

Software License Management and Usage

1. Big picture: what this domain is about

“This domain is about making sure Government only uses software it is legally licensed for, knows what it owns, how it is used, and does not waste money or expose itself to legal and security risks.”

2. Why ICTA dedicates a full domain to software licensing

This domain exists because ICTA has observed recurring problems such as:

- Use of unlicensed or pirated software,
- Paying for licenses that are not used,
- Licenses expiring without renewal,
- Vendors locking Government into expensive agreements,
- No visibility of what software is installed where.

So ICTA introduces **formal controls** to ensure:

- Legal compliance,
- Cost control,
- Security,
- Accountability.

3. What falls under “Software License Management and Usage”

This domain covers **all software used by Government**, including:

- Operating systems,
- Application software,
- Databases,

- Middleware,
- Development tools,
- Subscription-based and cloud software (SaaS),
- Software embedded in systems and platforms.

If software is used in Government operations, **this domain applies.**

4. ICTA expectations under Software License Management

(What institutions must do)

1 Maintain a software license inventory

(“Know what software you own and use”)

Institutions must:

- Keep an up-to-date inventory of all software,
- Record:
 - License type,
 - Quantity,
 - Expiry dates,
 - Deployment location.

You cannot manage or comply with what you don't know you have.

2 Ensure all software is legally licensed

(“No illegal software”)

Institutions must:

- Only install and use properly licensed software,
- Avoid pirated, cracked, or unauthorised software,
- Ensure licenses match actual usage.

This is a **legal and reputational requirement**, not just ICT policy.

3 Align software usage with license terms

(“Use software only as permitted”)

Institutions must ensure:

- Software is used according to license conditions,
- Usage does not exceed licensed limits,
- Licenses are not shared improperly across users or systems.

Buying a license does not mean “use it however you want”.

4 Control installation and access to software

(“Who installs software?”)

Institutions must:

- Restrict who can install software,
- Prevent unauthorised installations,
- Ensure ICT oversight of software deployment.

This reduces:

- Security risks,
- Licensing violations,
- System instability.

5 Plan for license renewal, upgrade, and termination

(“Manage the license lifecycle”)

Institutions must:

- Track license expiry dates,
- Plan renewals in advance,

- Terminate licenses when software is retired or unused.

This supports:

- Budget control,
- Avoidance of service disruptions,
- Value for money.

6 Avoid vendor lock-in and promote cost efficiency

(“Think long-term”)

Institutions are expected to:

- Prefer flexible and standards-based licensing,
- Avoid licenses that restrict future migration,
- Consider total cost of ownership, not just purchase price.

This aligns with:

- Government procurement principles,
- Sustainability of systems.

5. Software usage governance (very important)

ICTA expects institutions to treat software usage as a **governance issue**, not a technical one.

This includes:

- Defining acceptable use policies,
- Monitoring compliance,
- Taking corrective action where misuse is detected.

“Everyone installs what they want” is non-compliant.

6. How this links to earlier domains

This domain ties directly to:

- **Acquisition** → licenses must be planned and procured properly
- **Development** → development tools must be licensed
- **Maintenance & Retirement** → licenses must be updated or terminated
- **Web Systems & Hosting** → hosting and SaaS licenses must be governed

Software licensing cuts across the **entire system lifecycle**.

7. Annexes supporting Software License Management

While the core requirements sit in **Section 8.1 onwards**, the domain is supported indirectly by annexes that cover:

- **Asset management concepts**
→ Treating software as an ICT asset with a lifecycle
- **Lifecycle management guidance**
→ Acquisition, usage, maintenance, retirement, and disposal
- **Procurement and governance alignment**
→ Ensuring licenses are planned and approved, not ad-hoc

Even where an annex does not explicitly say “licenses”, ICTA expects institutions to **apply annex lifecycle principles to software licenses**.

8. What auditors typically look for

Auditors usually check:

- Software license inventories,
- Proof of licensing and renewals,
- Alignment between licenses purchased and software installed,
- Controls over installation and usage,
- Terminated licenses for retired systems.

A common audit finding is:

Institutions paying for licenses they no longer use, or using software without valid licenses.