ICT Standards

Certification and Accreditation Template

Document number: ISMF-ICT/3.03 - ICT Security/MISP/SD/C&A Template
Version: 1.10
1 Document control
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MISP</td>
<td>Ministry Information Security Program</td>
</tr>
<tr>
<td>C&amp;A</td>
<td>Certification and Accreditation</td>
</tr>
<tr>
<td>SSAA</td>
<td>System Security Authorization Agreement</td>
</tr>
<tr>
<td>SLC</td>
<td>System Life Cycle</td>
</tr>
<tr>
<td>AA</td>
<td>Approving Authority</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>ISO</td>
<td>Information Security Office</td>
</tr>
<tr>
<td>PM</td>
<td>Program Manager</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>SSP</td>
<td>System Security Plan</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Plan</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
</tr>
</tbody>
</table>
1.2 Purpose of this Document

The Certification an Authorization Template is an attachment to the Certification an Authorization Guide which is a supporting document to the MISP Policy and MISP Handbook. It is part of the ICT Security package that has been produced within the scope of the ICT Standards project. This project is one of the three sub-projects executed under the global project name “Software Development and Technical Assistance for NISFED, e-Government and ICT Standards Applications”, started 20/08/2006 and rolled out within the scope of the ISMF programme1.

This template provides a sample format for a System Security Authorization Agreement (SSAA). Brief descriptions are provided for each section with additional details provided as necessary. The SSAA produced for each system may be tailored to meet the specific directorate requirements applicable to the system. The following format provided may be used as a basis for developing system-specific SSAAAs.

---

1 For a complete list of documents related to the ICT Standards project, refer to the Project Master Plan; ISMF-ICT/3.01, V.2.00.
2 Mission Description and System Identification

Notes □ The mission description and system identification should state the system’s name and identification and provide an overall description of the system and its functionality, such as system capabilities and criticality to the overall mission. A summary of the system’s concept of operations should also be included.

2.1 System Name and Identification

Notes □ This section identifies the system undergoing C&A activities. Information contained in this section should include the name, organization, and the location and organizations of the system’s end users.

2.2 System Description

Notes □ This section should focus on the relevant information security features of the system and describe the purpose of the system and desired capabilities. A high-level description of the system architecture also should be included. If possible, the description should be augmented with a diagram or drawing of the architecture.

2.3 Functional Description

Notes □ This section should clearly outline which functions and capabilities are desired in the accredited system. The C&A process should not begin until sufficient information is available to provide a thorough functional description. The following subsections should be included in the Functional Description.

2.3.1 System Capabilities

Notes □ The functions and capabilities expected in the fully accredited system should be clearly defined. Functional diagrams of the system, including data-flow diagrams, should be included where possible

2.3.2 System Criticality

Notes □ The system’s criticality, which helps determine the level of acceptable risk for the system, should be identified. The system’s criticality should consider the impact on the Ministry’s or directorate’s ability to achieve its mission if the system were not operational

2.3.3 Classification and Sensitivity of the Data Processed
Notes  □  The type and sensitivity of the data processed by the system should be defined

2.3.4  System User Description

Notes  □  The system’s user community should be described in detail to ensure that adequate controls are in place to prevent the inadvertent disclosure of Ministry / directorate proprietary information and that unauthorized users do not gain access to Ministry / directorate information

2.3.5  System’s Life-Cycle Description

Notes  □  The system’s life cycle should be defined, including a brief description of where the system currently is in its life cycle.

2.4  Summary of the System’s Operations Concept

Notes  □  This section should briefly describe what the system is supposed to do, how it operates, its environment, as well as any functions that are performed jointly with other systems. The complete concept can be attached as an appendix to the SSAA.
3 Environment Description

The environment description should provide in detail the system’s operating environment, including any potential threats to the system. In addition, a description of the system’s development environment should be included. The description of the operating environment should include details of all physical, administrative, development, and technical functions. Any threats that could be directed specifically at the system should also be described in detail.

3.1 Operating Environment

This section should describe the physical, personnel, communications, hardware, software, and operational security features necessary to support site and system operations. The measures should be designed to prevent unauthorized personnel from gaining access to system equipment, facilities, material, and documents and to protect them from compromise or destruction. The following subsections should be included in the Operating Environment.

3.1.1 Facility Description

The facility in which the system will operate should be described, including floor plans, equipment placement, electrical and plumbing supplies, communications equipment, Heating, Ventilation, and Air Conditioning units, sprinkler systems, fences, and wall construction within the facility.

3.1.2 Physical Security

Information required to protect the organization from potential threats (both internal and external) to it should be provided, including safety procedures and security practices.

3.1.3 Administrative Security

All administrative procedures, including manual processes that exist to counter threats to the system, should be identified.

3.1.4 Personnel Security

The numbers and types of personnel required to maintain and operate the system should be identified, and the controls and procedures in place to address these security issues should be described.

3.1.5 Maintenance Procedures
Special maintenance procedures required for efficient system operation should be documented, including information on the type of special maintenance and the number and type of personnel required to conduct this maintenance.

### 3.1.6 Training Plans

The training requirements of persons accessing the system should be addressed. The training should be evaluated to ensure it is commensurate with the individual's level of responsibility. The training should be tailored to the users' needs and should address security policy, potential threats, and existing countermeasures.

### 3.2 Software Development Cycle and Environment

This section should describe the system development approach and the environment in which it is conducted. Incorporation of security into the system development life cycle will ensure that security is considered throughout every stage of the life cycle.

### 3.3 Threat Description

This section should discuss any potential threats or single points of failure that exist within the system boundaries and that could have an adverse impact on the confidentiality, integrity, or availability of the system. In addition to the threat description, an evaluation of the expected frequency of the threat should be incorporated where possible.
4 System Architecture Description

Notes □ The system architecture description provides a high-level overview of the hardware, software, and interfaces that the system relies on for operations. This section should be maintained and updated as the system evolves. The description should include the configuration of any equipment or interconnected systems and subsystems that interface with the system.

4.1 Description

Notes □ This section should describe the overall system architecture, providing detailed information about the system, the network on which it resides, and any interdependencies it may have with other systems. This section includes information about the hardware, software, and firmware employed by the system. Available network diagrams should be included in this section. The following subsections should be included in the description:

4.1.1 Hardware

Notes □ The system’s hardware should be documented and its functionality briefly described. An inventory of the hardware should accompany the description.

4.1.2 Software

Notes □ The system’s software should be described in full, including the operating system and any supporting software applications that are used. The description should include whether the application is commercial off-the-shelf or internally developed.

4.2 System Interfaces and External Connections

Notes □ This section should describe any interactions or interdependencies that the system has with other systems or networks of systems. These interfaces and connections could pose an increased threat to security. Coordinating with the owners of these systems is important to ensure that the required protection is in place.

4.3 Data Flow

Notes □ This section should include a description of the system’s internal interfaces, data flows, and data transmission methods. Data flow diagrams should be provided to further explain the process.

4.4 Certification and Accreditation Boundary
Notes  □  This section should describe the boundaries of the system covered by the SSAA. Diagrams and textual descriptions of the system to be evaluated should also be included. Any components within the boundary must have an accompanying description in the system’s description section. Any elements outside of the boundary that interface with the system should be detailed in the external interfaces section.
5  System Security Requirements

Notes  □ The system security requirements task defines the rules and requirements governing the overall system security. The requirements may affect the resources required to maintain and operate the system.

5.1 National Security Requirements

Notes  □ This section must document the national requirements governing system security that apply to the system under evaluation

5.2 Organizational Security Requirements

Notes  □ For this section, system owners should document which MISP-specific policies, procedures, and guidelines govern the development, operation, and maintenance of the system

5.3 Data Security Requirements

Notes  □ For this section, system owners that interface with the system, as well as data owners, should be involved in determining which requirements exist. The type of data processed by the system will govern the data security controls required

5.4 System’s Operations Concept

Notes  □ This section should include system inputs and outputs, security controls, and interactions and connections with external systems. Graphical representations should be incorporated into the documentation, where possible.

5.5 Configuration and Change Management Requirements

Notes  □ This section should be reviewed to identify additional security requirements that might arise

5.6 Network Connection Rules and Restrictions

Notes  □ This section should highlight any additional security concerns or controls that should be addressed before allowing users and systems to connect to the system.
6 Organizations and Resources

Notes □ This section should identify the organizations, persons, the resources, and training requirements involved in the system's C&A process. External organizations and persons supporting the Ministry in the C&A process should be included.
7 Appendixes

The appendices should provide the supporting documentation to complete the C&A process. Optional appendices may be added to meet specific needs. All documentation relevant to the system’s C&A should be included in the SSAA.

The SSAA should include the following appendices at a minimum:

- Appendix A  Acronyms
- Appendix B  Definitions
- Appendix C  References
- Appendix D  Security Requirements and Requirements Compliance Matrix
- Appendix E  Security Test and Evaluation Plan and Procedures
- Appendix F  Certification Results
- Appendix G  Risk Assessment Results
- Appendix H  Certification Authority’s Recommendation
- Appendix I  System Security Policy
- Appendix J  System Rules of Behaviour
- Appendix K  Security Operating Procedures
- Appendix L  Contingency Plans
- Appendix M  Security Awareness and Training Plan
- Appendix N  Personnel Controls and Technical Security Controls
- Appendix O  Incident Response Plan
- Appendix P  Memorandums of Agreement – System Interconnection Agreements
- Appendix Q  Applicable System and System Development Documentation
- Appendix R  Accreditation Documentation and Accreditation Statement