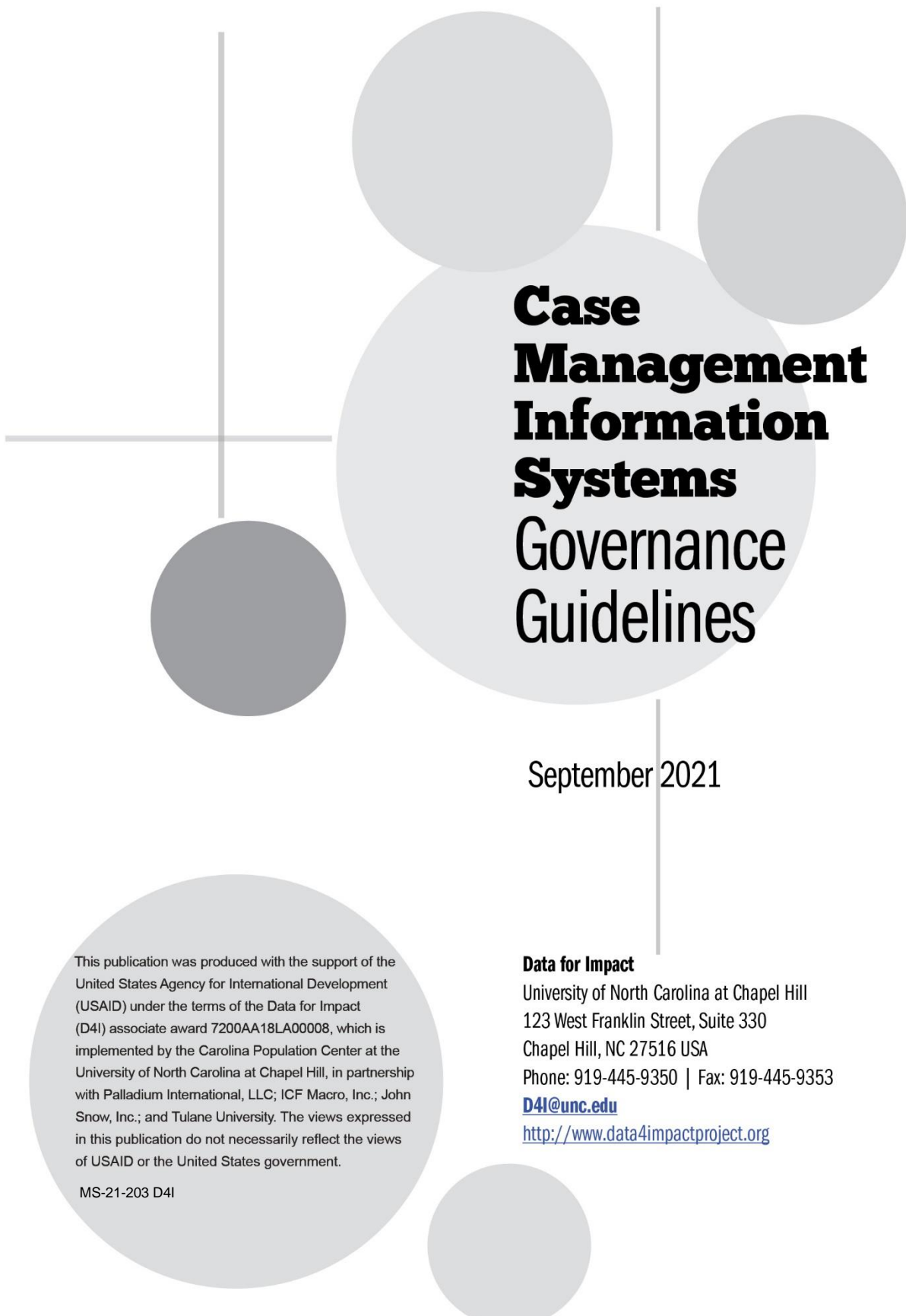# Case Management Information Systems

Governance Guidelines

September 2021

Case Management Information Systems
Governance
Guidelines

September 2021

Data for Impact
University of North Carolina at Chapel Hill
123 West Franklin Street, Suite 330
Chapel Hill, NC 27516 USA
Phone: 919-445-9350 | Fax: 919-445-9353
D4I@unc.edu
http://www.data4impactproject.org

Acknowledgments

Contents

List of Figures

List of Tables

Introduction

Many countries are implementing Case Management Information Systems (CMIS) as part of a global effort to enhance child protection interventions and case management services. CMIS is a digital tool used by members of the social service workforce to facilitate case management through the capture, storage, and processing of longitudinal data for effective tracking of social protection services provided to children. This information is used to enhance case management and promote impactful decision-making practices.

CMIS are designed with a wide range of functionalities to support the core steps in the case management process. These include registration of child profiles, performing initial and complex assessments, scheduling tasks for the different stakeholders involved in a case, displaying alerts and notifications for each case, establishing the status of the case, performing referrals to specialized services, making information available to collaborating agencies or organizations, performing transfers of the case to other case managers, defining and recording actions of individual assistance plans, registering incidents, registering case closure information, etc. The system produces data that can be used to generate longitudinal indicators and dashboards that show information related to case management. At the same time, district and national level authorities can have access to the aggregated data generated by the CMIS to plan childcare initiatives.

A good governance approach plays a critical role in ensuring that CMIS development, implementation, and use strategies are aligned with national child protection and care policies, and that the CMIS delivers the functionality and services in-line with the current and planned needs of the government. Strong and mature governance practices ensures successful implementation of the CMIS at a national or sub-national level for impactful interventions in child protection. Despite an increase in CMIS implementations globally, the lack of a standardized approach, driven by an overarching governance framework, has hampered the adoption and successful implementation of CMIS due to the lack of ownership, accountability, and planning for sustainability.

Data for Impact

The United States Agency for International Development (USAID) works in countries around the world to improve the lives of the most vulnerable children in keeping with the objectives established in the U.S. Government (USG) strategy for Advancing Protection and Care for Children in Adversity (APCCA). In support of country priorities and in line with APCCA objectives, USAID-funded activities advance partner countries on their journey to self-reliance (https://www.usaid.gov/selfreliance) by helping governments build and strengthen their capacities to support, manage, and finance their child protection and care systems, using the best available data for decision making and employing research, implementation science, and programmatic learning to design evidence-based and evidence-informed policies, programs, and practices.

The USAID-funded Data for Impact (D4I) project builds on and reinforces current USG support for priority countries to realize the power of data as actionable evidence that can improve policies, programs, and outcomes (https://www.data4impactproject.org).Under the MEASURE Evaluation Phase IV activity, USAID developed the Information Systems Framework for the Case Management of Child Protection and Care (hereafter, referred to as the "CMIS framework") to consolidate lessons learned from those who have developed, implemented, and used such systems and agreed-upon best practices when approaching the design and strengthening of such systems. The framework presents three perspectives and related processes that should be considered together to ensure a holistic approach to CMIS development. Though some of the processes have standardized tools and/or resources for child protection/care, for many processes, standards do not exist.

This toolkit builds upon the lessons learned through the CMIS framework. Also, D4I reviewed tools such as the mHealth Assessment and Planning for Scale (MAPS) toolkit and other frameworks used during MEASURE Evaluation Phase IV CMIS assessments.

The toolkit is the product of a participatory design process, through which a technical working group validated the tools. The group involved 14 women and 15 men from country governments, USAID country missions, the Office of HIV/AIDS, UNICEF headquarters and field offices, case management experts, monitoring and evaluation (M&E) experts, and digital solution experts. The group included members representing Armenia, Colombia, Ghana, Guatemala, Kenya, Moldova, Rwanda, Uganda, and the United States.

Background

Increased demand for timely and accurate child protection data by decision makers and social workers has created an urgency and a great opportunity to build impactful CMIS implementation. The sensitive and dynamic nature of child protection activities has necessitated the need to not only automate service delivery but also to build strong systems that comply to technological and ethical standards while promoting innovation and best practices. Successful implementation not only requires the highest safety and security standards, government ownership, and well-defined accountability mechanisms, but it also underlines the need for a strong policy and regulatory base. Countries are at different levels with implementation of CMIS, and these systems are evolving from paper-based generation, transmission, and storage to web-based systems. A concerted effort is necessary to safeguard the gains by strengthening governance for these information systems.

D4I is supporting the development of a global governance guidance document for implementation and oversight of CMIS. This guidance document is part of the larger governance activity by D4I in development of a CMIS Assessment and Planning Toolkit designed to improve the capacity of governments in evaluating digital systems to support child protection and care and to assess their potential for scale-up and long-term sustainability.

This guidance document has taken into consideration some of the critical governance gaps that have been highlighted from assessments of information management systems for case management, such as the MEASURE Evaluation assessment of the Children First Software in Uganda (March 2019) and an assessment report of prerequisites for a social welfare information management system in Ghana[1] (March 2020). A major barrier for CMIS sustainability, documented in recent assessments, is the ultimate government leadership and ownership for CMIS system implementation and the establishment of accountability mechanisms to ensure that the right decisions are made, through the right consultative processes, by the right stakeholders. This guide, therefore, consolidates governance components that inform the design, implementation, oversight and strengthening of such systems. It is written from a multisectoral perspective of CMIS implementation for the need to converge in a common governance approach. It designates responsibilities and decision-making in a way that ensures that the most appropriate parties contribute and that roles and responsibilities of each substructure within the governance structures are defined. Implementation and oversight of CMIS is led by the country-specific government agency with responsibility for children—but a CMIS that is longitudinal in nature also has information relevant to different ministries and may need to interoperate with those. Data sharing is critical as there are other sectors involved in case management for children, such as security, education, judiciary, and health, and this will vary depending on country-specific context.

Establishment of a governance structure for the implementation of the longitudinal information system seeks to ensure that the decisions required for CMIS operation are made in a timely manner and are aligned with the country's priorities under a governance framework. This guidance document elaborates on the mechanisms used to endorse institutional decisions related to information systems, identify the officials who are assigned the responsibility of endorsing these decisions, hold officials accountable for the results of these decisions, and identify the organizations (or departments) that must meet to discuss these decisions.

---

[1] https://www.measureevaluation.org/resources/publications/tr-20-396.html

Process of Developing the Guidance Document

The CMIS Governance Guidelines have been developed through a wide stakeholder consultative process, led by a global CMIS Technical Working Group (TWG). This group included representatives from governments, development partners, implementing partners, and academia. For a full list of the members who participated in the TWG refer to Appendix 5.

The CMIS Governance Guidelines and the maturity model toolkit were piloted in Kenya by the Department of Children Services between May and August 2021. The results of the pilot confirmed applicability in the local context and feedback was incorporated into the final document.

Objectives

This CMIS Governance Guidelines have been developed to:

- Define a governance framework for large-scale CMIS Implementation.
- Provide operational guidance for use by countries in strengthening CMIS governance.
- Outline the structures and processes representing the norms, values, and rules for CMIS governance.
- Highlight actionable steps towards achieving higher maturity levels in CMIS governance.
- Provide a CMIS Governance Maturity Model to help countries in assessing and determining the degree of maturity of their CMIS governance processes.

CMIS Governance Components

The CMIS governance components are a set of interrelated domains and elements that represent a mature CMIS governance ecosystem.

The CMIS governance components diagram in Figure 1 provides a contextual view of the CMIS governance components and delineates a sequential and iterative approach towards strengthening governance for successful implementation of the CMIS at a large scale.

Figure 1. CMIS governance components diagram
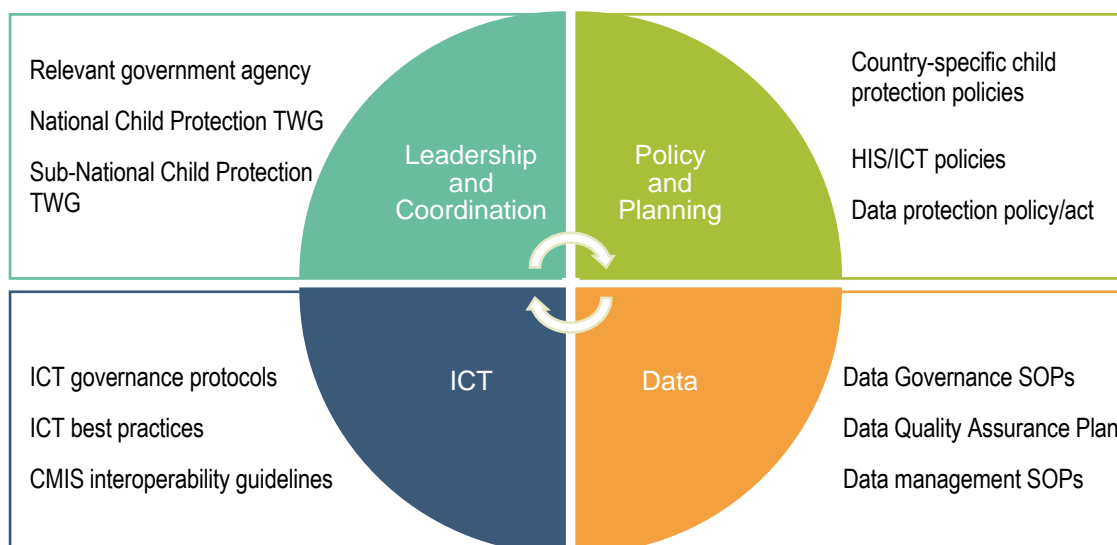
Strengthening CMIS Governance

The prescribed steps for strengthening CMIS governance are aligned to the four domains identified in Figure 1; Leadership and Coordination, Policy and Planning, Data, and ICT, and the guidance presents a sequential approach to CMIS governance strengthening activities that has been further illustrated in the sample CMIS Governance and Implementation Roadmap in Appendix 1.

Although the steps illustrated are designed for countries that plan to start implementing the CMIS, those countries already implementing CMIS should utilize the CMIS Maturity Model at the onset to determine their baseline maturity level and identify any existing governance gaps. The gaps identified should inform the necessary steps to be taken in further strengthening the current governance approach.

Leadership and Coordination

In these guidelines, leadership refers to the decision makers responsible for developing, deploying, and providing oversight of the adopted CMIS strategies. The leadership operates within defined organizational structures that facilitate a hierarchical arrangement of lines of authority, communications, rights, and duties.

All activities towards strengthening CMIS governance should be led by the country-specific government agency in charge of child protection and care, through a collaborative process with relevant stakeholders within and outside of government. CMIS development and implementation requires coordinated efforts among the actors and structures with a shared responsibility between the national and subnational levels. A defined approach towards coordination of CMIS stakeholders should not only improve efficiency and accountability but also ownership by the government. Effective coordination will reduce or eliminate duplication of investments.

Key leadership roles include:

- Defining policy and guidelines for CMIS

- Providing the vision statement to describe the purpose, values, and aspirations for its case management information systems

- Defining user regulations

- Ensuring use of the data from CMIS to inform decision making, planning, and program management actions

- Providing oversight for CMIS implementation through policy compliance tracking

- Coordinating evaluation and periodic review of the CMIS

- Maintaining the centralized CMIS database

- Ensuring sufficient resources are available for implementation of CMIS, including human, technical, and financial

The department of ICT or equivalent government entity is critical in the development and maintenance of CMIS and will be responsible for providing guidance on ICT regulations of data protection, data sharing, cyber security and storage of data, interoperability of systems, and interagency data sharing.

The critical steps in strengthening the CMIS leadership and coordination are to:

Determine the baseline level of CMIS governance maturity.

The CMIS governance maturity refers to the level of experience that a country has achieved with reference to the CMIS governance components described in this guidance document. The CMIS Maturity Model has been provided later in this guidance document (see Table 5), as a tool to help countries determine their

maturity levels and strengths, as well as their gaps, to inform priority interventions to improve their performance within the metrics described. A separate and customizable toolkit has been provided with this guidance to help countries assess their maturity levels.

The relevant national agency in charge of child protection and care should work with the relevant players in the government to determine the baseline CMIS governance maturity level, identify gaps in CMIS governance, and utilize the gaps identified to inform development of the Country CMIS Governance and Implementation Roadmap.

Develop a CMIS vision and strategy.

Leadership should develop a CMIS vision and strategy that provides a reference in the determination of CMIS goals. This strategy should direct investments, efforts, and coordination. The priority interventions for strengthening CMIS should be captured in the CMIS strategy document or linked to a higher-level digital strategy. Being a unique long-term plan or framework, the CMIS strategy should also guide other micro-plans such as annual work plans and budgets. Sustainability of CMIS needs to be carefully considered in the strategy—including the priority capacity strengthening interventions—to build government and local capacity required for CMIS, including the required financial and human resources for CMIS implementation and resource mobilization efforts.

Define country-specific CMIS governance structures.

Referring to the gaps identified at the leadership and governance domain in the maturity model, the national agency in charge of child protection should define, refine, document, and adopt an organizational structure that outlines individuals, groups, and committees responsible for providing CMIS implementation oversight and direction. The defined structures should build on existing national and sub-national institutions. The national agency in charge of child protection and care should provide overall leadership of the CMIS governance structures with well-defined linkages to relevant ministries, including ICT, security, judiciary, health, and planning. A staffing plan for implementation of CMIS with the required skills sets from data entry, child protection officers, M&E officers, and ICT should be developed to guide staffing decisions and investments.

Establish national and sub-national CMIS coordination and collaboration mechanisms.

It is expected that the national governments have established or are in the process of establishing overarching child protection coordinating bodies; for example, a child protection TWG at the national and subnational levels. This TWG's role is to coordinate the multisectoral entities and partners in developing and implementing child protection strategies that include CMIS implementation oversight.

To ensure ownership, resource allocation, and alignment of the system to the overall strategy, the child protection TWG should establish standing subcommittees of experts to advise or lead in specific CMIS technical components. Table 1 below lists the roles of the TWG at the national and subnational levels.

Table 1. Coordination mechanisms for CMIS implementation

Coordination structure	Roles
National Child Protection Technical Working Group *Membership should be drawn from* Ministries/ departments responsible for: ICT, health, police, planning, education, judiciary, social services, as well as child protection, intergovernmental forums, implementing partners, and development partners. TWG subcommittees should be established to provide technical leadership in necessary areas; e.g., data, ICT, and M&E.	• Ensure adequate consultations and participation of child protection stakeholders and other implementing departments and agencies in CMIS use • Support development and review of requisite policy, protocols, and strategies • Joint monitoring of compliance CMIS standards and guidelines • Resource mobilization • Coordinate data quality assurance • Enable partners to become jointly responsible for planning, monitoring, reviews, and reporting • Resource mobilization and prioritization • Interagency data sharing • Use of CMIS data • Align stakeholders supporting CMIS to a government-led joint vision, strategy, and workplan • Hold all sector partners jointly accountable for achieving results
Sub-National Child Protection Technical Working Groups *Members at sub-national level could be drawn from:* Departments responsible for health, security, planning, ICT, education, judiciary, social services, as well as child protection implementing partners, civil society, community and faith-based organizations	• Joint implementation and monitoring of compliance on CMIS SOPs • Coordinate data entry from the different agencies • Hold all sector partners jointly accountable for achieving results • Interagency data sharing • Coordinate data quality • Advocate for resources for CMIS implementation • Use of data from CMIS

Use data for action.

The goal of a CMIS is to generate quality data to inform decision-making. From a governance perspective, and to enhance ownership, it is expected that government leaders from the relevant Ministries and national TWGs will utilize data from CMIS for planning, program management, and decision-making. Through utilization of data, this will also improve oversight capacity by the leaders for CMIS. Countries should develop and implement data use plans (see example in Appendix 3) as part of the efforts to enhance use of data from CMIS for program management.

Policy and Planning

Policies are the guidelines, sets of principles, rules, and regulations which guide the government in its course of action. Planning entails the action intended for the future or a roadmap to achieve the goal. This guidance document recognizes policy and planning for CMIS as critical for standardization and sustainability. Planning for the CMIS should be integrated into the larger department or ministry responsible for child protection planning and budgeting processes. The CMIS planning should ideally be bottom-up. To enhance inclusivity and ownership in CMIS planning, the national TWG should coordinate and participate in the process. This will contribute to the development of one overarching CMIS plan.

Critical Steps in Strengthening CMIS Policy and Planning

Understand the Legal Environment

National governments are legally obliged to uphold children's rights through enactment of relevant laws and provision of services. Countries developing CMIS should ensure that both the policies and systems align to the various global and country-specific child protection and data protection laws.

Strengthen the Policy Environment for CMIS

Case management information systems must align to country policies, protocols, and standard operating procedures. The policy frameworks will differ country to country but will provide a deliberate system of principles to guide standardization. The approach in implementation of CMIS policies should involve three key steps:

1. Mapping relevant country-specific policies on ICT and data management and understanding their provisions—these policies may include data protection guidelines, ICT regulations, data sharing SOPs, and data exchange SOPs, among others.

2. Adapting the relevant policy provisions where they are available or developing protocols specific to information systems for case management where they are lacking.

3. Implementing policy, including defining coordination mechanisms, financing mechanisms, roles and responsibilities, and oversight systems.

CMIS should adhere to overarching ICT policies and uphold data protection provisions. The relevant policies should be used to inform other operational and administrative processes, such as the code of regulations for staff and contractors that have responsibilities in CMIS, terms of reference (TOR) for TWGs, and interagency collaborative agreements.

Monitoring mechanisms should be put in place to observe compliance with policies. Sanctions and rewards should be developed and executed. Rewards do not need to be monetary and can include things such as non-monetary awards, government endorsements, etc. Stakeholders that comply with policy implementation should be rewarded appropriately, while those that do not should face sanctions such as non-renewal of licenses.

The policy implementation process depends on the CMIS governance maturity level. In countries where systems are nascent, some of the critical interventions should include mapping the relevant policies and developing a policy inventory; developing a roadmap with critical steps to adopt these policies; and sensitizing stakeholders on the policy provisions. In countries with advanced systems, the focus will be on customization of specific policies for CMIS, capacity building of stakeholders; and monitoring compliance with policies. Table 2 outlines relevant CMIS policies and guidelines.

Table 2. Description of CMIS policies

Policy		Description
	COUNTRY-SPECIFIC CHILD PROTECTION ACTS/POLICIES	Implementation and oversight of CMIS should uphold children's rights and welfare as prescribed in the global and country-specific policies.
	ICT POLICIES	CMIS development and implementation should align to the overarching country-specific ICT regulations. Relevant ministries in charge of child protection and care should adopt the country-specific ICT regulations and develop a child welfare digital ICT strategy.
	DATA PROTECTION POLICIES	CMIS should align to the data protection guidelines to ensure integrity and privacy of data for children, which is most commonly classified as sensitive.

Develop and Implement a CMIS Change Management Protocol

Change management refers to the process of selecting which changes to encourage, which to allow, and which to prevent, according to provided criteria such as schedule and cost. The Child Protection TWG should develop a CMIS change management protocol that will define roles and responsibilities, critical project decision points, communication, escalation processes, change planning, and time standards for implementing changes, measurement metrics, and evaluation. In addition, a change management tool shall be developed or adopted for change tracking and reporting.

Conduct Advocacy Activities

Because the national child protection coordinating body or TWG is the collaborative mechanism for development and implementation of the national child protection strategy, the responsible agency should advocate for inclusion of CMIS strategies, work plans, and budgets within the overarching government and stakeholder plans.

Resource Mobilization and Financing

The relevant government agency responsible for CMIS implementation should provide costs for CMIS requirements in the overarching child protection strategies collaboratively with the national TWG and mobilize resources within the government and from partners. The critical steps are:

- Provide costs for the CMIS requirements at the different levels from systems development, maintenance, and use
- Work with line ministry to allocate resources within their budget
- Work with the national child protection TWG to map the potential sources of support
- Initiate resource mobilization efforts
- Track the resource utilization of resources as part of mutual accountability

Establish Accountability Mechanisms

Accountability mechanisms provide a basis for answering to various actors and establish responsibility and expectations, monitoring and reporting, and evaluation and feedback. Accountability mechanisms for CMIS should be used in tandem with relevant policy provisions and aligned to the coordinating structures. All relevant actors should be involved in determining accountability mechanisms through the child protection TWG.

To ensure accountability mechanisms, the TWG should:

- Develop a CMIS responsibility matrix: A CMIS responsibility matrix is one of the tools that should be developed to guide the oversight process. The responsibility matrix will break down the specific tasks, outline the government entity/partner responsible for the task, resources required, approximate cost, and timelines for implementation. This responsibility matrix will provide a tool for mutual accountability among the partners and guide regular tracking of CMIS implementation. See Appendix 2 for a sample responsibility matrix used in Kenya. The responsibility matrix will be useful in discerning the expertise required in CMIS implementation for the specific tasks. This matrix should be jointly tracked with all stakeholders on at least a quarterly basis.

- Establish performance monitoring systems: Performance monitoring systems should include monitoring and evaluation frameworks for CMIS policies and strategies, service charters for institutions with CMIS roles, performance indicators for institutions and individuals with responsibility for CMIS, and feedback mechanisms. Application of these monitoring systems will be informed by organizational and system maturity levels. At the nascent level, countries should define the performance indicators for a CMIS and institute regular monitoring of the same. Where systems are advanced, a monitoring and evaluation framework for the CMIS strategy should be in place to guide the process.

- Define rewards and sanctions for CMIS: Sanctions and rewards are considered a culmination of accountability mechanisms. Countries should define mechanisms to reinforce excellence in CMIS implementation and sanctions to deal with non-compliance with the country CMIS strategy/ implementation plan. To be effective, however, rewards and sanctions must be embedded within a clear policy framework—one which is understood and respected by all actors engaged in accountability relationships.

Data

The National Child Protection TWB, working through a technical committee consisting of data experts, should lead the development and implementation of data handling protocols around data governance and data quality. These protocols should be referenced throughout the development and implementation of the CMIS.

The two main categories of data handling protocols are further elaborated in the key steps below.

Adopt and Implement Data Governance Protocols

Data governance entails a set of principles and practices that help to ensure that data is usable, accessible, and protected. CMIS data governance results in improved data security and quality, decreased data management costs, and increased access to data for all stakeholders.

Countries should develop and implement requisite data standards, data access guidelines, data use guidelines, and data sharing agreements for CMIS in line with the existing legal and policy requirements. Recommended guidelines are described in Table 3.

Table 3. Recommended CMIS data guidelines

Data governance guidelines	Key question to ask
DATA PROTECTION GUIDELINES	Is there any formal data protection guideline for CMIS?
DATA FLOW SOP	Has a data flow[2] SOP been defined and shared with all stakeholders?
DATA ACCESS SOP	Do formal procedures exist on data access and dealing with security violations?
DATA CHANGE SOP	Is there any formal written SOP detailing processes and documentation for changes to data collection tools, indicators, processes for development, approval, endorsement, retirement of tools versions, and all matters of version control?
DATA QUALITY SOP	Is there any formal data quality SOP that defines data quality, data quality assurance processes, data quality calendar, tools, roles, and responsibilities with regards to data quality?
DATA SHARING SOP	Is there any formal data sharing SOP guiding how child protection data is shared among the agencies[3]?
DATA VERIFICATION SOP	Is there a formal SOP guiding verification of data in the CMIS and other relevant source documents?

The relevant guidelines should be used to inform other operational and administrative processes such as code of regulations for staff and contractors that have responsibilities in CMIS, TOR for technical working groups, and interagency collaborative agreements.

Develop a CMIS Data Quality Assurance Plan

A technical committee responsible for data should be established within the overarching TWG. This committee should develop and oversee implementation of a Data Quality Assurance (DQA) plan. A DQA plan is used to define the criteria and processes that ensure and verify that the data meet specific data-quality objectives throughout the data lifecycle. A sample DQA plan is provided in Appendix 4.

---

[2] Data flow defines how data moves from the point of collection to storage and roles of the various team members.
[3] Data sharing agreements should be developed based on the SOP whenever there is data sharing.

The DQA plan should be designed to ensure that CMIS data meet minimum thresholds in the data quality dimensions, as listed in Table 4.

Table 4. Dimensions for data quality assurance

Dimension	How it's measured
Accuracy	How well does a piece of information reflect reality?
Completeness	Does it fulfil user expectations of what's comprehensive?
Consistency	Does information stored in one place match relevant data stored elsewhere?
Timeliness	Is the information available when it's needed?
Validity	Is information in a specific format, does it follow business rules, or is it in an unusable format?
Uniqueness	Is this the only instance in which this information appears in the database?

ICT

Development and operationalization of the CMIS is dependent on an ICT environment to facilitate data capture, access, information exchange, and use of the systems. The CMIS should comply with ICT governance, systems development and implementation, and interoperability protocols to ensure that the user and technical requirements—including quality, reliability, stability, and availability of the data—are met. In addition, the agency in charge of child protection and care should have, or be able to source, the expertise of ICT professionals in the sub-domains of governance, infrastructure, and software to ensure appropriate representation within an ICT sub-committee.

The critical steps in strengthening the ICT domain are detailed below.

Develop and Adopt ICT Governance Protocols

ICT governance protocols including standards and guidelines must be observed in the development and implementation of the CMIS. The ICT committees should make sure that a minimum set of documentation is produced to guide the development of the CMIS. The documentation should include technical requirements, CMIS specifications, guidelines, characteristics, and/or procedures that should be aligned to local and international digital standards; for example, International Organization for Standardization (ISO),[4] Institute of Electrical and Electronics Engineers (IEEE) Standards Association,[5] and country-specific e-Government standards. Local standards should be developed through consensus and ratified by leadership. Implementers should be required to adopt and implement standards that are publicly available.

CMIS protocols should, at a minimum, describe the below requirements:

- *Security and Privacy* – Safeguard data, safeguard user identity, and maintain confidentiality
- *Stability* – Return to a steady state when subjected to a disturbance
- *Scalability* – Add resources to the system as the number of child cases and users grow
- *Usability* – Meet the user requirements and ensure the quality of a user's experience
- *Infrastructure Requirements and guidelines* – Developed for CMIS to guide hardware and network minimum standards and preferences
- *Support and Maintenance Guidelines* – Developed to guide ongoing help-desk support and maintenance

---

[4] https://www.iso.org/home.html
[5] https://standards.ieee.org/

Adopt Best Practices in Systems Development and Implementation

Countries should adopt development principles and best practices described in this section to enable software developers and implementers to carry out their roles and responsibilities in the most efficient and effective manner. Digital development principles and best practices that could be used include:

- *The Principles for Digital Development*[6] are nine living guidelines that are designed to help integrate best practices into technology-enabled programs and are intended to be updated and refined over time. They include guidance for every phase of the project life cycle, and they are part of an ongoing effort among development practitioners to share knowledge and support continuous learning.

Figure 2. The principles for digital development

Design with the User
User-centered design starts with getting to know the people you are designing for through conversation, observation. and co-creation.

Understand the Existing Ecosystem
Well-designed initiatives and digital tools consider the particular structures and needs that exist in each country, region, and community.

Design for Scale
Achieving scale requires adoption beyond an initiative's pilot population and often necessitates securing funding or partners that take the initiative to new communities or regions.

Build for Sustainability
Building sustainable programs, platforms, and digital tools is essential to maintain user and stakeholder support, as well as to maximize long-term impact.

Be Data Driven
When an initiative is data driven, quality information is available to the right people when they need it, and they are using those data to take action.

Use Open Standards, Open Data, Open Source, and Open Innovation
An open approach to digital development can help to increase collaboration in the digital development community and avoid duplication of work that has already been done.

Reuse and Improve
Reusing and improving is about taking the work of the global development community further than any organization or program can do alone.

Address Privacy and Security
Addressing privacy and security in digital development involves careful consideration of which data are collected and how data are acquired, used, stored, and shared.

Be Collaborative
Being collaborative means sharing information, insights, strategies, and resources across projects, organizations, and sectors, leading to increased efficiency and impact.

- *The Systems Development Life Cycle (SDLC)* is a multistep, iterative process for planning, creating, testing, and deploying an information system. This process provides a framework for technical and non-technical activities to deliver a quality system that meets user requirements. There are many common SDLC models (e.g., Waterfall, Agile, Interactive), but the government agency in charge of development of the CMIS should use the standards agreed by the ICT Committee.

---

[6] https://digitalprinciples.org/

Figure 3. Phases of the SDLC[7]
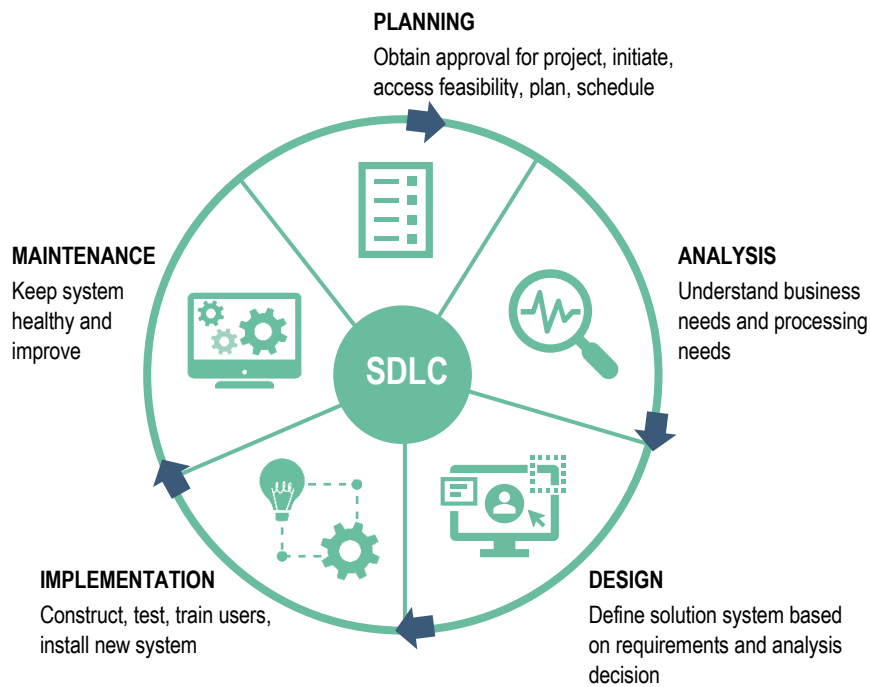
This process of adopting development principles and best practices should result in a high-quality system that meets expectations, reaches completion within time and cost evaluations, and works effectively and efficiently in the current and planned information technology infrastructure.

Promote CMIS Interoperability

The ability to exchange information between CMIS and their subsystems plays a vital role in the achievement of case management of child protection and care goals. As a subset within the broader ICT governance, a common and standardized approach towards CMIS interoperability will not only improve efficiency in data management and accountability but will also enhance data availability for all the actors at global, national, and sub-national levels, especially given the multiplicity of data sources for CMIS data that often reside across different sectors.

The common approach in the implementation of CMIS interoperability should encompass three broad areas:

- **Understand the interoperability ecosystem** – This comprises individuals, systems, and processes that want to share, exchange, and access all forms of information. Local and international institutions, government agencies including law enforcement, education stakeholders, health systems, parents, individuals, researchers, and community-based organizations are potential stakeholders within this ecosystem. Each is involved in the creation, exchange, and use of CMIS information. Reference should be made to existing national or departmental enterprise architecture (EA), which is a framework that governments design to manage and align government agency IT assets, people, operations, and projects with its operational characteristics. EA describes how IT resources will support the government operations and provide benefit. EA usually includes a blueprint of the systems that will exchange data with each other and the data sharing agreement that should be in place. In some countries, EA is ruled by an ICT Ministry or similar agency. In the absence of a defined EA, mapping and understanding of the ecosystem should be done and presented from an architectural point of view. All data systems that collect or transmit CMIS data should be mapped. Specific data sources should also be mapped to the actors within the ecosystem.

---

[7] https://www.tutorialspoint.com

The TWG should develop and then refer to the CMIS interoperability framework. An example of this is provided in Figure 4.

Figure 4. Sample CMIS interoperability framework
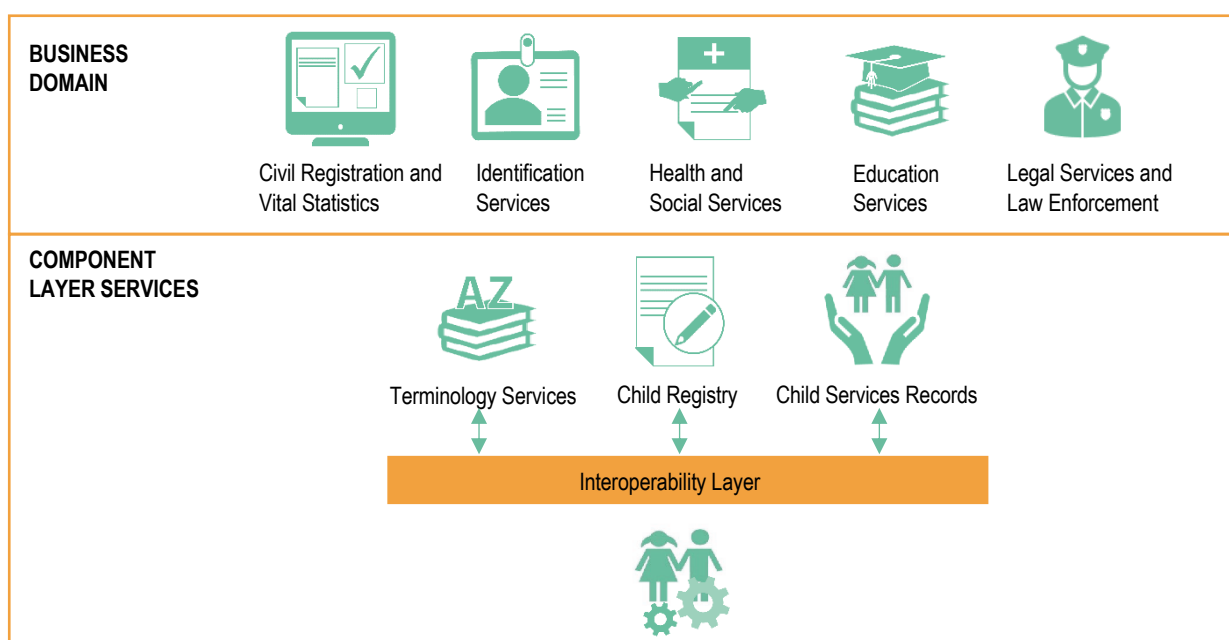
A phased approached towards interoperability should be encouraged by identifying and prioritizing use cases where data coming from external data sources to the CMIS will help case managers gain a more comprehensive view of the child's situation.

- **Develop or adopt interoperability standards** that provide a common language and set of expectations to enable interoperability between systems. CMIS should adopt open standards and follow global and country e-Government interoperability standards. Specific areas of standardization should include:

  o Vocabulary/terminology standards that address the ability to represent concepts unambiguously between a sender and receiver of information, and a fundamental requirement for effective communication. Information systems that communicate with each other rely on structured vocabularies, terminologies, code sets, and classification systems to represent child protection concepts. CMIS are required to adopt the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse,[8] Minimum Standards for Child Protection in Humanitarian Action,[9] and country-specific vocabularies in areas of interest—i.e., health, education, and law enforcement.[10]

  o Transport and messaging standards should be adopted to address the format of messages exchanged between computer systems, document architecture, case templates, and user interface and child data linkage. Standards center on "push" and "pull" methods for exchanging information. Application Programming Interface (API) standards defined in the country-specific EA should also be defined and adopted, where necessary.

---

[8] https://www.unicef.org/documents/terminology-guidelines
[9] https://alliancecpha.org/en/glossary-minimum-standards-child-protection-humanitarian-action-2019-edition
[10] Most countries have adopted the ICD-10 and ICD-11: The International Statistical Classification of Diseases and Related Health Problems (ICD), a medical classification list by the World Health Organization (WHO) for health data.

- **Identifier standards** should be implemented based on National Personal Identifiers, as defined in each country's legal and policy frameworks. Identifier standards provide a universal method to identify entities such as children, case managers, healthcare providers, or healthcare organizations.

- **Privacy and security standards** should be based on country-specific privacy and security laws and privacy and security standards. Recommended standards include Role-Based Access Control (RBAC), an approach to restricting system access to authorized users, and the Advanced Encryption Standard (AES)[11] that specifies a Federal Information Processing Standards (FIPS)-approved cryptographic algorithm.

---

[11] https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf
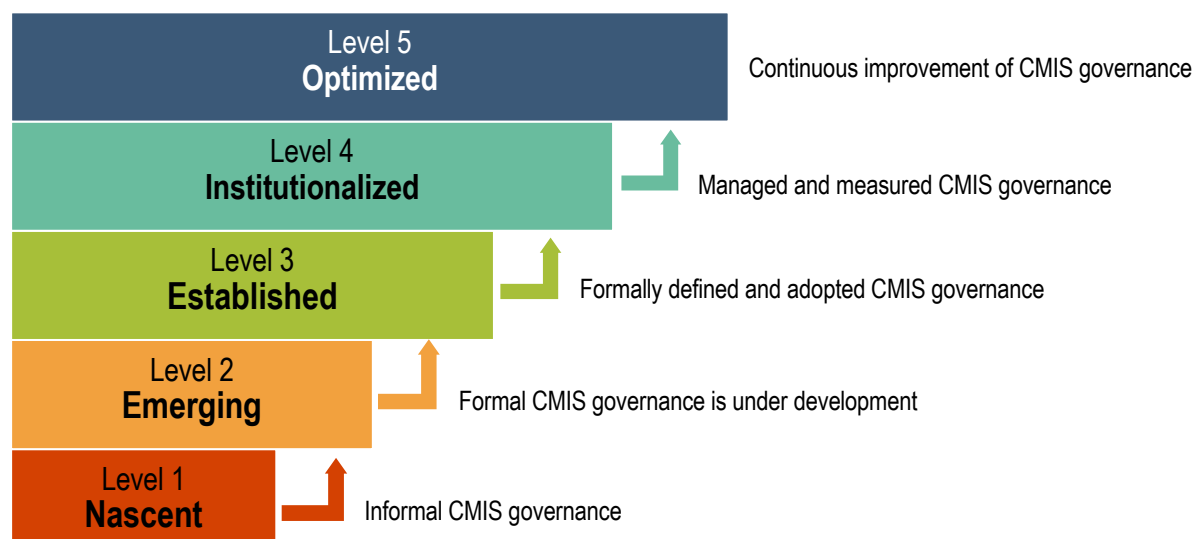
CMIS Governance Maturity Model

A maturity model is a set of structured levels that depict the organizational behaviors, practices, and processes that reliably and sustainably produce required outcomes (Hammond, Bailey, et al., 2010). The CMIS maturity model is a tool that helps countries assess their current maturity levels in CMIS governance, as described in this guidance document. It also supports the identification of the CMIS governance components that countries need to acquire to improve their performance. The gaps identified should be used to inform development of country-level roadmaps towards improved maturity.

CMIS Governance Maturity Levels

The CMIS maturity model is structured as a series of levels that reflect the capability and effectiveness of the country in successfully implementing CMIS governance (Figure 5). The higher the maturity level, the greater the chances of successful implementation of the CMIS at large scale.

Higher maturity levels mean that the CMIS implementation process is more likely to withstand interruptions, such as changes in government structures and staffing, fluctuation of funds, changing legal and policy environments, requirements, data needs, or the effects of rapidly evolving technology.

Figure 5. CMIS governance maturity levels

Level 5 Optimized	Continuous improvement of CMIS governance
Level 4 Institutionalized	Managed and measured CMIS governance
Level 3 Established	Formally defined and adopted CMIS governance
Level 2 Emerging	Formal CMIS governance is under development
Level 1 Nascent	Informal CMIS governance

The CMIS governance maturity level characteristics form the metrics for calculating the CMIS governance maturity levels using the CMIS maturity model toolkit that is provided with this guidance document. These characteristics are grouped according to the main CMIS governance domains described in this guide (Leadership and Coordination, Policy and Planning, Data, and ICT), as illustrated in Table 5 below.

Table 5. CMIS governance maturity level characteristics

Level 1: Nascent	Level 2: Emerging	Level 3: Established	Level 4: Institutionalized	Level 5: Optimized
The country lacks CMIS governance capacity or does not follow processes systematically. CMIS activities happen by chance or represent isolated, ad hoc efforts (informal CMIS governance).	The country has defined CMIS processes and structures, but they are not systematically documented. No formal or ongoing monitoring or measurement protocol exists (formal CMIS governance is under development).	The country has documented CMIS structures and processes. The structures are functional. Metrics for performance monitoring, quality improvement, and evaluation have been developed (formally defined and adopted CMIS governance).	Government and stakeholders adhere to the national CMIS governance processes and follow standard practices. Metrics for performance monitoring, quality improvement, and evaluation are systematically used (managed and measured CMIS governance).	The government and stakeholders routinely review and modify CMIS governance structures and processes to adapt to changing conditions. Full country ownership, implementation, and oversight of CMIS (continuous improvement of CMIS governance).

The Maturity Model Toolkit

The maturity model toolkit that accompanies this guidance document is to be used by decision makers and departmental leads from the country agency responsible for child protection and/or the established coordination mechanism at the national or sub-national level, through a consensus building process. It is advisable to only apply this toolkit after country teams have garnered sufficient understanding of the CMIS Governance Guidelines, as the guidelines form the basis of the metrics referred to in this toolkit. This toolkit should be administered at baseline and after every 3-6 months of implementation of the CMIS Governance Guidelines. Remember to always set a target for the next period of performance.

This toolkit has been developed using a Microsoft Excel template and consists of four worksheets:

1. **Instructions** – This provides the background and instructions for use of the toolkit.

2. **CMIS Evaluation** – This is where a designated representative of the country team undertaking this exercise will enter the maturity levels determined by the meeting participants, based on the characteristics provided. This is the main data entry screen.

3. **CMIS Maturity Score** – This worksheet summarizes the CMIS maturity areas score and provides the final maturity level.

4. **Maturity Characteristics** – This provides an additional view of the Maturity Level Characteristics for reference.

Glossary

API: An Application Programming Interface, or API, enables two different programs to communicate with each other by making some parts of the website code available to developers.

Architecture is the structure and organization of a software application embodied in its components, as well as their relationships to each other and to the environment.

Dashboard: Dashboards are interactive software tools with data visualizations and charts which often provide at-a-glance views of indicators relevant to a particular objective or process. Different types of stakeholders can use dashboards to make decisions based on data.

Data backup: A backup, or data backup, is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.

Data standards are rules by which data are described and recorded. In order to share, exchange, and understand data, we must standardize the format as well as the meaning. Without data standardization, software applications may interpret data differently.

Database: A set of related data and the way it is organized comprise a database. Access to this data is usually provided by a database management system (DBMS) consisting of an integrated set of computer software that allows users to interact with one or more databases and provides access to all data contained in the database (although restrictions may exist that limit access to particular data). The DBMS provides various functions that allow entry, storage, and retrieval of large quantities of information and ways to manage how that information is organized.

Encryption is the translation of data into a code to keep the information secure from anyone but the intended recipient.

ICT refers to information and communications technology (or technologies). ICT involves the distribution of data.

Interoperability allows different software applications to exchange data via a common set of business procedures, and to read and write the same file formats and use the same protocols.

Operating system: An operating system, or OS, is the program that, after being initially loaded into the computer, manages all the other application programs in a computer. The application programs make use of the OS by making requests for services. Microsoft Windows is an example of an operating system.

Programming language is a set of instructions and statements that software developers use to give instructions to a computer. It's used to build software applications.

Public good is a resource or commodity provided without profit to all members of society, typically by a government, institution, or company. Open-source software is considered to be a public good.

Server: Computers that provide data or services to other computers over a network are referred to as servers. Websites and web applications are hosted on servers which then are accessed via the Internet through the user's web browser.

Usability is the degree to which software can be used by its intended users to perform tasks and achieve objectives with effectiveness, efficiency, and satisfaction.

User interface: Similar to the front-end concept, the user interface is the part of a software application that the user sees and interacts with.

References

Cannon, M., Herrera, S., & Mechael, P., (2020). *Case Management Information Systems: Promoting Appropriate Care for Children: A framework for Engagement.* Chapel Hill, NC, USA: MEASURE Evaluation.

Greijer, S., & Doek, J. (2016). *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.* Bangkok, Thailand: ECPAT International. Retrieved from https://www.unicef.org/documents/terminology-guidelines.

Hammond, W., Bailey, C., Boucher, P., Spohr, S., Whitaker, P. (2010). Connecting Information to Improve Health. *Health Aff (Millwood);* 29(2):284-8. DOI: https://doi.org/10.1377/hlthaff.2009.0903.

Herrera, S., Kanimba, A., & Ddumba-Nyanzi, I. (2019). *Assessment of the Children First Software in Uganda: Ability to Capture Priority Information Needs for Alternative Care.* Chapel Hill, NC, USA: 27516 USA: MEASURE Evaluation.

Otieno, P., Mutwiri, J., & Antwi-Boasiako, E. (2020). *An Assessment of the Prerequisites for a Social Welfare Information Management System in Ghana*. Chapel Hill, NC, USA: MEASURE Evaluation.

The Alliance for Child Protection in Humanitarian Action. (2021, September 20). Glossary: Minimum Standards for Child Protection in Humanitarian Action, 2019 Edition [Website]. Retrieved from https://alliancecpha.org/en/glossary-minimum-standards-child-protection-humanitarian-action-2019-edition.

Appendix 1. Sample CMIS Governance Strengthening Activities Roadmap

Quarter 1	Quarter 2	Quarter 3
1. Assign designated office/officer to oversee CMIS 2. Map stakeholders involved in CMIS implementation 3. Identify, map, and establish an inventory of existing policies 4. Develop a road map for adoption and formulation of various CMIS policies and standards	1. Establish a national child protection TWG and develop its TOR document 2. Develop a responsibility matrix to guide CMIS implementation 3. Adopt/develop CMIS ICT policy and standards 4. Sensitize stakeholders on CMIS governance policy and standards 5. Budget and include CMIS requirements in the ministry budgets 6. Map the various systems that need to interoperate with CMIS	1. Develop a CMIS strategy to provide direction in CMIS implementation 2. Establish a sub-national child protection TWG 3. Utilize the National Child Protection TWG for joint planning and review of CMIS implementation 4. Define interagency data sharing arrangements

Maturity Interventions

Appendix 2. Kenya CPMIS Responsibility Matrix Template

CPIMS Investment Pillar	Activities	Resources Required	Timelines	Responsibility Matrix	
				Role of DCS	Role of partners (mention specific role)
Infrastructure					
Data capture					
Data quality and reporting					
Data demand and use					

Appendix 3. Sample Data Use Template

Programmatic Questions	Indicator	Data Source	Method of Analysis	Data Disaggregation	Data Visualization	Frequency	Proposed Action Decisions	Decision Maker	Communication Channel

Appendix 4. Sample Data Quality Assurance Plan

Components	Quarter 1	Quarter 2	Quarter 3	Quarter 4	Responsible	Budgets
1. Prioritize data quality assessments/data quality improvement activities, annual work plan, and county budget						
1.1. Conduct data quality assessments prior to quarterly, biannual, and annual performance review						
1.2. Include data quality assessment/data quality improvement activities in annual work plans						
1.3. Allocate funds for data quality assessment/data quality improvement in CMIS budget line						
2. Conduct regular data quality assessments, data checks/validations, and desk reviews						
2.1. Conduct monthly data checks/validations						
2.2. Utilize desk review approaches to flag data quality issues and inform data quality improvement activities prior to conducting on-site data quality assessments						
2.3. Conduct periodic data quality assessments						
2.4. Develop data quality improvement plans to address gaps identified by data quality assessments, data checks/validations, and desk reviews						
2.5. Document data changes after data quality assessments, data checks/validations, and desk reviews						
2.6. Update CMIS with final verified numbers after data quality assessments, data checks/validations, and desk reviews						
2.7. Conduct data quality forums/meetings or utilize existing forums to share recent data quality assessment findings						
3. Continuously monitor implementation of data quality improvement plans						
3.1. Immediate supervisory level continuously monitors implementation of data quality improvement plans						
3.2. Conduct data quality forums/meetings or utilize existing forums to review implementation status of data quality improvement plans						

Appendix 5. Key Participants

Name	Affiliation	Country
Global TWG		
Narine Rushanyan	Division on Children Related Issues of MOLSA	Armenia
Anahit Hovhannisyan	Department on Provision of Equal Opportunities	Armenia
Angela Ghassabian		Armenia
Anahit Kalantaryan	Division on Children Related Issues	Armenia
Anahit Hovhannisyan	Division on Children Related Issues	Armenia
Karine Badalyan	Division on Children Related Issues	Armenia
Narine Rushanyan	Division on Children Related Issues	Armenia
Tamar Sevadjian	Division on Children Related Issues	Armenia
Araksia Svajyan	National Pedagogical Psychological Center	Armenia
Hasmik Ghukasayan	Palladium	Armenia
Mr phi No		Cambodia
Khauv Paneth		Cambodia
Chandina Sry		Cambodia
Suman Khadka	UNICEF	Cambodia
Daniel Ballesteros Sánchez		Colombia
Abena Dufie Akonu-Atta	Head Office of the Department of Social Welfare in the Ministry of Gender, Children and Social Protection	Ghana
Emmanuel Antwi Boasiako		Ghana
Stuardo Herrera	Palladium	Guatemala
Onyango, Brian	USAID Kenya	Kenya
Anastasia Gruzin		Moldova
Valeriu Galaicu	ICT Unit	Moldova
Vasile Postolachi	Electronic Governance agency	Moldova
Vitalie	D4I/Palladium	Moldova
Camelia Gheorghe	D4I/Palladium	Moldova
Octavian		Moldova
Gilbert MUNYEMANA	NCDA/MIGEPROF	Rwanda
Marius Ange Marius UWURUKUNDO	NCDA/TMM	Rwanda
James NDUWAYO	NCDA/TMM	Rwanda
Declercq ZANINKA	NCDA/MIGEPROF	Rwanda
Thierry MUGIRANEZA	NCDA	Rwanda
Alain Placide NSABIMANA	NCDA	Rwanda
Patricia LIM AH KEN	UNICEF	Rwanda
Uwitonze, Fils	Palladium	Rwanda
Shafiq Butanda	Department of Youth and Children Affairs (DYCA), MGLSD	Uganda
Susan Kajura	Batwana, ICYD Activity	Uganda
Irene Oluka	UNICEF	Uganda
Fred Opok	USAID	Uganda
ETOMA Charles Onzima	MGLSD	Uganda
Barbra Aber	CRS	Uganda
Emmanuel Yeka	IT unit, MGLSD	Uganda

Name	Affiliation	Country
Majwara William	IT unit, MGLSD	Uganda
Charles Kavuma	USAID/Strategic Information Technical Support (SITES)	Uganda
Jamie Gow	USAID CECA	US
Seghan Haile	USAID OHA	US
Allison Connolly	Palladium	US
Ismael Ddumba Nyazi	Palladium	Uganda
Molly Cannon	Palladium	US
Kenya Pilot		
Salome Waithaka	DCS – Nakuru	Kenya
Alice Wanyonyi	DCS – Nakuru	Kenya
Collins Oduor	DCS – Nakuru	Kenya
Viola Yego	DCS – Nakuru	Kenya
Agnes Makena	DCS – Nakuru	Kenya
Irene Chemailan	DCS – Nakuru	Kenya
Eunice Njeri Njuguna	DCS – Nakuru	Kenya
Samuel Ochieng	DCS – National	Kenya
Joyce Nyaboga	Palladium – Tupime Kaunti Project	Kenya
Polycarp Odoyo	Palladium – Tupime Kaunti Project	Kenya
George Gititu	Palladium – Tupime Kaunti Project	Kenya
Fredrick Onyango	Palladium – DIAS	Kenya

Data for Impact
University of North Carolina at Chapel Hill
123 West Franklin Street, Suite 330
Chapel Hill, NC 27516 USA
Phone: 919-445-9350 | Fax: 919-445-9353
D4I@unc.edu
http://www.data4impactproject.org