



MEDIUM-TERM INFORMATION AND COMMUNICATIONS TECHNOLOGY HARMONIZATION INITIATIVE (MITHI) STEERING COMMITTEE

RESOLUTION NO. 2026-02

INSTITUTING THE REVISED ISSP TEMPLATE AND MANUAL, ALIGNING THE SAME WITH GOVERNMENT BUDGETING, INVESTING, AND AUDITING FRAMEWORKS, AND DIRECTING THE DEVELOPMENT OF A NATIONAL ISSP PORTAL

WHEREAS, Title XVII, Section 02 of Executive Order (E.O.) No. 292, Series of 1987,¹ otherwise known as "*The Administrative Code of 1987*," stipulates that the Department of Budget and Management (DBM) shall be responsible for the formulation and implementation of the National Budget to attain the nation's socio-economic plans and objectives, along with ensuring the efficient and sound utilization of government funds and revenues to effectively achieve the country's development objectives.

WHEREAS, Section 06 of the Republic Act (R.A.) No. 10844,² otherwise known as the "*Department of Information and Communications Technology Act of 2015*," stipulates that the Department of Information and Communications Technology (DICT) shall be responsible for the formulation, recommendation, and implementation of national policies, plans, programs, and guidelines that will promote the development and use of Information and Communications Technology (ICT) with attention to the returns of convergence and emerging technologies.

WHEREAS, Section 05 of R.A. 12145,³ also known as the "*Economic, Planning, and Development Act*," stipulates that the Department of Economy, Planning, and Development (DEPDev) shall ensure that the annual and multi-year appropriations for various programs and projects are aligned with the long-term development frameworks and national and subnational development plans towards optimal use of financial resources.

WHEREAS, Joint Memorandum Circular No. 2024-01,⁴ issued by the DBM, the DICT, and the NEDA, constituted the revival of the Medium-Term Information and Communications Technology Harmonization Initiative (MITHI) – constitution of the MITHI Steering Committee (MSC), Technical Working Group (TWG), and Secretariat, thereby ensuring the harmonization and interoperability of ICT resources.

¹ Executive Order (E.O.) No. 292, Series of 1987 – The Administrative Code of 1987.

² Republic Act (R.A.) No. 10844 – An Act Creating the Department of Information and Communications Technology, Defining its Powers and Functions, Appropriating Funds Thereof, and For Other Purposes.

³ R.A. 12145 – An Act Reorganizing the National Economic and Development Authority (NEDA) into the Department of Economy, Planning, and Development (DEPDev), and Reconstituting the NEDA Board into the Economy and Development Council, Repealing for the Purpose Executive Order No. 230, Series of 1987, and Amending Executive Order No. 292, Series of 1987, and Appropriating Funds Thereof.

⁴ Department of Budget and Management (DBM), Department of Information and Communications Technology (DICT), and NEDA Joint Memorandum Circular No. 2024-01 – Revival of the Medium-Term Information and Communications Technology Harmonization Initiative (MITHI) and Reconstitution of the MITHI Steering Committee and Other Functions Thereof.

**INSTITUTING THE REVISED ISSP TEMPLATE AND MANUAL, ALIGNING THE SAME
WITH THE GOVERNMENT BUDGETING, INVESTING, AND AUDITING FRAMEWORKS,
AND DIRECTING THE DEVELOPMENT OF A NATIONAL ISSP PORTAL**

WHEREAS, Section 16 of R.A. 12254,⁵ otherwise known as the "*E-Governance Act*," provides that the government entities shall ensure that all their Information Systems Strategic Plans (ISSP) and ICT projects are updated and considered annually in their Budget Preparation activities, along with accountability of the government entities in the effective and efficient implementation of said plans.

WHEREAS, the General Appropriations Acts⁶ and DBM National Budget Memoranda⁷ issued annually, stipulate that ICT budget proposals shall be aligned with the government entity's ISSP and compliant with the rules and regulations promulgated by the MITHI.

WHEREAS, Section 05 of R.A. 9485,⁸ also known as the "*Anti-Red Tape Act of 2007*," stipulates the reengineering of systems and procedures with frontline services relative to time and motion studies, evaluation and upgrading of systems and procedures, and reengineering the same if deemed necessary to reduce bureaucratic red tape and processing time.

WHEREAS, E.O. 14, S. 2023,⁹ mandates the adoption of the Philippine Development Plan (PDP) 2023-2028, to which government programs and projects shall be prioritized relative to the strategic outcomes provided in the said Plan.

WHEREAS, Part IV, Chapter 11, Subchapter 11.2, Outcome 2 of the PDP 2023-2028,¹⁰ defines the improvement of the bureaucracy's efficiency as an agile, efficient, and technology-adept workforce, along with the simplification of systems that will duly enhance productivity, minimize red tape, and promote citizen satisfaction with the performance of the government.

WHEREAS, DICT Department Circular No. HRA-001, Series of 2025¹¹ mandates the compliance of all government entities with the ISSP Minimum Quality Standards, adopting a standards-based approach rather than a control-based approach; thus modifying the previous process of the ISSP submission, evaluation, and endorsement processes.

WHEREAS, there is a need to reevaluate and refine the ISSP Template and streamline component redundancies to ensure the seamless design of agency, corporation, or institution ISSPs while upholding a comprehensive layout of the government entity's ICT vision, roadmap, architecture, and resource requirements.

WHEREAS, there is a need to refine ISSP evaluation frameworks and processes with government budgeting, investing, and auditing frameworks, along with the standardization of ISSP submission, evaluation, endorsement, and other relevant processes to ensure alignment of proposed ICT projects with national and international standards, sound fiscal management, and global best practices on ICT project implementation.

⁵ R.A. 12254 – An Act Institutionalizing the Transition of the Government to E-Governance, Strengthening the ICT Academy, and Appropriating Funds Thereof.

⁶ The latest being R.A. 12314, otherwise known as the "*General Appropriations Act (January 1 – December 31, 2026)*."

⁷ The latest being DBM National Budget Memorandum No. 156.

⁸ R.A. 9485 – An Act to Improve Efficiency in the Delivery of Government Service to the Public by Reducing Bureaucratic Red Tape, Preventing Graft and Corruption, and Providing Penalties Thereof.

⁹ E.O. 14, S. 2023 – Approving and Adopting the Philippine Development Plan for the Period 2023-2028.

¹⁰ Philippine Development Plan 2023-2028.

¹¹ DICT Department Circular No. HRA-001, Series of 2025 – Adoption of a Standards-Based Approach to Information Systems Strategic Plan (ISSP) Compliance.

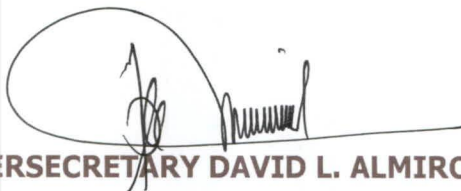
**INSTITUTING THE REVISED ISSP TEMPLATE AND MANUAL, ALIGNING THE SAME
WITH THE GOVERNMENT BUDGETING, INVESTING, AND AUDITING FRAMEWORKS,
AND DIRECTING THE DEVELOPMENT OF A NATIONAL ISSP PORTAL**

WHEREAS, there is a need to simplify the ISSP submission, evaluation, endorsement, and other processes to eliminate bureaucratic redundancies and transition from manual and paper-based to digital and paperless processes that will further induce effective and efficient ISSP processes as a series of government transactions.

THEREFORE, it is hereby **RESOLVED** that the MSC duly promulgates the following directives for the immediate cascading of the Technical Working Group (TWG) and Secretariat, and compliance of all government entities formulating their ISSPs:

1. Cascading of the **Revised ISSP Template**, herein attached as **Annex A**, for the guidance and perusal of the National Government Agencies (NGA), Government-Owned and Controlled Corporations (GOCCs), State Colleges and Universities (SUCs), and other government instrumentalities.
2. Cascading of the **ISSP Manual**, herein attached as **Annex B**, as guidance and perusal of the NGAs, GOCCs, SUCs, and other government instrumentalities.
3. Resetting the **Coverage Period** of ISSPs to cover **F.Y. 2028 to 2030**, including those already submitted, acknowledged, and endorsed by the DICT or the MITHI.
4. Directing the TWG to **reevaluate and refine the ISSP evaluation** and align the same with the government's budgeting, investing, and auditing frameworks.
5. Directing the DICT to develop a **National ISSP Portal** and transition the ISSP as a digital and paperless document across all government entities.
6. Directing the TWG and Secretariat for the immediate **cascading of the Revised Template and Manual** through various facilitative means and other mechanisms necessary for the promulgation of this Resolution.

Done this 30th day of April 2026.



UNDERSECRETARY DAVID L. ALMIROL, JR.

Chairperson, MITHI Steering Committee

Department of Information and Communications Technology



UNDERSECRETARY MARIA FRANCESCA M. DEL ROSARIO

Co-Chairperson, MITHI Steering Committee

Department of Budget and Management

**INSTITUTING THE REVISED ISSP TEMPLATE AND MANUAL, ALIGNING THE SAME
WITH THE GOVERNMENT BUDGETING, INVESTING, AND AUDITING FRAMEWORKS,
AND DIRECTING THE DEVELOPMENT OF A NATIONAL ISSP PORTAL**



UNDERSECRETARY MA. MONICA P. PAGUNSAN

Vice-Chairperson, MITHI Steering Committee

Department of Economy, Planning, and Development



ASSISTANT SECRETARY FLORRY SHERRY M. BASQUIÑEZ

Member, MITHI Steering Committee

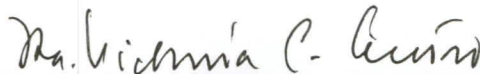
Department of Economy, Planning, and Development



ASSISTANT SECRETARY GERARDO E. MAULA

Member, MITHI Steering Committee

Department of Budget and Management



ASSISTANT SECRETARY MARIA VICTORIA C. CASTRO

Member, MITHI Steering Committee

Department of Information and Communications Technology



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

(Replace with agency's logo)

INFORMATION SYSTEMS STRATEGIC PLAN (ISSP)

☐ REGULAR ISSP

☐ AMENDMENT <1st/2nd/3rd>

For the period <start year> to <end year>

<Name of Department/Agency>

<Website URL>

PREPARED BY:

Name & Signature of Chief Information Officer

Scope

☐ Department-Wide

☐ Department - Central Office / Head Office

☐ Central Office only

☐ With Regional Offices / Field Offices ☐ With Bureaus

☐ Agency-Wide

☐ Central Office only

☐ With Regional Offices / Field Offices

☐ Other Government Entity

☐ LGU

APPROVED BY:

Name & Signature of Agency Head

Table of Contents

DEFINITION OF TERMS	3
PART I. AGENCY PROFILE & STRATEGIC CONTEXT	1
A. MANDATE, VISION, MISSION, AND ORGANIZATIONAL OUTCOME	1
A.1. MANDATE	1
A.2. VISION STATEMENT	1
A.3. MISSION STATEMENT	1
A.4. ORGANIZATIONAL OUTCOME	1
B. ORGANIZATIONAL STRUCTURE	1
B.1. CHIEF INFORMATION OFFICER (CIO)	1
B.2. HUMAN CAPITAL	2
C. STAKEHOLDER ANALYSIS	2
PART II. CURRENT ICT ASSESSMENT	3
A. STRATEGIC CONCERNS FOR ICT USE	3
B. EXISTING NETWORK INFRASTRUCTURE	4
B1. LAN/WAN SET-UP INCLUDING CONNECTIVITY TYPE AND BANDWIDTH	4
B2. CYBERSECURITY CONTROL CHECKLIST	5
C. EXISTING/OPERATIONAL INFORMATION SYSTEMS (IS) INVENTORY	6
D. E-GOVERNMENT PROGRAMS (EGP) CHECKLIST	8
PART III. PROPOSED ICT STRATEGY	11
A. PROPOSED NETWORK INFRASTRUCTURE	11
A.1. LAN/WAN SET-UP INCLUDING CONNECTIVITY TYPE AND BANDWIDTH	11
A.2. CYBERSECURITY CONTROL CHECKLIST	12
B. ENTERPRISE ARCHITECTURE	13
C. PROPOSED ICT HUMAN CAPITAL	14
D. PROPOSED INFORMATION SYSTEMS	15
E. ICT PROJECTS	17

E.1. INTERNAL ICT PROJECTS	17
E.2. CROSS-AGENCY ICT PROJECTS	19
F. PERFORMANCE MEASUREMENT FRAMEWORK	21
F.1. INTERNAL ICT PROJECTS	21
F.2. CROSS-AGENCY ICT PROJECTS	22
PART IV. RESOURCE REQUIREMENTS	23
A. DETAILED RESOURCE DEPLOYMENT AND COST BREAKDOWN	23
A.1. [YEAR #1]	23
A.2. [Year #2]	27
A.3. [Year #3]	31
B. SUMMARY OF INVESTMENTS	35
B.1. GENERAL SUMMARY	35
B.2. FUND SOURCE	35
B.3. STATEMENT OF EXPENDITURE	35
B.4. OBJECT OF EXPENDITURE	36

DEFINITION OF TERMS

Terms	Definition
Agency	Refers to any bureau, office, commission, authority, or instrumentality of the national government, including government-owned or-controlled corporations (GOCC), authorized by law or by their respective charters to contract for or undertake information and communications technology networks and databases, infrastructure or development projects.
Business Process	A collection of business transactions between business partners and/or internal activities within one business. These transactions and/or activities together support the objective of the business process.
Chief Information Officer	Refers to a senior officer responsible for the development, planning, and implementation of the government entity's information systems strategic plan (ISSP) or ICT plan, and management of the agency's ICT systems, platforms, and applications;

PART I. AGENCY PROFILE & STRATEGIC CONTEXT

A. MANDATE, VISION, MISSION, AND ORGANIZATIONAL OUTCOME

A.1. MANDATE

- Legal Basis
- Function

A.2. VISION STATEMENT

A.3. MISSION STATEMENT

A.4. ORGANIZATIONAL OUTCOME

B. ORGANIZATIONAL STRUCTURE

B.1. CHIEF INFORMATION OFFICER (CIO)

- Name of CIO:
- Plantilla Position:
- Organizational Unit:
- E-mail Address:
- Contact Number/s:

- Name of ISSP Focal:
- Position:
- Organizational Unit:
- E-mail Address:
- Contact Number/s:

B.2. HUMAN CAPITAL

EMPLOYMENT STATUS	IT POSITIONS	NON-IT POSITIONS	SEX	
			MALE	FEMALE
Plantilla	[Physical Count]	[Physical Count]	[Physical Count]	[Physical Count]
Contractual	[Physical Count]	[Physical Count]	[Physical Count]	[Physical Count]
Outsourced (JO, COS, and HTC)	[Physical Count]	[Physical Count]	[Physical Count]	[Physical Count]
Grand Total	[Total Physical Count]	[Total Physical Count]	[Total Male]	[Total Female]

C. STAKEHOLDER ANALYSIS

Stakeholders	Transaction Processed	Complexity
		<Simple, Complex, Highly Technical>

PART II. CURRENT ICT ASSESSMENT

A. STRATEGIC CONCERNS FOR ICT USE

OO/SO/MFO	Critical Management, Operating, or Business System	Problem	Intended Use of ICT
OO/SO/MFO Program 1:	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

B. EXISTING NETWORK INFRASTRUCTURE

B1. LAN/WAN SET-UP INCLUDING CONNECTIVITY TYPE AND BANDWIDTH

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

B2. CYBERSECURITY CONTROL CHECKLIST

	<u>MANDATORY</u>	<u>OPTIONAL</u>
PHYSICAL SECURITY	☐ Perimeter Protection ☐ Access Control ☐ Surveillance System	☐ Detection System
PERIMETER SECURITY	☐ Next Generation Firewalls ☐ Intrusion Detection/Prevention Systems (IDS/IPS) ☐ Web Application Firewalls (WAFs)	☐ Demilitarized Zone (DMZ)
NETWORK SECURITY	☐ Data Encryption	☐ Network Segmentation
ENDPOINT SECURITY	☐ Anti-virus and Anti-malware Software ☐ Application Control ☐ BYOD Security	☐ Extended Detection and Response (XDR)
DATA SECURITY	☐ Data Classification ☐ Data Loss Prevention (DLP) ☐ Data Backups and Recovery	
APPLICATION SECURITY	☐ Regular Security Scanning and Testing	
OTHER MEASURES	☐ Vulnerability Assessment ☐ Patch Management ☐ Strong Password Policies ☐ Multi-Factor Authentication (MFA) ☐ Access Reviews ☐ Security Logs	☐ Log Analysis ☐ Incident Response Plan ☐ Security Information and Event Management (SIEM) ☐ Penetration Testing ☐ Secure Software Development Life Cycle (SDLC)

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

C. EXISTING/OPERATIONAL INFORMATION SYSTEMS (IS) INVENTORY

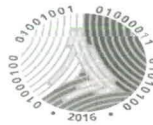
INFORMATION SYSTEM NAME	
CLASSIFICATION	☐ Support to Operations ☐ General Administrative Systems ☐ Operations If yes, indicate whether the system supports: ☐ Frontline Service (<i>directly used for public/client service delivery</i>) Identify if: ☐ Online Provide link: _____ ☐ On-premise ☐ Hybrid ☐ Non-Frontline Service (<i>supports core mandate but not directly used by clients/public</i>)
DESCRIPTION & PURPOSE	
DEVELOPMENT STRATEGY	
DEVELOPMENT PLATFORM	
DATABASE NAME	
DATA STORAGE	
INTERNAL USERS	

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

EXTERNAL USERS	
OWNER	
INTEROPERABILITY	☐ Integrated with another system <i>(If the system exchanges data or is technically integrated with another system)</i> If yes, specify the system name Internal System: _____ External System: _____ ☐ Generates data that is utilized by other system <i>(The system generates and produces data that is consumed, referenced, or reused by another system)</i> ☐ Processes data generated from other system <i>(The system receives and processes data generated from another system)</i> ☐ Deployed on a shared platform <i>(The system is hosted on the same platform or infrastructure with other systems)</i>
PRIVACY IMPACT ASSESSMENT (PIA)	Is the system processing personal information? <i>(Does the system collect, store, or process names, addresses, photos, or any info that can identify an individual?)</i> ☐ Yes ☐ No If Yes, did the system undergo PIA? ☐ Yes ☐ No

D. E-GOVERNMENT PROGRAMS (EGP) CHECKLIST

1. ELECTRONIC LOCAL GOVERNMENT UNIT (ELGU) SYSTEM <i>(Applicable only to LGUs)</i>	Is your LGU already utilizing the eLGU system? ☐ Yes ☐ No	If Yes, Indicate url: _____ If No, ☐ Using equivalent system: IS name: _____ Indicate url: _____ ☐ Manual Transaction
2. GOVERNMENT DIGITAL PAYMENT SYSTEM FOR COLLECTION AND DISBURSEMENT	Is your agency utilizing eGovPay? ☐ Yes ☐ No	If No, ☐ Using other digital or electronic payment platform ☐ Manual Transaction ☐ Proposed development of equivalent system
3. GOVERNMENT PUBLIC KEY INFRASTRUCTURE (PKI) PROGRAM	(For GSSPD's consideration to consult GDTB-DCD) <i>(percentage of adoption of PNPKI; Ratio of Total number of employees with active PNPKI certificates over Total number of employees)</i>	
4. HUMAN CAPITAL	Is your agency utilizing the HCMIS?	If No,



INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

MANAGEMENT INFORMATION SYSTEM (HCMIS)	☐ Yes ☐ No	☐ Using equivalent system: IS name: _____ ☐ Manual processing ☐ Proposed development of equivalent system
5. INTEGRATED FINANCIAL MANAGEMENT INFORMATION SYSTEM (IFMIS)	Is your agency utilizing the IFMIS? ☐ Yes ☐ No	If No, ☐ Using equivalent system: IS name: _____ ☐ Manual processing ☐ Proposed development of equivalent system
6. ONLINE PUBLIC SERVICE PORTAL	What are the existing consumer protection and citizen assistance, feedback and grievance mechanisms in your agency? ☐ Website ☐ Email ☐ Landline ☐ Social Media ☐ Mobile	Are these mechanisms already connected with online public service portals? ☐ Yes ☐ No
7. PROCUREMENT SYSTEM	Is your agency utilizing the Philippine Government Procurement System? ☐ Yes ☐ No	If No, ☐ Using equivalent system: IS name: _____ ☐ Manual processing ☐ Proposed development of equivalent

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

		system
8. RECORDS AND KNOWLEDGE MANAGEMENT INFORMATION SYSTEM	Is there an existing repository for Records and Knowledge Management in your agency? ☐ Yes ☐ No	If Yes, indicate the system: _____
9. PUBLIC SERVICE CONTINUITY PLAN	Is there an existing Public Service Continuity Plan in your agency? ☐ Yes ☐ No	

PART III. PROPOSED ICT STRATEGY

A. PROPOSED NETWORK INFRASTRUCTURE

A.1. LAN/WAN SET-UP INCLUDING CONNECTIVITY TYPE AND BANDWIDTH

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

A.2. CYBERSECURITY CONTROL CHECKLIST

	<u>MANDATORY</u>	<u>OPTIONAL</u>
PHYSICAL SECURITY	☐ Perimeter Protection ☐ Access Control ☐ Surveillance System	☐ Detection System
PERIMETER SECURITY	☐ Next Generation Firewalls ☐ Intrusion Detection/Prevention Systems (IDS/IPS) ☐ Web Application Firewalls (WAFs)	☐ Demilitarized Zone (DMZ)
NETWORK SECURITY	☐ Data Encryption	☐ Network Segmentation
ENDPOINT SECURITY	☐ Anti-virus and Anti-malware Software ☐ Application Control ☐ BYOD Security	☐ Extended Detection and Response (XDR)
DATA SECURITY	☐ Data Classification ☐ Data Loss Prevention (DLP) ☐ Data Backups and Recovery	
APPLICATION SECURITY	☐ Regular Security Scanning and Testing	
OTHER MEASURES	☐ Vulnerability Assessment ☐ Patch Management ☐ Strong Password Policies ☐ Multi-Factor Authentication (MFA) ☐ Access Reviews ☐ Security Logs	☐ Log Analysis ☐ Incident Response Plan ☐ Security Information and Event Management (SIEM) ☐ Penetration Testing ☐ Secure Software Development Life Cycle (SDLC)

B. ENTERPRISE ARCHITECTURE

C. PROPOSED ICT HUMAN CAPITAL

IT POSITION	EMPLOYMENT STATUS	PHYSICAL COUNT
Information Technology Officer III	Plantilla	[Physical Count]
Information Technology Officer II	Plantilla	[Physical Count]
	Job Order	[Physical Count]
Information Technology Officer I	Job Order	[Physical Count]
Grand Total		[Total Physical Count]

D. PROPOSED INFORMATION SYSTEMS

INFORMATION SYSTEM NAME	
CLASSIFICATION	☐ Support to Operations ☐ General Administrative Systems ☐ Operations If yes, indicate whether the system supports: ☐ Frontline Service <i>(directly used for public/client service delivery)</i> Identify if: ☐ Online Provide link: _____ ☐ On-premise ☐ Hybrid ☐ Non-Frontline Service <i>(supports core mandate but not directly used by clients/public)</i>
DESCRIPTION & PURPOSE	
STATUS	
DEVELOPMENT STRATEGY	
DEVELOPMENT PLATFORM	
DATABASE NAME	

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

DATA STORAGE	
INTERNAL USERS	
EXTERNAL USERS	
OWNER	
INTEROPERABILITY	☐ Integration with another system <i>(If the system will exchange data or will be technically integrated with another system)</i> If yes, specify the system name Internal System: _____ External System: _____ ☐ Generate data that will be utilized by other system <i>(The system will generate and produce data that will be consumed, referenced, or reused by another system)</i> ☐ Process data generated from other system <i>(The system will receive and process data generated from another system)</i> ☐ Deployment on a shared platform <i>(The system will be hosted on the same platform or infrastructure with other systems)</i>
PRIVACY IMPACT ASSESSMENT	Will the system process personal information? <i>(Will the system collect, store, or process names, addresses, photos, or any info that can identify an individual?)</i> ☐ Yes ☐ No

E. ICT PROJECTS

E.1. INTERNAL ICT PROJECTS

PROJECT TITLE	
DESCRIPTION	
OBJECTIVES	
STRATEGIC ALIGNMENT	☐ Public Investment Program ☐ National Cybersecurity Plan ☐ E-Government Master Plan ☐ Program Convergence Budgeting ☐ Others (Specify)
HARMONIZATION FRAMEWORK	☐ National Prioritization ☐ Resource Optimization ☐ Interoperability Framework ☐ Cross-Agency Collaboration ☐ Scalability and Sustainability
DURATION	
YEAR 1 DELIVERABLES/MILESTONE	
YEAR 2 DELIVERABLES/MILESTONE	
YEAR 3 DELIVERABLES/MILESTONE	



INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

IMPLEMENTING UNIT	
TOTAL PROJECT COST	
FUNDING SOURCE	☐ GAA ☐ Foreign-assisted projects ☐ Locally funded ☐ Other Income Generating Sources

E.2. CROSS-AGENCY ICT PROJECTS

PROJECT TITLE	
DESCRIPTION	
OBJECTIVES	
STRATEGIC ALIGNMENT	☐ Public Investment Program ☐ National Cybersecurity Plan ☐ E-Government Master Plan ☐ Program Convergence Budgeting ☐ Others (Specify)
HARMONIZATION FRAMEWORK	☐ National Prioritization ☐ Resource Optimization ☐ Interoperability Framework ☐ Cross-Agency Collaboration ☐ Scalability and Sustainability
DURATION	
YEAR 1 DELIVERABLES/MILESTONE	
YEAR 2 DELIVERABLES/MILESTONE	
YEAR 3 DELIVERABLES/MILESTONE	
IMPLEMENTING UNIT	

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

TOTAL PROJECT COST	
FUNDING SOURCE	☐ GAA ☐ Foreign-assisted projects ☐ Locally funded ☐ Other Income Generating Sources
LEAD AGENCY	
IMPLEMENTING AGENCY	

F. PERFORMANCE MEASUREMENT FRAMEWORK

F.1. INTERNAL ICT PROJECTS

ICT Project 1: *(Insert Project Title)*

HIERARCHY OF TARGETED RESULTS	KEY PERFORMANCE INDICATORS (KPIs)	BASELINE DATA	TARGETS	DATA COLLECTION METHODS	RESPONSIBILITY TO COLLECT DATA
INTERMEDIATE OUTCOME	[Percentage (%), No. of Units, or Ratios]	[Current Percentage (%), No. of Units, or Ratios]	[Additional Percentage (%), No. of Units, or Ratios]	Reports, Modules, etc.	[Department or Agency Bureau, Service, or Office]
IMMEDIATE OUTCOME	[Percentage (%), No. of Units, or Ratios]	[Current Percentage (%), No. of Units, or Ratios]	[Additional Percentage (%), No. of Units, or Ratios]	Reports, Modules, etc.	[Department or Agency Bureau, Service, or Office]
OUTPUT	[Percentage (%), No. of Units, or Ratios]	[Current Percentage (%), No. of Units, or Ratios]	[Additional Percentage (%), No. of Units, or Ratios]	Reports, Modules, etc.	[Department or Agency Bureau, Service, or Office]

F.2. CROSS-AGENCY ICT PROJECTS

Cross-Agency ICT Project 1: *(Insert Project Title)*

HIERARCHY OF TARGETED RESULTS	KEY PERFORMANCE INDICATORS (KPIs)	BASELINE DATA	TARGETS	DATA COLLECTION METHODS	RESPONSIBILITY TO COLLECT DATA
INTERMEDIATE OUTCOME	[Percentage (%), No. of Units, or Ratios]	[Current Percentage (%), No. of Units, or Ratios]	[Additional Percentage (%), No. of Units, or Ratios]	Reports, Modules, etc.	[Department or Agency Bureau, Service, or Office]
IMMEDIATE OUTCOME	[Percentage (%), No. of Units, or Ratios]	[Current Percentage (%), No. of Units, or Ratios]	[Additional Percentage (%), No. of Units, or Ratios]	Reports, Modules, etc.	[Department or Agency Bureau, Service, or Office]
OUTPUT	[Percentage (%), No. of Units, or Ratios]	[Current Percentage (%), No. of Units, or Ratios]	[Additional Percentage (%), No. of Units, or Ratios]	Reports, Modules, etc.	[Department or Agency Bureau, Service, or Office]

PART IV. RESOURCE REQUIREMENTS

A. DETAILED RESOURCE DEPLOYMENT AND COST BREAKDOWN

A.1. [YEAR #1]

ITEM	OFFICE LOCATION (DEPLOYMENT)	FUND SOURCE	UNIT COST	PHYSICAL TARGET	TOTAL COST
OFFICE PRODUCTIVITY					20,264,998.50
CAPITAL OUTLAY					7,500,000.00
[UACS Object Code]					7,500,000.00
Laptop	OUSEC	GAA	50,000.00	50	2,500,000.00
Desktop	OASEC	GAA	50,000.00	100	5,000,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					12,764,998.50
[UACS Object Code]					7,499,998.50
Laptop	OUSEC	GAA	49,999.99	50	2,499,999.50
Desktop	OASEC	GAA	49,999.99	100	4,999,999.00
[UACS Object Code]					4,500,000.00

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

Printer	OASEC	GAA	45,000.00	100	4,500,000.00
[UACS Object Code]					765,000.00
Office Productivity Suite	CPMS	GAA	8,500.00	30	255,000.00
	AS	GAA	8,500.00	60	510,000.00
INTERNAL ICT PROJECTS					42,500,000.00
[INTERNAL ICT PROJECT #1]					21,250,000.00
CAPITAL OUTLAY					1,250,000.00
[UACS Object Code]					1,250,000.00
Laptop	ICTSS	GAA	70,000.00	15	1,050,000.00
Network Attached Storage (NAS)	ICTSS	GAA	200,000.00	1	200,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					20,000,000.00
[UACS Object Code]					20,000,000.00
Software Development Contractor	ICTSS	GAA	20,000,000.00	1	20,000,000.00
[INTERNAL ICT PROJECT #2]					21,250,000.00
CAPITAL OUTLAY					1,250,000.00

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

[UACS Object Code]					1,250,000.00
Laptop	ICTSS	GAA	70,000.00	15	1,050,000.00
NAS	ICTSS	GAA	200,000.00	1	200,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					20,000,000.00
[UACS Object Code]					20,000,000.00
Software Development Contractor	ICTSS	GAA	20,000,000.00	1	20,000,000.00
CROSS-AGENCY ICT PROJECTS					21,250,000.00
[CROSS-AGENCY ICT PROJECT #1]					21,250,000.00
CAPITAL OUTLAY					1,250,000.00
[UACS Object Code]					1,250,000.00
Laptop	DICT-MISS	GAA	70,000.00	15	1,050,000.00
NAS	DBM-ICTSS	GAA	200,000.00	1	200,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					20,000,000.00
[UACS Object Code]					20,000,000.00

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

Software Development Contractor	DEPDev-ICTS	GAA	20,000,000.00	1	20,000,000.00
CONTINUING COSTS/EXPENSES					
MAINTENANCE AND OTHER OPERATING EXPENSES					8,000,000.00
[UACS Object Code]					5,000,000.00
Maintenance of HRMIS	ICTSS	GAA	5,000,000.00	1	5,000,000.00
[UACS Object Code]					3,000,000.00
Data Encoder (COS)	ICTSS	GAA	300,000.00	10	3,000,000.00
GRAND TOTAL					92,014,998.50

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

A.2. [Year #2]

ITEM	OFFICE LOCATION	FUND SOURCE	UNIT COST	PHYSICAL TARGET	TOTAL COST
OFFICE PRODUCTIVITY					18,765,000.00
CAPITAL OUTLAY					7,500,000.00
[UACS Object Code]					7,500,000.00
Laptop	OUSEC	GAA	50,000.00	50	2,500,000.00
Desktop	OASEC	GAA	50,000.00	100	5,000,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					11,265,000.00
[UACS Object Code]					6,000,000.00
Laptop	OUSEC	GAA	40,000.00	50	2,000,000.00
Desktop	OASEC	GAA	40,000.00	100	4,000,000.00
[UACS Object Code]					4,500,000.00
Printer	OASEC	GAA	45,000.00	100	4,500,000.00
[UACS Object Code]					765,000.00

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

Office Productivity Suite	CPMS	GAA	8,500.00	30	255,000.00
	AS	GAA	8,500.00	60	510,000.00
INTERNAL ICT PROJECTS					42,500,000.00
[INTERNAL ICT PROJECT #1]					21,250,000.00
CAPITAL OUTLAY					1,250,000.00
[UACS Object Code]					1,250,000.00
Laptop	ICTSS	GAA	70,000.00	15	1,050,000.00
Network Attached Storage (NAS)	ICTSS	GAA	200,000.00	1	200,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					20,000,000.00
[UACS Object Code]					20,000,000.00
Software Development Contractor	ICTSS	GAA	20,000,000.00	1	20,000,000.00
[INTERNAL ICT PROJECT #2]					21,250,000.00
CAPITAL OUTLAY					1,250,000.00
[UACS Object Code]					1,250,000.00
Laptop	ICTSS	FAP	70,000.00	15	1,050,000.00

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

NAS	ICTSS	FAP	200,000.00	1	200,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					20,000,000.00
[UACS Object Code]					20,000,000.00
Software Development Contractor	ICTSS	FAP	20,000,000.00	1	20,000,000.00
CROSS-AGENCY ICT PROJECTS					21,250,000.00
[CROSS-AGENCY ICT PROJECT #1]					21,250,000.00
CAPITAL OUTLAY					1,250,000.00
[UACS Object Code]					1,250,000.00
Laptop	DICT-MISS	FAP	70,000.00	15	1,050,000.00
NAS	DBM-ICTSS	FAP	200,000.00	1	200,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					20,000,000.00
[UACS Object Code]					20,000,000.00
Software Development Contractor	DEPDev-ICTS	FAP	20,000,000.00	1	20,000,000.00
CONTINUING COSTS/EXPENSES					8,000,000.00

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

MAINTENANCE AND OTHER OPERATING EXPENSES					5,000,000.00
[UACS Object Code]					5,000,000.00
Maintenance of HRMIS	ICTSS	GAA	5,000,000.00	1	5,000,000.00
[UACS Object Code]					3,000,000.00
Data Encoder (COS)	ICTSS	FAP	300,000.00	10	3,000,000.00
GRAND TOTAL					90,515,000.00

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

A.3. [Year #3]

ITEM	OFFICE LOCATION	FUND SOURCE	UNIT COST	PHYSICAL TARGET	TOTAL COST
OFFICE PRODUCTIVITY					20,264,998.50
CAPITAL OUTLAY					7,500,000.00
[UACS Object Code]					7,500,000.00
Laptop	OUSEC	GAA	50,000.00	50	2,500,000.00
Desktop	OASEC	GAA	50,000.00	100	5,000,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					12,764,998.50
[UACS Object Code]					7,499,998.50
Laptop	OUSEC	GAA	49,999.99	50	2,499,999.50
Desktop	OASEC	GAA	49,999.99	100	4,999,999.00
[UACS Object Code]					4,500,000.00
Printer	OASEC	GAA	45,000.00	100	4,500,000.00
[UACS Object Code]					765,000.00

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

Office Productivity Suite	CPMS	GAA	8,500.00	30	255,000.00
	AS	GAA	8,500.00	60	510,000.00
INTERNAL ICT PROJECTS					42,500,000.00
[INTERNAL ICT PROJECT #1]					21,250,000.00
CAPITAL OUTLAY					1,250,000.00
[UACS Object Code]					1,250,000.00
Laptop	ICTSS	GAA	70,000.00	15	1,050,000.00
Network Attached Storage (NAS)	ICTSS	GAA	200,000.00	1	200,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					20,000,000.00
[UACS Object Code]					20,000,000.00
Software Development Contractor	ICTSS	GAA	20,000,000.00	1	20,000,000.00
[INTERNAL ICT PROJECT #2]					21,250,000.00
CAPITAL OUTLAY					1,250,000.00
[UACS Object Code]					1,250,000.00
Laptop	ICTSS	FAP	70,000.00	15	1,050,000.00

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

NAS	ICTSS	FAP	200,000.00	1	200,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					20,000,000.00
[UACS Object Code]					20,000,000.00
Software Development Contractor	ICTSS	FAP	20,000,000.00	1	20,000,000.00
CROSS-AGENCY ICT PROJECTS					21,250,000.00
[CROSS-AGENCY ICT PROJECT #1]					21,250,000.00
CAPITAL OUTLAY					1,250,000.00
[UACS Object Code]					1,250,000.00
Laptop	DICT-MISS	FAP	70,000.00	15	1,050,000.00
NAS	DBM-ICTSS	FAP	200,000.00	1	200,000.00
MAINTENANCE AND OTHER OPERATING EXPENSES					20,000,000.00
[UACS Object Code]					20,000,000.00
Software Development Contractor	DEPDev-ICTS	FAP	20,000,000.00	1	20,000,000.00
CONTINUING COSTS/EXPENSES					8,000,000.00

INFORMATION SYSTEMS STRATEGIC PLAN 20__ - 20__

MAINTENANCE AND OTHER OPERATING EXPENSES					5,000,000.00
[UACS Object Code]					5,000,000.00
Maintenance of HRMIS	ICTSS	GAA	5,000,000.00	1	5,000,000.00
[UACS Object Code]					3,000,000.00
Data Encoder (COS)	ICTSS	FAP	300,000.00	10	3,000,000.00
GRAND TOTAL					92,014,998.50

*All costs indicated in this section are based on the market research conducted by <Agency Name>

B. SUMMARY OF INVESTMENTS

B.1. GENERAL SUMMARY

CATEGORY	[YEAR #1]	[YEAR #2]	[YEAR #3]
OFFICE PRODUCTIVITY	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
INTERNAL ICT PROJECTS	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
CROSS-AGENCY ICT PROJECTS	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
CONTINUING COSTS	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
GRAND TOTAL	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]

B.2. FUND SOURCE

FUND SOURCE	[YEAR #1]	[YEAR #2]	[YEAR #3]
GENERAL APPROPRIATIONS ACT	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
FOREIGN-ASSISTED PROJECTS	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
LOCALLY FUNDED	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
OTHER INCOME GENERATING SOURCES	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
GRAND TOTAL	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]

B.3. STATEMENT OF EXPENDITURE

EXPENDITURE CLASS	[YEAR #1]	[YEAR #2]	[YEAR #3]
CAPITAL OUTLAY	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
MAINTENANCE AND OTHER OPERATING EXPENSES	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
GRAND TOTAL	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]

B.4. OBJECT OF EXPENDITURE

OBJECT CODE	[YEAR #1]	[YEAR #2]	[YEAR #3]
ICT EQUIPMENT	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
PRINTING EQUIPMENT	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
SEMI-EXPENDABLE ICT EQUIPMENT	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
SEMI-EXPENDABLE PRINTING EQUIPMENT	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
ICT SOFTWARE	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
ICT SOFTWARE SUBSCRIPTION	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]
GRAND TOTAL	[Total Amount in Pesos]	[Total Amount in Pesos]	[Total Amount in Pesos]



GUIDELINES IN ACCOMPLISHING THE REVISED ISSP TEMPLATE v. 2026

This guide provides comprehensive instructions for government agencies drafting their **Information Systems Strategic Plan (ISSP)** using the revised ISSP template.

PART I: AGENCY PROFILE & STRATEGIC CONTEXT

This section establishes the foundation of the ISSP by aligning ICT initiatives with the agency's legal mandate and leadership structure.

A. **Mandate, Vision, Mission, and Organizational Outcome:** Directly lift these statements from official documents like the Strategic Plan or Citizen's Charter.

A.1 Mandate: Describe the legal or official function and responsibilities of your agency as defined by law, executive order, or other official issuance

- **Legal Basis:** Cite the specific law or executive order (e.g., RA 10844 for DICT) that created the agency.
- **Function:** Ensure the functions listed are directly derived from the legal instrument cited in the "Legal Basis" bullet point (e.g., a Republic Act, Executive Order, or Presidential Decree).

A.2 Vision Statement: State the organization's intended future direction or long-term desired position. This should reflect what the agency aims to achieve in the long run.

A.3 Mission Statement: Outline the agency's core purpose and primary objectives. This should explain what the agency does, for whom, and how it delivers its mandate.

A.4 Organizational Outcome: Categorize outcomes based on agency type: Organizational Outcomes (OO) for NGAs, Strategic Objectives (SO) for GOCCs, or Major Final Outputs (MFO) for LGUs. Furthermore, include programs under each particular OO/SO/MFO



B. Organizational Structure:

B.1 CIO & ISSP Focal Person: Please provide the complete information of the CIO and ISSP focal person, as alternate. Ensure that all fields are filled-out accurately.

- **Name of CIO:** Enter the full name (First Name, Middle Initial, Last Name) of the CIO.
- **Plantilla Position:** Enter the plantilla position of CIO.
- **Organizational Unit:** Specify the office, division, or unit to which the CIO is assigned.
- **E-mail Address:** Provide the official e-mail address of the CIO for correspondence purposes.
- **Contact Number/s:** Write the current and active telephone or mobile number/s where the CIO can be reached.

- **Name of ISSP Focal:** Enter the full name (First Name, Middle Initial, Last Name) of the assigned focal.
- **Position:** Enter the position of focal.
- **Organizational Unit:** Specify the office, division, or unit to which the focal is assigned.
- **E-mail Address:** Provide the official e-mail address of the focal for correspondence purposes.
- **Contact Number/s:** Write the current and active telephone or mobile number/s where the focal can be reached.

B.2 Human Capital: Provide a physical count of personnel categorized according to employment status (Plantilla, Contractual, or Outsourced) and distinguish between IT and Non-IT roles. In compliance with Gender and Development (GAD) requirements, indicate the number of male and female employees as well.

C. Stakeholder Analysis: Identify the groups affected by your ICT programs (e.g., citizens, other agencies) and categorize the complexity of their transactions as Simple, Complex, or Highly Technical. Include citizens, other government agencies, LGUs, private sector partners, NGOs, and others who benefit from or contribute to your ICT programs.

Simple: Applications or requests that only require ministerial actions on the part of the public officer or employee.

- **Characteristics:** These involve straightforward, routine tasks that present only inconsequential issues for resolution.
- **Processing Time:** Maximum of three (3) working days.



Complex: Applications or requests that necessitate evaluation in the resolution of complicated issues by an officer or employee of the government office.

- Characteristics: These require more in-depth assessment compared to simple transactions and are determined as such by the office concerned.
- Processing Time: Maximum of seven (7) working days

Highly Technical: Applications or requests which require the use of technical knowledge, specialized skills, and/or training in the processing and/or evaluation thereof.

- Characteristics: Often involves complex engineering, specialized research, or significant, high-level evaluation requiring specific, in-depth expertise.
- Processing Time: Maximum of twenty (20) working days

PART II: CURRENT ICT ASSESSMENT

A detailed report of the agency's existing digital environment.

A. **Strategic Concerns for ICT Use:** Map your critical business systems to specific problems and explain how ICT is intended to solve them.

- a. **OO/SO/MFO:** Refer to the OOs/SOs/MFOs indicated in Part I.A.4. List each OO/SO/MFO which can be enhanced or facilitated by the adoption of ICT.
- b. **Critical Management, Operating, or Business System:** Describe the actual business operations/activities performed by the organization in relation to Col. 1.
- c. **Problem:** Refers to the barriers/obstacles that hinder or cause delay in the performance of the business operations/activities identified in Col. 2.
- d. **Intended Use of ICT:** Indicate the intended ICT solution to address the problems cited in Col. 3. Some considerations include:
 - Is it possible and necessary to automate/digitalize an existing manual process/system?
 - Will the ICT solutions mentioned improve the internal efficiency and provide efficient delivery of services to the agency's stakeholders?

B. **Existing Network Infrastructure:** Illustrate your agency's current network infrastructure including Cybersecurity components.

B.1. **LAN/WAN set-up including Connectivity Type and Bandwidth:** Illustrate the layout or configuration of the existing network architecture through a diagram. Specify the connectivity type (e.g. fiber, DSL, broadband, etc.) and



upload/download speeds per office or site and if IPV6 ready. Highlight the cybersecurity components in-place.

- i. For department-wide: should show the connectivity among the central office and its various attached offices and agencies.
- ii. The connectivity between the central office to its branches/regional offices should also be shown in the diagram.

B.2. Cybersecurity Control Checklist: This ensures compliance to a standardized security framework to protect government data.

PHYSICAL SECURITY

- Perimeter Protection (Mandatory) - Security control implemented at the outer boundary of an office/facility to prevent, deter, detect, and delay unauthorized access.
- Access Control (Mandatory) - Security control that regulates who or what is permitted to access specific physical locations, systems, applications, or data resources.
- Surveillance System (Mandatory) - Security control consisting of integrated video monitoring technologies designed to continuously observe, record, and store activities within and around a facility.
- Detection System (Optional) - Security control designed to identify and alert personnel to unauthorized access attempts, environmental hazards, or other security-related incidents within a protected area

PERIMETER SECURITY

- Next Generation Firewalls (Mandatory) - Advance network security control that performs deep packet inspection, application-level traffic control, and integrated intrusion prevention to detect and block sophisticated cyber threats.
- Intrusion Detection/Prevention Systems (IDS/IPS) (Mandatory) - Security controls that monitor network or system activity to detect malicious behavior (IDS) and automatically block or prevent identified threats (IPS) in real time.
- Web Application Firewalls (WAFs) (Mandatory) - Security control that monitors, filters, and blocks malicious HTTP/HTTPS traffic to protect web applications from attacks such as SQL injection, cross-site scripting (XSS), and other application-layer threats.
- Demilitarized Zone (DMZ) (Optional) - Segmented network zone that isolates publicly accessible systems (such as web or email servers) from



the internal network to reduce security risk and limit potential lateral movement in the event of a compromise.

NETWORK SECURITY

- Data Encryption (Mandatory) - Security control implemented to ensure confidentiality of sensitive information in transit and at rest.
- Network Segmentation (Optional) - Security control that divides a network into smaller, isolated segments to restrict unauthorized access, limit lateral movement, and reduce the impact of potential security breaches.

ENDPOINT SECURITY

- Anti-virus and Anti-malware Software (Mandatory) - Security control designed to detect, prevent, quarantine, and remove malicious programs such as viruses, worms and other forms of harmful code from endpoints and systems.
- Application Control (Mandatory) - Security control that restricts the execution of software on systems to only approved or authorized applications, typically through allowlisting or policy-based rules, to prevent unauthorized or malicious programs from running.
- BYOD Security (Mandatory) - A framework of policies and controls used to secure personally owned devices accessing organizational systems and data.
- Extended Detection and Response (XDR) (Optional) - Security control that collects and correlates data across endpoints, networks, servers, email, and cloud environments to provide centralized threat detection, investigation, and automated response capability

DATA SECURITY

- Data Classification (Mandatory) - Security control process that categorizes information based on its sensitivity, value, and regulatory requirements to determine appropriate handling, access controls, and protection measures.
- Data Loss Prevention (DLP) (Mandatory)- Security control that monitors, detects, and prevents unauthorized transmission, sharing, or exposure of sensitive data to reduce the risk of data leakage, misuse, or accidental disclosure.
- Data Backups and Recovery (Mandatory) - Security and resilience control involves regularly creating secure copies of critical data and implementing procedures to restore systems and information in the event of data loss, corruption, cyberattacks, or disasters.



APPLICATION SECURITY

- Regular Security Scanning and Testing (Mandatory) - Security practice that uses automated tools and manual assessments to identify vulnerabilities, misconfigurations, and weaknesses in systems and applications to enable timely remediation and risk reduction.

OTHER MEASURES

- Vulnerability Assessment - Systematic process of identifying, analyzing, and prioritizing security weaknesses in systems, networks, and applications to determine their potential impact and guide remediation efforts.
- Patch Management - Structured process for identifying, testing, deploying, and verifying software updates and security patches to remediate vulnerabilities and maintain system security and stability.
- Strong Password Policies - Set of security requirements that enforce robust password creation and management standards to reduce the risk of unauthorized access and credential compromise.
- Multi-Factor Authentication (MFA) - Authentication security control that requires users to verify their identity using two or more independent factors to enhance account protection.
- Access Reviews - Periodic security control process in which user accounts, roles, and permissions are evaluated to ensure access rights remain appropriate, up-to-date, and aligned with the principle of least privilege.
- Security Logs - System-generated records that capture security-relevant events to support monitoring, auditing, and incident investigation.
- Log Analysis - Process of reviewing and correlating security log data to identify anomalies, detect potential threats, investigate incidents, and support compliance and operational monitoring.
- Incident Response Plan - Documented framework that defines the procedures, roles, and responsibilities for detecting, responding to, containing, eradicating, and recovering from security incidents to minimize impact and restore normal operations.
- Security Information and Event Management (SIEM) - Centralized security platform that aggregates, correlates, and analyzes log and event data from multiple systems in real time to detect threats, generate alerts, and support incident response and compliance reporting.
- Penetration Testing - Controlled and authorized security assessment that simulates real-world cyberattacks to identify and exploit



vulnerabilities in systems, networks, or applications in order to evaluate security effectiveness and remediation priorities.

- Secure Software Development Life Cycle (SDLC) - Structured software development approach that integrates security practices throughout all phases of the development process to reduce vulnerabilities and improve overall application security

C. **Existing/Operational Information Systems (IS) Inventory:** For every operational system, detail its purpose, development strategy, and whether it processes personal information (requiring a Privacy Impact Assessment).

- **Information System Name:** Indicate the name of the IS. The name should be descriptive of the business process it represents.
- **Classification:** Identify the nature of the Information System whether it is one of the following:
 - i. **Support to Operations:** Select this for systems that facilitate internal agency processes but are not part of the core administrative "back-office" (e.g., library systems, internal knowledge bases, project management system).
 - ii. **General Administrative Systems:** This category is for "back-office" systems that keep the agency running, such as Human Resources (HRIS), Payroll, or Accounting systems.
 - iii. **Operations:** Select this if the system directly supports the agency's primary mandate or mission-critical functions.
 - 1. *Frontline Service (directly used for public/client service delivery)*
 - 2. *Non-Frontline Service (supports core mandate but not directly used by clients/public)*
- **Description & Purpose:** Describe each IS in terms of its salient features, functionalities, and reports generated.
- **Development Strategy:** Indicate whether the IS is for in-house development, outsourcing, or a combination of both. The use of ready-made software or off-the-shelf software may also be considered as another option.
- **Development Platform:** The foundation upon which software is built, encompassing tools and technologies that support the entire software development lifecycle, e.g. Visual studio, Supabase, Firebase, Retool, etc.
- **Database Name:** The name of the database should be related to the Information Systems it served and descriptive of the data sets it represents



- **Data Storage:** Identify how or in what form you intend to store/preserve the data.
- **Internal Users:** Units within the organization who may access the system in whole or in part.
- **External Users:** External organizations, stakeholders, private entities that may be given authority to access the system with certain restrictions
- **Owner:** This is the organizational unit for which the IS was developed based on their business process.
- **Interoperability:** This section is designed to evaluate how your agency's information systems connect, share, and process data within the broader government digital ecosystem. To accurately complete this section, you must evaluate the system's data exchange capabilities across four specific dimensions:
 - i. **Integrated with another system:** Check this box if the system has a direct technical connection or automated data exchange with another system.
 - i.a. **Internal Systems:** List specific software or databases within your own agency that this system connects to.
 - i.b. **External Systems:** Identify systems owned by other agencies (e.g., GSIS, PhilGEPS, or the DICT's eGov portal) that interface with your system.
 - **Data Generation for Others:** Indicate if this system acts as a "source of truth" or data provider. Check this if the system produces reports, API outputs, or datasets that are essential for the operation of *other* applications.
 - **Data Processing from Others:** Check this if your system relies on external data to function. This applies if your system consumes, receives, or processes information generated by a different internal or external system.
 - ii. **Deployed on a shared platform:** Specify if the system is hosted on a common infrastructure. This includes systems residing on the same physical server, a private cloud, or the **Government Common Platform** where it shares resources with other applications.
- **Privacy Impact Assessment:** Identify whether the Information System will process personal data. This ensures compliance with the Data Privacy Act of 2012 by identifying risks to personal information



- i. **Determine Personal Information Processing:** Identify if the system collects, stores, or processes "personal information". This includes data such as full names, home addresses, photos, or any other information that can specifically identify an individual.
- ii. **Mandatory Disclosure:** You must explicitly state "Yes" or "No" if the system processes personal data.
- iii. **Audit Status:** If "Yes," you must indicate if the system has already undergone a formal Privacy Impact Assessment. If it has not, this represents a gap that should be addressed in your proposed strategy.

D. **E-Government Programs (EGP) Checklist:** Report your adoption levels of national programs such as eLGU, eGovPay, PNPKI, HCMIS, and IFMIS.

PART III: PROPOSED ICT STRATEGY

The roadmap for future technology investments and developments.

A. **Proposed Network Infrastructure:** Illustrate your agency's proposed network infrastructure including Cybersecurity components.

A.1. **LAN/WAN set-up including Connectivity Type and Bandwidth:** Illustrate the layout or configuration of the proposed network architecture through a diagram. Specify the connectivity type (e.g. fiber, DSL, broadband, etc.) and upload/download speeds per office or site and if IPV6 ready. Highlight the proposed cybersecurity components to be put in-place.

- i. For department-wide - should show the connectivity and among the attached agencies.
- ii. The connectivity between the central office to its branches/regional offices should also be shown in the diagram.

A.2. **Cybersecurity Control Checklist:** Identifying compliance to mandatory and optional items like firewalls and anti-malware.

PHYSICAL SECURITY

- o Perimeter Protection (Mandatory) - Security control implemented at the outer boundary of an office/facility to prevent, deter, detect, and delay unauthorized access.



- Access Control (Mandatory) - Security control that regulates who or what is permitted to access specific physical locations, systems, applications, or data resources.
- Surveillance System (Mandatory) - Security control consisting of integrated video monitoring technologies designed to continuously observe, record, and store activities within and around a facility.
- Detection System (Optional) - Security control designed to identify and alert personnel to unauthorized access attempts, environmental hazards, or other security-related incidents within a protected area

PERIMETER SECURITY

- Next Generation Firewalls (Mandatory) - Advance network security control that performs deep packet inspection, application-level traffic control, and integrated intrusion prevention to detect and block sophisticated cyber threats.
- Intrusion Detection/Prevention Systems (IDS/IPS) (Mandatory) - Security controls that monitor network or system activity to detect malicious behavior (IDS) and automatically block or prevent identified threats (IPS) in real time.
- Web Application Firewalls (WAFs) (Mandatory) - Security control that monitors, filters, and block malicious HTTP/HTTPS traffic to protect web applications from attacks such as SQL injection, cross-site scripting (XSS), and other application-layer threats.
- Demilitarized Zone (DMZ) (Optional) - Segmented network zone that isolates publicly accessible systems (such as web or email servers) from the internal network to reduce security risk and limit potential lateral movement in the event of a compromise.

NETWORK SECURITY

- Data Encryption (Mandatory) - Security control implemented to ensure confidentiality of sensitive information in transit and at rest.
- Network Segmentation (Optional) - Security control that divides a network into smaller, isolated segments to restrict unauthorized access, limit lateral movement, and reduce the impact of potential security breaches.

ENDPOINT SECURITY

- Anti-virus and Anti-malware Software (Mandatory) - Security control designed to detect, prevent, quarantine, and remove malicious programs such as viruses, worms and other forms of harmful code from endpoints and systems.



- Application Control (Mandatory) - Security control that restricts the execution of software on systems to only approved or authorized applications, typically through allowlisting or policy-based rules, to prevent unauthorized or malicious programs from running.
- BYOD Security (Mandatory) - A framework of policies and controls used to secure personally owned devices accessing organizational systems and data.
- Extended Detection and Response (XDR) (Optional) - Security control that collects and correlates data across endpoints, networks, servers, email, and cloud environments to provide centralized threat detection, investigation, and automated response capability

DATA SECURITY

- Data Classification (Mandatory) - Security control process that categorizes information based on its sensitivity, value, and regulatory requirements to determine appropriate handling, access controls, and protection measures.
- Data Loss Prevention (DLP) (Mandatory)- Security control that monitors, detects, and prevents unauthorized transmission, sharing, or exposure of sensitive data to reduce the risk of data leakage, misuse, or accidental disclosure.
- Data Backups and Recovery (Mandatory) - Security and resilience control involves regularly creating secure copies of critical data and implementing procedures to restore systems and information in the event of data loss, corruption, cyberattacks, or disasters.

APPLICATION SECURITY

- Regular Security Scanning and Testing (Mandatory) - Security practice that uses automated tools and manual assessments to identify vulnerabilities, misconfigurations, and weaknesses in systems and applications to enable timely remediation and risk reduction.

OTHER MEASURES

- Vulnerability Assessment - Systematic process of identifying, analyzing, and prioritizing security weaknesses in systems, networks, and applications to determine their potential impact and guide remediation efforts.
- Patch Management - Structured process for identifying, testing, deploying, and verifying software updates and security patches to remediate vulnerabilities and maintain system security and stability.



- Strong Password Policies - Set of security requirements that enforce robust password creation and management standards to reduce the risk of unauthorized access and credential compromise.
 - Multi-Factor Authentication (MFA) - Authentication security control that requires users to verify their identity using two or more independent factors to enhance account protection.
 - Access Reviews - Periodic security control process in which user accounts, roles, and permissions are evaluated to ensure access rights remain appropriate, up-to-date, and aligned with the principle of least privilege.
 - Security Logs - System-generated records that capture security-relevant events to support monitoring, auditing, and incident investigation.
 - Log Analysis - Process of reviewing and correlating security log data to identify anomalies, detect potential threats, investigate incidents, and support compliance and operational monitoring.
 - Incident Response Plan - Documented framework that defines the procedures, roles, and responsibilities for detecting, responding to, containing, eradicating, and recovering from security incidents to minimize impact and restore normal operations.
 - Security Information and Event Management (SIEM) - Centralized security platform that aggregates, correlates, and analyzes log and event data from multiple systems in real time to detect threats, generate alerts, and support incident response and compliance reporting.
 - Penetration Testing - Controlled and authorized security assessment that simulates real-world cyberattacks to identify and exploit vulnerabilities in systems, networks, or applications in order to evaluate security effectiveness and remediation priorities.
 - Secure Software Development Life Cycle (SDLC) - Structured software development approach that integrates security practices throughout all phases of the development process to reduce vulnerabilities and improve overall application security
- B. **Enterprise Architecture:** Illustrate your agency's proposed enterprise architecture that defines your structure and operation. Identifying and rationalizing legacy systems, business processes, data assets, and ICT infrastructure; designing interoperable, secure, and scalable digital government solutions; guiding digital investment decisions and aligning them with your agency's strategic outcomes and public service delivery goals.



- C. **Proposed ICT Human Capital:** Please provide information about your agency's proposed ICT human capital to effectively support your agency's day-to-day operations and proposed ICT project implementations.
- D. **Proposed Information Systems:** List information systems that are proposed for development or for enhancement, with a brief description of their objectives, scope, key features, and target users. Indicate development approach (e.g., in-house, outsourced, COTS, hybrid), development platform, and database information.
- **Information System Name:** Indicate the name of the IS. IS name should be descriptive of the business process it represents.
 - **Classification:** When identifying the classification of a system, you must select the primary role it plays within the agency's operations:
 - i. **Support to Operations:** Select this for systems that facilitate internal agency processes but are not part of the core administrative "back-office" (e.g., library systems, internal knowledge bases).
 - ii. **General Administrative Systems:** This category is for "back-office" systems that keep the agency running, such as Human Resources (HRIS), Payroll, or Accounting systems.
 - iii. **Operations:** Select this if the system directly supports the agency's primary mandate or mission-critical functions.
 - Frontline Service (*directly used for public/client service delivery*)
 - Non-Frontline Service (*supports core mandate but not directly used by clients/public*)
 - **Description & Purpose:** Describe each IS in terms of its salient features, functionalities, and reports generated. For the IS that will be enhanced, indicate the enhancement to be done.
 - **Status:** Write whether the identified IS is for development or for enhancement.
 - i. **For Development -** This status applies to entirely new information systems that do not currently exist within the agency's inventory.
 - The system is being built from scratch to address a newly identified strategic concern or mandate.
 - The agency is transitioning from a manual process to an automated/digital transaction
 - **Description & Purpose:** Clearly define the objectives, scope, and key features of the new system.
 - **Development Strategy:** Specify if the new build will be In-house, Outsourced, COTS, or a Hybrid approach.
 - **Resource Alignment:** Ensure the "Year 1 Deliverables" in Part III.E



reflect the initial design or procurement phase for this new system.

- ii. For Enhancement - This status applies to existing/operational systems listed in your Part II inventory that require significant upgrades.
 - Adding new modules or functionalities to an existing platform.
 - Upgrading the **Development Platform** (e.g., migrating from an old framework to a modern one like React or VS Code tools).
 - Improving **Interoperability** (e.g., modifying a standalone system to now integrate with the eGov portal or external databases).
 - **Gap Identification:** The enhancement should directly address "Problems" identified in the Current ICT Assessment (Part II.A).
 - **Target Users:** Specify if the enhancement will expand the user base to external stakeholders or additional internal units.
 - **Privacy Check:** If the enhancement involves collecting more data points, you must re-evaluate if the system will now process personal information (PIA).
- **Development Strategy:** Indicate whether the IS is for in-house development, outsourcing, or a combination of both. The use of ready-made software or off-the-shelf software may also be considered as another option.
- **Development Platform:** The foundation upon which software is built, encompassing tools and technologies that support the entire software development lifecycle, e.g. Visual studio, Supabase, Firebase, Retool, etc.
- **Database Name:** The name of the database should be related to the Information Systems it served and descriptive of the data sets it represents
- **Data Storage:** Identify how or in what form you intend to store/preserve the data.
- **Internal Users:** Units within the organization who may access the system in whole or in part.
- **External Users:** External organizations, stakeholders, private entities that may be given authority to access the system with certain restrictions
- **Owner:** This is the organizational unit for which the IS was developed based on their business process.
- **Interoperability:** This section is designed to evaluate how your agency's information systems connect, share, and process data within the broader government digital ecosystem. To accurately complete this section, you must evaluate the system's data exchange capabilities across four specific dimensions:
 - i. **Integration with another system:** Check this box if the system will have a direct technical connection or automated data exchange with another system.



- i.c. **Internal Systems:** List specific software or databases within your own agency that this system will connect to.
 - i.d. **External Systems:** Identify systems owned by other agencies (e.g., GSIS, PhilGEPS, or the DICT's eGov portal) that will interface with your system.
 - **Data Generation for Others:** Indicate if this system will act as a "source of truth" or data provider. Check this if the system will produce reports, API outputs, or datasets that are essential for the operation of *other* applications.
 - **Data Processing from Others:** Check this if your system will rely on external data to function. This applies if your system will consume, receive, or process information generated by a different internal or external system.
 - ii. **Deployment on a shared platform:** Specify if the system will be hosted on a common infrastructure. This includes systems residing on the same physical server, a private cloud, or the **Government Common Platform** where it shares resources with other applications.
- **Privacy Impact Assessment:** Identify whether the Information System will process personal data. This ensures compliance with the Data Privacy Act of 2012 by identifying risks to personal information
 - i. **Determine Personal Information Processing:** Identify if the system collects, stores, or processes "personal information". This includes data such as full names, home addresses, photos, or any other information that can specifically identify an individual.
 - ii. **Predictive Assessment:** You must project whether the future system *will* process personal information once developed or enhanced.
 - iii. **Strategic Planning:** If a proposed system is marked "Yes" for processing personal data, ensure that the project deliverables in your roadmap include a PIA phase and the implementation of privacy-by-design features.



E. ICT Projects

E.1. Internal ICT Projects: Indicate the major milestones and expected outputs of each ICT Project annually. Include completion targets and status updates for progress monitoring.

- **Project Title:** Indicate the name/title of the proposed ICT Project. Use a distinct, formal name. Avoid generic titles like "Software Update." Use specific names such as "Integrated Cloud-Based Human Resource Management System (IC-HRMS)."
- **Description:** Provide a concise, high-level summary defining the nature and scope of the project. Clearly classify the initiative (e.g., Enterprise Web Application, Infrastructure/Network Overhaul, Cloud Data Migration, or Cybersecurity Enhancement) to establish the technical context for the budget recommendation.
- **Objectives:** Provide brief discussion on why the project is being proposed. Focus on the "Why." State the specific pain points identified in Part II (Strategic Concerns) that this project will solve (e.g., "To reduce processing time of business permits from 5 days to 24 hours").
- **Strategic Alignment:** Map the project to national or agency-level plans/goals. Identify its alignment with the following:
 - i. **Public Investment Program:** A six-year programming document that translates the goals of the Philippine Development Plan (PDP) into a prioritized list of capital-intensive programs and projects. It serves as the basis for the multi-year resource allocation and the annual budget preparation.
Check this if your project requires a **Capital Outlay (CO)** exceeding the threshold for regular office equipment and is intended to support the long-term socio-economic targets of the Philippine Development Plan.
 - ii. **National Cybersecurity Plan:** The official whole-of-nation roadmap for the integrated development and strategic direction of the country's cybersecurity. It aims to protect Critical Information Infrastructure (CII) and ensure a resilient cyberspace for the government and its citizens.
Check this if the project includes the procurement of security software (Firewalls, WAF, MFA), establishing a Security Operations Center (SOC), or protecting systems that process sensitive national or personal data.
 - iii. **E-Government Master Plan:** The primary framework for harmonizing all government ICT resources. It outlines the



blueprints for interoperability, shared services, and the digital transformation of public service delivery to achieve "One Digitized Government."

Check this if your system is designed to integrate with other agencies, uses national shared services (like GovNet or PNPKI), or aims to digitize manual frontline services.

- iv. **Program Convergence Budgeting:** A results-based budgeting approach where multiple agencies coordinate the planning and execution of programs targeting a common national outcome. It facilitates a "whole-of-government" approach to budgeting, ensuring that funds from different departments are synchronized for maximum impact.

Check this if your project is part of a joint initiative with other agencies (e.g., a shared database between DSWD and DOH) where the funding is requested by multiple government offices to achieve a single goal.

- v. **Others (specify):** Specify if the ICT project is aligned with other national or agency-level plans/goals not listed above.

- **Harmonization Framework:** Identify how this project fits into the broader government ICT ecosystem. Specify its alignment with the following:

- i. **National Prioritization:** Agencies must demonstrate how the project directly supports the "High-Priority" digital initiatives of the National Government. This includes projects identified in the **Philippine Development Plan (PDP) 2023-2028** and those classified under the **Three-Year Rolling Infrastructure Program (TRIP)**.

Check this if the project is a "Cabinet-level" priority or is mandatory for the agency's participation in a national platform (e.g., the eGov PH Super App).

- ii. **Resource Optimization:** This focuses on achieving **Economies of Scale** and avoiding reinventing the wheel. Agencies are encouraged to use **Common-Use Supplies and Equipment (CSE)** for ICT or shared infrastructure (e.g., GovNet, Government Cloud) instead of building standalone data centers or purchasing isolated server hardware.

Check this if the project leverages existing government resources to reduce redundant capital outlay (CO) or maintenance expenses.

- iii. **Interoperability Framework:** Projects must comply with the **Philippine e-Government Interoperability Framework (PeGIF)**. This ensures that the system can exchange data



seamlessly with other agencies via standardized APIs. It specifically prioritizes systems that can integrate with the **National Government Data Exchange**.

Check this if your system includes an API layer or a data-sharing module intended for cross-agency consumption.

- iv. **Cross-Agency Collaboration:** This identifies projects that require "Program Convergence." It refers to initiatives where multiple agencies share the same technical objective to achieve a common sectoral outcome (e.g., the Department of Health and DSWD collaborating on a unified social protection database).

Check this if your project is part of a **Joint Memorandum Circular (JMC)** or a shared service agreement with other government entities.

- v. **Scalability and Sustainability:** This criterion ensures long-term project viability through rigorous risk assessment, performance monitoring, and financial governance

Check this if your project includes a Security and Privacy Assessment for Risk reporting mechanism, with KPIs that align with the **DBM Program Expenditure Classification (PREXC)** for automated progress monitoring.

- **Duration:** State the duration of the project (e.g. 2026-2028) in accordance with the ISSP coverage.
- **Year 1 Deliverables/Milestone:** Provide the year 1 deliverables (e.g. policies for issuance, training to be conducted, covered Information Systems, infrastructure, etc.)
- **Year 2 Deliverables/Milestone:** Provide the year 2 deliverables (e.g. policies for issuance, training to be conducted, covered Information Systems, infrastructure, etc.)
- **Year 3 Deliverables/Milestone:** Provide the year 3 deliverables (e.g. policies for issuance, training to be conducted, covered Information Systems, infrastructure, etc.)
- **Implementing Unit:** Identify the specific office or division responsible for the project (e.g., "Information Technology Division" or "Procurement Service").
- **Total Project Cost:** Provide the total estimated budget for the entire duration. This must match the sum of the yearly costs listed in the Detailed Resource Deployment and Cost Breakdown (Part IV).
- **Funding Source:** Indicate funding source whether GAA, Foreign-Assisted, Locally Funded, Other Income Generating Sources.



E.2. Cross-Agency ICT Projects: Projects that involve digital initiatives that transcend a single agency's boundaries, requiring collaboration between multiple government entities to deliver unified public services. Indicate the major milestones and expected outputs of each ICT Project annually. Include completion targets and status updates for progress monitoring.

- **Project Title:** Use a descriptive name that reflects the collaborative nature of the project (e.g., "National Single Window System" or "Inter-Agency Health Data Exchange").
- **Description:** Summarize the cross-agency project and clearly state which government processes are being linked and how data and collaboration will exchange between agencies.
- **Objectives:** Discuss the specific inter-agency problem being solved (e.g., eliminating redundant data submission for citizens or improving data-sharing speed between different government offices)
- **Strategic Alignment:** Map the project to national or agency-level plans/goals. Identify its alignment with the following:
 - i. **Public Investment Program:** A six-year programming document that translates the goals of the Philippine Development Plan (PDP) into a prioritized list of capital-intensive programs and projects. It serves as the basis for the multi-year resource allocation and the annual budget preparation.
Check this if your project requires a **Capital Outlay (CO)** exceeding the threshold for regular office equipment and is intended to support the long-term socio-economic targets of the Philippine Development Plan.
 - ii. **National Cybersecurity Plan:** The official whole-of-nation roadmap for the integrated development and strategic direction of the country's cybersecurity. It aims to protect Critical Information Infrastructure (CII) and ensure a resilient cyberspace for the government and its citizens.
Check this if the project includes the procurement of security software (Firewalls, WAF, MFA), establishing a Security Operations Center (SOC), or protecting systems that process sensitive national or personal data.
 - iii. **E-Government Master Plan:** The primary framework for harmonizing all government ICT resources. It outlines the blueprints for interoperability, shared services, and the digital transformation of public service delivery to achieve "One Digitized Government."
Check this if your system is designed to integrate with other



- agencies, uses national shared services (like GovNet or PNPKI), or aims to digitize manual frontline services.
- iv. **Program Convergence Budgeting:** A results-based budgeting approach where multiple agencies coordinate the planning and execution of programs targeting a common national outcome. It facilitates a "whole-of-government" approach to budgeting, ensuring that funds from different departments are synchronized for maximum impact.
Check this if your project is part of a joint initiative with other agencies (e.g., a shared database between DSWD and DOH) where the funding is requested by multiple government offices to achieve a single goal.
- v. **Others (specify):** Specify if the ICT project is aligned with other national or agency-level plans/goals not listed above.
- **Harmonization Framework:** Identify how this project fits into the broader government ICT ecosystem. Specify its alignment with the following:
- i. **National Prioritization:** Agencies must demonstrate how the project directly supports the "High-Priority" digital initiatives of the National Government. This includes projects identified in the **Philippine Development Plan (PDP) 2023-2028** and those classified under the **Three-Year Rolling Infrastructure Program (TRIP)**.
Check this if the project is a "Cabinet-level" priority or is mandatory for the agency's participation in a national platform (e.g., the eGov PH Super App).
- ii. **Resource Optimization:** This focuses on achieving **Economies of Scale** and avoiding reinventing the wheel. Agencies are encouraged to use **Common-Use Supplies and Equipment (CSE)** for ICT or shared infrastructure (e.g., GovNet, Government Cloud) instead of building standalone data centers or purchasing isolated server hardware.
Check this if the project leverages existing government resources to reduce redundant capital outlay (CO) or maintenance expenses.
- iii. **Interoperability Framework:** Projects must comply with the **Philippine e-Government Interoperability Framework (PeGIF)**. This ensures that the system can exchange data seamlessly with other agencies via standardized APIs. It specifically prioritizes systems that can integrate with the **National Government Data Exchange (NGDX)**.
Check this if your system includes an API layer or a



- data-sharing module intended for cross-agency consumption.
- iv. **Cross-Agency Collaboration:** This identifies projects that require "Program Convergence." It refers to initiatives where multiple agencies share the same technical objective to achieve a common sectoral outcome (e.g., the Department of Health and DSWD collaborating on a unified social protection database).

Check this if your project is part of a **Joint Memorandum Circular (JMC)** or a shared service agreement with other government entities.

- v. **Scalability and Sustainability:** This criterion ensures long-term project viability through rigorous risk assessment, performance monitoring, and financial governance

Check this if your project includes a Security and Privacy Assessment for Risk reporting mechanism and/or with KPIs that align with the **DBM Program Expenditure Classification (PREXC)** for automated progress monitoring.

- **Duration:** State the duration of the project (e.g. 2026-2028) in accordance with the ISSP coverage.
- **Year 1 Deliverables/Milestone:** Provide the year 1 deliverables (e.g. policies for issuance, training to be conducted, covered Information Systems, infrastructure, etc.)
- **Year 2 Deliverables/Milestone:** Provide the year 2 deliverables (e.g. policies for issuance, training to be conducted, covered Information Systems, infrastructure, etc.)
- **Year 3 Deliverables/Milestone:** Provide the year 3 deliverables (e.g. policies for issuance, training to be conducted, covered Information Systems, infrastructure, etc.)
- **Implementing Unit:** Identify the specific office or division responsible for the project (e.g., "Information Technology Division" or "Procurement Service").
- **Total Project Cost:** Provide the total estimated budget for the entire duration. This must match the sum of the yearly costs listed in the Detailed Resource Deployment and Cost Breakdown (Part IV).
- **Funding Source:** Indicate funding source whether GAA, Foreign-Assisted, Locally Funded, Other Income Generating Sources.
- **Lead Agency:** Identify the primary agency responsible for the overall project management and accountability.
- **Implementing Agency:** List the partner agencies responsible for specific technical components or contributions.



- F. **Performance Measurement Framework:** Establish Key Performance Indicators (KPIs) for each internal and cross-agency ICT project/s. There should be one table for each ICT project with the project title above each table. You must define the necessary information for the following:
- **Hierarchy of targeted results** - Write the hierarchy of outcomes of the ICT Project clustered into intermediate outcome, immediate outcome and outputs.
 - **Intermediate Outcome** - refers to changes in behavior of targeted stakeholders as a result of the implementation of the ICT project.
Example: Enhancement of a monitoring system for field operations activities
 - **Immediate Outcome** - refers to enhancements in institutional capabilities of the Agency upon implementation of the ICT project.
Example: Streamlined and efficient near-real-time monitoring of land acquisition activities
 - **Output** - related to the installation/implementation of the ICT project in the agency within the lifetime of the project. These are completed deliverables of the project.
Example: Enhanced Land Tenure Improvement Operational Tool (LTI OPTOOL)
 - **Key Performance Indicators** - List measurable indicators that will prove that the outcomes and outputs mentioned in column 1 have been achieved.
Example: Percentage of Agrarian Reform Beneficiaries (ARBs) with individual/collective titles
 - **Baseline Data** - State corresponding baseline data of the indicator mentioned in column 2 prior to the implementation of the ICT project.
*Example: <Current> % ARBs with individual/collective titles;
18%-75% of total ARBs.*
 - **Targets** - Enumerate targets of the project for each KPI in column 2 and use the information in column 3.
*Example: Percentage of increase of ARBs with individual/collective titles;
80%-100% increase of ARBs with individual/collective titles.*
 - **Data Collection Method** - Identify data collection method for gathering the required data.
Example: Mandatory reporting, Business intelligence module
 - **Responsibility to collect data** - Identify the Unit, internal or external to the agency, responsible for collecting the data. Information will have to be analyzed and submitted by the Monitoring and Evaluation Teams to DICT.



PART IV: RESOURCE REQUIREMENTS

The financial and logistical breakdown of the three-year plan.

- A. **Detailed Resource Deployment and Cost Breakdown:** Provide annual tables (Year 1, 2, and 3) listing every item (e.g., laptops, printers, software acquisition or subscription, services) with their unit costs and physical targets. Consolidate the detailed costs into these four strategic categories:

Office Productivity: Costs for general hardware and software that support daily administrative tasks (e.g., standard PCs, MS Office licenses).

Internal ICT Projects: Costs directly linked to the development and implementation of your agency-specific systems (from Part III.E.1).

Cross-Agency ICT Projects: Your agency's financial contribution to integrated government projects (from Part III.E.2).

Continuing Costs/Expenses: Recurring costs which may be from maintenance expenses of existing systems, license renewals, and annual support contracts, among others.

To align with DBM requirements, it is necessary to classify the line items according to accounting standards:

Capital Outlay (CO): Expenses for assets that last more than a year and exceed the capitalization threshold (e.g., servers, high-value ICT equipment, perpetual ICT software licenses).

Maintenance and Other Operating Expenses (MOOE): Recurring costs and small-value items (e.g., internet and software subscriptions, ICT supplies, repairs and maintenance).

Object Codes (UACS): Ensure every item is mapped to its correct **Unified Accounts Code Structure** (e.g. ICT Equipment, ICT Software, ICT Office Supplies).

To accomplish Sections A.1, A.2, and A.3 of Part IV, you must create three separate tables (one for each year) that detail the specific resources required to execute the ICT projects and maintenance activities defined in the earlier parts of the ISSP.

A.1 [Year #1] - List all ICT requirements following the guidelines mentioned above for the 1st year of the ISSP coverage.

A.2 [Year #2] - List all ICT requirements following the guidelines mentioned above for the 2nd year of the ISSP coverage.

A.3 [Year #3] - List all ICT requirements following the guidelines mentioned above for the 3rd year of the ISSP coverage.



Item - Identify the specific ICT requirements necessary under the identified four strategic categories. These are categorized into hardware, software, ICT training and services.

Office Location - Identify the location where the item/s will be deployed or used for, whether by the central office or their respective regional offices.

Fund Source - Indicate the item's funding source whether GAA, Foreign-Assisted, Locally Funded, Other Income Generating Sources.

Unit Cost - Provide the current market price per unit. Ensure these are realistic and include taxes and delivery fees among others.

Physical Target - Indicate how many units are needed per year (Year 1, Year 2, and Year 3).

Total Cost - Automatically calculated as (Unit Cost x Quantity).

Guidelines:

1. Consistency Check: The Grand Totals in this section must exactly match the Grand Totals in the Summary of Investments.
2. Project Linkage: Ensure the costs listed here directly support the milestones written in Part III.E. For example, If "Training" was listed as a Year 2 milestone, there should be a corresponding budget line for "Training Expenses" in Year 2 of Part IV.
3. Inflation Cushion: When projecting Year 3 costs, it is standard practice to include a slight adjustment for potential market price increases or currency fluctuations for imported hardware.

B. **Summary of Investments** - This is the section where all costs from the detailed breakdown are consolidated into high-level categories.

B.1 General Summary - This table groups the total ICT investments into functional categories to show how the budget is proposed to be distributed across agency operations

- **Office Productivity:** This includes the cost of standard hardware (laptops, desktops) and software (Office suites, basic PDF editors) used for day-to-day administrative tasks.
- **Internal ICT Projects:** This must match the total cost of all projects listed in **Part III. E.1**. It represents the investment in systems unique to your agency's operations.
- **Cross-Agency ICT Projects:** This must match the total cost of projects listed in **Part III. E.2**. It reflects your agency's share in "whole-of-government" digital initiatives.
- **Continuing Costs:** This includes recurring costs for existing systems such as annual software maintenance, license renewals, and hardware repair services.

B.2 Fund Source - This section identifies the financial origin of the budget for each of



the three years.

- **General Appropriations Act (GAA):** Most common source; refers to the regular budget provided by the National Government.
- **Foreign-Assisted Projects (FAP):** For projects funded through international loans or grants (e.g., World Bank, ADB).
- **Locally Funded:** For special projects funded by the government outside the regular agency budget.
- **Other Income:** Applicable for GOCCs or agencies authorized to use their own revenue/retained earnings.

Guideline: Ensure the "Grand Total" across all fund sources matches the Grand Total in the General Summary.

B.3 Statement of Expenditure - This categorizes the budget according to the nature of the expense, which is vital for DBM budget preparation.

- **Capital Outlay (CO):** Refers to physical assets or intangible assets (like software licenses with perpetual licenses) that have a useful life of more than one year and exceed the government's capitalization threshold (usually PHP 50,000 per unit). This includes major hardware and initial system development costs.
- **Maintenance and Other Operating Expenses (MOOE):** Refers to recurring costs, subscriptions, consumables, and low-value assets. This includes internet and software subscriptions, cloud hosting fees, minor repairs, and ICT office supplies.

B.4 Object of Expenditure - This section requires mapping the costs to the Unified Accounts Code Structure (UACS). Some examples are found below:

- **ICT Equipment:** Physical ICT hardware.
- **Printing Equipment:** Dedicated printers and plotters.
- **Semi-Expendable ICT Equipment:** ICT items valued below the PHP 50,000 threshold.
- **ICT Software:** Perpetual licenses or capitalized software development costs.
- **ICT Software Subscription:** Recurring monthly or annual software subscription fees.

Guideline: Check the latest DBM UACS manual to ensure you are using the correct object codes, as these are frequently audited.

Key Filling-In Reminders:

1. **Horizontal and Vertical Consistency:** The "Grand Total" must be identical in all



four tables (General Summary, Fund Source, Statement of Expenditure, and Object of Expenditure).

2. **PREXC Alignment:** Ensure that the totals here align with the **Program Expenditure Classification (PREXC)** of your agency to ensure the budget is linked to specific organizational outputs.
3. **Inflation Adjustment:** For Years 2 and 3, it is advisable to account for a 3-5% inflation buffer for hardware and subscription costs.

UNIFORMITY:

The following format shall be observed by the Agency to promote uniformity:

- Font type: Palatino Linotype
- Page Orientation: Landscape
- Font size: 11
- Spacing: 1.5
- Paper type: A4 (210 x 297 mm)
- Page margin: 1 inch on all sides
- Header: Replace the DICT logo with the Agency logo



ANNEX 1: EXISTING INFORMATION & COMMUNICATIONS TECHNOLOGY (ICT) ASSET INVENTORY

This annex shall provide a comprehensive inventory of all existing ICT assets currently owned, leased, or utilized by the agency. The information will be used to assess the agency's current ICT capacity, identify gaps, and support ICT planning under the ISSP.

1. **ICT Equipment Inventory:** List down all existing ICT equipment currently owned, leased, or utilized by the agency. The information gathered will help assess the agency's current ICT resources, determine equipment utilization, and support planning for upgrades, replacement, and future ICT requirements.
2. **ICT Software Inventory:** List down all software applications and licenses currently used, managed, or maintained by the agency. The information collected will help assess existing software resources, monitor license compliance, and future ICT initiatives.

ANNEX 2: DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN (DRBCP) FOR ICT RESOURCES

A critical subset of an agency's ISSP, ensuring that mission-critical information systems and infrastructure remain operational or are restored quickly following a natural or man-made disaster.

The following formal guidelines are structured to align with DICT standards, ISO 22301 (Business Continuity Management), and MITHI Resolution 2025-01 requirements for sustainability and risk reporting.

1. Plan Governance and Strategy

The foundation of the DRBCP must define the organizational framework for disaster response.

- **Establishment of an ICT Disaster Recovery Team (DRT):** Identify key personnel (Commanders, Coordinators, and Technical Leads) with their 24/7 contact details.
- **Risk Assessment (RA):** Identify potential threats (e.g., earthquakes, typhoons, cyber-attacks/ransomware, power outages) and their likelihood of occurrence.
- **Business Impact Analysis (BIA):** Determine which ICT services are "Mission-Critical." Classify systems based on:
 - **Maximum Tolerable Period of Disruption (MTPD):** The time a service can be down before the agency suffers irreparable harm.
 - **Recovery Time Objective (RTO):** The target time for restoring a system.



- **Recovery Point Objective (RPO):** The maximum tolerable data loss (e.g., "Must restore data up to 4 hours before the crash").

2. Comprehensive ICT Component Inventory

The plan must explicitly detail every ICT component affected by a disaster:

- **Hardware & Infrastructure:** Servers (physical/virtual), storage arrays (SAN/NAS), and network equipment (routers, switches, firewalls).
- **Data and Databases:** Location of primary databases and the status of personal information processing (linked to the Privacy Impact Assessment).
- **Applications/Software:** Core administrative systems (HRIS, Payroll) and frontline service portals.
- **Connectivity:** Internet leased lines, GovNet connections, and VPN gateways.
- **Support Utilities:** Uninterruptible Power Supply (UPS), precision cooling units, and fire suppression systems in the Data Center.

3. Recovery Strategies (Technical Architecture)

Agencies must define the technical "How" of restoration:

- **Off-site Backup Management:** Maintain copies of data in a geographically separate location (at least 30km away) to ensure a single event does not destroy both primary and backup data.
- **Cloud-Based Recovery:** Leverage the **Government Common Platform (GovCloud)** for "Hot" or "Warm" standby sites, allowing for near-instant failover.
- **Redundancy (High Availability):** Implement redundant hardware and dual-ISP providers to prevent a Single Point of Failure (SPOF).
- **Data Synchronization:** Define the method of data replication (Synchronous for zero data loss or Asynchronous for periodic updates).

4. Operational Procedures (The Action Plan)

Formal Step-by-Step Response:

- **Declaration Phase:** Criteria for when a "Disaster" is officially declared and the DRBCP is activated.
- **Evacuation & Safety:** Procedures for securing physical hardware and ensuring staff safety before technical recovery.



- **Restoration Phase:** Technical procedures to restore servers, reconfigure networks, and verify data integrity.
- **Resumption Phase:** Transitioning from backup systems back to primary systems once the disaster is over ("Failback").

5. Compliance, Scalability, and Sustainability

In accordance with MITHI Resolution 2025-01 and the SPAR (Security and Privacy Assessment for Risk) reporting:

- **Cybersecurity Integration:** The DRBCP must include a "Cyber-Recovery" component to address data corruption or encryption caused by malware/ransomware.
- **Testing and Maintenance:** Mandate at least **one (1) full-scale DR simulation per year** and semi-annual tabletop exercises.
- **Audit and Review:** The plan must be reviewed annually or whenever a major change in the ICT infrastructure occurs (e.g., migrating to a new development platform).
- **UACS and Budgeting:** Ensure that maintenance and "Continuing Costs" in **Part IV** of the ISSP include budget for off-site storage, DR site subscriptions, and emergency equipment repairs.

Key Performance Indicators (KPIs) for DRBCP

Indicator	Target Metric
System Availability	99.9% Up-time (excluding planned maintenance)
RTO Achievement	Recovery within [X] hours of declaration
Backup Success Rate	100% successful daily automated backups
Testing Frequency	1 Comprehensive Exercise per Year



ANNEX 1: EXISTING INFORMATION & COMMUNICATIONS TECHNOLOGY (ICT) ASSET INVENTORY

1. ICT Equipment Inventory

ICT RESOURCES	OFFICE LOCATION	OPERATIONAL	END OF LIFE	BACKUP
Servers	Central Office	30	5	1
	Field/Regional Office	10	3	0
Total		40	8	1
Desktop	Central Office	120	15	10
	Field/Regional Office	60	8	5
Total		180	23	15
Laptop	Central Office	80	10	6
	Field/Regional Office	40	5	3
Total		120	15	9
Mobile Phone	Central Office	55	12	8
	Field/Regional Office	25	6	3
Total		80	18	11
Tablet	Central Office	30	7	4
	Field/Regional Office	15	3	2
Total		45	10	6
Printer	Central Office	25	5	3
	Field/Regional Office	12	2	1
Total		37	7	4



Network Switch	Central Office	50	8	6
	Field/Regional Office	20	3	2
Total		70	11	8
Others, please specify (continue on a separate sheet if necessary)				

2. ICT Software Inventory

ICT RESOURCES	OFFICE LOCATION	PERPETUAL	SUBSCRIPTION
Office Productivity Tool	Central Office	30	5
	Field/Regional Office	10	3
Total		40	8
Grammar checker	Central Office	120	15
	Field/Regional Office	60	8
Total		180	23
Graphics and Simulation Software	Central Office	80	10
	Field/Regional Office	40	5
Total		120	15
Antivirus	Central Office	55	12
	Field/Regional Office	25	6
Total		80	18
IT Help Desk Tool	Central Office	30	7
	Field/Regional Office	15	3
Total		45	10
Photo and Video Editing Software	Central Office	25	5
	Field/Regional Office	12	2



Total		37	7
Web Application Firewall	Central Office	50	8
	Field/Regional Office	20	3
Total		70	11
Others, please specify (continue on a separate sheet if necessary)			



ANNEX 2: SAMPLE DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

This sample **Disaster Recovery and Business Continuity Plan (DRBCP)** is modeled for a **sample generic** National Government Agency (NGA) that manages both internal administrative systems and public-facing frontline services.

1. Plan Overview & Governance

Agency Name: National Bureau of Resource Management (NBRM - Generic Reference)

Version: 2026.1

Approval Date: March 15, 2026

Disaster Recovery Team (DRT)

Role	Responsibility	Contact
Incident Commander	Declares disaster and authorizes DR site activation.	Director, ICT Service
Infrastructure Lead	Restores servers, networks, and cloud connectivity.	Chief, Network Div.
Data/App Custodian	Ensures database integrity and application failover.	Lead Programmer
Security Officer	Monitors for cyber threats during the recovery phase.	CISO

2. Business Impact Analysis (BIA) Summary

The agency has identified the following criticalities for its ICT components:

System Name	Classification	RTO (Restoration Time)	RPO (Data Loss Limit)
Public Licensing Portal	Frontline / Mission-Critical	4 Hours	1 Hour



Integrated HR & Payroll	Administrative / Support	24 Hours	12 Hours
Official Website	Information / Support	8 Hours	24 Hours
Document Tracking	Support to Operations	48 Hours	24 Hours

3. ICT Component Inventory & Affected Assets

When a disaster (e.g., Fire at Central Office or a Ransomware Attack) occurs, the following assets are identified as at-risk:

- **Primary Data Center (Central Office):** 10 Physical Servers, 2 SAN Storage Units, Core Switches.
- **Connectivity:** 200Mbps Dedicated Internet Leased Line; GovNet Fiber Link.
- **Data Assets:** SQL Databases for 1.2M citizen records; 5TB of digitized PDF archives.
- **Power:** 100kVA Generator Set; 3 x 10kVA UPS Units.

4. Technical Recovery Strategy

NBRM utilizes a **Hybrid-Cloud Recovery Model** to ensure scalability and sustainability:

1. **Off-site Backup:** Daily encrypted backups are sent to a secondary physical site located in a different region (e.g., Cebu Regional Office).
2. **Cloud Failover (GovCloud):** Mission-critical applications (Licensing Portal) are replicated in real-time to the **DICT GovCloud**. In a disaster, traffic is rerouted via DNS update.
3. **Redundancy:** Dual ISP providers (PLDT/Globe) are configured in an active-passive setup to prevent connectivity loss.

5. Standard Operating Procedures (SOP)

Phase I: Detection and Declaration

- **Trigger:** System monitoring alerts or physical site damage report.
- **Action:** ICT Director evaluates the scale. If the RTO cannot be met at the primary site, the DRBCP is activated.



Phase II: Activation and Execution

- **Step 1:** Notify the DRT via SMS/Instant Messaging.
- **Step 2:** Redirect Public Portal URL to the **GovCloud DR Instance**.
- **Step 3:** Restore the latest "clean" database backup (RPO check).
- **Step 4:** Verify application functionality and security protocols (MFA/WAF).

Phase III: Failback (Return to Normal Operations)

- **Requirement:** Primary site is declared safe and stable.
- **Action:** Synchronize data changes made at the DR site back to the Primary Data Center. Schedule a maintenance window for the final switch-over to prevent data collision.

6. Maintenance and Sustainability

To comply with MITHI Resolution 2025-01 and SPAR Reporting:

- **Quarterly Backup Drills:** Randomly selecting one system to restore from backup to verify data readability.
- **Annual DR Simulation:** A full "shut-down" drill of the primary server to test GovCloud failover.
- **Budgetary Support:** Funding for off-site storage and cloud subscriptions is categorized under MOOE in Part IV of the ISSP (Object Code: *ICT Software Subscription*).