the-open-contracting-playbook/
3. https://framework.scaledagile.com/government
4. https://www.reuters.com/legal/legalindustry/streamlining-federal-contracting-push-acquire-products-services-speed-scale-2025-05-06/

4.2 Challenges Addressed by GovSpecs

GovSpecs confronts the same constraints that drive global reform covered in section 4.1.

AI-centred service delivery depends on components that an agent can discover, chain, and audit. GovSpecs will mandate machine-readable API descriptions, event schemas linked to life-event vocabularies, and interface hooks for provenance logging and bias checks. Reference conformance suites will prove that any compliant block can plug into conversational workflows without custom code.

Interoperability only works if all layers - especially technical - are aligned. If one layer does not match, the whole system can fail, making reliable data exchange impossible. GovSpecs focuses on the technical layer, ensuring each requirement is supported by clear data models and process documentation. While organisational, legal, and semantic aspects are essential for full interoperability, GovSpecs supports these layers mainly by providing references and pointing to best practices or external frameworks (such as PAERA), rather than defining them directly.

Vendor lock-in is avoided by using open, versioned specifications and patterns. Proprietary extensions cannot block the replacement or integration of software. If a vendor adds custom features, these must not interfere with the standard interfaces, so it is always possible to replace or upgrade the software with another GovSpecs-compliant solution without major

changes. This makes it possible to swap any conformant software module for another without changing the rest of the system, keeping the ecosystem open to new solutions and reducing the risk of being tied to one vendor.

Security and regulatory mandates force uniform controls. GovSpecs will embed zero trust patterns – strong identity assertions, policy enforcement points, and immutable audit trails – into the base profile where reasonable. Data-portability and localisation clauses can meet EU Data Act, NIS2, and similar rules, further expanded by implementation guides published alongside specifications. Automated scans could become part of the certification pipeline. Privacy-by-design requirements are met through tagged data classes, consent receipts, and retention metadata built into relevant interfaces.

GovSpecs can support the goal of digital inclusion and resilience by recommending – and in some cases requiring – that building blocks or interfaces include features such as low-bandwidth support, fallback options, and accessibility standards, where these are relevant to the specific service or component. The level of requirement depends on the context of each specification, aiming to make digital public services more usable and accessible to all users, regardless of their device or connection quality.

Open-source stewardship is locked in through license requirements for reference implementations, public issue trackers, and continuous-integration pipelines. Every change proposal will go through an open review, making community maintenance part of the formal lifecycle.

GovSpecs – within the larger GovStack initiative – turns global challenges into a practical and verifiable framework, allowing countries to modernise at speed without sacrificing control or trust.

5. Strategic Principles and Assumptions

The GovStack initiative is grounded in a set of principles[8] that ensure digital public infrastructure is inclusive, scalable, sustainable, and human-centered. These principles emphasize designing with the user in mind, understanding local ecosystems, building for scale and sustainability, and committing to open standards and collaboration. They also stress the importance of data-driven decision-making, safeguarding privacy and security, promoting accessibility, maintaining transparency, and upholding international human rights. Iterative development, reuse and improvement of existing work, and a focus on delivering real services over simple web interfaces are all critical to achieving meaningful, lasting impact.

This GovSpecs strategy is fully aligned with these principles. It ensures that the development of technical specifications for GovStack Building Blocks is done transparently, inclusively, and collaboratively. Specifications are designed to be implementation-agnostic, open, and adaptable to different local contexts. The strategy promotes reuse, supports multiple solutions per specification, and emphasizes privacy, security, and accountability. By following these principles, GovSpecs supports GovStack's broader vision of enabling governments to deliver better digital services that work for everyone.

Core assumption and the expectation

Commonly agreed and communicated principles and assumptions are critical for long term success of this strategy for realizing the potential of GovStack and its specifications and to help organizations implementing GovStack solutions in achieving success in their digital transformation journeys.

These principles (5.1 to 5.4) guiding this strategy are expected to be agreed by every leader, expert and community member working with GovStack and applying its specifications and implementing their solutions.

[8] https://www.govstack.global/about/govstack-principles/

GovSpecs scope is intended to support higher initiatives of GovStack. GovSpecs is meant to support *Public Administration Ecosystem Reference Architecture* (PAERA)[9].

5.1 GovSpecs are developed by an open and inclusive expert community

While GovStack as an initiative is centrally governed and collaborates with governments, institutions, and organizations globally, it also benefits from a broader advisory community that provides strategic guidance, direction, and vision. Core GovSpecs team (see 8) are both experienced and qualified for leading these fundamental strategic efforts. Experts that have prior experience and capacity in their related roles lead working groups.

Within this structure, the development of GovSpecs is intentionally open to a wider community of contributors in various roles. Participation is based on clear, published guidelines and is focused on individuals with relevant technical expertise. Working groups operate with autonomy to define and evolve building block specifications, drawing on diverse regional, cultural, and professional backgrounds. This ensures the process remains inclusive and transparent, while maintaining the technical quality and practical relevance of the specifications.

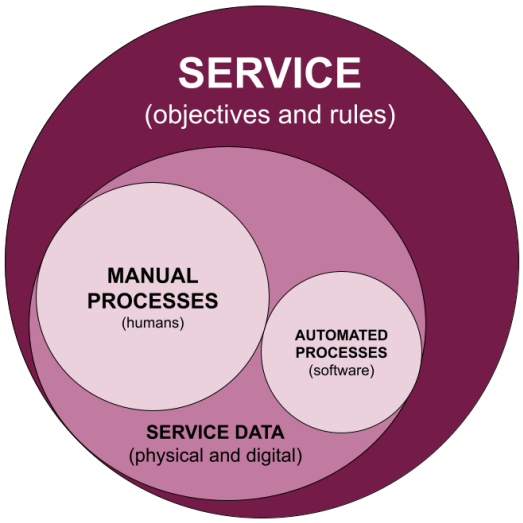
5.2 GovSpecs prioritizes long-term sustainability and forward compatibility

GovSpecs are developed with a forward-looking mindset to ensure long-term sustainability, adaptability, and technical stability. Specifications must be designed to evolve with technological and policy changes, but updates must be carefully managed to avoid unnecessary disruption. Backwards compatibility should be preserved unless there is a strong, justified need for breaking changes. Any such changes must be preceded by a thorough impact analysis, community discussion, and clear migration guidance. This approach ensures that implementations built on earlier versions remain functional and relevant over time, reducing risk and increasing trust.

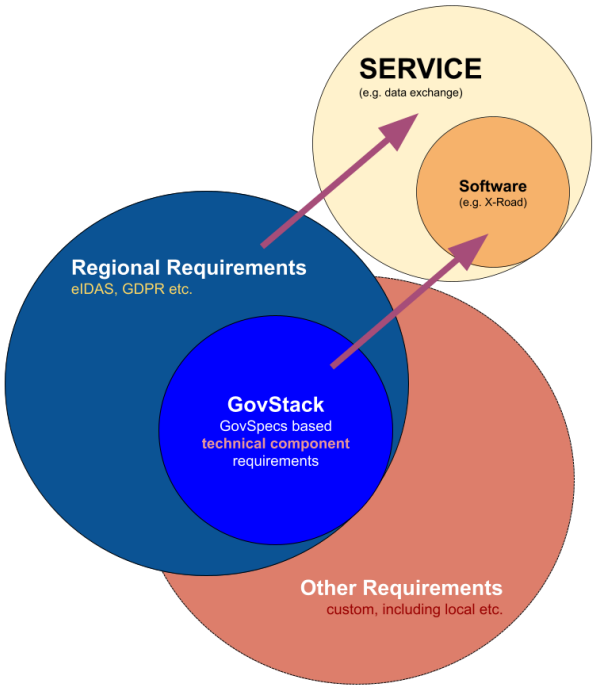
[9] https://govstack.gitbook.io/paera-doc

5.3 GovSpecs scope is technical

GovStack specifications are technical specifications for software components - so called GovStack building blocks. Building Blocks are software modules that can be deployed and combined in a standardized manner. Each building block is capable of working independently, but they can be combined to do much more. The scope of a specification is expected to be a specification for such software modules. Building Block's role is the Software part of the larger business service (primarily tackling the automation of routines and processes within the business service). And both rely upon service data to function, as shown below:



To avoid conflicts of specifications growing out of scope it is important to keep focus on the technical requirements of the specification. As such it is fundamental to understand the clear distinction between a service and a software component. Specifications are not meant to be government service specifications, but specifications for technical software components that can be used (in part or in whole) to provide government services.



GovStack specifications must be designed so that digital services can meet important regional regulations, such as eIDAS and GDPR. Simply using GovStack specifications does not automatically make a service fully compliant with all laws and regulations, because legal compliance involves much more than just the technical side. Many other factors outside of the software itself, like business processes and organizational practices, also play a role.

However, it is important that GovStack specifications do not create any barriers that would make it impossible for a service to follow these regulations. In other words, GovStack should not introduce requirements or limitations that block legal or regulatory compliance. Instead, GovStack should ensure that its technical standards are flexible and supportive enough so that organizations can build services that meet all necessary regional laws and requirements when needed.

5.4 GovSpecs are vendor-neutral

GovStack specifications are designed to be vendor-neutral. They do not favor any specific product, provider, or technology stack. The goal is to define open, clear, and implementation-agnostic technical specifications that allow for interoperability, reusability, and flexibility across different contexts and countries.

However, being vendor-neutral does not mean excluding vendors. Experts from technology providers and vendors are encouraged to actively participate in the specification process. Their technical knowledge, implementation experience, and practical insight are essential to ensuring that specifications are grounded, usable, and aligned with real-world needs.

At the same time, the development and governance of GovSpecs must be led as a community effort. No vendor or stakeholder should dominate or steer the direction of a specification. The goal is to have a plurality of implementations for each specification - open source, proprietary, and hybrid - to ensure that governments and implementers have true choice and flexibility in how they meet their needs.

6. Key Value Objectives for the Two-Year Period

While GovSpecs has multiple dependencies to other initiatives in GovStack (covered in 2.3), to support the success of GovStack there are only these key high level objectives for this strategy that the rest of this document focuses on. All activities and budgetary focus of GovSpecs must have a clear contribution to the four objectives defined below.

6.1 GovSpecs building block specifications are actively maintained and sustainable long-term

Active maintenance of GovStack specifications are important for the long-term sustainability for the interoperability that specifications are intended to support. As a result **there must not be any specifications that have not had a working group validate its quality** every year. *To measure this GovSpecs team will keep track of specification validation dates. Specifications that are not further maintained will remain as part of the GovStack family, but will be labeled as outdated.*

6.2 There are 2+ software solutions available for each building block

Specifications have no practical value unless there are implementations available for each specification. It is a key goal that **all building block specifications have at least 2 solutions available on GovMarket**. *To measure this GovMarket solutions will be validated yearly by the GovSpecs team. Specifications that will not have 2 solutions by the end of the strategy period will continue to remain as part of the GovStack family, but will be labeled as outdated.*

6.3 GovSpecs related community is active and growing

Community growth is critical to the GovStack initiative overall. Working groups need to be staffed. **All foundational building block specifications must have an active working group meeting at least quarterly with a clearly defined leadership** and **all feature building blocks must have a working group that has met at least once every year**. *To measure this GovSpecs team will validate the health of every working group regularly.*

6.4 GovSpecs are actively used in country implementations

Actual use of GovSpecs specifications is important for validating the quality and usefulness of the work being done to develop the specifications. As such **it is important that all building block specifications are used in country implementations** by the end of this strategy, or they will be deprecated from GovSpecs portfolio and picked up once a need arises through further country implementation. This use is defined by either using a solution from GovMarket or its specifications in the tenders and developments. *To measure this GovSpecs team will keep track of country implementations in relation to specifications used.*

7. Strategic Targets

Strategic targets describe the desired future state of the GovSpecs portfolio: how specifications and their delivery must look once the strategic roadmap completes.

One of the biggest shifts within this strategy is the change from variable compatibility of GovStack specifications based on percentages of requirements compatibility to a new target: GovStack compatibility is achieved if all REQUIRED requirements are met by the solution with only RECOMMENDED requirements be used for percentage - the former becomes a baseline and the latter becomes a quality signifier.

Categorization of building block specifications

Cross-functional specifications, formerly called *cross-cutting*, capture principles and rules that govern every specification in the portfolio. They cover areas such as security, accessibility, versioning, and compliance processes, ensuring that no building block drifts from the common baseline.

Foundational building blocks serve as universal dependencies for the rest of the digital government ecosystem. Digital identity, the information-mediator for data exchange, workflow orchestration are in this category, because almost every other component relies on them to authenticate users, move data, coordinate steps, or store authoritative records. Registry is also considered a foundational specification, albeit for different reasons: it is foundational as a lot of services would depend on registry building block specification based solutions.

Feature building blocks provide stand-alone functions - payments, messaging gateways, geospatial services, document generation, and similar modules - that improve the stack without being prerequisites for all others. They integrate through the foundational layer but remain replaceable or optional, letting countries choose what fits their context without breaking overall interoperability.

7.1 Designed-for-AI Digital Government Stack

GovStack is to become the first AI-focused and designed-for-AI digital government principles and specifications govtech stack in the world.

The future of next generation digital services - both in public sector and private - are going to be conversational - similarly to how humans communicate with other humans. Web forms and complex (albeit beautiful) branded user interfaces will remain important only in day to day environments that users wish to use for their core digital needs. Services will be delivered in the environments that the users are most comfortable with and the concept of multi-service branded applications is going to be deprecated over time. This change is going to happen in the public sector primarily due to the user not having to use public sector services frequently and preferring comfortable environments for complex needs.

What this means is that service deliveries are going to happen in both physical and digital environments that the users are using the most: messaging environments on their devices, digital map applications, audio and video applications and more. Just like you would be able to buy tickets or rent a car using popular mobile apps for maps, you will be able to call phone numbers and send messages to governments and related organizations.

Importantly the future will also provide an opportunity for digital twins and personal data vaults to emerge. Digital twin concept will mean that users will be able to assign some of the service automation to a digital representative of themselves - such as to an AI - and give it tasks, such as tax declarations or a change of a name. Personal data vaults will mean that the user will have more direct control over their personal data instead of leaving it in government or private sector control.

Conversational digital services, digital twins and assistants as well as personal data vaults each set particular requirements to how services should be developed and built to be interoperable with a larger ecosystem.

7.1.1 Key Targets

AI-ready - GovStack will be the first digital government stack designed for AI from day one. Specifications will assume conversational delivery, event-driven coordination, and policy-aware automation as default patterns.

Modern service experience - Today most digital government services are either fully digital or semi-digital and provided through complex websites and web forms used for processing. While GovStack specifications will continue to provide this design pattern, it needs to support the future digital services where people will obtain public services more and more in the channels they already use: chat, voice, maps, and other everyday interfaces. Branded multi-service portals will fade as AI assistants mediate transactions. Public services will appear inside familiar private-sector apps and physical touchpoints alike.

Digital twins and personal data vaults - Most government digital services of today are architecturally built in the way that governments directly hold citizen data within their own systems, however this trend will change with the emergence of wallets, personal data vaults and digital twins. As such it is important for GovStack that specifications for govtech stack will support digital representatives that act on a person's behalf, performing tasks such as filing tax returns or updating personal records. Personal data vaults will let individuals store and share attributes under their own control, reducing the need for agencies to copy data.

7.1.2 Requirements for Specifications

To enable this shift, the current GovSpecs specifications will have to be updated and take into account the following criteria in their developments:

- Machine-readable API descriptions with rich semantics that AI agents can discover and compose.
- Defined event schemas tied to life-event vocabularies so workflow engines can chain services autonomously.
- Mandate strong identity, consent, and audit hooks to safeguard and support automated interactions.
- Provide reference conformance suites, tests or examples so implementers can prove compatibility before deployment.

By aligning cross-functional rules, foundational dependencies, and modular feature blocks around these AI-centric needs, the portfolio will let governments assemble services quickly, swap components without disruption, and meet rising expectations for seamless, human-style interaction.

7.2 Implementation-Centric Specification Lifecycle

GovSpecs will succeed only if its specifications are used in real projects. Every specification must prove its value in running code, in country environments, and under regional law. The lifecycle therefore begins with design guidance that links business architecture to technical detail, moves through implementation guides that show how to apply a building block, and closes with structured feedback from each deployment. This loop keeps requirements grounded, drives rapid correction, and guards against theoretical deliverables that nobody can use.

New specifications are created when real implementation needs emerge.

Specifications become obsolete when no one needs them anymore.

Implementations are both the source of new specifications and the reason existing ones may be retired. When a GovStack collaboration with a country reveals the need for a new service that could be supported by a reusable specification not yet available, the GovSpecs team evaluates the need and scope together with relevant working groups. Conversely, if a specification sees no uptake in country implementations and lacks market solutions, it is considered outdated and labeled accordingly.

7.2.1 Service Design Guides

Service Design Guides will sit between PAERA's high-level ecosystem view and the technical requirements in GovSpecs. Each guide will describe how to shape a digital government service from problem statement to measurable outcome, mapping business capabilities to the building blocks that realise them. Topics will include value definition, user-journey modelling, data stewardship, non-functional targets, and indicators that show when the service is delivering its intended benefit. The guides will also outline how to run discovery

sprints, choose foundational components, and plan incremental releases, giving teams a direct route from strategy to code.

Where relevant, Service Design Guides should also include reference approaches from leading enterprise architecture frameworks such as TOGAF, and will encourage the use of methods like Domain Driven Design (DDD) to align business needs with technical delivery. These frameworks provide structured processes for translating strategic objectives and organisational context into actionable designs and solutions.

Service Design Guides will be an evaluation of GovStack Playbook, the latter of which focuses on GovStack building block approach for the government, but with a focus on digital services as the focus.

Integration of enterprise architecture methods as part of design guides

- **TOGAF (The Open Group Architecture Framework)** - Guides may draw on TOGAF principles for describing architecture vision, developing target architectures, and managing requirements throughout the transformation lifecycle. This supports the creation of consistent architectural artefacts, stakeholder views, and change management practices that fit the wider public sector context.
- **Domain Driven Design (DDD)** - Service Design Guides can recommend using DDD principles where services need to closely reflect complex business domains. This means identifying bounded contexts, defining ubiquitous language, and organising building blocks according to real business processes and rules—improving alignment between stakeholders and technical teams.

By using these practices then the Service Design Guides also support governments and delivery teams in building services that are not just technically sound, but also aligned with organisational structure and strategic goals.

7.2.2 Implementation Guides (region-neutral and region-specific)

Implementation Guides will live inside the specification sets for individual building blocks. They will explain how to deploy a block in practice, cover default configurations, reference integrations, and compliance checkpoints. A single specification may ship with several

guides: one generic pattern, plus region-specific versions that address legislation such as eIDAS for identity or PSD2 for payments. Countries adopting GovStack will treat these guides as required deliverables; lessons learned and local extensions will flow back into the shared repository, sharpening the guidance for the next adopter.

7.2.3 Country Feedback Mechanism

Before a GovStack project starts in any country, the GovSpecs team will review the planned architecture and identify which building blocks and guides apply. During delivery the team will provide technical support on specification questions. After go-live, implementers will submit structured feedback covering gaps, work-arounds, and successes. Participation is mandatory for projects using the GovStack label. The collected evidence feeds the working groups, triggers specification updates, and informs new versions of Service Design and Implementation Guides, ensuring that field experience drives continuous improvement.

Country feedback includes:

- *GovStack Implementation Report*, covering successes and failures.
- *Use Cases and Examples* of GovStack implementation in the related country, covering which building blocks specifications or solutions were used and for what purpose.

7.3 Specification Modernization and Quality Framework

GovSpecs will reorganise every existing document into a clear, object-oriented structure. Each building-block specification behaves like a class: it owns strict interfaces, inherits common traits from the cross-functional layer, and allows controlled extension. The framework lets teams add features without rewriting the core and guarantees that validation, certification, and market listings all reference the same canonical artefacts.

Key definitions for specifications:

- Each specification has a defined name following the pattern *"govstack-[type]-[name]"*. This is to unify the naming convention and allow clearly understood use

beyond just GovStack (such as for referencing in tenders). *This is expanded further in 7.3.2*.

    - Currently specifications are listed as "bb-messaging" and under the new naming convention it will be "govstack-bb-messaging".
    - Core GovStack specifications have currently no specification type. After the update they will have, e.g. *govstack-cfr-architecture*.
    - Types of specifications include (not a complete list):
        - **cfr** - cross-functional-requirement
        - **bb** - building block
        - **ig** - implementation guide
- Each specification will have a new *major.minor.patch* versioning scheme applied. *This is covered further in 7.3.3*.

Key definitions for specification requirements:

- Each requirement will have a unique identifier derived from the specification name, e.g. *govstack-cfr-architecture-1.1*
- Each requirement will have a new classification: REQUIRED, RECOMMENDED, DRAFT, DEPRECATED, INAPPLICABLE. *This is covered further in 7.3.4*.
- Each requirement will have a mutability defined: IMMUTABLE, EXTENSIBLE, REPLACEABLE. *This is covered further in 7.3.5*.

The five elements below give further details to each of the expected changes.

7.3.1 High Level Architecture Principles

While GovStack currently supports business-oriented principles through PAERA, the initiative lacks a unified set of high-level digital government architecture principles that guide the design, composition and evolution of the digital government stack itself.

To address this, a new strategic goal is the development of a concise, technology-agnostic architecture principles framework specifically tailored for digital government contexts. These principles should define the architectural expectations for modularity, interoperability, replaceability, lifecycle management, service decoupling, and alignment with global digital governance trends such as zero-trust security, AI-readiness, and cloud-native patterns.

Including these principles will ensure coherence across building block specifications, reduce integration risks, and offer governments a clear foundation to align their enterprise architecture with GovStack implementations.

It will also support GovStack's role as a global reference model by enabling architectural consistency, promoting resilience in public digital infrastructure, and supporting procurement and transformation efforts with clear, technology-neutral guardrails.

7.3.2 Requirements Identification and Traceability

Identifiers are important for referencing within GovStack as well as outside GovStack (for example in tender documentations).

Cross-functional roots (the core overarching requirements of GovStack) are fixed:

- govstack-cfr-development (to be created)
- govstack-cfr-deployment (to be created)
- govstack-cfr-architecture
- govstack-cfr-quality (to be created)
- govstack-cfr-security
- govstack-cfr-data (to be created)

An example requirement could be govstack-cfr-architecture-12 (meaning number 12 requirement of specifications document govstac-cfr-architecture).

7.3.2.1 Building block requirements identifications

Building-block documents follow the same pattern - e.g., *govstack-bb-messaging-3*. A mapping table would be used that shows how each rule links to its test, where it is explained, and which certifications it affects, making it easy for auditors and implementers to find all related information in one place. This is especially valuable for use in tenders where exact versioned specification may be critical.

Identifiers anchor a complete trace chain. The specification repository maintains a machine-readable matrix that links each rule to its normative text, rationale, test cases, conformance badges, and related entries in Service Design or Implementation Guides. When an overlay

reclassifies a rule or adds a local extension, the overlay file cites the original identifier, records its new status, and supplies additional tests. Tools can therefore assemble a resolved view of all applicable requirements for a given jurisdiction, generate a targeted test suite, and publish compliance results to GovMarket without manual interpretation.

The numbering scheme survives version changes. If a rule is corrected in a patch or expanded in a minor release the identifier remains stable. Only a major version that breaks compatibility can retire an identifier, in which case the retired entry remains in the registry with status DEPRECATED to prevent reuse. This disciplined approach prevents drift, simplifies automated validation, and allows historical audits to reproduce exactly which rules applied to any certified solution at any point in time.

7.3.3 Versioning (major.minor.patch)

Every GovSpecs specifications document (which includes the whole document, all of its individual requirements) adopts a three-part semantic version number. The label appears in the header of the human-readable text, in the machine-readable schema, and in the metadata that GovMarket can use.

A **major** increment signals a change that can break an existing integration. Examples include removal or fundamental rewriting of a REQUIRED rule, alteration of an immutable interface signature, or a shift in the data model that forces re-migration. When the major digit changes, dependent specifications must assess and, if necessary, revise their own versions before release. The workgroup provides a migration note that lists breaking points, affected test cases, and a recommended upgrade path.

A **minor** increment adds new capability while preserving full backward compatibility. This can involve new OPTIONAL or RECOMMENDED rules, extensions to an existing enumerated value set, or clarifications that broaden but do not narrow acceptable behaviour. Implementations that follow earlier minor versions continue to pass validation without code changes, though they may adopt new tests to display improved coverage in GovMarket.

A **patch** increment corrects errors or omissions that prevent a rule from working as intended. Typical patches fix typographical mistakes, update references to external standards, or align

an example with normative text. No behaviour visible to an integration partner may change in a patch; therefore, automated test suites should continue to pass without modification.

7.3.4 New Requirements Classification

The modernised portfolio assigns every rule a status tag that drives validation, market display, and lifecycle management. The tag appears in both human-readable text and the machine-readable schema, so tooling can decide immediately whether a solution passes, earns quality credit, or may ignore a draft element.

REQUIRED marks a rule that every conformant solution must satisfy exactly as written. Failure to meet a single REQUIRED element disqualifies the product from GovStack compliance and removes its GovMarket listing for that specification.

RECOMMENDED designates a rule that improves quality but remains optional. GovMarket will calculate the proportion of RECOMMENDED rules a solution meets and expose that figure to buyers as an additional decision signal.

DRAFT captures a proposal that has reached public view yet still needs evidence or consensus. It reserves an identifier and lets implementations experiment, but no compliance test will fail if a DRAFT rule is absent.

DEPRECATED freezes a rule that once applied but is now retired. The identifier persists for audit and traceability; future versions will never reuse it, preventing confusion in historical records.

INAPPLICABLE appears only in an overlay or extended specification. It formally switches off an inherited extensible or replaceable rule for a given context, without altering the parent text, and records the rationale so automated validators understand why the rule no longer applies.

Together these categories give implementers a precise contract, let the marketplace signal quality tiers, and allow the portfolio to evolve without breaking existing deployments.

7.3.5 Extensibility and Replaceability Rules

GovSpecs adopts an object-oriented philosophy: each building-block specification behaves like a class, inheriting common traits from the cross-functional layer and exposing controlled variation points. To make that inheritance explicit, every requirement now carries a mutability tag that determines how child specifications or local overlays may treat it .

IMMUTABLE - the rule is considered frozen and static. Later versions may refine wording for clarity but must not alter its intent, scope, input, or output. Integrations built against an immutable requirement are guaranteed to keep working across all minor and patch releases. *For example, govstack-cfr-architecture-5.12 ("5.12 Enforce Transport Security") would be immutable; breaking this guarantee would demand a new major version of the entire specification that depends on it.*

EXTENSIBLE - additional constraints or features can be layered on without changing the original text. The base wording stays immutable, ensuring upward compatibility, while overlays can tighten or elaborate the rule or add additional functionalities to the same rule. Tests for the overlay must still confirm that all base behaviour passes unchanged.

REPLACEABLE - the rule may be swapped out wholesale, provided the external contract - inputs, outputs, behaviour - remains identical. This enables technology substitution where policy or local ecosystems demand it.

To implement variation safely, GovSpecs introduces machine-readable extended specifications, which explains:

- the parent specification version it extends (with its own unique specification name);
- a list of requirement reclassifications (e.g., RECOMMENDED→REQUIRED, REQUIRED→INAPPLICABLE);
- new requirements with unique identifiers;
- dependency statements that show why each change is legal (immutable rules cannot be altered; extensible rules can be tightened; replaceable rules can be disabled or replaced).

This approach somewhat mirrors profiling in HL7 FHIR and extension taxonomies in XBRL. Validators first enforce the base spec, then apply overlay rules, ensuring deterministic outcomes and auditability.

7.3.6 Specification compliance framework

To ensure that GovSpecs specifications are meaningful and enforceable in practice, a structured compliance framework must be applied across all specifications. This framework enables countries, vendors and auditors to verify that implementations meet the required criteria, support interoperability, and remain consistent with the intended architecture vision of GovStack. The compliance process focuses on traceability, automation, and transparency.

The high-level steps for assuring specification compliance are:

1. **Specification Quality and Goal Conformance Validation**
   All specification documents must use unique, versioned identifiers for each requirement (as described in 7.3.2), with clear classification (REQUIRED, RECOMMENDED, etc.) and mutability (IMMUTABLE, EXTENSIBLE, REPLACEABLE) tags. These tags determine what is mandatory for compliance and what is optional or variable.
2. **Machine-Readable Specification Format**
   Specifications must be published in a structured, machine-readable format (e.g. JSON/YAML schemas) that maps each requirement to its description, status, validation rule and corresponding test cases. This enables automation of validation and certification pipelines.
3. **Reference Conformance Tests and Suites**
   Before a specification is approved or updated, it must undergo a quality review to ensure it aligns with the strategic goals of GovSpecs, including AI-readiness, modularity, interoperability, and compliance with cross-functional requirements. This includes both manual review by domain experts and automated checks using AI-based analysis tools (to be developed). Compliance checks should be automated where possible. Implementations must be able to submit artifacts to a validation pipeline that checks them against relevant specification rules and produces a

compliance report, including pass/fail status for REQUIRED rules and a coverage score for RECOMMENDED rules.

4. **Certification and Market Eligibility**
   Only solutions that meet 100% of REQUIRED requirements for a given version of a specification can be marked as GovStack-compliant and listed in GovMarket. As part of new specifications, appropriate tags should be set to solutions on GovMarket.
5. **Audit Trail and Traceability**
   All compliance checks must be traceable. The compliance framework must maintain historical records linking versioned requirements, validation results, associated test cases and updates. This enables auditability for public tenders, procurement and dispute resolution.
6. **Governance and Exception Management**
   The compliance framework must include a governance mechanism for handling exception cases, version transition rules, and disputes over conformance. This includes allowing phased compliance for legacy systems and formal processes for revalidating after updates.

This kind of compliance framework would ensure that GovSpecs are enforceable, measurable and support repeatable implementation. It protects the integrity of the stack while enabling flexible local adaptations.

7.3.7 Establishment of common terminology

A unified terminology is necessary to ensure consistency, clarity, and interoperability across the GovStack ecosystem. Currently, individual specifications often define their own terms, resulting in fragmented understanding and possibly duplication. Without a shared vocabulary, cross-domain integration may be hindered, implementation can become ambiguous and the risk of misinterpretation increases, especially as specifications grow more complex and are reused globally.

The targeted goal is to create, maintain and apply a core set of definitions and terms that all GovStack specifications reference and build upon. This enables smoother integration between building blocks, reduces onboarding time for new contributors, and lowers the learning curve for governments, vendors, and implementers. A common terminology also

supports automated validation and possibly machine-readability and traceability across specifications and related implementations.

The establishment of common terminology is therefore not just a matter of editorial quality but a critical foundation for long-term scalability and interoperability of GovStack solutions. This effort will result in a glossary, reviewed and updated regularly, to which all specifications must conform, ensuring a shared understanding at every level of design and delivery.

7.4 Expectations to GovStack Workgroups

To achieve the aforementioned targets in GovStack initiative and for the GovSpecs to deliver the value expected long-term, there are multiple expectations to other organizations, working groups and other GovStack teams that are expected to contribute and implement many of the relevant changes.

7.4.1 Validation and review of specifications to be AI-ready

Each specification workgroup of GovStack is expected to validate the AI-ready expectations of their specifications. Specification descriptions themselves should be understood by AI systems especially when it comes to requirements to the API's of the systems. This can be manually tested by giving specification documents to an AI (OpenAI ChatGPT, Gemini etc.) and validating if it understands the specification functionalities and requirements similarly to a domain expert.

Key expectation: All specification working groups to validate their specification for AI-readiness and share a report about this with the GovSpecs team.

7.4.2 Creation of Design Guides

Future digital government services will rely less upon user interfaces and web environments as we know them and more on ecosystems where AI and semi-automated-assistants can navigate, seek information and provide mechanisms for service navigation in multiple different platforms and environments. As such the scope of current UX/UI[10] should be

[10] https://govstack.gitbook.io/specification/govstack-ui-ux-guidelines

expanded to include digital government service design aspects beyond just the technical implementation. UX/UI workgroup experience is best suited for the creation of GovStack Digital Service Design Guides and relevant materials to act as a glue between PAERA and the GovSpecs specifications and to become a useful guide for all country implementations utilizing GovStack as well as for any organization that wishes to benefit from GovStack specifications and GovMarket solutions.

Key expectation: UX/UI working group to expand the scope of the UX/UI and include Digital Service Design Guide as part of the scope. It is important to use the GovStack Playbook as the basis to see what needs to be added and to be changed. *The key focus of the service design guide however is the focus on government business service.*

7.4.3 Creation of Implementation Guidelines

GovStack initiative includes multiple projects where GovSpecs specifications are implemented in different regional contexts (Africa, EU etc.). There are multiple regional differences due to laws and regulations, which make implementing some specifications in some regional contexts more difficult than expected. As such it is important to make sure that GovStack implementation projects consider adding a creation of specification implementation guide in X context as part of project deliverables. This implementation guide would be provided as part of GovSpecs specification added materials to support further implementations of that specification in the future.

Key expectation: Every new GovStack country implementation project to consider if it is useful to create an implementation guide for specific specifications as part of the project deliverables. If decided to create it, this implementation guideline should be shared with the GovSpecs team as well as the specification working group team.

7.4.4 Updating the specifications to match the new targets

Key expectation: Each specification workgroup of GovStack is expected to implement changes to their specifications based on the 6.3 of this strategy document.

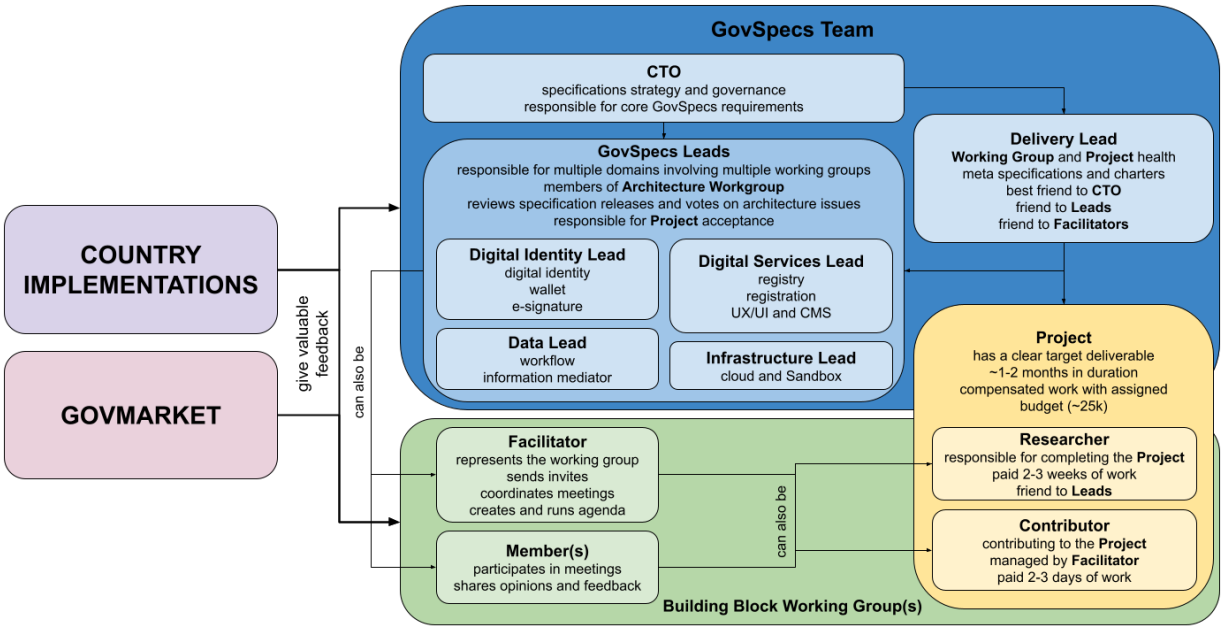
7.4.5 Country feedback mechanism implementations

GovStack initiative includes multiple organizations and projects that are not directly involved with the GovSpecs specification delivery work. GovStack principles and specifications are applied within multiple international projects. It is expected for those projects to have in place a feedback mechanism implemented together with the GovSpecs team to create a feedback loop of GovSpecs specifications used in said projects.

Key expectation: Each GovStack country implementation project that implements GovSpecs specifications to provide feedback regarding the success or struggles of the implementation with the GovSpecs team.

8. Organization and Governance

To deliver the expected targets from this strategy, GovStack needs a team with a mandate to deliver the results. GovSpecs core team under the GovStack CTO is responsible for the leadership and delivery of this strategy.



GovSpecs team consists of the following roles:

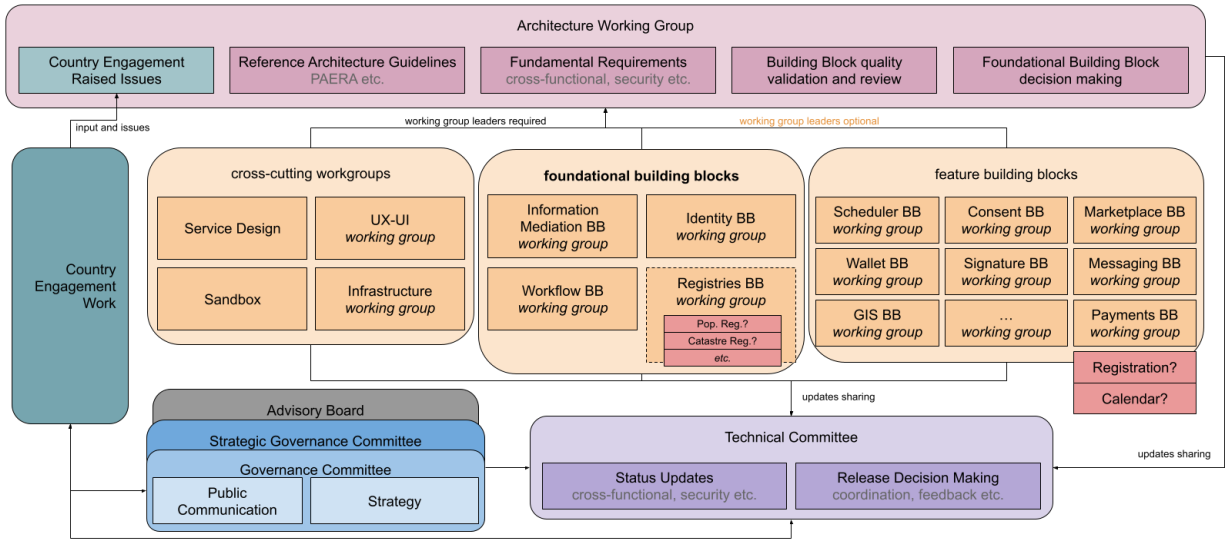
- **GovStack Chief Technology Officer** - Responsible for the leadership of GovSpecs and execution of this strategy.
- **GovSpecs Delivery Lead** - Responsible for the high quality delivery of GovSpecs specifications and the health of working groups.
- **GovSpecs Leads** - responsible for specific foundational GovSpecs specifications and their quality.
    - **Digital Identity Lead** - digital identity, wallet and e-signature building blocks
    - **Digital Services Lead** - registry, registration, CMS building blocks and UX/UI guidelines
    - **Data Lead** - data exchange related information mediator and workflow building blocks
    - **Infrastructure Lead** - infrastructure related cloud building block and GovStack Sandbox delivery

GovSpecs core team is operating under Estonia's EstDev coordination and will be part of the future GovStack Foundation structure.

8.1 Collaboration within the GovStack Initiative

GovSpecs team is in close collaboration with the other teams within the GovStack initiative through two key collaborations: **Architecture Working Group** and the **Governance Committee**.

Below is an overview of GovStack working groups and teams and their relations.



8.1.1 (Strategic) Governance Committee and the Advisory Board

GovStack initiative is coordinated at a high level by the Strategic Governance Committee that convenes every month and the related Governance Committee that convenes every week. This group is responsible for the high level strategic decisionmaking of the GovStack Initiative and which will provide oversight and coordination of the future GovStack Foundation, which will include the activities of GovSpecs work.

Strategic Governance Committee also organizes and upholds the network of Advisory Board, a group of international experts in technology and public sector governance and management which offer their input and feedback to the activities of GovStack.

The GovSpecs team reports their activities to the Strategic Governance Committee of GovStack. The Strategic Governance Committee approves the activities related to this Strategy as well as any changes and updates applied to this Strategy.

8.1.2 Architecture Working Group

The GovStack Architecture Working Group is tasked with leading the development of core technical standards and architecture principles for GovStack (cross-functional requirements). The core objective of the Architecture WG is to ensure that central GovStack architecture principles and cross-functional requirements are well-defined, actively maintained, and of the highest quality. The group ensures that the GovStack architecture remains interoperable and effectively reviews dependencies across all building blocks. The Architecture WG is responsible for creating and maintaining reference architecture guidelines, defining these essential cross-functional requirements within the GovStack ecosystem.

This workgroup is also involved in regularly reviewing and updating these principles to remain relevant in the face of evolving technological and business needs. The Architecture Working Group is also tasked with ensuring that all GovStack components adhere to these architectural standards, thereby promoting consistency across the ecosystem.

In addition, the group plays a critical role in identifying and mitigating technical debt, proactively addressing potential risks and ensuring the long-term sustainability and scalability of GovStack's architecture.

The Architecture Working Group also provides regular status updates and actively participates in the activities of the GovStack Technical Committee.

This working group is led by the GovStack Chief Technology Officer and is the direct working group collaborating to achieve the high level architectural goals of this strategy.

8.1.3 Tech Community Group (previously Technical Committee)

GovStack Tech Community Group is primarily a delivery and communication related committee which can be attended by everyone contributing to GovStack development

efforts. New specification releases,GovMarket solution updates and country implementation success stories and lessons learned will be shared in this committee.

This working group will be led by the GovStack Delivery Lead.

8.1.4 GovStack Specification Working Groups

GovStack specification working groups are semi-autonomous expert communities focused on a specific domain (e.g. payments, registries). Working groups are following the GovStack Meta-specification process in delivering or updating GovStack specifications.

Feature specification working groups are able to release new versions of specifications at their own consensus vote, with concerns addressed individually prior to release. Foundational specifications (see introduction to 7) require mandatory review and approval process with the Architecture Working Group.

Each specification working group is led by a Facilitator who schedules meetings and organizes high level activities of the working group and who represents the working group in other formats, if necessary (such as the Technical Committee or Architecture Working Group). Facilitators are collaborating with the GovStack Delivery Lead to assure high level delivery quality of specifications.

Working group members are expected to be domain experts related to the domain of the specification being developed.

8.1.4.1 Working group health metrics

To ensure each specification working group remains effective and accountable, the following indicators must be tracked and reported quarterly:

Metric	Target	Rationale
Facilitator in place	Named facilitator recorded in GovStack governance directory.	Ensures clear leadership, agenda setting and conflict resolution.
Meeting cadence	≥ 1 formal meeting every 4 weeks, minutes published within 5 days.	Maintains momentum and transparent decision-making.

Attendance rate	≥ 50 % of listed members attend meetings.	Confirms active commitment, prevents dormant groups.
Member diversity	≥ 3 distinct organisations and ≥ 2 regions represented.	Avoids single-vendor or country dominance, broadens expertise.
Specification activity	New version, amendment, validation or archival decision published ≤ 6 months ago.	Proves spec is maintained or formally retired.
GovSpecs 2.0 strategy alignment check	Working group activities are aligned with GovSpecs 2.0 strategy.	Ensures that workgroup activities also align and are interoperable with the strategy.

8.1.5 Country Engagement Teams

Country engagement and implementation teams are organized per project within the GovStack Initiative (either by EstDev, ITU or GIZ). The GovSpecs team requires collaboration and feedback mechanisms in place to assure practical quality of GovStack specifications (see 7.4.5).

8.1.6 Engagement with Vendors, Countries, and Communities of Practice

GovSpecs team is a partner where necessary to countries and vendors who are interested in implementing GovStack principles and specifications, to private sector companies interested in developing solutions based on GovStack principles as well as to the govtech community as a whole.

While no formal process is in place for this collaboration, GovSpecs team can be contacted whenever collaboration opportunities arise or support is needed. The team will either assist directly or offer advice regarding how to proceed in the related engagements.

8.3 Staffing Needs

GovStack initiative has been understaffed since the exit of Digital Impact Alliance (DIAL) from the project. As such, management has operated at minimum since the middle of 2024. It is

critical that for the effective execution of this strategy the following roles are fulfilled as part of this strategy, in order of importance:

Role	Profile and Responsibilities
Digital Identity Lead	**A person in this role needs to be experienced in both policy and implementation of digital identity related technologies in the public sector.** This role is responsible for strategic leadership of GovSpecs in relation to digital identity related specifications, including foundational digital identity as well as wallet, e-signature and other related feature building blocks.
Digital Services Lead	**A person in this role needs to have experience designing digital services in environments requiring ecosystem interoperability. Experience with user experience design and service architecture is expected.** This role is responsible for strategic leadership of GovSpecs in relation to digital service design, UX/UI and various CRUD[11]-style registries and data processing.
Infrastructure Lead	**A person in this role needs to have experience in modern cloud platforms and infrastructure, including both public and private clouds.** This role is responsible for the cloud specifications of GovStack and assuring that specifications are following expectations in regards to cloud-native requirements. This role is part of the review team from this perspective. This role is also responsible for maintenance and quality of the GovStack Sandbox environment.
Data Exchange Working Groups Facilitator	**A person in this role needs to have good administrative and managerial experience in running working groups while also having domain experience in regards to interoperability and data exchange.** This role is responsible for assuring that the data exchange related working groups - workflow and information mediator - are actively managed and meet regularly to fulfil the expectations of this strategy. This role is a close partner to GovSpecs Data Lead and will work in collaboration with that Lead.

[11] https://en.wikipedia.org/wiki/Create,_read,_update_and_delete

9. Two-Year Roadmap and Milestones

9.1 EOY 2025 - Refresh of the Foundation

GovSpecs strategy is approved	**Q3 2025**
Two-year strategy is vital to assure commonly understood focus to activities related to the GovStack specification developments.	**Metrics:** ● GovStack community feedback is implemented to this strategy ● This strategy is approved with a decision from the Strategic Governance Committee
Cross-functional Requirements align with the strategy	**Q3 2025**
Core GovStack specifications *(currently Architecture and Security)* have been updated and align with the new expectations laid out in this strategy. Additional categorization *(to Data, Development etc.)* is mapped for further development.	**Metrics:** ● govstack-cfr-architecture 2.0.0 released ● govstack-cfr-security 2.0.0 released
Digital Identity Lead is in place	**Q3 2025**
Digital identity related issues are critical to long term success of GovStack specifications. An expert with experience in policy and technology implementation of digital identity is hired for this role. eIDAS 2.0 knowledge is expected from this role to assure GovStack value for EU implementation projects as well.	**Metrics:** ● Digital Identity Lead role is filled ● Initial vision for the updated specifications is created by the Lead
Digital Identity related EU implementation guide created	**Q3 2025**
EU related digital identity and wallet policies have caused friction within GovStack working group developments. As a result a separate implementation guide will be created to assure alignment of GovStack digital identity specifications to the EU environment.	**Metrics:** ● Wallet Implementation Guide created for govstack-wallet specification ● *Need for further guides is clarified and defined.*
New cross-functional specifications and high level architecture principles have been released	**Q4 2025**
With the new structure of GovStack specifications laid out in this strategy, further cross-functional requirements will be created. This also incorporates the new high level architecture principles of GovStack. Some requirements have been migrated from previous architecture and	**Metrics:** ● govstack-cfr-development released ● govstack-cfr-deployment released ● govstack-cfr-quality released ● govstack-cfr-data released

security requirements. Estonian CFR[12] is followed for inspiration.	
Digital Services Lead in place	**Q4 2025**
Digital Services Lead is a role responsible for both the registry, registration and UX/UI working groups as well as the owner of planned Service Design guide.	**Metrics:** ● Digital Services Lead role is filled ● Initial vision for the updated specifications is created by the Lead
Service Design Guide created	**Q4 2025**
As per 6.4.1, service design guides will act as a glue between PAERA and the technical specifications of GovStack. This guide will be the handbook for digital service designers and architects when implementing new digital services, utilizing GovStack components and specifications.	**Metrics:** ● GovStack community feedback is implemented to this strategy. ● Guide has been published.
Specification Validation Process is created	**Q4 2025**
Specification validation should be a regular activity within GovStack. The process is created and implemented to working groups to assure that this validation is actively happening yearly. This includes: • validating GovMarket solutions that use the particular specification • validating specification use in GovStack country implementations • validating specification quality against the expectations of GovSpecs strategy • publishing a report on the state of specification health • validating use of terminology and compatibility with core GovStack architecture, security and related specifications	**Metrics:** ● Process is implemented with focus to all active GovStack specification working groups.
GovSpecs budget for 2026 activities is approved	**Q4 2025**
The GovSpecs team has been operating under an assigned budget from EstDev. With the creation of GovStack Foundation, GovSpecs team requires an operating budget to assure deliverables set out in this strategy.	**Metrics:** ● Budget is created and approved by the GovStack Foundation. ● Funding sources for the activities are confirmed.

[12] https://koodivaramu.eesti.ee/e-gov/cfr

Common terminology established and updated	Q4 2025
Common terminology of GovStack is established. Many specifications today list their own terminology, however for long-term success of GovStack it is beneficial to apply some of the terminology and understanding across the whole of GovSpecs.	**Metrics:** ● Common terminology of GovStack is created and the first version is published.

9.2 EOY 2026 - AI Readiness and Modernization

This is an initial estimated list of activities for 2026. Activities each year will be updated and enhanced by the GovSpecs team and approved by the GovStack Strategic Governance Committee.

AI Readiness guide created for specifications	Q1 2026
This strategy aims to ensure GovStack specifications are AI-ready. To make sure all working groups and experts understand this the same way, a guide will be created for validating specifications. This includes things such as building block readiness for use in RAG, MCP etc.	**Metrics:** ● AI Readiness validation guide created.
Specification Validation Process is implemented in all working groups	**Q1 2026**
Specification validation is a process used to validate the current health and state of GovStack specifications.	**Metrics:** ● All active working groups are following meta specification ● All active working groups have implemented specification validation process
Data Exchange Working Group Facilitator in place	**Q1 2026**
Data exchange related issues will become an important point of focus in 2026 due to expansion of the EU Data Spaces[13] concept. Additional demands and requirements will be faced by the data exchange related specifications to organize the working groups and assure relevant updates to specifications together with the Data Lead.	**Metrics:** ● Facilitator role has been filled with an expert who will manage the relevant working groups.
Facilitators in place for all GovStack specification working groups	**Q2 2026**
For the sustainability of GovStack specifications there	**Metrics:**

[13] https://digital-strategy.ec.europa.eu/en/policies/data-spaces

needs to be a responsible representative for all working groups. While some of the facilitating roles are filled by the GovSpecs team (such as for Architecture Working Group), domain expertise is expected in some working groups. It is important that all active GovSpecs specifications have a defined role of Facilitator filled to keep activities in line with this strategy.	● Facilitators have been assigned and communicated ● All facilitators have been trained to follow meta specification ● All facilitators have been trained to follow specification validation process ● Working groups have met following the expected process.
Infrastructure Lead in place	**Q2 2026**
Infrastructure lead is in place. This role will be responsible for GovStack infrastructure related specifications and principles as well as the Sandbox environment leadership.	**Metrics:** ● Infrastructure Lead is hired. ● Initial vision for new Sandbox is created. ● Sandbox management is transferred to new Lead.
All building blocks are following the new specification framework	**Q2 2026**
Alignment of GovStack specifications to this strategy are critical for further sustainability and deliverables of this strategy and relevance of GovStack.	**Metrics:** ● All feature building blocks have been updated to follow the new specification expectations.
Specification Validation Reports have been published	**Q2 2026**
All active GovStack specification workgroups have published a report on specification current state and health.	**Metrics:** ● Each specification working group has published relevant reports.
At least 2 foundational building block solutions are available on GovMarket	**Q2 2026**
It is important for the long term relevance and sustainability of GovStack to have multiple solutions available on the GovMarket. Multiple solutions minimizes the risk of vendor lock in and for technology to dominantly affect the specification.	**Metrics:** ● GovMarket includes 2+ Digital Identity, Information Mediator, Workflow, Registry and Registration/CMS solutions.
Country feedback mechanism implemented	**Q2 2026**
Country feedback mechanism is important to get active feedback regarding GovMarket solution implementation difficulties and the specification implementation difficulties.	**Metrics:** ● Country implementations are publishing a report regarding GovStack implementation difficulties and successes.

At least 1 feature building block solution is available on GovMarket	Q4 2026
It is important for the long term relevance and sustainability of GovStack to have actual solutions available on the GovMarket.	**Metrics:** ● GovMarket includes at least 1 solution for each feature building block of GovStack.
Yearly Specification Validation is Complete	**Q4 2026**
This process involves validating the relevance of GovStack specifications. Country implementations and GovMarket solutions are reviewed and decisions made regarding which specification to archive/deprecate and which to introduce.	**Metrics:** ● All GovStack specifications have gone through validation process.
GovSpecs budget for 2027 activities is approved	**Q4 2026**
GovSpecs team requires an operating budget to assure deliverables set out in this strategy for 2027 activities.	**Metrics:** ● Budget is created and approved by the GovStack Foundation. ● Funding sources for the activities are confirmed.

9.3 EOY 2027 - Global Engagement Expansion

This is an initial estimated list of activities for 2027. Activities each year will be updated and enhanced by the GovSpecs team and approved by the Strategic Governance Committee.

Every specification has an implementation project ongoing	Q1 2027
To expand the use of GovStack, it is vital that not only solutions be available on GovMarket, but solutions or GovSpecs specifications are implemented in actual country implementation projects.	**Metrics:** ● Each GovStack specification is in use either directly or through a compatible solution from GovMarket in at least one of the country implementation projects.
GovStack Sandbox 2.0 released	**Q2 2027**
The new Sandbox has been released, demonstrating the implementation and use of GovStack principles, specifications and solutions. The project is the result of Infrastructure Lead's work.	**Metrics:** ● New Sandbox is released, demonstrated and communicated.
At least 2 feature building block solutions is available on	**Q3 2027**

GovMarket	
It is important for the long term relevance and sustainability of GovStack to have multiple solutions available on the GovMarket. Multiple solutions minimizes the risk of vendor lock in and for technology to dominantly affect the specification.	**Metrics:** ● GovMarket includes 2+ solutions for each feature building block of GovStack.
GovSpecs 3.0 Strategy 2028-2029 is created	**Q3 2027**
Two-year strategy is a healthy way to drive an initiative in the size of GovSpecs.	**Metrics:** ● New strategy is created and approved by Strategic Governance Committee.
Yearly Specification Validation is Complete	**Q4 2027**
This process involves validating the relevance of GovStack specifications. Country implementations and GovMarket solutions are reviewed and decisions made regarding which specification to archive/deprecate and which to introduce.	**Metrics:** ● All GovStack specifications have gone through validation.
GovSpecs budget for 2028 activities is approved	**Q4 2027**
GovSpecs team requires an operating budget to assure deliverables set out in this strategy for 2028 activities.	**Metrics:** ● Budget is created and approved by the GovStack Foundation. ● Funding sources for the activities are confirmed.

10. Risks and Mitigations

Implementing GovStack 2.0 strategy carries with it various risks, however the following risks are meant to look beyond just the implementation of the strategy, but its impact on GovStack ecosystem that GovSpecs intends to support (as well as the ecosystem where GovStack specifications are intended to function, including country implementations).

10.1 Adoption Barriers

Long contracts tie agencies to custom systems, making it expensive to switch and hard to request open-standard solutions. Tender rules still favour the lowest-price single vendor, so teams avoid modular buys. Many staff do not yet know containers, event-driven APIs, or automated compliance, all assumed by GovSpecs. Leaders also worry about bad press from early AI mistakes or privacy leaks, so they see an AI-ready stack as a risk rather than a gain.

Risk	Mitigation
High exit costs from existing solutions and long outsourcing deals *(countries may already be implementing older and non-GovStack solutions)*	Active support by GovSpecs team. Providing patterns and phased migration playbooks. Offering high quality service design guide and implementation guides.
Tender laws may ignore open standards	Publish model clauses that let agencies require GovSpecs compliance inside existing procurement frameworks
Skills gaps in modern DevSecOps when it comes to implementing GovSpecs	Run regional or domain focused academies (such as GovStack architects training) and share reference implementations
Fear of AI-related missteps (AI might seem dangerous)	Include AI-awareness fact-vs-fiction as part of training programs and documentations of GovStack.

10.2 Fragmentation Risks

Un-coordinated extensions can split the portfolio into incompatible forks. Region-specific overlays (extended specifications) may reclassify or replace core rules without following version discipline, breaking interoperability. Some implementation guides can drift from the base spec, confusing suppliers and auditors. Unsynchronised release cycles across building

blocks risk dependency clashes where one component upgrades its major version while another still relies on the previous interface.

Risk	Mitigation
Jurisdictions create incompatible forks	Require machine-readable overlays that reference an exact parent version and forbid edits to immutable rules
Local guides diverge from core text	Mandate pull-request submission of all derived guides to the central repository for review and merge
Asynchronous major releases break dependencies	Active communication and involvement across GovStack communities. Publish a dependency graph so workgroups align major changes.
Loss of traceability across versions	Enforce permanent identifiers, deprecate instead of delete, and retain full diff history in the specification repository.

10.3 Vendor Resistance and Ecosystem Readiness

Large suppliers profit from proprietary interfaces and long-term lock-in, so they lobby against mandatory open APIs and push custom "GovStack-compatible" labels that dilute the brand. Smaller firms welcome standards but lack capacity to certify products or maintain security patches at the pace GovSpecs may demand. Audit firms and public clouds must update tooling to ingest machine-readable overlays, yet many have not planned the investment, slowing market rollout. Awareness of GovStack in general is non-existent in some sectors.

Risk	Mitigation
Big suppliers refuse to follow GovStack's open specification rules.	Tie GovMarket listing to third-party conformance results and deny use of GovStack branding without full compliance. GovStack label to give value to the brand.
Proprietary "compatible" claims confuse buyers	Register "GovStack" as a certification mark and enforce usage through legal agreements

SME suppliers struggle with certification cost	Offer simplified validation support and reference examples to cut validation effort. GovSpecs team to actively work with interested vendors.

10.4 Capability Gaps

Many administrations lack in-house architects who can map business services to building blocks, and few have DevSecOps pipelines mature enough for automated conformance testing. Data stewardship, AI ethics, and zero-trust security skills are sparse outside early-adopter states. Budget cycles do not earmark funds for continuous specification updates, leaving teams on outdated versions. Governance bodies that should coordinate cross-agency reuse often sit outside ICT divisions, slowing decision flow.

Risk	Mitigation
Shortage of architects and DevSecOps engineers	Launch further GovStack training programmes and pair country teams with experienced mentors
Limited expertise in data governance and AI ethics	Publish modular training and include mandatory competency checks in projects
Budgets cover build but not lifecycle updates	Recommend multi-year funding lines tied to GovStack initiative specification development for further improvements and collaboration (based on the tiers/phases/levels)
Governance silos delay alignment with international efforts such as GovStack	Support creation of interoperability working groups that are partners in country implementation projects of GovStack

11. Appendices

11.1 Definitions

Term	Definition
AI-Driven Conversational Services	Public-sector digital services delivered via chat, voice or similar natural-language channels, where an AI agent brokers user requests instead of static web forms.
AI-Readiness	Degree to which a specification, building block or architecture provides machine-readable semantics, discoverable APIs and event hooks that allow autonomous AI agents to understand, compose and audit services.
Agile Procurement	Contracting approach that buys small, outcome-focused increments matching two-to-six-week delivery sprints, rather than multi-year monolithic IT projects.
Architecture Working Group	GovStack body of technical experts that maintains cross-functional specifications and reviews new or changed building-block proposals for architectural fit.
Audit Trail	Chronological, tamper-evident log capturing every significant event (API call, data change, validation) required for legal, security and compliance investigations.
Auditability	Capability to recreate exactly what happened, by whom and under which rule set, across specification versions and solution deployments.
Building Block	Reusable, autonomous software module defined by a GovSpecs document; exposes standardised APIs, can be independently deployed and composed with other blocks.
Certification	Formal decision, backed by automated reports and governance sign-off, that a solution satisfies 100 % of REQUIRED rules in a specific specification version.

Compliance Framework	End-to-end process, tooling and governance that ensure specifications and solutions conform to GovSpecs rules, from authoring through certification and audit.
Compliance Report	Machine-generated artefact listing pass/fail for each REQUIRED rule, plus percentage coverage of RECOMMENDED rules, referenced by GovMarket listings.
Conformance Suite	Executable set of reference tests linked to specification rule IDs, used to produce compliance reports for building-block implementations.
Country Implementation	National or regional project that adopts GovStack principles, specs or marketplace solutions, often with feedback obligations to GovSpecs working groups.
Cross-Functional Requirement	Specification whose rules (e.g., security, versioning, data quality) apply horizontally to every building block in the portfolio.
DEPRECATED	Status flag for a rule or specification that is retained only for historical traceability and must not be used in new implementations.
Data Governance	Policies and technical measures that ensure data quality, lineage, consent handling and regulatory compliance across services.
Digital Identity	Foundational building block providing verified electronic identification, authentication and e-signature capabilities.
Digital Inclusion	Design principle ensuring all citizens, regardless of connectivity, ability or income, can access digital public services.
Digital Service Design Guide	GovStack guidance linking business capabilities and user journeys to technical building blocks, referencing PAERA and enterprise-architecture methods.
Digital Twin	Software agent, often AI-powered, authorised by an individual to perform administrative tasks (e.g., filing taxes) on their behalf via standard APIs.

Event-Driven Architecture	Integration style where components communicate via asynchronous events, enabling loose coupling and real-time reactions.
Extensible	Rule attributes indicating additional constraints or functionality may be layered on without breaking existing behaviour or contracts.
Foundational Building Block	Essential module (e.g., identity, information mediator, workflow) that most other blocks rely on for core platform capabilities.
GovLearn	GovStack knowledge hub providing training, playbooks, PAERA and community resources for digital-government practitioners.
GovMarket	Marketplace that lists GovSpecs-compliant building-block solutions together with their compliance score, audits and community feedback.
GovSpecs	Portfolio of technical specifications, versioned requirements and compliance processes that define how GovStack building blocks must operate.
GovStack	Multi-stakeholder initiative establishing modular, open and interoperable digital-government architecture, specifications and community governance.
Governance Committee	Executive structure within GovStack providing strategic oversight, budget approval and prioritisation for specification work.
Implementation Guide	Companion document to a specification describing concrete deployment patterns, default configurations and regional compliance add-ons.
Information Mediator	Foundational building block enabling secure, policy-enforced data exchange between government systems via standardised APIs or message buses.

Interoperability Layer	One of the stacked dimensions (legal, organisational, semantic, technical) that together deliver end-to-end interoperability.
Machine-Readable API	Interface fully described in structured schema (e.g., OpenAPI, AsyncAPI) that tools and AI agents can parse without human mediation.
Major Version	First digit in specification versioning that indicates breaking changes requiring re-evaluation of dependent specs and solutions.
Minor Version	Second digit signalling backwards-compatible feature additions to a specification.
Mutability	Descriptor showing whether a rule is IMMUTABLE, EXTENSIBLE or REPLACEABLE in derivative specifications or overlays.
NIS2 Directive	Directive mandating cyber-security risk management and incident reporting for essential and important entities, including public sector.
Overlay	Formally declared document that extends, tightens or disables base specification rules for regional or domain-specific needs while preserving traceability.
PAERA	Public Administration Ecosystem Reference Architecture providing high-level business and organisational principles complementing GovSpecs.
Patch Version	Third digit in versioning that fixes typos or non-behavioural defects without affecting compatibility or interfaces.
Personal Data Vault	Repository that stores an individual's attributes under their control, allowing selective sharing with public-sector services.
Privacy-by-Design	Mandate to embed data-protection safeguards such as minimisation, purpose

	limitation and consent in architecture from the outset.
Quality Badge	GovMarket indicator reflecting how many RECOMMENDED rules an implementation satisfies beyond the REQUIRED baseline.
RECOMMENDED	Optional rule whose adoption improves quality; counted toward a percentage score but not mandatory for baseline compliance.
REQUIRED	Mandatory rule that a solution must pass to be labelled GovSpecs-compliant and listed in GovMarket.
Reference Implementation	Open or proprietary example code that demonstrates exactly how a specification can be implemented and helps clarify semantics.
REPLACEABLE	Rule attribute allowing wholesale substitution in overlays provided external contracts (inputs/outputs) remain identical.
Sandbox	Isolated environment where developers can test building blocks and run conformance suites without affecting production systems.
Service Design Guide	See Digital Service Design Guide.
Specification	Normative document describing requirements, interface contracts, quality criteria, versioning and compliance process for a building block.
Strategic Governance Committee	Monthly GovStack forum comprising founding organisations that sets overall initiative direction and approves major changes.
Sustainability (Green ICT)	Practices and metrics aimed at reducing the energy use and carbon footprint of digital-government infrastructure and services.
Traceability	Linkage of each rule to its rationale, test case, validation result and marketplace listing, across versions and overlays.

Vendor Lock-In	Dependence on a single supplier due to proprietary data, interfaces or contract terms that hinder easy replacement.
Vendor-Neutral	Design principle stating that specifications must not privilege any particular vendor or technology stack.
Versioning (major.minor.patch)	Semantic scheme tracking breaking, additive and corrective changes to specifications and their rule sets.
Workflow Orchestration	Co-ordination of multiple building blocks into a complete business process via events or API calls, often managed by a workflow engine.
Zero Trust Security	Security model where no actor is trusted by default; every request must prove identity, context and policy compliance before access.