Unified Communication Standards

1. What "Unified Communication" is

"Unified Communication is about how Government communicates internally and externally using digital tools — like email, messaging, voice calls, video conferencing, and collaboration platforms — in a coordinated, secure, and controlled way."

Instead of every department using:

- Different email systems,
- Different messaging apps,
- Different video tools,

The standard encourages Government to **treat communication as a shared, managed service**, not as scattered personal choices.

2. Why ICTA cares about Unified Communication

The standard recognises that communication tools:

- Are **core business systems**, not casual tools,
- Carry **official Government information**,
- Can expose Government to **security, legal, and reputational risks** if unmanaged.

Common problems ICTA is trying to fix include:

- Officers using personal email or WhatsApp for official work,
- No record of official communications,
- Poor security and data leakage,
- Duplication of tools and unnecessary costs.

So Unified Communication is about **order, control, and accountability**.

3. What falls under Unified Communication

Unified Communication covers **all official digital communication tools**, including:

- Email systems
- Instant messaging and chat tools
- Voice and IP telephony
- Video conferencing platforms
- Collaboration tools (shared workspaces, calendars, file sharing)
- Official use of social media and digital messaging platforms

If it is used to communicate **official Government business**, it falls under this domain.

4. What institutions are expected to do

(The core requirements explained simply)

A) Standardise official communication platforms

("Use approved tools")

Institutions are expected to:

- Use **approved and standard communication platforms**,
- Avoid uncontrolled use of personal or unofficial tools for official work.

This does not mean:

- Staff cannot own personal accounts,
- But official business must happen on **official platforms**.

This ensures consistency, security, and traceability.

B) Ensure security and access control

("Protect official communication")

Institutions must ensure that:

- Access to communication tools is controlled,

- User accounts are managed formally,
- Communication systems are protected against misuse.

This includes:

- User authentication,
- Role-based access,
- Secure configuration of platforms.

Communication systems are treated like any other Government system — not casually.

C) Support records management and auditability

(“Communication must be traceable”)

Official communication is a **Government record**.

Institutions are expected to:

- Retain communication records where required,
- Support retrieval for audits, investigations, or legal purposes,
- Avoid platforms that offer no audit trail.

“We chatted on WhatsApp” is not an acceptable record.

D) Enable integration and interoperability

(“Systems should work together”)

Unified Communication systems should:

- Integrate with other Government systems where appropriate,
- Support shared directories and identity management,
- Enable collaboration across departments and agencies.

This supports the **whole-of-government approach**.

E) Ensure reliability and availability

("Communication must always work")

Institutions must:

- Ensure communication platforms are reliable,
- Plan for outages and continuity,
- Avoid single points of failure.

This is especially critical for:

- Emergency response,
- Citizen-facing communication,
- Executive decision-making.

F) Provide governance and usage policies

("Set the rules of use")

Institutions must define:

- What tools are approved,
- How they should be used,
- What is prohibited,
- Responsibilities of users.

This helps manage:

- Misuse,
- Data leaks,
- Reputational risks.

5. What Unified Communication is NOT

The standard is clear (implicitly) that Unified Communication is **not**:

- About banning all new tools,
- About micromanaging personal communication,

- About forcing one tool for every scenario.

6. Why this section matters from an audit perspective

Auditors typically check:

- Whether official email systems are standardised,
- Whether personal tools are being used for official work,
- Whether communication records can be retrieved,
- Whether access is properly controlled.

A common audit finding is:

Official decisions communicated through personal or unmanaged platforms.

7. How this links back to earlier domains

Unified Communication connects directly to:

- **Enterprise Viewpoint** → How Government works and communicates
- **Information Viewpoint** → Communication as information assets
- **Security and Governance controls** → Risk management