Government of Malta

Reference: GMICT X 0004-1:2014
Version: 7.0
Effective: 07 January 2014

ICT Governance Framework

This document is part of the GMICT Policy Framework
http://ictpolicies.gov.mt
Underlined terms are defined in the Vocabulary.

Purpose

The purpose of the ICT Governance Framework for the Government of Malta is to regulate the introduction and use of technology within the Public Sector.

Scope and Applicability

This document focuses on the Government of Malta’s Policy Management function and its processes.

The MITA Statute states that:

“It shall be a purpose of the Agency to ... deliver and manage the execution of all programmes related to the implementation of information technology and related systems in Government with the aim of enhancing public service delivery.”

(Statement 3(1b))

Amongst such programmes being managed by MITA is the deployment of an effective ICT Governance Framework for the adoption and use of information technology across the Public Sector, consisting of Government ICT Policies (known as GMICT Policy).

1. Corporate Governance

Effective corporate governance is intended to uphold a number of common principles, including:

- Transparency of information and internal procedures
- Accessibility of information, based on the premise that information that is not easily accessible is no information at all
- Authenticity of information which calls for the need to protect integrity of information (information management)
- Third party audit to verify compliance to rules and practices
- Directors’ responsibility and accountability to ensure legal compliance with the mandatory corporate governance framework
- Information technology enablement whereby technological tools, processes and practices are recognized as reliable sources for good corporate governance.

Since ICT permeates practically all aspects of business, the generation and sustainability of information requires governance from an ICT perspective.

2. ICT Governance

ICT governance has been defined as:
‘the board's ability to direct and control the enterprise's use of IT resources in line with strategic goals.’ (COBIT, 2010)

and also as:

‘addressing the definition and implementation of processes, structures and relational mechanisms in the organisation that enable both business and IT professionals to execute their responsibilities in support of business-IT alignment and the creation of business value from IT enabled business investments.’ (Van Grembergen and De Haes, 2009)

The latter definition extends the simpler COBIT definition and for the purposes of this ICT Governance Framework in a Public Sector context is adapted as follows:

**ICT governance addresses the definition and implementation of processes, structures and relational mechanisms within the public sector, that enable its professionals to execute their responsibilities in support of the alignment of Government business and Information and Communications Technology (ICT) strategies and objectives as well as the creation of value from ICT enabled investments.**

### 3. Basis for the ICT Governance Framework

This ICT Governance Framework is based upon applicable adaptations the Control Objectives for Information and related Technology (COBIT) framework. Reference to this framework shall facilitate a shared, common understanding among all stakeholders involved.

COBIT was developed by the IT Governance Institute (an ISACA research institute) which provides a holistic set of control objectives, processes, measures and best practices for information technology management. It has emerged out of another framework developed by the Committee of Sponsoring Organisations (COSO), which focuses on internal and financial controls.

The development of COBIT versions 3 and 4 had seen its increased alignment to other internationally recognised standards and best practices such as Information Technology Infrastructure Library (ITIL), ISO 27001 and PRojects IN Controlled Environments (PRINCE2). In fact, in organisations where these last-mentioned standards and frameworks are already implemented, it is recommended that they are used in conjunction with COBIT.

The latest version of COBIT (version 5) builds upon version 4.1 and integrates into it the IT Governance Institute's own Val IT 2.0 and Risk IT frameworks, and also aligns itself more fully to the ISO/IEC 38500 domains.

COBIT has also evolved from an audit framework in 1996 into a framework for the governance and management of enterprise IT in 2012 that presents policies as a fundamental factor for influencing proper governance and management over IT.

COBIT 5 is based upon seven enablers as support tools for the implementation of governance and management of enterprise IT, one of which is Principles, Policies and Frameworks. Good Practices, Goals and metrics, Stakeholders and Life Cycle are the four enabler dimensions of a policy framework.

### 4. Policy Management Good Practices

#### 4.1 The delineation of Management and Governance

COBIT 5 delineates between management and governance. Governance ‘ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on objectives to be achieved, setting direction through prioritisation and decision making; and
monitoring performance and compliance against agreed on direction and objectives'. On the other hand, management 'plans, builds, runs and monitors activities in alignment with direction set by the governance body to achieve the enterprise objectives'.

4.2 GMICT Policy documentation

GMICT Policy documentation is organised in the following content types:

<table>
<thead>
<tr>
<th>GMICT Policy documentation type</th>
<th>Scope (in terms of the delineation)</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMICT Policy</td>
<td>Governance</td>
<td>A direction, line, manifesto, principle or stance of a strategic nature stating the official intention of Government. A lucid, vendor-neutral statement about Government's intentions in the Information and Communications Technology (ICT) field. Statements intended to regulate Public Sector behaviour with respect to the adoption and use of ICT in Government.</td>
</tr>
<tr>
<td>GMICT Specification / Standard</td>
<td>Management</td>
<td>A specification or configuration required for ICT related products, services or operations.</td>
</tr>
<tr>
<td>GMICT Directive</td>
<td>Management</td>
<td>Instructions related to the implementation of Policies and Standards.</td>
</tr>
<tr>
<td>GMICT Procedure</td>
<td>Management</td>
<td>An official (and authorised) way of doing something. This is normally expressed as a workflow.</td>
</tr>
<tr>
<td>GMICT Form</td>
<td>Management</td>
<td>Specifies various items of information required, usually as part of a Procedure.</td>
</tr>
</tbody>
</table>

Table 1

4.3 GMICT Policy Management Roadmap

The GMICT Policy Management Roadmap (GMICT X 0004-2) that accompanies this Framework outlines published and intended GMICT policy activity over a three year period and which is updated every six months.

From a COBIT perspective, the GMICT Policy Roadmap, reflects the management, and specifically the planning aspect of policy.

5. Policy Management Goals

5.1 Underlying Principles

The following principles for the GMICT Policy Management function are drawn from the National ICT Strategy as reflected in the MITA Strategic Plan 2009-2012:

- Transformation-driven approach to allow for more value and lower cost for Government
- Monitoring of emerging trends within the information society fields

2 www.isaca.org/COBIT/Documents/COBIT5-Introduction.ppt
- Continuous improvement in policy management
- Independence from operational functions that may impair objectivity in policy management
- Risk averse approach with respect to Government security interests
- Open standards and technology approach
- Close collaboration with other aspects of ICT governance, which include, but are not limited to, Business, Information Security governance, Data governance and Compliance
- Communication and involvement of all stakeholders concerned.

5.2 Terms of Reference

Following the underlying principles, the following Terms of Reference are drawn for the GMICT Policy Management function:

1. To identify new GMICT Policy requirements and to recommend appropriate GMICT Policy development to the Chief Technology Officer.
2. To act as the point of reference with respect to interpretation of published GMICT Policy.
3. To oversee the development of GMICT Policy drafted by its primary policy contributor and be responsible for its review, leading to publication.
4. To foster further collaboration with all stakeholders, including but not limited to the Office of the CIOs, the Security Governance function, the Data Governance function and the Compliance Management function.
5. To induce awareness of GMICT Policy established among the stakeholders concerned.

6. GMICT Policy Stakeholders

The key stakeholders for ICT Governance Framework are:

- MITA (the Agent) that formulates the GMICT Policy principles on behalf of Government, based upon Government’s technology direction and legislation
- the Public Sector that implements these principles.
Policy Management Lifecycle

PHASE 1 - Plan (Plan Policy Roadmap)

Stakeholders (MITA & Public Sector)

Management (CTO)

Policy Contributor

GMICT Policy Management function

External process/document

- Including but not limited to:
  - (i) Existing GMICT Policy
  - (ii) MITA Strategic Plan
  - (iii) Relevant Government publications
  - (iv) Relevant EU publications
  - (v) Feedback from Compliance Management
  - (vi) Policy mandates

- Provide feedback for Roadmap review

- Authorise Policy Roadmap

- Scheduled Roadmap update

- Policy Roadmap update

- Authorise Policy Roadmap

- Publish Policy Roadmap

- Schedule policy work based on Published Roadmap

- Required content received?
  - Yes
  - Vet policy content
  - Further revisions required?
  - Yes
  - Escalation Procedure (Fig. 6)
  - No
  - Issue Draft for Review

- It is the prerogative of the Chief Technology Officer (CTO) to decide whether a draft policy should be subject to external review or not.

- For External Review?
  - Yes
  - Issue Draft for Review
  - No

- Escalation Procedure (Fig. 6)

- Official Documentation

- GMICT Policy Roadmap

- GMICT Policy Template

- B
  - Fig. 2, 3

- E
  - Fig. 2

Figure 1

Policy Management Lifecycle
The Chief Technology Officer (CTO) shall be the first reference point for authorisation. The CTO may refer the Policy to the Chief Executive Officer (CEO) for approval, particularly in cases where a Policy is deemed of critical importance.

Feedback is to be provided within timeframes as established by the Policy Management function.

No

Yes

The CTO may refer the Policy to the Chief Executive Officer (CEO) for approval, particularly in cases where a Policy is deemed of critical importance.

Finalise and Publish Policy

Compliance Audits

Gauge policy implementation

Feedback

Figure 2

Policy Management Lifecycle

PHASE 3 - Plan and Organise (Plan Policy Content) leading to Delivery and Support (Policy implementation upon publication)

Provide feedback

Changes Required?

Yes

No

Major changes required?

Yes

No

Contribute to updates accordingly

Update policy draft accordingly

Authorise Policy

Authorised?

Yes

No

GMICT Policy

Compliance Audits

Gauge policy implementation

Feedback

Includes but may not be limited to Exemption Trend Analysis

Includes but is not limited to ongoing feedback from CIOs and MITA stakeholders

Stakeholders (MITA & Public Sector) Management (CTO) Policy Contributor GMICT Policy Management function External process/document

A

Fig. 1

B

Fig. 1

C

Fig. 1

D

Fig. 1

E

Fig. 1

Unclassified

Page 6 of 11
### Policy Management Lifecycle

<table>
<thead>
<tr>
<th>Stakeholders (MITA &amp; Public Sector)</th>
<th>Management (CTO)</th>
<th>Policy Contributor</th>
<th>GMICT Policy Management function</th>
<th>External process/document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fill in Policy Mandate form</td>
<td></td>
<td></td>
<td>Determine where changes need to be applied</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>As planned in Roadmap?</td>
<td></td>
</tr>
<tr>
<td>i.e. is this a new policy not factored in the roadmap or a policy that is included in the roadmap but that needs to be re-prioritised in the roadmap?</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Review mandate request</td>
<td></td>
<td></td>
<td>Nutakes Necessary?</td>
<td></td>
</tr>
<tr>
<td>Decide on Mandate</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Clarifications Required?</td>
<td></td>
<td></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>May be required if the necessary updates are not given accordingly</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Escalate?</td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Authorised?</td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td>No</td>
<td>Inform the requestor accordingly</td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3**
Policy Management Lifecycle: EscalationProcedure

External process/document
GMICT Policy Management
function
Stakeholders (MITA & Public Sector)
Management (CTO)
Policy Contributor

Apart from GMICT Policy (drafting or update), may include GMICT Policy Mandate for further clarification

Generally 2 weeks are allowed

If this is not the first reminder, escalate to Policy Contributor’s Line Management for possible re-prioritisation of tasks

If this is not the first reminder, escalate to Policy Contributor’s Line Management for possible re-prioritisation of tasks

Send a reminder (in writing) to the Policy Contributor

Inform Primary policy contributor accordingly re. closure

Strike off pending documentation from Policy Register

Escalation Procedure Closure

Figure 4
6.1 GMICT Policy Authorisation

The GMICT Policy management lifecycle essentially calls for management involvement particularly during the policy authorisation process. GMICT Policy documentation shall therefore be authorised at the appropriate management level within MITA, based upon criteria as indicated in Table 2, below.

<table>
<thead>
<tr>
<th>Potential Criteria</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Acronym</td>
<td>Meaning of Acronym</td>
<td>Further explanation</td>
</tr>
</tbody>
</table>
| STR | Strategic Importance of the Policy to the Public Sector | Implies the significance of the policy upon:
  o the public, society, national interest,
  o any other matter which carries significant sensitivity to Government interests e.g. security, Government policy |
| OPR | Degree of change expected to operational business practices in the Public Sector (including MITA) through introduction of the Policy | Implies the degree of change required in current work practices / processes for conformance to the Policy |

Table 2

7.2.3 GMICT Policy Compliance

Any GMICT Policy document carries an Effective Date, which refers to the date from when the provisions of the particular document start to apply. However, it is also understood that there may be instances when it is not possible for the provisions of a GMICT policy document to be implemented with immediate effect as from the Effective Date.

Therefore, the GMICT Policy Management function addresses such a possibility in two ways, prior to GMICT Policy document publication, specifically during the drafting and the review stages:

(i) The GMICT Policy template includes an optional Section related to Compliance. This Section is expected to provide parameter(s) of applicability, transition requirement(s) and corresponding date(s) by which part or all of a Policy document is expected to be complied with. The Transition requirements are not expected to be highly specific, particularly where various implementation scenarios are known to exist within the context under consideration. However they should at least be expected to outline the common high level requirements expected across all of the various potential scenarios.

(ii) The review process of draft GMICT Policy documents is inherently expected to provide first-hand feedback from its effected stakeholders. The feedback is
mainly expected to focus on the validity of the principles underlying Policy statements as well as any potential issues of enforcement of the proposed Policy document. It should therefore serve as a mechanism for assessing the impact of the Policy and for any compliance parameters or timelines to be established prior to the Policy’s publication.

Please refer to the Compliance Management Framework (GMICT X 0018).

7. References


5. MITA Strategic Plan 2009-2010


### Modification History

<table>
<thead>
<tr>
<th>Version</th>
<th>Effective Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>08/11/2010</td>
<td>Initial Release</td>
</tr>
<tr>
<td>2.0</td>
<td>18/11/2010</td>
<td>Second Release</td>
</tr>
<tr>
<td>3.0</td>
<td>23/11/2010</td>
<td>Third Release - based on update to Policy Management Lifecycle</td>
</tr>
<tr>
<td>4.0</td>
<td>13/06/2011</td>
<td></td>
</tr>
<tr>
<td>5.0</td>
<td>16/04/2012</td>
<td>Addition of the Policy Lifecycle: Escalation procedure</td>
</tr>
<tr>
<td>6.0</td>
<td>06/12/2012</td>
<td>Addition of Scope of GMICT Policy Suite (Section 7.2)</td>
</tr>
<tr>
<td>7.0</td>
<td>07/01/2014</td>
<td>Simplification of general content and update of GMICT Policy Management Lifecycle</td>
</tr>
</tbody>
</table>

**Issuing Authority**

This document has been issued with the authority of the *Malta Information Technology Agency*.

**Unclassified**

Page 10 of 11
Contact Information


Any suggestions, queries or requests for clarification regarding Government ICT Policies, Directives and Standards may be forwarded to ictpolicies@gov.mt.