Integration & Interoperability Framework and Systems Integration

1. Big picture

"These sections are about making sure Government systems can talk to each other and share information in a controlled, secure, and standard way."

Up to this point, the standard has focused on:

- How systems are planned,
- Built,
- Managed individually.

Systems working in isolation create duplication, inefficiency, and poor service delivery.

So ICTA introduces an Integration & Interoperability Framework and rules for Systems Integration to support whole-of-government digital services.

2. Integration & Interoperability Framework

(The rules and structure for system communication)

2.1 What "integration" and "interoperability" mean

- **Integration** means systems are technically connected so they can exchange data.
- **Interoperability** means systems can **understand and use** the data they exchange.

2.2 Why ICTA needs an Integration & Interoperability Framework

ICTA observed that:

- Systems were being built without considering others,
- Data was duplicated across institutions,
- Integration was done in an ad-hoc, insecure way.

The framework ensures:

- Standard ways of connecting systems,
- Controlled data sharing,
- Reduced duplication,
- Better citizen experience.

2.3 ICTA expectations under the Integration & Interoperability Framework

Institutions are expected to:

a) Design systems with interoperability in mind

Systems must be:

- Designed to integrate from the start,
- Built using standard interfaces,
- Avoid hard-coded or closed designs.

b) Use common standards and protocols

Institutions must:

- Use approved data formats,
- Use standard communication protocols,
- Avoid proprietary or undocumented interfaces.

This ensures systems can:

- Scale,
- Integrate later,
- Be maintained independently of vendors.

c) Support whole-of-government data sharing

Institutions must:

- Share data where legally and operationally allowed,

- Avoid re-collecting data already held by another Government entity,
- Respect data ownership and privacy rules.

Government data should be **shared once, used many times**.

d) Apply security and access controls to integrations

All integrations must:

- Be authenticated and authorised,
- Be logged and monitored,
- Protect data in transit.

Integration is treated as a **security-sensitive activity**, not just a technical task.

2.4 Key highlights

- Integration must follow a **formal framework**, not ad-hoc connections.
- Systems must be **open, standards-based, and interoperable**.
- Data sharing must be **controlled, secure, and lawful**.
- Interoperability supports **shared services and digital Government**.

3. Section 8: Systems Integration

3.1 What Systems Integration is about

"Systems integration is the practical act of connecting systems so they exchange data and support business processes."

3.2 ICTA expectations for Systems Integration

Institutions are expected to:

a) Plan integrations formally

Before integrating systems, institutions must:

- Identify systems to be integrated,
- Define data to be shared,
- Assess risks and dependencies.

Integration should be **planned and approved**, not improvised.

b) Use standard integration mechanisms

Integrations should:

- Use APIs or service interfaces,
- Follow agreed data definitions,
- Be documented and version-controlled.

This avoids fragile, point-to-point integrations.

c) Avoid tight coupling between systems

Systems should:

- Remain independent,
- Not break when another system changes,
- Support incremental upgrades.

Integration should not make systems dependent on each other's internal workings.

d) Test integrations thoroughly

Institutions must:

- Test data exchange,
- Validate error handling,
- Ensure integrations perform under load.

Integration failures affect **multiple systems**, so testing is critical.

e) Monitor and manage integrations

Once live, integrations must be:

- Monitored for failures,
- Logged for audit,
- Maintained and updated securely.

Integration is not a “set-and-forget” activity.

5. What auditors typically look for

Auditors usually check:

- Whether systems were designed for interoperability,
- Existence of documented integration interfaces,
- Use of standard protocols,
- Security controls on data exchange,
- Avoidance of duplicated data collection.

A common audit finding is:

Systems integrated informally with no documentation, approvals, or security controls.