Website Development and Management

1. What It Is About

"Government websites are official systems and must be planned, built, managed, secured, and retired in a controlled and accountable way."

ICTA is very intentional here:

- A website is **not just a communication tool**,
- It is a **public-facing Government system**,
- Anything public-facing carries **high risk** (reputation, security, trust).

So Section 6.5 lays down **specific controls** for how websites are:

- Developed,
- Managed,
- Governed over their entire lifecycle.

2. Website Development

(How Government websites should be built)

"Before a Government website goes live, what must be done to ensure it is useful, secure, and official?"

ICTA expectations during website development

Institutions are expected to:

a) Treat website development like any other system development

Websites must:

- Follow planning, analysis, and design processes,
- Have clear objectives and scope,

- Be aligned to the institution's mandate.

b) Design websites around users

Institutions must ensure websites:

- Are easy to use,
- Are accessible to the public,
- Present information clearly.

This supports:

- Citizen access,
- Transparency,
- Service delivery.

c) Ensure consistency with Government branding and standards

Websites must:

- Follow approved Government branding,
- Present a consistent Government identity,
- Avoid misleading or unofficial appearances.

Citizens must immediately recognize a site as **official Government**.

d) Build security into the website from the start

Website development must consider:

- Secure authentication for administrators,
- Protection against common web threats,
- Secure handling of data.

Security is **not optional** because websites are public-facing.

3. Website Governance

(Who controls the website and content)

"Who owns this website, who approves content, and who is accountable?"

Why ICTA brings governance into websites at all

A Government website is a digital public asset, not just an ICT product.

Because of this, decisions about:

- Creating a website,
- Adding major features,
- Publishing digital services,
- Retiring or consolidating websites,

cannot be left to individuals or departments acting alone.

This is where the **Digitization Asset Committee (DAC)** comes in.

What the Digitization Asset Committee is

"The Digitization Asset Committee is a formal internal committee that oversees and approves Government digital assets, including websites and web systems."

In simple terms:

- It treats websites as **institutional assets**,
- It ensures websites support the institution's mandate,
- It prevents random or duplicated digital initiatives.

Why the Digitization Asset Committee is relevant to Web Governance

ICTA expects institutions to **centralise oversight of digital assets**, and websites are among the most visible of these assets.

Under Section 6.5, the DAC plays a key role in ensuring:

- Websites are **necessary and justified**,

- Digital initiatives are **aligned to strategy**,
- There is **no duplication or fragmentation**,
- Websites are properly **owned and governed**.

In essence, the DAC is the **gatekeeper** for Government websites.

What ICTA expects institutions to do (DAC-specific expectations)

a)Approval of new websites and web systems

("No website without approval")

Institutions are expected to:

- Present proposals for new websites or major web systems to the DAC,
- Justify the need, scope, and purpose,
- Confirm alignment with institutional mandate and Government digital strategy.

A website should not be developed or launched without **DAC approval**.

b) Oversight of website consolidation and reuse

("Do we really need another website?")

The DAC is expected to:

- Assess whether an existing website or platform can be reused,
- Recommend consolidation instead of creating new sites,
- Support shared or centralised web platforms.

This directly supports:

- Cost efficiency,
- Interoperability,
- Whole-of-government digital presence.

c) Assignment of ownership and accountability

(“Who owns this digital asset?”)

Through DAC oversight, institutions must:

- Assign a clear **business/content owner**,
- Assign a clear **technical/ICT owner**,
- Define content approval and publishing authority.

The DAC ensures no website is left without ownership.

d) Oversight of lifecycle decisions (enhancement, retirement, disposal)

(“Websites must also have an end-of-life”)

The DAC is expected to:

- Approve major changes or enhancements to websites,
- Endorse decisions to retire or decommission websites,
- Ensure retirement aligns with records management and data policies.

This prevents:

- Abandoned websites,
- Orphaned domains,
- Security risks from forgotten systems.

What ICTA is preventing

- Consultants publishing content without oversight,
- Outdated or incorrect information online,
- Websites surviving long after projects end.

4. Domain Name Management

“What web address does the website use, and who controls it?”

ICTA expectations on domain management

Institutions must:

- Use **official Government domains** (e.g. .go.ke),
- Register domains through authorized channels,
- Ensure domains are:
    - Owned by Government,
    - Renewed on time,
    - Not controlled by vendors or individuals.

A domain name is treated as a **Government asset**.

What ICTA is preventing

- Loss of Government websites due to unpaid renewals,
- Vendors holding domains hostage,
- Citizens accessing fake or misleading sites.

5. Website Hosting and Infrastructure

"Where does the website actually run?"

ICTA expectations on hosting

Institutions must:

- Host websites on **approved and secure environments**,
- Ensure hosting provides:
    - Availability,
    - Performance,
    - Backup and recovery,
    - Security monitoring.

They must also:

- Know where data is hosted,
- Avoid unmanaged or personal hosting services.

Hosting decisions are **governance decisions**, not just technical ones.

6. Website Content Management (6.5.x – content subsection)

"What information is published, how often it is updated, and who approves it."

ICTA expectations on content management

Institutions must:

- Ensure content is:
    - Accurate,
    - Current,
    - Officially approved,
- Remove outdated or misleading information,
- Maintain editorial controls.

Poor content management is treated as **poor governance**.

7. Integration and Interoperability

"Can the website work with other Government systems?"

ICTA expectations on interoperability

Institutions must ensure websites:

- Integrate with backend systems where needed,
- Use standard data formats and interfaces,
- Avoid becoming standalone information silos.

This supports:

- Online services,
- Shared platforms,
- Seamless citizen experience.

8. Website Security

Because websites are public-facing, institutions must:

- Secure administrative access,
- Protect against cyber threats,
- Monitor and update websites regularly.

9. Website Retirement and Decommissioning

ICTA expects institutions to:

- Formally retire obsolete websites,
- Redirect users where appropriate,
- Decommission hosting and domains safely.

10. What auditors typically check in Section 6.5

Auditors usually look for:

- Approval to develop and run websites,
- Domain ownership records,
- Hosting arrangements,
- Content governance structures,
- Security controls,
- Evidence of updates or retirement.

A common audit finding is:

Government websites existing with no clear governance, no domain control, and outdated content.