Contents

Enterprise Viewpoint

“The Enterprise Viewpoint is about making sure Government understands its work, responsibilities, and services first, before building or buying any ICT system.”

In simple terms:

- It is **not about software**
- It is **not about servers or databases**
- It is about **how Government works as an organisation**

It asks very basic but critical questions:

- What is this institution legally mandated to do?
- What services does it offer to citizens, businesses, or other agencies?
- Which processes are involved in delivering those services?
- Who else does the institution need to work with?

2. What institutions are expected to do

From an institutional point of view, the Enterprise Viewpoint expects **four main things**.

A. Be clear about your mandate and role

(“Why do you exist?”)

An institution is expected to:

- Clearly understand and document its **legal mandate**
- Identify the **functions and responsibilities** assigned to it by law or policy
- Ensure systems directly support these responsibilities

This prevents systems being built “because funds were available” rather than because there was a real mandate.

In practice, this means:

- Being able to link a system to a law, policy, or strategic objective
- Avoiding systems that duplicate what another agency is legally responsible for

B. Understand and document your business processes

(“How do you do your work?”)

Institutions are expected to:

- Document **how services are delivered**, step by step
- Identify pain points, delays, and overlaps
- Re-engineer processes where necessary before automation

You don’t automate a broken process — you fix it first.

In practice, this means:

- Mapping workflows before system design
- Designing systems around **end-to-end service delivery**, not departmental silos

C. Align systems to Government-wide strategy and architecture

(“How do you fit into the bigger Government picture?”)

Institutions must:

- Align systems to **Government Enterprise Architecture (GEA)**
- Consider existing platforms, shared services, and standards
- Avoid isolated or standalone solutions

This is where **whole-of-government thinking** comes in.

In practice, this means:

- Checking whether a similar system already exists

- Designing systems to integrate and share data
- Supporting G2C, G2B, and G2G services

D. Respect legal, policy, and regulatory requirements

(“Are you operating within the law?”)

Institutions are expected to ensure systems:

- Comply with existing laws and regulations
- Protect data and privacy
- Reflect lawful procedures and approvals

This ensures systems are:

- Defensible,
- Auditable,
- Legally sound.

3. Where these expectations sit in Annex 1 (Section mapping)

Expectation	**What it Covers**	**Annex 1 Section**
Mandate & purpose	Institutional roles, authority, responsibilities	**Legal & Institutional Framework**
Business processes	How services are delivered	**Enterprise / Business Context**
Alignment to strategy	GEA, e-Government, shared services	**Reference Framework**
Service focus	G2C, G2B, G2G, citizen-centric services	**Service Delivery Model**
Compliance	Laws, policies, regulations	**Legal & Regulatory Framework**

The Information Viewpoint

1. What the Information Viewpoint is about

“The Information Viewpoint is about understanding Government data — what data exists, who owns it, how it is used, and how it is shared.”

The Information Viewpoint focuses on **the information Government handles** to do that work.

It answers questions like:

- What data does this institution collect?
- Why is that data collected?
- Who owns the data?
- Who is allowed to use or share it?
- How long should the data be kept?

It ensures Government treats data as a **strategic public asset**, not as random system by-products.

2. What institutions are expected to do

From an institutional perspective, the Information Viewpoint expects **five key things**.

A. Identify and classify data

(“What data do we have?”)

Institutions are expected to:

- Identify the types of data they collect and manage
- Classify data based on sensitivity and importance

- Distinguish between:
    - Core (primary) data, and
    - Supporting (secondary) data

This prevents confusion and uncontrolled data growth.

In practice, this means:

- Maintaining a data inventory
- Knowing which data is critical and which is not

B. Define data ownership and responsibility

("Who is responsible for this data?")

Every dataset must have a clear owner.

Institutions are expected to:

- Assign responsibility for data accuracy, integrity, and updates
- Avoid situations where "everyone uses the data but no one owns it"

This improves accountability and data quality.

In practice, this means:

- Clear data stewardship roles
- Defined custodianship within departments

C. Ensure data quality, integrity, and consistency

("Can we trust the data?")

The standard emphasizes that data must be:

- Accurate,
- Complete,
- Consistent across systems.

Poor-quality data undermines service delivery and decision-making.

In practice, this means:

- Validation rules
- Standard definitions for data elements
- Avoiding multiple versions of the same data across systems

D. Enable secure data sharing and interoperability

(“How is data shared?”)

The Information Viewpoint strongly supports:

- Data sharing between Government institutions
- Use of common formats and standards
- Interoperability across systems

At the same time, it insists on:

- Proper access controls
- Security and privacy safeguards

In practice, this means:

- Using open standards (e.g. XML, common data formats)
- Sharing data only where legally and operationally justified

E. Manage data throughout its life cycle

(“What happens to data over time?”)

Institutions are expected to manage data from:

- Creation,
- Use,
- Storage,
- Archiving,
- Disposal.

This includes compliance with records management and retention requirements.

In practice, this means:

- Defined retention periods
- Secure disposal of obsolete data
- Alignment with records and archives policies

3. Where these expectations sit in Annex 2

Expectation	**What it Covers**	**Annex 2 Focus Area**
Data identification	Types and sources of data	Information assets
Data ownership	Responsibility and accountability	Data stewardship
Data quality	Accuracy, integrity, consistency	Data management
Data sharing	Interoperability and reuse	Information exchange
Data lifecycle	Retention and disposal	Information lifecycle

The Computational Viewpoint

1. What the Computational Viewpoint is about (Layman explanation)

“The Computational Viewpoint is about what the system actually does — the functions it performs and how those functions interact.”

While:

- The **Enterprise Viewpoint** focuses on *Government work*, and
- The **Information Viewpoint** focuses on *Government data*,

The **Computational Viewpoint** focuses on **system behaviour**.

It answers questions like:

- What functions does the system perform?
- What services does it provide?
- How do different parts of the system interact?
- Where do responsibilities begin and end within the system?

In short, it describes the system as a **set of logical building blocks**, not yet worrying about technology or infrastructure.

2. What institutions are expected to do (Practically)

From an institutional point of view, the Computational Viewpoint expects **five key actions**.

A. Break systems into clear functional components

(“What are the parts of the system?”)

Institutions are expected to:

- Identify and define system functions clearly
- Break large systems into **manageable components or services**
- Avoid building monolithic systems where everything is tightly coupled

In practice, this means:

- Defining modules or services (e.g. registration, billing, reporting)
- Keeping responsibilities of each component clear

B. Define interactions between components

("How do the parts talk to each other?")

The standard expects institutions to:

- Clearly define how system components communicate
- Specify inputs, outputs, and interfaces between components

This ensures predictable system behaviour and easier integration.

In practice, this means:

- Documented service interfaces
- Well-defined workflows and interactions

C. Support interoperability and reuse

("Can parts of this system be reused or integrated?")

The Computational Viewpoint encourages:

- Designing reusable services
- Supporting interoperability across systems
- Avoiding tightly coupled logic that blocks integration

This aligns directly with Government's **shared services** agenda.

In practice, this means:

- Service-oriented or modular design
- APIs or service interfaces that can be reused

D. Separate business logic from technical concerns

("Are we mixing business rules with technology?")

A key idea here is **separation of concerns**.

Institutions are expected to:

- Keep business rules independent of user interfaces and infrastructure
- Ensure system logic reflects business processes, not technical shortcuts

This makes systems easier to change when policies or processes change.

In practice, this means:

- Business rules defined clearly
- Logic not hard-coded into presentation layers

E. Enable controlled evolution of systems

("Can the system change without breaking everything?")

The standard expects systems to:

- Be designed for change
- Allow new functions to be added without major rewrites
- Support incremental improvements

In practice, this means:

- Modular design
- Clear contracts between components

3. Where these expectations sit in Annex 3

Expectation	**What it Covers**	**Annex 3 Focus Area**
Functional breakdown	What the system does	System functions
Component interaction	How functions communicate	Interfaces
Reuse & interoperability	Shared services	Service design
Separation of concerns	Clean logic design	Business logic
Evolvability	Support for change	Modular architecture

The Engineering Viewpoint

1. What the Engineering Viewpoint is about

"The Engineering Viewpoint is about how the system is physically put together and deployed — where the parts run, how they connect, and how reliability and security are ensured."

While:

- The **Computational Viewpoint** talks about *what the system does*,
- The **Engineering Viewpoint** talks about *how those functions are distributed and connected in the real world*.

It answers questions like:

- Where do system components run?
- How do systems communicate across networks?
- How is performance, availability, and security achieved?
- How do we make sure the system keeps running?

2. What institutions are expected to do

From an institutional point of view, the Engineering Viewpoint expects **five key things**.

A. Define system deployment and distribution

(“Where does each part of the system live?”)

Institutions are expected to:

- Clearly define where system components are deployed
- Decide whether components are centralized, distributed, or hybrid
- Understand dependencies between systems and infrastructure

This avoids poorly planned deployments that cause performance or security issues.

In practice, this means:

- Clear deployment diagrams
- Defined environments (production, testing, disaster recovery)

B. Ensure reliable communication between components

(“How do systems talk across networks?”)

The standard expects institutions to:

- Define communication mechanisms between components
- Ensure reliable, secure, and efficient data exchange

This is especially critical for **integrated Government systems**.

In practice, this means:

- Use of standard protocols
- Secure communication channels
- Monitoring of connections and failures

C. Address performance, availability, and scalability

(“Will the system cope with real-world use?”)

Institutions must consider:

- Expected system load
- Response times
- Availability requirements
- Future growth

This prevents systems from failing once usage increases.

In practice, this means:

- Capacity planning
- Load balancing
- Failover and redundancy

D. Build in security and resilience

(“How do we protect and sustain the system?”)

Security is not an afterthought at this stage.

Institutions are expected to:

- Protect systems from unauthorized access
- Ensure data is secure in transit and at rest
- Prepare for failures, disasters, and cyber incidents

In practice, this means:

- Secure network design
- Access controls
- Backup and disaster recovery planning

E. Support system operation and maintenance

(“Can ICT teams run and support this system?”)

The Engineering Viewpoint ensures systems are:

- Operable,
- Monitorable,
- Maintainable.

Institutions must plan for:

- System monitoring,
- Logging,
- Incident response,
- Routine maintenance.

In practice, this means:

- Monitoring tools
- Clear operational procedures
- Support documentation

3. Where these expectations sit in Annex 4 (Section mapping)

Expectation	**What it Covers**	**Annex 4 Focus Area**
Deployment	Physical distribution	System infrastructure
Communication	Connectivity and protocols	Network architecture
Performance	Capacity and scalability	System performance
Security	Protection and resilience	Security architecture
Operations	Monitoring and support	Operational management

The Technology Viewpoint

1. What the Technology Viewpoint is about

“The Technology Viewpoint is about the actual tools we choose — the software platforms, databases, operating systems, and technologies used to build and run Government systems.”

By the time we reach this viewpoint:

- We already know **what Government does** (Enterprise),
- **What data is involved** (Information),
- **What the system must do** (Computational),
- **How it will be deployed and operated** (Engineering).

Only now do we ask:

“So which technologies do we use to make all this happen?”

This viewpoint makes sure **technology choices support Government needs**, not the other way around.

2. What institutions are expected to do

From an institutional perspective, the Technology Viewpoint expects **six key things**.

A. Choose technologies that align with Government standards

(“Are we using approved and compatible technologies?”)

Institutions are expected to:

- Use technologies that comply with Government ICT standards
- Align with ICTA guidelines and approved architectures
- Avoid unapproved or ad-hoc technology choices

This ensures consistency across Government.

In practice, this means:

- Referencing ICTA standards during procurement
- Avoiding unsupported or obsolete platforms

B. Prefer open standards and interoperability

(“Can this technology work with others?”)

The standard strongly encourages:

- Use of open standards
- Avoidance of vendor lock-in
- Interoperable platforms and formats

This supports long-term flexibility and integration.

In practice, this means:

- Use of open data formats
- Systems that expose standard APIs
- Technologies that can integrate with other Government systems

C. Ensure security is built into technology choices

(“Is the technology secure by design?”)

Security is not just about configuration — it starts with technology selection.

Institutions must:

- Choose platforms with strong security features
- Ensure support for encryption, access control, and auditing
- Avoid technologies with known or unmanaged risks

In practice, this means:

- Secure databases and frameworks

- Regular patching and updates
- Compliance with information security standards

D. Plan for support, maintenance, and sustainability

("Can we support this technology long-term?")

Institutions are expected to think beyond initial deployment.

They must consider:

- Availability of skills
- Vendor or community support
- Upgrade and patch cycles
- End-of-life risks

In practice, this means:

- Avoiding niche or unsupported technologies
- Planning for technology refresh and upgrades

E. Support scalability and performance

("Will this technology cope as demand grows?")

Technology choices must:

- Handle increasing users and data volumes
- Support scalability without major redesign
- Meet performance expectations

In practice, this means:

- Scalable platforms
- Technologies that support load balancing and clustering

F. Avoid vendor lock-in and promote value for money

(“Are we stuck with one vendor forever?”)

The standard is clear that Government must:

- Avoid technologies that lock it into a single vendor
- Ensure value for money over the system’s lifespan

In practice, this means:

- Preference for standards-based solutions
- Clear exit and migration strategies

3. Where these expectations sit in Annex 5 (Section mapping)

Expectation	**What it Covers**	**Annex 5 Focus Area**
Standards compliance	Approved technologies	Technology standards
Interoperability	Open formats and APIs	Open standards
Security	Secure platforms	Technology security
Sustainability	Support and lifecycle	Technology lifecycle
Scalability	Performance and growth	Platform capability
Vendor neutrality	Lock-in avoidance	Procurement & value