International Labour Organization
issa INTERNATIONAL SOCIAL SECURITY ASSOCIATION
DEVELOPMENT PATHWAYS
United Nations | Department of Economic and Social Affairs

Governance of social protection systems: a learning journey

Module #2: Information and Communication Technologies & Data

Governance of social protection systems: a learning journey

Module #2: Information and Communication Technologies & Data

Governance of social protection systems: a learning journey
Module #2: Information and communication technologies and data

Language: English

ISBN: 978-9-22-035072-0 (Web PDF)

information technology / communication / data analysis / data management / social protection

The designations employed in ILO publications, which are in conformity with United Nations practice, and the presentation of material therein do not imply the expression of any opinion whatsoever on the part of the International Labour Office concerning the legal status of any country, area or territory or of its authorities, or concerning the delimitation of its frontiers.

The responsibility for opinions expressed in signed articles, studies and other contributions rests solely with their authors, and publication does not constitute an endorsement by the International Labour Office of the opinions expressed in them.

Reference to names of firms and commercial products and processes does not imply their endorsement by the International Labour Office, and any failure to mention a particular firm, commercial product or process is not a sign of disapproval.

Information on ILO publications and digital products can be found at www.ilo.org/publns

Produced by the ILO in partnership with UNDESA and with technical support from ISSA and Development Pathways.

Graphic and typographic design, manuscript preparation, copy-editing, layout and composition, proofreading, printing, electronic publishing and distribution.

The ILO endeavours to use paper sourced from forests managed in an environmentally sustainable and socially responsible manner.

Cover photo: © Hadyn Yah

Introduction

This learning module is part of a series of working papers "Governance of social protection systems: a learning journey" developed in the context of the project "Achieving SDGs and ending poverty through Universal Social Protection", implemented from January 2019 until June 2021 under the 2030 Agenda for Sustainable Development sub-fund of the United Nations Peace and Development Trust Fund (UNPDF). The project is jointly implemented by the Division for Inclusive Social Development of the United Nations Department of Economic and Social Affairs (UN DESA), and the Social Protection Department (SOCPRO) of the International Labour Office (ILO), in the framework of ILO's Global Flagship Programme for Social Protection Floors and as part of the overall campaign for Universal Social Protection (USP 2030).

The project has pursued a two-fold strategy. In two focus countries, Pakistan and Cambodia, the ILO offices provided technical support to strengthen capacities of institutions and practitioners on different aspects identified as critical in social security governance.

Simultaneously, at global level, the project has developed a knowledge base of good practices as well as learning modules in order to better support policy makers in their capacity to take strategic decisions in the field of social protection. In this sense, it is important to acknowledge the partnership with the International Social Security Association (ISSA) and Development Pathways, which, along with the ILO and UNDESA, has produced a learning approach at the crossroads of policy and technicality. The project has thus attempted to highlight in a practical way the main drivers of different operational components inherent to all systems, starting with three core topics:

- **Module #1: Coordination**
- **Module #2: Information and Communication Technologies & Data**
- **Module #3: Compliance and Enforcement of Legal Frameworks**

In order to deepen this learning journey rooted in reality but driven by the ideal of social protection for all, the project has proceeded in three phases by developing successively:

- A global research, including analysis and case studies, notably in Argentina, Kenya, Mauritius and Fiji, and a specific paper on the Chinese model;
- An online experts' meeting to share and discuss those learnings with specialists, practitioners and decision-makers in the South;
- Three learning modules bringing together this information in a synthetic form, with a view to the further development of a training programme, notably with the ILO's International Training Centre of the ILO in Turin (ITC/ILO).

International Labour Organization

United Nations | Department of Economic and Social Affairs

issa

DEVELOPMENT PATHWAYS

Governance of social protection systems: a learning journey

Experts meeting webinar

Date / 25 June 2021
Time / 10:00-11:40 CAT / 16.00-17:40 CST
Register here and select your topic: cutt.ly/splearning

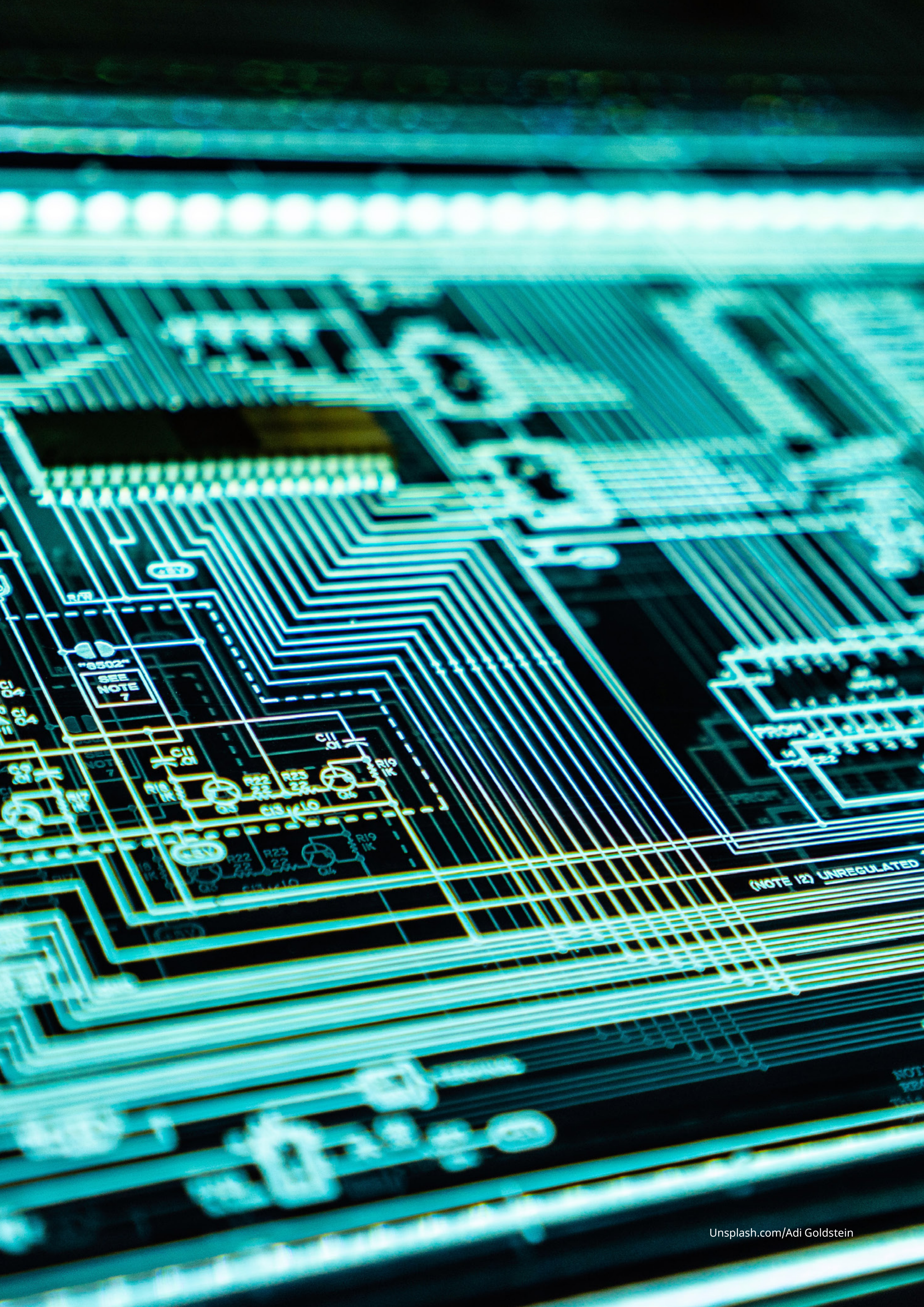
Acknowledgements

The series “Governance of social protection systems: a learning journey” was prepared by the department of social protection (SOCPRO) of the ILO under the coordination of Jean-Louis-Lambeau with the contributions and policy-driven orientations provided by Valérie Schmitt, Pal Karuna, Christina Behrendt, Veronika Wodsak, André Picard, Maya Stern-Plaza, Kroum Markov, Luisa Fernanda Carmona Llano, Mira Bierbaum, Simeon Bond, Aurélie Klein, Rabia Razzaque, Saad Gilani, Luis Frota, Ingrid Christensen, Jie Yu Koh , Sokgech Heng, Nuno Cunha, Mariko Ouchi, Rodrigo Assumpção, Kagisanyo Kelobang, Patience Matandiko, Valentina Barca, Robert Venne, Oleg Serezhin, Wenyan Yang, Raul Ruggia-Frick, Stephen Kidd, Shea McClanahan, Richard Chirchir, Alexandra Barrantes, Sarina Kidd, David Hillson, Carlos Galian, Dianne Dunkerley, Alia Shahid, Nazar Ali, Hong MI, Qiyini MA, Huilin MIAO, Rong YAN, Ziqi YU.

The author of the module #2 on Information and Communication Technologies & Data is Rodrigo Assumpção (ILO).

This module owes much to a series of strong collaborations going back a long way:

- The International Social Security Association (ISSA), whose guidelines, and in particular the one on "Information and Communication Technology ", are intrinsically linked to this module, not only in terms of content, so close to the issues at hand, but also because many of these reflections were developed during the courses on the ISSA ICT Guidelines organized by the International Training Center of the ILO (ITCILO) in Turin: students, colleagues and ITCILO staff, each contributed to bringing these considerations to light ;
- The Social Protection Interagency Cooperation Board (SPIAC-B) was also extremely helpful in sharpening many of the concepts presented here. All who participated in these discussions were extremely generous in sharing their expertise;
- The Social Protection Approaches to COVID-19 - Expert advice helpline (SPACE), through its manager, Valentina Barca, generously allowed the use of its illustration of the social protection constellation that inspired some of the core reflections of the module.
- The Social Security Information Technology Enterprise - DATAPREV for providing the practical knowledge that fueled the work of this module in the implementation of governance and management processes.



Unsplash.com/Adi Goldstein

Contents

▶ © Unsplash.com/ Lagos Techie

Decipher me or I will devour you

The governance and management of ICT and data in social protection

This module seeks to illustrate the central role of governance and management of both information and communication technologies (ICT) and data in social protection institutions. There is a vast and far-reaching discussion and literature available concerning variations on social protection policies, the struggle to expand coverage and the efforts to consolidate the right to social protection for all. The governance and management of the concrete applications of these policies – especially the use of technology in the daily operation of social protection – could benefit from more discussion and study.

More discussion may be especially helpful for low and middle-income countries, in which a consolidated ICT industry might not be established; the use of technology in government institutions may be dispersed and uncoordinated; and the availability of trained individuals to operate, develop and monitor the necessary applications and infrastructure may be either lacking or unaffordable.

These challenges have become central to social protection due to the increasing importance of data and information in implementing social policies. While it is true that only comprehensive and well-structured policies and strong institutions can ensure social protection rights, it is also true that the best-designed policies will not succeed if they are not adequately implemented and managed. Moreover, the success of social protection policies depends increasingly on the quality of ICT and data and their effective governance and management, which determine the quality of the results obtained through their use.

This module examines the structures and procedures that need to be implemented in order to ensure that ICT and the organizational entities responsible for its operation are focused on strategic institutional objectives and do not become isolated, self-referential, overreaching, underperforming, resource-intensive entities that the institution can neither control nor discard.

The governance and management of ICT and data enables the control of the operational capacities of social protection institutions, as well as the sharing and integration of data from other entities. Data and information are the fundamental assets that enable registration, collection, payments and operations in a social protection context. The data gathered also constitutes a strategic public asset, which is usually a prime candidate to be included in the national data infrastructure.

The data gathered by the institution must be understood in all its potential; organized strategically to allow legitimate data-sharing between systems and institutions; constantly improved through the use of data-quality procedures; and properly classified and stored, with a profound awareness of the increasing privacy and security concerns around the use of personal data.

This means that gathering, preserving, using, analysing and sharing data is the central role of ICT in the social protection organization. This requires the continuous application and evolution of governance and management activities. Beyond assuring that the technology is available, there is a need to ensure that the necessary human resources, intellectual resources, implemented processes, funds, policy decisions, data and time are also available.

Institutions should implement in a comprehensive manner the governance and management processes that align their ICT processes with their institutional objectives. They should clearly define the related responsibilities and decision-making processes in the organization and establish a strategic long-term plan for ICT that conforms to institutional goals. This plan should analyse opportunities for innovation or improvement; establish or update the definitions and implementation of the enterprise technological architecture; and align them with current and future business process needs.

▶ © Oedipus and Sphynx, Walter Crane

There is a delicate but crucial balance between institutional governance, ICT governance and ICT management. **Institutional governance** defines the directives, monitoring and incentives for transparency, stakeholder involvement, accountability and responsibility over the financial, physical, human, intellectual property, ICT, informational and relational assets of the organization. **ICT governance** generally focuses on who decides what, when and how, defining what are the right things to be done in terms of ICT, as well as how to do things right for a given project. It helps the institution to monitor ICT decisions and balance critical decisions on investments, infrastructure, architecture, ICT principles and business process alignment. **ICT management** defines the specific processes required for planning, developing, executing and monitoring the activities necessary to reach the strategic goals, and policies established by ICT and corporate governance.

This module starts by exploring the broad ICT governance and management issues around the organization, implementation and operation of systems. This means defining principles, strategies, processes and roles related to ICT activities in general, as well as managing data, infrastructure and investments and ensuring business continuity in the technological environment. The module emphasizes the need for high-level governance and strategic planning and explores some of the International ICT standards and frameworks available for reference. Then it examines the facilities, infrastructure and capacity-management procedures, the disciplines of information security management and change management, and the complex process of acquisitions, investment and vendor management in ICT.

The second part of the module reviews the governance and management of management information systems (MISs). Most social protection organizations either have gone beyond paper-based processes or are actively trying to implement digital systems in order to execute their mandates. The result is that all aspects of social protection, including policymaking, oversight, scheme management and the delivery of benefits and services, are permeated by ICT.

In this context, the MIS is usually the structuring core of service delivery that makes policies and programmes tangible. It operates as the interface between business processes, information, beneficiaries, staff and external organizations. The MIS is therefore the foundation of effective social protection service delivery and is crucial for ensuring the potential fulfilment of rights. These systems execute business processes such as the registration of contributors and beneficiaries; contribution collection; collecting declarations and payroll information; adjudication of eligibility; receiving benefit applications; accounting and finance, including for the calculation and payment of benefits; case management, including appeals and complaints; and the monitoring and evaluation of operational processes.

The final part of the module deals with data and data governance, which has become one of the central issues of our time. Discussions of data privacy, data security, data ownership, data usage, data governance and data management reach us daily. Everywhere data is being collected, processed, analysed, used, reused and commercialized. New uses and new forms of data are being created in real time and at a granular level. The speed of all these processes is increasing and shows no signs of diminishing. In the social protection context, the situation is no different and the issues of master data, data quality, data analytics, data operations, data privacy and data-based management are examined.

As in the mythical riddle posed by the Sphinx, social protection organizations need to decipher their ICT and data operations or run the risk of being devoured by the growing budgetary demands and diminishing results of their ICT systems. The answer to the riddle lies in implementing governance and management processes to daily increase the capacity, efficiency and effectiveness of their use of technology. The continuous process of improving the understanding, maturity and ability to harness ICT and data is a necessary condition that – coupled with sound and comprehensive social policies – will enable institutions to ensure social protection rights for all.

© Unsplash.com/Mayofi

I. The governance and management of information and communication technology

Information and communication technology (ICT) or information technology (IT) has become pervasive in most aspects of our societies all around the globe. This pervasive presence and determining influence seems to be both increasing and accelerating in nearly every aspect of modern human existence. This presents new challenges to social protection institutions, both in their internal arrangements and use of ICT and in meeting the demand to change and evolve their policies.

ICT is instrumental for all aspects of the mission of social protection institutions – providing services; managing operations; ensuring the efficiency of processes; analysing actions; and answering to constituents. In recent years, the demand for a broader and more intensive use of technology in social protection has grown in response to the challenges arising from institutional evolution; changes to policies and programmes; the increasing need for integration and coordination among different programmes; and global emergencies such as the COVID 19 pandemic.

However, the effective use of ICT remains one of the daunting challenges facing social protection institutions. The complexities of ICT systems are increasing and the material resources and human capacity necessary to engage with these complexities are not increasing in the same pace. Unfortunately, this is often accompanied by frustration when expectations for the use of ICT are not fulfilled.

The factors that contribute to this difficult situation include:

- increasing expectations for the digitalization of transactions;
- the need for more flexibility and faster delivery of policies to respond to changes in social protection and society at large;
- a quantitative deficit in human capacity as the demand for ICT professionals far exceeds the numbers of these professionals available in most country contexts;
- a qualitative human capacity deficit as much of the new technology introduced far outpaces the retraining abilities of staff;
- an ICT market that invests far more in selling licenses than in providing support and training for the products sold; and
- an ever-growing demand for ICT budget allocation.

The list goes on; these are just a few examples of contributing factors that must be continuously understood and addressed by the governance and management process.

It is also important to recognize that, especially when well applied, ICT will induce change. It will affect the way the work is conducted, the distribution of labour and the business processes. It will change the way knowledge is gathered, used, retained and disseminated, both internally and externally to social protection institutions. It will change power structures and their distribution within and between institutions and their stakeholders. All this change is at the same time disruptive and necessary for positive institutional evolution and has to be effectively managed.

ICT itself is in an accelerating flux of innovation and evolution, driven by new developments in technology; market forces; the network effect of growing ICT pervasiveness; and various challenges in the deployment environment, such as the COVID-19 pandemic. This hectic pace of evolution and change frequently leads to fear and uncertainty regarding the cost–benefit equation and the best approaches to successfully govern and manage the necessary and prevalent use of ICT in social protection.

International ICT standards and frameworks

The widespread application of ICT across all societies and activities has given rise to the development of many international standards and frameworks to orient its use and application. Social protection institutions should use these standards extensively, not only to avoid “reinventing the wheel” but also as a means to enhance their institutional capacity to cooperate and interoperate with peers, stakeholders, the ICT market and society in general, using global knowledge and experience.

The standards produced by the International Organization for Standardization (ISO), especially ISO/IEC 38500, are a good starting point. ISO/IEC 38500 defines six high-level principles for “good corporate governance of IT” and focuses on the role of high-level authorities and their responsibility concerning ICT governance. The frameworks present in the Control Objectives for Information and Related Technology (COBIT®) are process-based and cover general ICT governance and management. The IT Infrastructure Library® (ITIL®) is a set of best practices recommendations to manage the ICT service life cycle in relation to business requirements. The Data Management International (DAMA-DMBOK) covers data management activities. The Capability Maturity Model Integrated (CMM/CMMI) addresses software development. Other relevant standards and framework organizations are OASIS, W3C, OMG and Dublin Core, which have produced technical standards on interoperability, metadata and semantic and web-related technologies.

Especially relevant to social protection institutions are the International Social Security Association (ISSA) ICT guidelines, which provide extensive practical orientation on the governance and management of ICT and were prepared specifically with social protection institutions in mind.

These international standards and frameworks are examples of the ample resources available to social protection institutions that can point to proven and tested procedures for governing and managing the complex range of ICT usage.

Governance and management

The governance and management of ICT in social protection is concerned with the organization, implementation and operation of systems. This means defining principles, strategies, processes and roles related to ICT activities in general, as well as managing data, infrastructure and investments and ensuring business continuity in the technological environment.

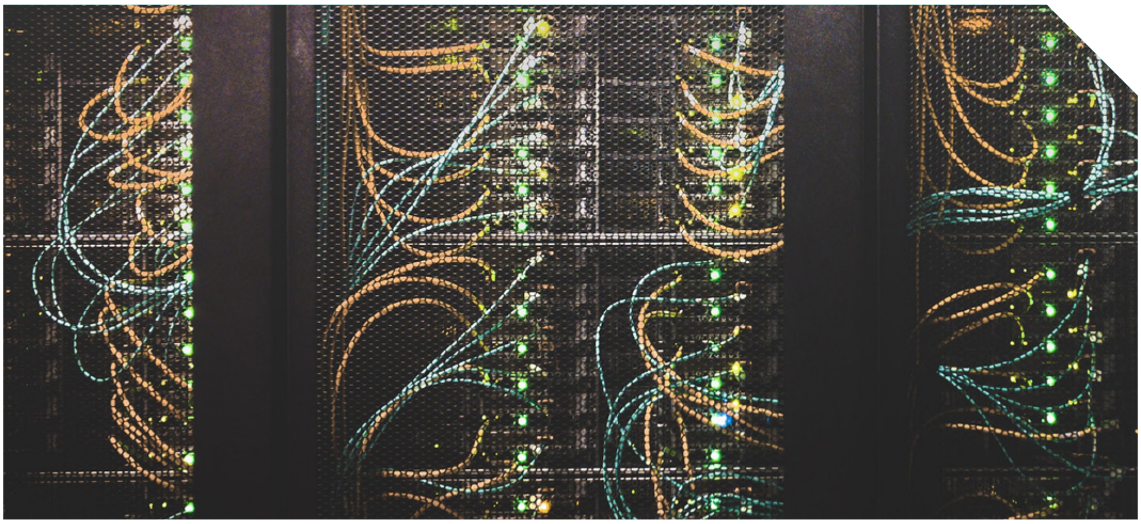
There is a delicate but crucial balance between institutional governance, ICT governance and ICT management:

Institutional governance defines the policies, monitoring and incentives related to transparency, stakeholder involvement, accountability and responsibility for financial, physical, human, intellectual property, ICT, informational and relational assets. It is a broad mandate that determines the strategies that will orient institutional development over time.

ICT governance generally focuses on who decides what, when and how. It defines what are the right things to be done and how to do things right. It helps institutions to monitor ICT decisions and balance critical decisions on investments, infrastructure, architecture, ICT principles and business process alignment. ICT governance decisions formalize the relevant goals for ICT-related activities.

ICT management defines the structure, processes and controls for planning, developing, executing and monitoring the activities necessary to reach the strategic goals and policies established by ICT and corporate governance

ISO/IEC 38500 defines the governance of ICT as: “The system by which the current and future use of IT is directed and controlled, Corporate Governance of IT involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve plans”. This includes the strategy and policies for using ICT within an organization.



▶ © Unsplash.com/Sammy Yayo

The standard is based on the following six principles for orienting good corporate governance of ICT.

Establish responsibilities. Individuals and groups in the organization know their responsibilities in terms of both supply and demand of ICT. Those with responsibilities also have the authority to meet them.

Strategy. Institutional business strategies should be aligned with the institutional ICT possibilities and all ICT within the organization should support the business strategies.

Acquisition. All ICT investments must be made for valid reasons with appropriate analysis. There must be regular monitoring to assess that there is appropriate balance between benefits, opportunities, costs and risks, in both the short and long terms.

Performance. ICT use must lead to institutional benefits, providing the services, levels of service and service quality to meet current and future business requirements.

Conformance. ICT use must help ensure that business processes comply with legislation and regulations. Policies and practices are clearly defined, implemented and enforced.

Human behaviour. ICT policies, practices and decisions respect human behaviour and acknowledge the needs of all the people in the process.

These principles touch most aspects of institutions' activities and can only be applied with the involvement of not only ICT professionals and technical staff but also the staff involved in managing administrative, audit, human resources and business processes, together with the institutions' authorities.

Based on these principles, ICT governance will evaluate institutional objectives and goals in order to determine the priorities and actions to be undertaken, monitoring performance and compliance in light of the formalized plan. ICT management will focus on planning, building, executing and monitoring activities aligned with the direction set by ICT governance.

The size, complexity and impact of social protection work usually dictate that these institutions must have a long-term perspective on ICT and its usage. The crucial roles these institutions have in achieving the Sustainable Development Goals and addressing the many emerging global challenges, as well as the increasing complexity of the programmes they implement, demand the use of reliable and rigorously managed ICT services that can deliver services with quality and continuity. It is difficult to imagine let alone implement relevant social protection efforts without extensive use of ICT; it often determines the limits between what can and cannot be done.

ICT governance and management can help institutions to take control of their processes, improve their performance and engage with the complexities of ICT. This is crucial in order to understand and face financial and technological dependency implications, as well as the multiplicity of actors, products and services in ICT. The development and operation of social protection programmes need rigorous and standardized approaches to achieve coordination and service quality.

The need for high-level governance

The decisive importance of ICT governance demands that it involve the highest levels of institutional authority. The responsibilities for the administration of such crucial resources, which are an indispensable enabler for the provision of benefits and services, cannot rest solely with ICT staff. The situation is somewhat ironic: ICT has become too important to be left solely in the hands of ICT staff. This means that since the strategies and objectives of social protection institutions are critically affected by the decisions concerning ICT, these decisions must ultimately be the responsibility of those with the high-level institutional authority to provide direction.

The precise format of high-level authority can take many forms – a Board, a CEO, a President or a Director-General. If this authority is well informed about ICT, so much the better. However, if this is not the case this authority should require ICT staff and management to explain in a detailed manner not only the proposals but also the consequences of their choices and strategies. This communication initiative can then be expanded beyond high-level authorities to the whole institution, thereby enhancing the understanding and coherence of ICT governance and management decisions.

Strategic planning

Social protection organizations are not ICT organizations but they increasingly depend on effective ICT usage. Once institutions have established adequate responsibilities and decision-making processes, they should formalize an ICT strategy that is aligned with their institutional strategy. There are many methodologies and processes that can be followed with reasonable results, but perhaps the most important element of the ICT strategy is its long-term scope and its focus on continuous incremental improvement.

In social protection institutions, the gathering, preservation, use, analysis and sharing of data is the central role of ICT in the Organization. To fulfil this role, continuous governance and management activities are a key enabler. Beyond assuring that technology is available, there is a need to ensure that the necessary human resources, intellectual resources, implemented processes, funds, policy decisions, data, understanding of data and time are also available.

The classic planning cycle proposes strategic objectives that are feasible within the allotted time frame and relevant for the evolution of ICT operations. This is followed by rigorous implementation of planned activities; monitoring of implementation to improve the process and understand the changes brought by the planned activities; and closing the loop by adjusting strategic objectives in the light of the new context created by implementation of the plan. This continuously repeated cycle is the best way to harness the desired positive results of establishing an ICT governance and management process.

Clear governance and management decisions will allow for the elaboration, understanding and communication of the ICT strategy, which should reflect:

- the governance and management framework that will be adopted to achieve the desired outcomes;
- the organization's current business processes or standard operating procedures and ICT environment;
- the institutional issues that drive change and the projects that will be implemented to address them;
- the measurable outcomes and deliverables that will be achieved by implementing the strategies and projects outlined;
- the ICT investment budget, which should reflect potential opportunities for ICT to drive change and support the organization;
- resource management (budgeting and costs, human resources, suppliers, assets and service agreements), service quality management and risk management;
- facilities, infrastructure and ICT platforms;

- the demands and requirements arising from new systems and the evolution of implemented systems, including an ICT architecture that allows for modular and interoperable development of databases, transaction engines and interfaces;
- security management processes;
- change management process, including risk assessment; and
- acquisitions and vendor management processes.

The list above is not complete and illustrates the complexity of the issue at hand and the importance of addressing it in a continuous and incremental manner. Since this is not a pain-free endeavour, the application of strategic ICT planning that is coherent with the international standards mentioned above requires significant institutional effort and the willingness to face challenges to organizational culture and processes. The impact of these changes can become an obstacle to the planning and implementation of the ICT governance and management process. To overcome these obstacles, the institution must consider the long-term scope of its objectives and goals and recognize that the most important outcomes will result from changes in institutional culture and a cumulative increase in the institutional capacity to govern and manage ICT.

ICT Service Delivery Management

The delivery and support of ICT services enable and sustain the delivery of the social protection services that the organization provides. This is where policy and scheme design come together with staff and the people who receive social protection services to coalesce into a social protection outcome, mediated by ICT. Service delivery aims to provide defined and measured levels of service to users, encompassing all systems implemented by the institution. It is through service delivery that the institution, its peers and society perceive the value provided by the hardware, software, telecommunications and business process in general.

Service delivery must provide users with access to the services offered by the institution, which should happen through a variety of channels in order to provide for multiple groups of users. It must ensure that access is granted only to those authorized to interact with these services. It must minimize the occurrence and impact of any interruption of ICT systems and any resulting impact on the services provided. It must ensure that the organization's business processes are resilient and capable of continuing the operation of key processes and preserving the availability of information in the event of significant disasters or disruptions. Through effective and efficient use of ICT, social protection services and the systems that support them must be seen as trustworthy and capable of delivering specific functions.

In order to attain these objectives, service delivery covers the systems and services life cycle, including planning, design, development, operations and maintenance. ICT service delivery management provides a standardized framework to manage software applications, technical issues, system operations, change requests and incidents. The most relevant international standards for referral are ISO/IEC 22301, COBIT® and ITIL, as well as the ISSA guidelines on ICT.

The steps to implement service delivery management are similar to those described previously for other disciplines. The services required by the different business units must be identified, listed and prioritized. This should be done in consultation with all the involved stakeholders to ensure that it actually addresses all institutional needs. Another useful action is to classify the ICT services, whether they relate to business processes and systems or to commodity ICT services, such as providing and supporting desktops, handhelds, printers and so on.

The following prioritized list should be communicated throughout the organization to disseminate not only the list and priorities but also the criteria and objectives of the service provision. Once the objects of the ICT service delivery management process are communicated in the organization, those responsible should develop and execute an action plan to address short- and mid-term improvement needs. These actions and subsequent results must be monitored, measured, evaluated and communicated in order to restart the cycle with a perspective of continuous improvement.

ICT service delivery is a continuous balancing act and those responsible will always have to make difficult choices between conflicting objectives. System stability often conflicts with timely responsiveness, while quality will usually be opposed to cost and available budget, and the decisions on how to react to issues that arise are often obstacles to anticipating problems by acting proactively.

These persistently difficult choices have to be made in alignment with the institutional goals and objectives and with the adequate participation of the organization's decision-makers, bringing us back from the realm of management to the realm of governance.

Facilities, infrastructure and capacity management

Among the fundamental elements to be considered in the ICT environment are the physical installations where the hardware and servers that contain the ICT systems will be located. This is often the first challenge in many institutions – how to administer the facilities, infrastructure and capacity that support the hardware of the institutional ICT systems. This is a complex issue since the physical environment must be protected from variations in temperature and humidity; rendered secure from unauthorized access; provided with a reliable energy source; and protected from disasters such as fire and flooding. All these elements related to the critical nature of the information and data stored will probably determine a need for redundancy and contingencies for each of the environmental infrastructures used. It is clear that even before starting on the hardware itself, there is already a lot of complexity and there are associated costs to manage. Maintaining a high-quality environment for ICT infrastructure is a crucial starting point for the ICT governance and management processes.

However, the high-level institutional objective is that the systems, information and data should be stored in a manner that meets professional industry standards. Having and maintaining some kind of data centre may be the only alternative available for social protection institutions in many countries. However, other alternatives are becoming increasingly available and should always be assessed.

As many governments face the challenges of their overall ICT governance and management processes, some are establishing national government data centres that can accommodate the systems of social protection institutions. In many countries, commercial alternatives for hosting both hardware and systems may be available. As with any acquisition and contracting, detailed cost–benefit analysis is necessary, but this should be conducted with a strategic long-term perspective.

An increasingly available option is to contract a cloud provider, which can offer an infrastructure, a platform or software as a service (IaaS, PaaS and SaaS respectively). Such options provide flexible, scalable and increasingly affordable on-demand ways to provide capacity to run and operate ICT systems.

Many of the recurrent concerns relating to cloud services focus on the fact that the services are based outside the country and that critical social protection data would then be stored outside the borders and jurisdiction of the country. While relevant, this concern should be balanced with the fact that, unless the institution has access to an adequate data centre, the greater and more immediate threat to the institutional data will come from deficient infrastructure rather than the risk of loss of control coming from a foreign-based cloud-provider.

As with most ICT governance options, rigorous cost–benefit analysis must be balanced against compliance with laws and regulations and strategic choices. These choices can have profound consequences and impacts. Establishing a data centre and buying all the associated facilities and hardware require large upfront investments and relatively lower maintenance costs. Contracting this capacity as a service, will greatly reduce the initial and recurrent investments but will raise considerably the operational costs. The ability to conduct a financial analysis of the total cost of ownership alongside the strategic aspects of these various options is a relevant institutional capacity that must be nurtured.

Once the strategic choices are clear, institutions must establish a capacity management process to administer their ICT infrastructure capacity in close alignment with their business needs, ensuring business process availability and performance requirements. The institutional objective here is to balance business demand affecting the demand for services with service demands affecting the demand on infrastructure.

This process starts by identifying and prioritizing systems according to their availability and performance requirements. This is consolidated in an actionable capacity management plan that defines all the infrastructure configurations in the hardware and software components that support the ICT systems. The sequence continues by defining the services to be provided with their attending service-level agreements (SLAs); implementing the procedures that will provide the performance and capacity of the infrastructure elements; and implementing service-desk activities and incident and problem-management actions related to ICT capacity. The process also includes the gathering and analysis of information on service capacity, service usage and service performance. As this cycle develops, the growing maturity of the capacity management process will allow ICT management to exert control over this foundational aspect of its operations.

ICT operations management

Within the broader framework of service delivery management, special attention is necessary for the discipline of operations management. The complex task of maintaining ongoing ICT operations and service delivery capacity while implementing new versions, improvements and even new systems is daunting. To face them, rigorous governance and management processes are the most potent tool at hand.

ICT operations management is responsible for the operations required to deliver the agreed level of ICT services to the organization. It consists of daily activities and procedures for running the systems responsible for social protection operations, back-end processes, and corporate and administrative functions. Operational processes such as administering infrastructure availability and capacity, as well as system changes, configuration, releases, patches, deployments and so on, are managed together with many interconnected operating parts, such as storage; databases; directories; middleware; networks; virtualization solutions, back-up solutions, to name a few. This challenge grows exponentially with every new element added.

To address this complexity, one of the key elements is monitoring and control of the operational status of all these elements and establishing procedures that allow appropriate corrective action when needed. This is best accomplished by setting up a central point with standardized methods that, in turn, will require additional systems that also need to be monitored. In ICT operations, complexity tends to increase.

ICT operations management usually occurs in a tense and high-pressure environment. The responsibility of keeping the systems up and running while at the same time preventing future problems and implementing the necessary new or evolved systems is challenging. Here, the inevitable trade-offs between the need for change and the need for stability, the limited resources and the growing demands and expectations for ICT services are felt most acutely. Because of this, it is here also that the discipline and standardized practices of ICT management are most essential.

The organization should establish service-level agreements (SLAs), both internal and external, in order for the ICT operations management processes to run in an efficient manner. These SLAs will be the benchmark for monitoring and control and will also act as milestones for the continuous improvement process. They consist of a constantly evolving set of formal statements that cover the scope, operating times, service performance and other relevant criteria to define, understand, document, monitor, measure, review and plan the level of provision of ICT services.

Planning the operations management process based on defined SLAs usually means conducting regular gap analysis between business process requirements and available services. This allows the ICT management team, in constant consultation with the business process stakeholders, to identify the business requirements and translate them into ICT requirements. With these in hand, a clearer picture of the hardware, software or infrastructure upgrades necessary can be prioritized, budgeted and planned in order to meet the quality of service needs and capacities of the institution.

Managing events, problems and incidents

In ICT management, an **incident** is a singular and unplanned interruption or a sudden significant reduction in the performance of an IT service. An **event** is a lesser change in the state of the system or service in the IT infrastructure. Events and incidents are perceived in the monitoring and control of operations or reported by users through the help desk. The expectation is that an event or incident can be quickly resolved. A **problem**, on the other hand, is usually recurring and of larger proportions and is often the root cause of incidents. Therefore, if incidents and events occur, this may be an indication of a system failure occurring in the future. The monitoring, analysis and fixing of events and incidents are necessary for effective problem management.

Incidents have a negative impact on operations and must be dealt with expediently in order to restore normal services as fast as possible. Events are indicative of possible incidents and problems and should be monitored and managed. Problems are usually more complex in nature and need a systematic approach, including proactive and preventive practices that will often involve change in systems and applications.

The procedures and workarounds to manage and resolve incidents, events and problems constitute, together with the monitored elements of systems, the knowledge base used to analyse the root cause of these undesirable occurrences. This allows the operations management process to proactively detect, treat and prevent future events, incidents and problems.

ICT service continuity management

The risks involved in any interruption of a business process are many and high and if they are compounded with risks of data loss or data corruption, the impact to the social protection organization can be severe. Financial loss, reputational damage, regulatory risks and liabilities can all follow a critical service continuity interruption.

One of the most important disciplines in operations management is service continuity. The back-up procedures of the critical operations and services are often where operations management activities start. However, these are just the first steps necessary to ensure service continuity. Service continuity means that the organization is prepared to recover its ICT services if they are damaged or put out of action by a sudden disaster or attack. Service continuity management is the reactive and proactive process that structures the contingency planning for this recovery.

The data must be protected by a regular back-up procedure and this must be tested and checked constantly to verify that data can be recovered effectively. The systems also need to have functioning copies that can be recovered if a disaster provokes an interruption. The hardware and connectivity must have contingency solutions in the event that they are compromised. Facilities such as energy supply, no breaks, generators, climatizing structures, cabling and other installations must also have contingencies. Usually these contingencies are located at a distance in another location to avoid disasters that have widespread effects (fires, floods, earthquakes and so on).

Then there is the time-to-recovery issue. How long is it acceptable for the systems not to function after a disaster? The shorter the time, the more contingencies with synchronicity of data, hardware and software must be provided for. The complexity and costs quickly increase.

Careful planning, with appropriate categorization and prioritization of the critical processes and services, is crucial to maintain the availability and continuity of ICT services at an acceptable level. This constitutes the service continuity management plan – the policies, objectives and scope for the actions necessary for the continuity of critical ICT processes and services.

These actions seek to ensure the continuity of critical ICT services and cover the systems, applications, data and documentation maintained or processed by the institution or third parties. They must take account of all critical information and services, implementing the necessary contingency measures. Evidently, although essential, these actions can consume enormous amounts of resources and are similar in nature to insurance – very expensive insurance. This is why a rigorous cost-benefit and viability analysis is so important in this discipline in order to allow the governance structure to make the difficult

▶ © Unsplash.com/Ian Spinosa

choices on how to ensure that the social protection organization will have the capacity to recover and continue providing its services in the event of a disaster.

However, adequate ICT continuity management unfortunately does not guarantee overall business continuity for the organization. For this, the social protection organization must develop, implement and test a broader business continuity process with corresponding management elements, including other necessary dimensions such as staff and logistical arrangements that, together with the ICT services, will ensure the continued delivery of the services that comprise the institutional mandate.

System life cycle management

Developing and managing software applications throughout their life cycle, including requirements, design, structure, deployment, operation and optimization, is a daunting task. Social protection organizations must remember that their primary focus, their core business, is not ICT; they must focus much more on management and control than on development and maintenance. Orchestrating all the ICT services and keeping them interoperable requires the definition of institutional standards to be followed in the long term. These standards and this framework must take into account the often rapid obsolescence of ICT products, as well as the financial and technological dependency related to the choices made in relation to technologies and products.

When analysing the total cost of ownership of an ICT system, the institution must consider the whole life cycle. This includes budgeting hardware requirements, maintenance requirements, human resource requirements and development costs. The long-term costs of development are often much higher that estimated. Perhaps after these considerations, institutions will consider that the best course of action concerning systems is to begin by making the effort to reuse applications or parts of applications to attend to their needs. If that is not possible, then the possibility of contracting the application as a service provided by external vendors should be considered. If that in turn is not possible, acquiring codes or systems that are ready off the shelf is the next option. Some institutions will even analyse abandoning the project as a possibility before developing the system in house. However, if in-house development is unavoidable, exerting proper control on the process is critical. Managing this in a holistic manner is the function of the discipline here described.

A systems development life cycle begins with a **preliminary analysis** that will understand the nature and scope of the issue, propose solutions, describe costs and benefits and come up with recommendations. Then the **requirements definition** should define the functions and operations of the intended application. This demands gathering and interpreting facts, diagnosing problems and recommending improvements to the system. This leads to the **systems design** phase, for which desired features and operations are described in detail, including business rules, process diagrams and other documentation. The next step is **development**, during which the coding is done. This is followed by **integration and testing**, during which the pieces of code are brought together into a testing environment and checked for errors, bugs and interoperability. If successful, this is followed by the **acceptance, installation and deployment** phases, during which the software is put into production and runs the business process. Throughout its existence, the software will require **maintenance**, during which, among constant adjustments and changes, it will also be assessed and evaluated. During **evaluation**, the organization can check whether it meets the business requirements and objectives and is reliable and functional. At some point, the answers to those questions will not be satisfactory and the **disposal** phase begins. The organization will plan to archive, discard or destroy information, hardware and software that is being replaced. This must be done following security requirements to prevent unauthorized disclosure of data. The planning must also ensure the migration to a new system.

If parts of this cycle are being carried out by external organizations, as is often the case with development, the defined institutional framework must be included in the contracts and SLAs. Also central to all these processes is the extensive and formal documentation of all proceedings. It is the only way that the institution will retain full control of the knowledge involving the systems and services. This is necessary to ensure that the tacit knowledge built into the codes and systems by internal or external developers is formalized and transformed into actionable institutional knowledge that allows the adequate future management of the systems and services.

All solutions developed or acquired must have default audit tracks, monitoring tracks and data-analysis capabilities. This will also enable a data-driven approach in terms of monitoring and control, as well as the possibility to evaluate both the ICT services and the institutional performance and social protection programmes.

Governments are also facing their digitalization processes, in many cases by structuring national policies for e-government and establishing the framework for developing and managing software applications. Social protection organizations need to understand, take into account and integrate these efforts, as well as being compliant with national regulations for public administration in general.

Demand management process

ICT governance is what allows for the adequate arbitration and balancing of all the different interests and different perspectives of the institutional objectives. This is especially relevant in the process. Constant alterations and customization of ICT systems consume resources and time and threaten, sometimes critically, the smooth running of systems. These are the prices paid by the ICT team. The absence of functionalities to respond to business process needs and regulatory or scheme design alterations can gravely impact service delivery. These are the prices paid by those responsible for the business process. Both these prices ultimately impact the organization as a whole, which is an example of why high-level governance is necessary to arbitrate what are the institutional interests to be addressed, at what cost-benefit levels that should be done, who it should impact and how the cost should be met.

The demand management process seeks to understand, anticipate and influence the demand for ICT services in order to rationalize and optimize the use of resources. This can only be done in close relationship with those within the organization who are responsible for business processes. The governance objectives for ICT systems, aligned with institutional objectives, structures this relationship between different entities of the organization. This will result in a strategic long-term plan for ICT service demands, with due consideration for innovation or improvement.

In addition to a deep and constant dialogue with those responsible for business processes, the ICT team should use the data collected and analysed in the monitoring and control of the operations management process, as well as the service desk data regarding incidents, requests and problems. To a certain extent, some inference of demand prognosis can be structured by measuring the frequency, volume, duration and location of service usage.

While preparing and implementing improvements and capacity increases, the demand-management process will allow the institution to exert control over service consumption in order to maintain the minimum service levels agreed.

Change management

As stated previously, the impact of changes brought about by ICT systems can be daunting. In order to face these impacts, orient changes towards positive outcomes and control the risks and possible negative consequences, social protection institutions can establish a change-management process. This will allow for the evolution of business processes and ICT systems and infrastructure within controlled conditions.

ITIL defines changes in the ICT environment as the addition, modification or removal of any authorized, planned or supported service or service component that could have an effect on ICT services. In order to effect these changes in a way that minimizes risks and optimizes the possibility of success, the institution must implement a change-management process. This allows for the understanding of the changes to be implemented, as well as the associated risks and measures, in order to minimize the negative impact on operations and stakeholders. Change management includes risk assessment relating to the proposed changes in all affected systems and services, as well as contingency plans for possible problems. As with all governance and management processes, change management must also be formalized, monitored, evaluated and improved in a continuous manner.

It is important to note that most of the challenges concerning change management arise not from technology – although attention must be given to this dimension – but rather from the human element, which will always have a complex and multifaceted relationship with change in the work environment and work processes.

Information security management

Information security management is at the core of ICT governance and management since the confidentiality, integrity and availability of information held within these systems is the bedrock upon which trust in the data and information is maintained. The role of information security management is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. These issues include but are not limited to natural disasters, computer or server malfunction and physical theft.

A social protection institution must implement an information security management process to protect its data and information resources from threats or losses. The objective is to keep the information and data available, reliable and usable by authorized users, as well as keeping its ICT systems resilient from attacks and capable of resisting or recovering from failures. The most relevant international standards are ISO 27001 and ITIL v3 – Service Operation.

These standards address the following five key elements.

Control. Establish an organizational structure to prepare, approve and implement the information security policy. Assign responsibilities and establish and document the process.

Plan. Design and recommend appropriate security measures, based on an understanding of the requirements of the organization.

Implement. Put in place appropriate procedures, tools and controls to support the security policy.

Evaluate. Perform regular audits of the technical security of ICT systems to supervise and verify compliance with the security policy and security requirements.

Maintain. Continuously improve security measures and controls, as well as the mechanisms by which they are monitored and controlled, in order to maintain an effective information security regime.

The measures to be implemented to minimize threats and the impact of human errors are usually classified as follows.

Preventive measures. These focus on the prevention of security incidents. Measures such as access rights control, authorization, identification, authentication and access control for the institutional information systems are necessary for these preventive security measures to be effective.

Reductive measures. These aim to minimize any damage resulting from security incidents. Deploying contingency plans and executing automated backups of critical data and systems are examples of these measures.

Detective measures. These consist of monitoring systems that aim to identify a risk or threat.

Repressive or suppressive measures. These are put in place to counter any recurring security incidents, automatically blocking connections or usernames from suspicious IP addresses for example.

Corrective measures. These repair the damage caused by errors or incidents, whenever possible.

All these elements and measures must take into account the dynamic balance between the need to access and use institutional information and data and the need to secure that information and data. Complete security means no access or usage, while complete liberty means no security and no possibility of trust in information and data. This dynamic balance is the essence of information security management.

Another crucial point is that information security is not predominantly a matter of applied technology; rather, it is a process to manage human interaction and behaviour concerning information and data. The human element is the source of the majority of security incidents and human behaviour and organizational culture are the keys to adequate information security. More than any other governance and management issue, it is efficient communication and widespread institutional awareness that are critical to the information security processes.

Acquisitions, investment and vendor management

Institutions with adequate governance and management procedures should always conduct a rigorous cost–benefit analysis in their ICT budgets in order to enhance their efficiency and effectiveness. ICT is costly and usually accounts for a large portion of any investment and operational budget. In difficult times when there is a need to cut costs, the ICT budget can come under adverse scrutiny. Without a deep understanding of business requirements and a clear link to institutional business goals, the ICT budget can be questioned, especially when ICT investments and costs are already on an upward trend.

This is aggravated by the frequent inability of ICT management to clearly explain the added value of technological investments. ICT investment needs are presented as: system x needs an upgrade on the application servers because it is version y and the market standard is already version z. These proposals need to be presented in a different light, such as: this proposed upgrade will allow us to service x per cent more beneficiaries in y per cent less time. A clear statement of the value added in the business processes should be provided.

ICT governance and management is a crucial and central part of overall institutional governance and management. It ensures that adequate resources in the ICT environment (budget, human resources, suppliers, assets and service agreements) are available, while clearly defining what constitutes its value and what parts of the organization it will benefit. It should help the institution to select and execute investments and manage assets and optimize value with affordable resources at an acceptable level of risk.

Organizations that that save money with ICT usually present better and more consistent results over time when compared to organizations that save money on ICT. However, it is always necessary to conduct rigorous investment and value management analysis, as well as due consideration of the results with a return-on-investment evaluation.

ICT investment management consists of a complex mix of hardware, software licences, software applications and services. This mix includes not only the acquisition of ICT elements but also periodic payments corresponding to software licences, upgrades and renewals, as well as technical support and contracts on ICT services in general. In addition, the ICT investment management process should take account of all relevant national and institutional legislation and regulations pertaining to procurement, contracting and acquisition.

Most of the important changes and results brought into the institution by ICT will come through acquisition and contracting. This is an important focus area, in which profound knowledge of the ICT industry and the environment of the country where the institution is located is necessary. Training of acquisition and contracting specialists, focused on ICT, will be required in order to acquire and implement the best and most adequate solutions. In ICT, price is at least as important as efficiency, efficacy and effectiveness. The institution will have to learn to balance investments between supporting the present and building the future.

This delicate balancing act is also necessary when dealing with proprietary versus open-source systems. The issue is made more complicated by the need to understand and calculate the total cost of ownership; this outlook focuses on the long-term sustainability of the systems involved, where hidden and indirect costs can be attached to necessary complementary products, maintenance and additional services. Also present are various vendor and technological lock-in strategies that are common in the ICT market. To prepare for this, constant risk assessments must be undertaken for all investment proposals, in particular for external contracts and outsourcing.

As with all other governance and management processes, managing ICT investments involves permanent monitoring and evaluation of results and constant and transparent communication of the strategy, framework, processes and results.

Service desk and request fulfilment

As mentioned, trust in ICT and in its governance and management within the organization is central to the smooth operation of social protection. In order for the users of the systems to have trust in the ICT services beyond all the actions discussed, it is also necessary to establish a single point of contact for all user requests. This point of contact, commonly called the **service desk** in the industry, is the nerve centre of ICT services, both in importance as well as in its potential to cause problems.

This point of contact for all user requests, information and complaints about services and procedures uses systematic and standardized practices and, as with all elements of ICT management, the service desk needs to have formal and clear roles, responsibilities and procedures. This is important for transparency and accountability, as well as for monitoring and evaluation. All requests should be logged and tracked, escalated if necessary and closed when the user is satisfied. Some of the common issues addressed are: requests for information; access to systems; password resets; hardware maintenance; peripherals maintenance; reports of ICT events, incidents, problems and failures; managing, categorizing and prioritizing incidents and requests; and so on.

The service desk can consume a large amount of the resources and energy dedicated to ICT in social protection organizations; this is a trap to avoid. The user often has a tense relationship with the available ICT functions. Issues can arise in many areas, from problems in relevant social protection systems to very basic issues with hardware, peripherals or basic office automation systems. The extent and variety of user demands is enormous and satisfying them may, if allowed, consume most of the available time and energy of ICT services, as well as most of its human, financial and technical resources.

The main function of ICT in social protection organizations is not to support the needs of the internal or external users in relation to hardware, peripherals and systems. Rather, it is to keep the social protection business processes functioning, while gathering, preserving, using, analysing and sharing data and information.

An imbalance in the allocation of resources to the help desk can be a large obstacle to increasing the maturity of ICT governance and management. This can be aggravated by the fact that the activities around the help desk function tend to demand less skilled staff, who are usually more readily available for hiring by the institution. The risk of mission drift is considerable. In fact, the help desk activities in the ICT industry environment of many countries can be outsourced and managed as a service contract. This should be considered in order to liberate resources and energy for the more crucial and advanced challenges of digitalizing social protection operations.

© Pexels.com/Agung Pandit

II. The governance and management of Management Information Systems (MIS)

Good governance of ICT in social protection organizations means understanding how to conduct all the procedures discussed in this module and the reasons why they should be conducted. Establishing clearly who decides what, when and how sums up the essence of governance and management. This means defining how to do the right things and how to do them well.

Nowhere this is more important than in the central core of service delivery – the Management Information System (MIS). Most social protection organizations either have gone beyond paper-based processes or are actively trying to implement digital systems in order to execute their mandates. The result is that all aspects of social protection, including policymaking, oversight, scheme management and delivery of benefits and services, are permeated by ICT. In this context, the MIS is usually the structuring core of service delivery that makes policies and programmes tangible. It operates as the interface between business processes, information, beneficiaries, staff and external organizations.

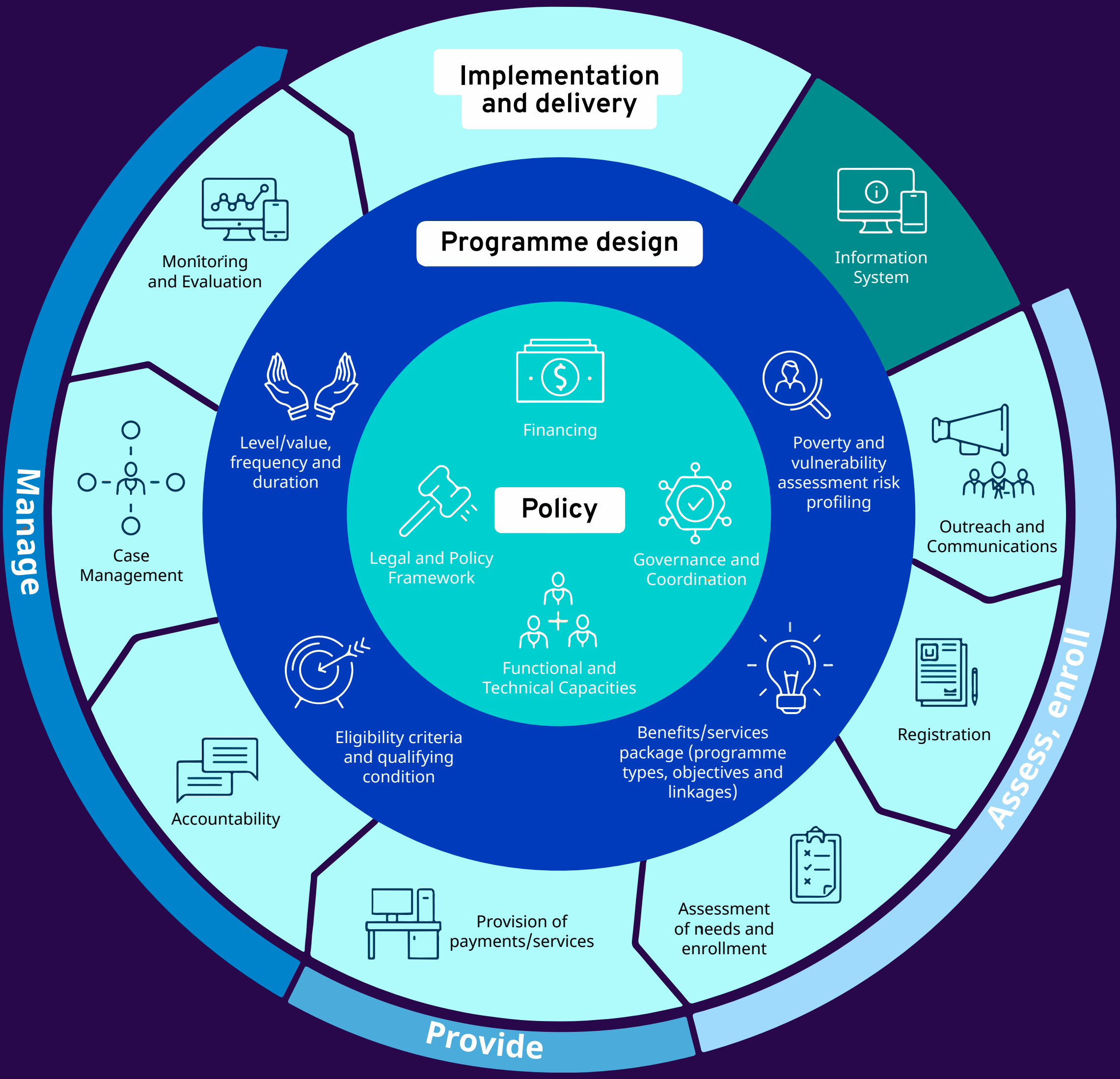
The MIS is therefore the foundation of effective social protection service delivery and is crucial to ensuring the potential fulfilment of rights. These systems execute business processes such as registration of contributors and beneficiaries; contribution collection; collecting declarations and payroll information; adjudication of eligibility; receiving benefit applications; accounting and finance, including calculating and paying benefits; case management, including appeals and complaints; and the monitoring and evaluation of operational processes.

An information system that is central to institutional operation and is largely responsible for the effectiveness of institutional goals and objectives must be analysed in a holistic manner. The governance and management of an MIS system – including design, development, implementation, operation and maintenance – is a process that combines technical and political elements. The figure below illustrates this constellation of interconnected levels, which must work well together in order to be effective and efficient.

At the level of social protection policy, key elements include the definition of the legal framework; the financial structure; the functional and technical capacities; and the structure of the coordination, governance and management arrangements. This includes extensive political modalities that have evolved over long periods and are evidently decisive for the quality and impact of results.

The programme design is where most of the all-important details, characteristics and programme choices will be expressed. Here the concrete criteria used to assess rights and benefits are defined and built into the information system and key elements are selected and combined, such as the types of benefits and services; the values, frequency and duration; the eligibility criteria and qualifying conditions; and the risk assessments.

▸ The social protection (solar!) system


Implementation and delivery
Programme design
Policy
Financing
Legal and Policy Framework
Governance and Coordination
Functional and Technical Capacities
Level/value, frequency and duration
Poverty and vulnerability assessment risk profiling
Eligibility criteria and qualifying condition
Benefits/services package (programme types, objectives and linkages)
Information System
Outreach and Communications
Registration
Assessment of needs and enrollment
Provision of payments/services
Accountability
Case Management
Monitoring and Evaluation
Manage
Provide
Assess, enroll

Source: SPACE

The level of implementation and delivery is often overlooked and, especially in the context of ICT, it may not receive the high-level governance it needs to function in harmony with the other levels. This is a significant problem because good policies and well-designed schemes simply do not exist without effective implementation and delivery. Most of the functions of implementation and delivery are contained within the MIS or the suite of systems that functions as an MIS. The only function that is frequently outside the MIS is outreach and communication and even that frequently depends on the information provided by the MIS. Most other functions – such as registration; assessment of needs and enrolment; provision of payments and services; case management; monitoring and evaluation; and analysis of the information necessary for accountability – are contained in the MIS.

The MIS is evidently central to most institutional objectives since it is essential for financial planning and sustainability; accountability and transparency; monitoring and evaluation; planning and coordination; addressing error and fraud; and providing data on beneficiaries, disbursements, complaints and systems that allow evidence-based decision-making or data-driven management.

The figure also illustrates the fact that all these elements must be taken into account and balanced holistically. The social protection system demands political and technical design processes that operate in a cycle of assessment, enrolment, provision of benefits, management and improvement. The governance and management process is one of the main tools for ensuring that this dynamic mechanism achieves institutional goals and objectives while respecting the core principles of social protection.

In order to exist in a sustainable manner, a social protection policy must be implemented efficiently and in order to achieve its objectives it must be implemented in an effective way. Consequently, in order to achieve the results and social changes envisaged the policy must be implemented in an efficacious way. This usually depends on the quality of the policy proposal rather than on operational implementation. Orchestrating all these complex moving parts is a significant and central challenge for social protection organizations.

Recognizing these different levels and their different but interconnecting roles in the social protection system is important. Policy design shortcomings are seldom solved by effective implementation, while poor implementation will render useless the best-intentioned and best-designed policies. Each level must perform consistently and in accord with its inherent characteristics and be integrated in a coherent whole in order for the desired results to be achieved.

More and more, these results need broad stakeholder consultation and consensus-building, which are fundamental for the design of policies and programmes and for implementation and delivery.

To keep all these moving parts in concert, a disciplined and relentless governance and management process is critical. Since the MIS is usually the backbone of the service delivery process, it is where everything comes together – business processes; interaction with data produced both internally and externally; stakeholders; financing; legislation and regulation; staff; and high-level decision-makers. Beyond these coordination challenges, the MIS is also where most of the technical management challenges that were addressed in section I above are concentrated and most critical. The MIS is where data security, data integrity, operations management, systems life-cycle management, among many other things, all come together in the most critical manner and determine the success or failure of institutions' service delivery.

When designing, developing or improving an MIS, it is useful to recognize that different system components have different dynamics with regard to their life cycle. Probably the longest life cycle will be found in the databases serving the MIS systems. These will gather, organize and preserve data for decades. This is especially true in the social protection context, in which data will be relevant for extended periods as benefits may be related to recurring events that happen over decades and results may also last for decades, even beyond the life of individuals, as for example in survivors' benefits. Efforts to carefully plan and streamline database design, apply data-quality procedures and avoid transaction rules that relate to specific scheme designs will pay good dividends since the MIS will be used for extended periods of time. Therefore, databases connecting to the MIS should be well planned; autonomous; dedicated to the values of master data management and data quality; and able to exchange data with other systems within and outside institutions. Such data exchange should be enabled through standard international procedures so that the capacity to be interoperable will be available even with systems and demands that have not yet been created and defined.

The transactional rules that comprise scheme designs usually have a medium-term life cycle. Alterations to such rules arise when adjustments are made to the terms and conditions of policies. They can arise from legislative or regulatory changes or changes caused by coverage expansion, design modification, actuarial revisions or technological necessities. Such alterations usually are demanded in an environment of short-term schedules and technical uncertainties and in a high-pressure and high-expectation atmosphere. They will typically happen within a five-year span and may be the result of cumulative small changes. For all these reasons, it is recommended that transactional rules not be hardwired into data but rather function in a modular arrangement, similar to a transaction rules engine.

The user interface is usually the component with the shortest life-cycle span. Changes in technology and in society's adoption of technology has a fast-moving dynamic. As digital inclusion has accelerated in recent years, this dynamic has encouraged the use of multiple-interface solutions to access the same services. It is not uncommon to see services being offered by social protection entities simultaneously over mobile platforms, web-based platforms, client-server based systems and even with offline and paper-based procedures in a commendable effort to include all those in need of such services. However, this presents significant governance and management challenges, as well as technical hurdles for development and maintenance. The time frame of the user-interface life cycle can be as short as two years. Decoupling this from the database and the transaction engine will greatly ease the development and maintenance efforts and improve the overall stability of the system.

This modular architectural approach is inspired by service-oriented architecture (SOA) which integrates distributed, separately maintained and deployed software components through a communication protocol over a network. In this context, the software components are the database, the rules engine and the user interface. This section illustrates some of the many governance and management choices that must be made concerning the MIS. Taking into account its critical nature and establishing a rigorous, disciplined, documented governance and management process will make these choices clearer and more likely to succeed.

The MIS governance and management process is often the focal point of the broader ICT governance and management process, since it is both the beating heart and scintillating brain of the institutional operation. The ISSA guidelines on ICT are the most relevant international standards covering these processes. They are especially useful as they go into relevant detail on many of the issues discussed.

One of the useful concepts covered in the ISSA guidelines are business processes; they provide a useful perspective with which to integrate and manage the different areas and functions of the organization. The term is used to describe the end-to-end sequence of tasks and information exchange by which service is delivered in alignment to institutional objectives. The process usually starts with a request, input or demand and follows a sequence of procedures to an outcome for the stakeholders and the organization. Focusing on the process, they cut across different areas and departments within the organization and help orient activities towards an outcome for a stakeholder.

The end-to-end business process perspective also helps to integrate important subsidiary processes – such as compliance enforcement, fraud detection, accounting processes, budget management and human resource management – into the overarching orchestration of systems and processes. It also allows additional business process-oriented improvements across different systems, such as security controls and preventive measures to minimize error, evasion and fraud.

The business process perspective helps to link the coordination needs of the ICT governance and management process with other organizational units. It encourages the integration of cross-cutting responsibilities, actions and choices that usually impact beyond the systems and ICT services that are directly involved. It presents an opportunity to evolve ICT governance and management procedures to a broader organization-wide governance, planning and management practice. It helps the ICT unit and the institution as a whole to overcome the isolated nature of ICT processes.

The MIS is also where data exchange with databases outside the social protection organization is most likely to happen. This compounds the need to pay attention to MIS governance and management due to the crucial nature of the data and processes happening within the system. It also expands the scope of governance and management beyond the limits of the organization. It is necessary to understand the ecosystem in which the data and the systems that support it originate. Is there a broader e-government context to be aware of? Are there other institutions with oversight capacities that the organization should engage with? Are there government frameworks for ICT and interoperability that the institution needs to comply with? Are there preferred service and infrastructure providers within or outside the government context that need to be consulted?

After understanding the ecosystem, its denizens need to be analysed: what other information systems have useful data for the institutional objectives? National ID schemes, civil registration and vital statistics systems, tax databases, employers' databases, labour databases, disability databases, health system databases, educational system databases, property registries, other social protection databases – all these contain important information and can be extremely relevant for the needs of the MIS and for the institutional objectives.

It is necessary to rigorously analyse these needs and the needs that these databases and their parent institutions have for the data within the social protection organization. Subsequently, the pursuit of meaningful connections starts, the interinstitutional dance of regulations, memoranda of understanding, formal agreements, political pressure, technical protocols, construction of APIs (Application Programming

Interface, a software construct that allows two applications to talk to each other), data quality procedures and so on. This usually happens both ways between participating organizations. The MIS governance and management process is the tool for keeping abreast of all these endeavours as the exchange of relevant data is one of the levers for the improvement of efficiency and effectiveness in ICT operations.

The key concept here is interoperability, which lies at the heart of the competitive relationship between citizen data and government bureaucracy. Society is increasingly aware that its data is repeatedly required by several different government institutions, sometimes even within the same organization, and that this could be different.

One of the important lessons acquired from decades of trial-and-error efforts is the fact that while there are some technical hurdles with regard to the implementation of interoperable systems and data exchanges, most of these challenges are straightforward technological processes that can be overcome with technical skill, good system design and rigorous governance and management procedures. The difficult obstacles are usually organizational and political in nature – data hoarding, unwillingness to share information, struggles for resources and budgets and so on. Again, the MIS governance and management process will strengthen the institutional capacity to navigate these turbulent waters.

Social protection organizations should also keep in mind that, in an increasingly data-rich environment, there are many alternative paths for conducting extensive data-quality procedures with different elements of data. Cross-referencing multiple databases with indirect relationships to the data treated can lead to similar quality results as cross-checking with the precise data referred to. Many countries reach a high accuracy in uniquely identifying beneficiaries without the resource of a national ID scheme through the extensive cross-referencing of multiple databases.

It is clear that the MIS governance and management process should prioritize contingency planning for the system. Data is crucial and cannot be lost; transactions constitute mission-critical services; the operations and infrastructure supporting the MIS are what keeps the organization open for business. Therefore, the stable and continued functioning of the MIS is probably the most critical objective for the ICT team. On the other hand, the system's significance makes it the main target for changes and improvements through new functionalities and technologies. The need to change, develop and evolve at the risk of instability is counteracted by the need to remain stable, immutable and secure. This essential conflict lies at the heart of the ICT governance and management process and demands practice and maturity to be addressed. Planning to avoid loss and interruption and planning to mitigate the consequences of loss and interruption if they happen are central to the operations management process and the focus of these procedures will naturally gravitate to the MIS.

If the MIS is the beating heart and scintillating brain of a social protection institution, it becomes immediately clear that the organization cannot function without some form of management and information system in place. What is less clear but needs to be affirmed is that the opposite is also true – the brain and heart cannot function without all the other organs supporting them. A functioning MIS thrives in the effective orchestration of all the processes and components of the organization. Implementing a comprehensive ICT governance and management structure provides the conductor to lead this orchestration.

© Evgeniy Shkolenko

III. Data and data governance

Data has become one of the central issues of our time. Discussions of data privacy, data security, data ownership, data usage, data governance and data management reach us daily. Everywhere data is being collected, processed, analysed, used, reused and commercialized. New uses and new forms of data are being created in real time and at a granular level. The speed of all these processes is increasing and shows no sign of diminishing.

We are witnessing new conflicts relating to who can collect, control, use and profit from data, which are already being referred to as data wars. These clashes happen on various different and sometimes contradictory levels. The world is redefining the conceptual, legal, technical and social mores and forms of dealing with data as we go along and this will greatly influence what our future looks like.

Governments need data to improve programmes and policies, using it to evolve the design, execution and evaluation of public policies. Operation and execution, monitoring and evaluation, transparency and accountability – all aspects of government seem to be increasingly dependent on having and knowing how to use good data. The same can be said for its effects on the private sector, where most of the new business models, as well as most of the disruption and momentum, seem to originate in technologies and data. Concepts like the attention-driven economy and surveillance capitalism illustrate the pivotal role of data in the economy. Similarly, communities, individuals and social organizations daily increase their use of data to orient their activities and hold governments accountable.

The economic and social impact of establishing and managing a country's data infrastructure cannot be overstated and has been emphasized by many international institutions such as the World Bank, the International Monetary Fund, the Organisation for Economic Cooperation and Development, the European Union and so on. Slowly and in a piecemeal manner, national data infrastructures are being built. The aggregation and interaction of the most various types of data – geographical, statistical, actuarial, sensor-based, open, private, public, aggregated, metadata, static, dynamic, transmitted, centralized and dispersed, to name only a few – result in a virtual infrastructure that is as important as the physical one. The welfare and development capacities of countries and societies are increasingly dependent on consolidating their data infrastructure. This metaphor aptly illustrates the exponentially increasing importance and pervasiveness of organized and well-governed data for countries and societies.

As countries and societies in general are rushing to establish, grow and consolidate their data infrastructures, having adequate governance and management processes in place is a decisive factor that will greatly influence the qualitative differences in those infrastructures. A commitment to accountable data governance is a central factor in defining whether data will be a driver of economic and social progress that promotes confidence in data systems and nurtures equitable development for all or will allow a limitless databased value creation at the expense of human rights and digital inclusion.

These different approaches are proceeding at vastly different paces. In most countries, the private use of data develops faster and runs deeper than public use. The still unclear data-ownership rights and the grey areas between personal data and behavioural data are intensely exploited in the data-driven business models of many digital platforms. The consequences of this are usually increasing inequality and digital exclusion from services and goods, as well as from information and power.

Well-structured, disciplined and long-term focused governance procedures are still in the early days of their development in many parts of the world; this is particularly true in lower-income countries. Legal and regulatory frameworks for data governance and management are incomplete, while institutions with the administrative capacity, decision-making autonomy and financial resources necessary to sponsor concrete implementation are rare. In many cases, the available human and technical resources in crucial areas such as cybersecurity, data protection and interoperability are equally rare. The same can be said about the infrastructure needed to store, process and exchange data. Often this comes also with a very limited presence of ICT goods and services due to the limited economic capacities of lower-income countries.

To face these significant challenges, decision-makers should regard data infrastructure as foundational and focus on expanding access, reuse and analytics for both new and existing data. Also necessary are the efforts to harmonize definitions, standards and classifications to encourage interoperability across databases that enhance synergies across different data sources. Data from censuses, national surveys, government administrative data and data produced by civil society organizations all need to be integrated in order to help build a comprehensive data infrastructure, providing much needed information and knowledge for programmes and public policies.

This infrastructure reinforces the need for strengthening data protection, especially with regard to personal data that can identify individuals and non-personal data that can allow social groups to be inferred. The possibility for discrimination based on ethnicity, religion, race, gender, disability status or sexual orientation should be opposed at the same time that collecting this data is often necessary for the implementation of many social policies. There are also growing concerns about cybercrime and the potential for politically or commercially motivated surveillance. The response to these important concerns will probably be based on a strong regulation of the use of personal data in the context of human rights.

This turmoil surrounds the collection, governance, usage and management of data by social protection entities. This situation is compounded by the fact that, just as social protection is key to overcoming inequalities in the economic and social spheres, it is also key to rebalancing the presence and power of those excluded and left behind in the digital sphere, as data infrastructure is being built and its benefits are being reaped.

In many countries, social protection and digital identification schemes are some of the largest and most pervasive data-collection initiatives under way. Moreover, these initiatives are not linked to consumption, like many other data-collection practices. The broad and far-reaching scope of the data necessary for social protection means that the stakes for collecting, using and protecting such data and the information derived from them have never been higher.

It is clear that data and information are the fundamental assets of social security institutions. Most social protection institutions revolve around gathering, preserving, using, analysing and sharing data. It must also be noted that the scale and relevance of social protection activities add to the complexity and risks of its data governance and management. These institutions make decisions based on data and information that cover large numbers of people, their rights and entitlements over long periods of times. Errors or misuse of data may lead to significant social and political impacts. Therefore, building social protection data infrastructure is a demanding task due to the complex, costly and detailed processes that are necessary to implement and maintain them.

Good governance and management of data requires effective, efficient and continuous planning for the control and use of data resources throughout their life cycle. Therefore, data and information administration should be an inherent part of social protection institutions' corporate policies and practices. They represent the institutional interpretation and implementation of tried and tested international standards and processes to collect, access, process, analyse and share data. This systematic and standardized approach to data management will enable institutions to address these challenges as a journey of continuous improvement of their capacity to leverage the amazing power of data for furthering the objectives of social protection.

It is necessary now to delve into some of these practices in order to understand their importance and their connection to other aspects of governance and management. Broadly, data governance may be defined as the processes that an institution applies to address the availability, usability, integrity and security of the data in enterprise systems, as well as the inherent value and usage of the database itself. These processes are conducted according to the policies that define and control data usage and standards.

Data-governance framework

One of the first steps an institution starting its data-governance journey can take is to define a data-governance framework. This will help formalize authority and control over data assets. It will define how the planning, monitoring and enforcement of data decisions and activities will take place. It is a relevant and necessary place to start, but the institution should be aware that this framework is the start of a continuous cycle of improvement and not the final objective of the exercise. As time passes, the implemented framework will evolve to cover needs and problems that were not considered before and reach for more ambitious objectives that were not achievable or even conceivable with previous capabilities.

Finding international references to provide a starting point for this framework is not difficult. A comprehensive body of information can be found, for example, in the ISO/IEC reference model of data management: TR 10032 and also DAMA-DMBOK – the Data Management Body of Knowledge, both available in several languages.

However, believing that all the disciplines and aspects of these references are immediately applicable or even necessary is a trap that should be avoided. The social protection institution's framework should have sufficient ambition to impel progress, but it should also have sufficient pragmatism to implement procedures and help advance the understanding, capacity and control of the institution over its data. Above all, progress within all aspects of governance and management comes with continuous practice and improvement. The cycle of planning, implementing, evaluating and planning again is the key to the successful implementation of all governance and management practices; but within data governance, this is especially true due to the evolving usages, needs and demands placed upon social protection institutional data. Therefore, institutions should adapt the recommendations of international standards to their reality and adopt a steady incremental approach.

It is very desirable to involve the highest levels of institutional authority in the definition of governance and management procedures. As has been seen, the accelerating pace of technological adoption across all societies is profoundly altering how social protection delivers its services. This is especially true when it comes to data, as these institutions are custodians of strategic data that are part of a broader data infrastructure that needs to be organized, used and shared with society as a whole. In this sense, ICT and data-governance decisions have become too important to be left solely in the hands of ICT specialists.

Bringing governance responsibilities to the upper echelons of the institution also has the added benefit of forcing a marked improvement in communication between ICT technicians and institutional decision-makers. Decision-makers who are aware of the profound implications of the liabilities and costs of ICT and data-governance decisions will progressively familiarize themselves with the language, logic and constraints of technical decisions. Technicians for their part will be forced to stop hiding behind their jargon and often self-referenced software and hardware needs in order to structure their proposals in clear and understandable language and, more importantly, to provide clear and understandable analyses of the business process costs and gains of their proposals.

Therefore, the Board, CEO or higher authority that assumes governance duties in consulting ICT specialists should issue a policy statement that mandates a systematic approach to the governance of data as a critical institutional resource. They may determine that the ICT unit, in close collaboration with business units, should quickly define or refine, as the case may be, a data-governance framework.

The framework should determine the processes, procedures, authority and responsibilities for data governance. It should ensure regulatory compliance, stating which are the regulations that apply, such as a national data protection act or right-of-information legislation or an e-government regulation that applies to public institutions, as well as how these will be addressed within the institution.

In addition, it will be necessary at some point in the governance cycle to define the data strategy and policies in terms of acquiring, processing, preserving, using, analysing and sharing data. The same can be said for the definitions of standards that will be followed, the data architecture that will be implemented and the priorities and procedures that will be adopted for the gradual execution of these decisions.

The data-governance framework should take into account the various uses and forms of usage and access of data. In some cases, data can be used internally and accessed only by internal users. In other situations, datasets may need to be accessed only by machines with no human intervention or perhaps some must be made available to the public in an aggregated manner. Other datasets may be structured to be accessible automatically by external machines and downloads, while others will be available only to the people to whom the data refer.

These many variations must be understood and managed by the institution. Formalizing the processes, responsibilities and roles involved is the essence of the data-governance framework and in their continuous implementation lies the possibility of effectively controlling institutional data.

As mentioned, effective data governance depends on an understanding of the data and the business processes connected to the data. For example, data collection in social protection, much of which takes place in the context of the enrolment process, will influence the quality and the scope of datasets. In order to understand and manage this data, it is necessary to have a deep understanding of both the technological limitations and the business processes designed for enrolment.

In order to address this need, many institutions will appoint a data owner or steward to be responsible for the quality of the dataset. They will have the authority and responsibility for defining the datasets under their purview and addressing data-quality issues and reporting. Therefore, it is possible and sometimes necessary to create structures and responsibilities, such as data owners and process owners, in order to implement effective continuous governance. These structures and responsibilities need to be formalized in the data-governance framework.

Once a data-governance framework is agreed upon and the continuous implementation work starts, it is necessary for the high authorities involved in data governance to amply divulge and constantly empower this practice within the institution.

Master data model and implementation

It is important to realize that not all data is created equal: there are differences in several aspects, such as relevance, quality, temporality, sensitivity and so on. In social protection as in most operations, there is data that is central to the execution of the public policies and data that is more remote to these processes. After establishing a data-governance framework, one of the most important actions to be undertaken is to implement a programme to define, understand, refine and manage the core business data that is central to the operation of the social protection institution. This will help the institution gain maturity and agility in its data processes, while prioritizing the organization and control of its most important information objects.

By analysing its data with an eye on both the business process and the technical processes inherent to the data, the institution will be able to develop a master data model that will define the core data objects and corresponding relationships, such as persons, employers, enrolment periods, benefits and so on. This model should be set up as a stable and enduring definition of the crucial data used by the institution and can be incorporated into an autonomous database at the disposal of the various systems, enhancing the consistency of the information used throughout the institution.

There are many advantages to this approach, such as prioritizing the crucial information to undergo data-quality procedures; establishing a single, trustworthy source of truth in terms of institutional data; building autonomous and enduring quality databases that do not need to be altered when the business rules or the user interface are changed; building a deeper understanding of the data infrastructure managed by the institution that will orient all collection, data-quality and interoperability activities.

This approach leaves data objects associated with specific programmes and their operations apart from this core master data model. As examples of this, there are specific payroll information, variations upon benefits or temporary coverage expansion data.

The master data model can be implemented after these definitions by social protection institutions within an information system covering the core data objects for its operations. Depending on the scope and characteristics of the scheme, the model can have individual data, including (or not including) family ties, employers' data, social programmes data, relationship data between persons and employers and between persons and social programmes, working periods, contribution data, and benefits data. The list can be extensive and may vary greatly, strengthening the need for each institution to establish and implement their own master data model programme.

Some institutions will find that defining a specialized organizational structure to implement and administer the master data model and information system is a wise choice, while due to their smaller size and less available human resources others may wish to count on external help. This type of project usually relies on the joint efforts of business experts, who contribute data-specification and data-ownership tasks, and the ICT staff who are administering the master data system. The main task is to begin this journey by defining and documenting the proper accountability, roles and responsibilities of those involved.

As with any major ICT project, the implementation of a master data model and information system should be based on institutional models and standards: the institutional data-governance framework; the service-oriented architecture that disciplines the interoperability between applications; the shared data services; the data security and privacy standards; and the institution's technical standards.

Establishing a permanent master data programme that will identify the core data objects for social protection operations, their characteristics and parameters, including the information concerning the data itself and the associated metadata, is a task that once started will continue indefinitely, greatly enhancing the institution's capacity to collect, process, analyse, preserve and share its data.

Data-quality management

The next aspect to be analysed is data-quality management, which is also a core capacity that should be greatly enhanced in social protection institutions to allow them to reach their full potential as data custodians and key players in the data infrastructure being built by countries and societies in general. As data is fast becoming the most important asset for social protection operations, managing its quality is necessary. Data-quality management is the way for institutions to administer the data-quality attributes that will provide information for their social protection operations.

Like all governance and management processes, data-quality operations and management is a continuous practice that needs to be formalized within the institution. Data-quality management procedures should be included in the data management framework, the governance procedures and the institutional strategic plan. The international standards practices and references for this work are also abundant; a good place to start is the ISO 8000 and DAMA-DMBOK.

The main objective of data-quality management is to improve the reliability of data and information used by the institution through the application of rigorous and continuous procedures that check various aspects of the data being qualified and allow it to be corrected or improved. These characteristics are usually described as: accuracy and precision; legitimacy and validity; reliability and consistency; timeliness and relevance; completeness and comprehensiveness; availability and accessibility; and granularity and uniqueness.

Analysis of exactly how each of these characteristics apply to the different data objects and their impact on the business process of the social protection institution is where to begin the data-qualification journey. Following this, the ICT unit will be in a position to specify the data-quality requirements and the metrics and dimensions that will be used to continuously measure the defined data-quality indicators. With that in place, the work to be done is one of analysing and assessing the quality of existing data, which in turn will be followed by the correction of data defects and the implementation of procedures for the improvement of the data to be implemented in the prioritized information systems.

It is clear that high-quality data is what allows a social protection institution to make informed decisions and it is easy to see how poor data quality can lead to disastrous consequences. There are usually six steps in a data quality programme: define, assess, analyse, improve, implement and control.

The data-quality governance procedures define the business objectives for data-quality improvement, the data-quality framework, the data owners and the affected business processes. For example, the institution wishes to ensure that all the beneficiaries' records are unique and registered accurately (name, date of birth, address, phone numbers and so on), as well as consistent across multiple systems. It will then define that the data owner is the director in charge of registration, that the impacted business processes are registration, benefits and payroll. The data-quality framework also defines that all beneficiaries' names should be unique and verified with the national identity scheme as a verified database under certain rules and conditions.

With these decisions in place, the data can be assessed in the multiple characteristics and dimensions determined, such as accuracy, completeness, consistency, timeliness and so on. If the volume and variety of data permits and the objectives of the data quality indicate, both qualitative and quantitative analysis can be executed using profiling tools. At this stage, some metrics will emerge that will inform the institution of its situation with respect to data quality (the percentage of data entries that adhere to the set standards, the number of unique names that correctly match the identity scheme records, the number of duplicated names that are inconsistent, the number of non-null values in the attributes and so on).

Having obtained these metrics, the institution can analyse its situation and the root causes that lead to problems and plan for improvements on several fronts. Perhaps the number of inconsistencies arise from the way data is collected, or perhaps in order to run different systems the ICT unit has replicated the database without proper data consistency procedures in place. Whatever the cause, the knowledge necessary to identify has been gathered and measured and the institution is now in a position to act on the issue.

The analysis will lead to an improvement action plan, for which the ICT unit, in concert with the data owners and business process owners, can design and develop the improvements necessary with due consideration to the time frames, resources, and costs involved.

To implement these planned improvements, the institution needs to understand both the technical and business process-related changes. It is recommended to have and use a comprehensive change management plan in order to ensure that the institution is prepared for and thrives with the implemented changes.

In order to control the data-quality process, it is important to verify periodically that the data is consistent with the institutional needs and the data-quality framework and the results should be communicated to all involved on a regular basis.

Once the data-quality procedures are in place, the institution can also invest time and resources in preventive measures that will keep the levels of data quality at a high level. The formalized data-quality requirements must be known and understood and applied by those involved with software development, as well as those involved with operations and data entry. This includes any service or acquisition contracts that involve data; therefore, those involved in procurement must include these requirements in any specifications, contract documents and SLAs.

There is also a good opportunity for preventing data of inferior quality to be inputted by automatizing data entry filters at the points of data entry in the various information systems. This can only be done by stimulating a constant increase in data understanding and awareness. All these data- quality management actions, taken together, will greatly enhance the trust and confidence in the data, the business processes, the policies they embody and the institution that manages them.

Data analysis for actuarial work

The importance of the role of actuarial analyses in social protection institutions cannot be overstated; they are essential elements of the information and knowledge that orient adequate decisions. Understanding the possible evolution of variables over extended time in order to make choices concerning the volume of pensions and other social transfers, as well as how they interact with demographic, economic and fiscal environments, are some of the most data-dependent activities that these institutions undertake.

These actuarial analyses need the assurance not only of good-quality data but also of the capacity to collect, process and analyse data from different sources, both internal and external to the institution. The actuarial practices combine social, economic, demographic and actuarial data and knowledge to develop a long-term perspective of the evolution of the scheme or programme. As much of the necessary data may come from sources outside the institution, attention to the quality of the data collected in this manner is also very relevant. Once the institution has access to all the information it needs for policy formulation, decision-making, actuarial valuations, benefit calculations, policy appraisal and redesign, it must ensure that it is available in a form and in a quality standard, that ensures accuracy and completeness over long time periods.

Institutions may find that they need to develop specific data-quality measures to ensure the availability of sufficient and reliable data to perform actuarial work. Some of the references necessary to define the standards for the work and the related data can be found in the ISSA-ILO Guidelines on Actuarial Work for Social Security.

Data operations

With data-governance procedures, the institution will use the data in its systems in order to carry out its development and operation activities in a systematic manner. This section deals with the analysis, design, implementation, deployment and maintenance of data and information systems. Data operations focus on managing databases and data technology in order to support the availability of the institution's data throughout its life cycle in order to enhance the efficiency of the use of data within the systems and to protect the integrity of data assets.

Under the direction of the data-governance framework and with the collaboration of the business units, the ICT unit should establish SLAs and prioritized action plans to carry out data operations in a systematic and formalized way. This may include activities such as data-modelling; analysis, design, implementation and administration of information systems; database administration; and data-recovery management and operations. All these operations should be communicated clearly throughout the organization in the context of governance activities.

Data privacy

A data-governance framework is also one of the most effective ways that social protection institutions can ensure compliance with regulatory and legal requirements concerning data privacy or data protection. This is increasingly important as the whole world debates how to ensure that individuals have rights over their data and that personal data collected and stored in institutions is protected and used only for the stated legitimate purposes.

Addressing data privacy is not only a legal necessity but is also central to the confidence and trust placed in the social protection institution. Problems in this area may lead to grave reputational harm, as well as liabilities and damages.

Some of the risks mentioned above are covered by addressing data privacy. Data protection is one of the ways that institutions can ensure respect for human rights and protection of minorities and vulnerable populations. If critical personal data such as health information and disability or refugee status is not protected, people that register for social protection benefits or services may suffer harm or discrimination. Data security, data protection, the observance of privacy rights and the adequate use of personal data can usually be more effectively addressed within a governance framework that takes these elements into account in the design, operation and management of data systems.

Data-protection laws around the world try to allow individuals some control over their data, allowing them to know how it is being used, by whom and why. In order to adjust the data practices in an organization to comply with these relatively new regulations, clear procedures for handling, processing, collecting, archiving, deleting, correcting and sharing personal data must be put in place.

Although data security is discussed together with ICT security as a whole, it is important to recognize the distinction between data security and data privacy. Data security consists of the measures that an organization takes in order to prevent any unauthorized access to digital data or any intentional or unintentional alteration, deletion or disclosure of data. Data security mostly involves protection against malicious attacks and data breaches and usually covers elements such as access control, encryption, network security and so on. Without data security, there can be no data privacy. However, if data is secure and protected but is not collected, processed and used in a legitimate lawful manner, the institution will have data security but not data privacy.

Data for data-based management

Data-driven decision-making or data-based management is the practice of collecting data, analysing it and basing decisions on insights derived from that data. Data-driven decisions can be evaluated according to their impact on the chosen metrics. In order to have the data available for this type of process, institutions should include this type of data in the data-governance framework and develop the capabilities necessary to obtain and analyse this type of data. It is likely that some changes will have to be implemented within the systems in order to collect and track the necessary management data. Many institutions already collect some of this data for record-keeping and compliance, but the next step is to use it to orient institutional planning and decision-making.

Once an institution decides on this approach and makes it part of the data-governance and data-management activities it can reap many benefits. Using data to conduct decisions will provide greater transparency and accountability. The institution will progressively be seen as one in which objective data influences management choices, policies and planning. The objectives to be reached can be stated clearly and the results are measured, which leads to an increase of confidence in the institution both internally and externally.

For this to work, the data-governance framework should encourage the collection of administrative data in real time; the development of tools and capabilities to understand the data; the widespread distribution of data across the organization; the disposition towards experimenting on the basis of the insights provided by data analysis; and the institutional commitment to continuous improvement in data-governance operations and practices.

Data analytics

Data analytics can support social security institutions to improve their administrative effectiveness and efficiency by enabling them to understand the past, explain the cause of events, inform them what is likely to happen in the future and suggest actions they may wish to take. Social protection institutions may apply data analytics in a wide range of areas, such as health care, detecting and preventing error, evasion and fraud, proactive social policy and programme design, actuarial projections and improving service delivery, among others.

Data analytics is the process of churning the internal and external data that is relevant to the issues at hand in order to reach insights using various analytic approaches. The classic list of these approaches are **descriptive analytics**, which seeks to determine what has happened; **diagnostic analytics**, which seeks to determine why or how it happened; **predictive analytics**, which seeks to determine what, when and where it will happen; and **prescriptive analytics**, which seeks to draw inferences from data in order to prescribe actions to influence what will happen.

In order to be effective in this complex work, social protection institutions should establish the procedures, responsibilities and standards within the governance framework for the application of data analytics. Specialized structures may be needed to manage the application of data analytics within institutions, as well as the recruitment of people with specialized skills. In addition, special attention should be paid to data privacy and data-protection regulations when dealing with the often uncharted world of data analytics.

The international references are abundant. Some good starting points are ISO/IEC 10032, DAMA/DMBOK, ISO 19731:2017, ISO 9001 and CRI social protection-DM. Also abundant are the software resources commonly used for data analysis, such as ETL, OLAP and data-mining and data-visualization tools. The capabilities associated with their use are much rarer and need to be constantly developed.

In implementing analytics capabilities, the data-governance framework should help institutions avoid the risk of turning their ICT units into a data-analysis bottleneck. This happens when access to data analytics becomes the restricted province of the ICT unit, which may then become overwhelmed in a backlog of late management reports. In order to prevent that problem from arising, the establishment of a self-service data-analysis portal that can be mediated by data-visualization tools and is available to authorized business process staff is recommended. The more these analytical capacities are spread among business processes users, the more such capacity will have positive impacts on the work of the organization.

This area of data governance is incredibly dynamic and is undergoing profound and radical change. It is therefore extremely important that these disciplines be monitored constantly in order to be aware of the potential changes to society as a whole – and to social protection institutions specifically – that are likely to emerge from data analytics and machine-learning practices.

▶ © Getty Images/Clark

▶ Conclusion

The governance and management of ICT and data is a constant balancing act of conflicting choices and trade-offs. Stability versus flexibility; capacity versus investment; adapting business processes to systems versus adapting the systems to business processes; open source versus licensed software; contracting cloud services versus owning data centres; security versus interoperability; outsourcing versus in house development; performance versus innovation – the list goes on and could be presented in several different combinations. The need to make these choices are constant and always based on specific contexts. The focus must be on aligning these choices with strategic institutional goals rather than with narrow ICT considerations.

For this alignment to be effective, it must be understood and conducted with participation from all areas of the institution. This is especially relevant with regard to the entities responsible for the business processes of service provision. The definition of organizational strategic goals allows for the definition of strategic ICT goals that can be consolidated in a broad institutional planning process.

Strategic ICT activities often start with the implementation of management and control processes that will furnish the large quantities of data and information necessary for the realization of the strategic plan. This is a continuous process, in which the plan defines management and control implementation processes that provide more and better data and information. The implementation process also brings about the necessary controls and procedures to execute the decisions and choices determined by governance. In turn, this allows better, broader and more ambitious strategic choices. This process is a journey, not a destination, a journey of learning how to do better in order to be able to do more. Obtaining higher maturity levels of capacity and performance in governance and management is in itself one of the important goals of the process.

In order to follow the path of implementing effective governance and management of ICT and data, the institution must realize that the needs and requirements of ICT are secondary to the needs and requirements of providing services. Social protection institutions are not ICT institutions – technology is there to serve the organizational goals and not the other way round. All trade-offs, choices and considerations must therefore begin with this in mind.

An important part of the external context is the existence and objectives of broader ICT or digital government initiatives. These might articulate legislation or regulation that must be followed and provide opportunities for accessing and sharing data and resources that are beyond the social protection institution. This is especially relevant in the context of the data collected by social protection organizations; a strategic asset that is relevant for all societies, part of a national data infrastructure. Participating actively in these initiatives will bring positive results and increase the social protection organization's reach and capacity.

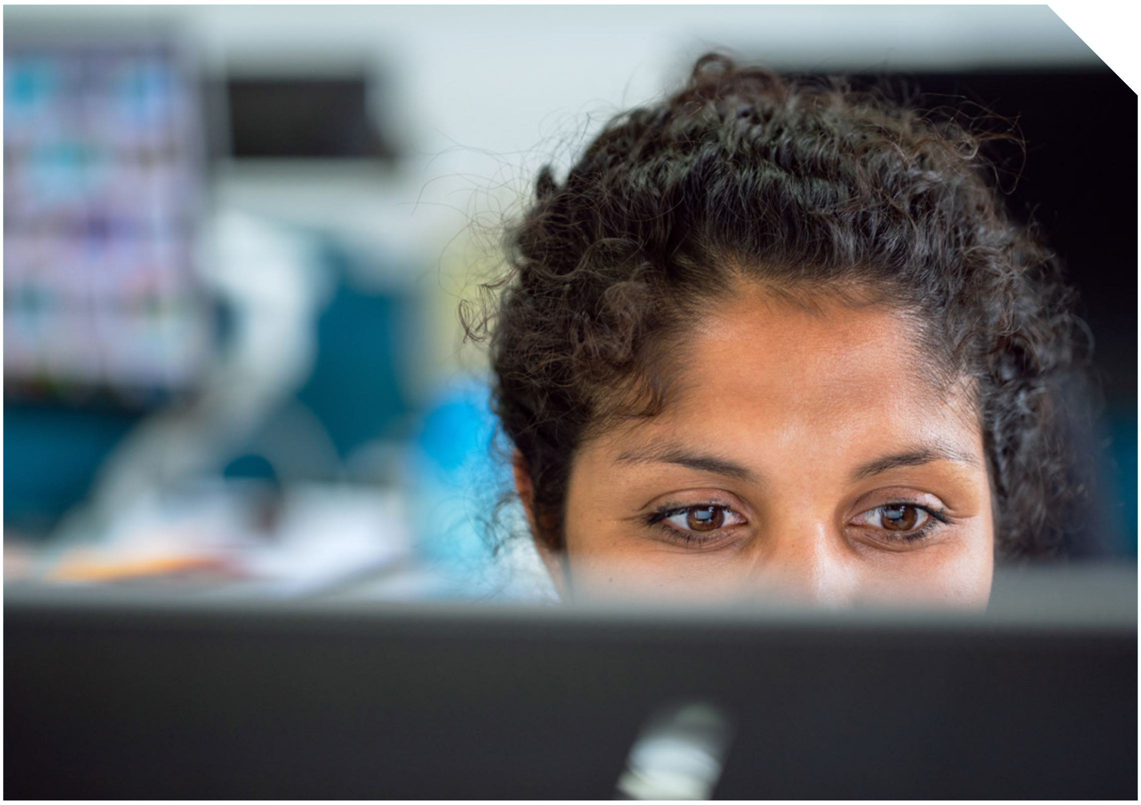
Implementing governance and management in the facilities, the infrastructure and the hardware and telecommunications are the foundational elements that support all other disciplines. If this is done correctly, the institution will have the basis for the management of its operations and its service delivery and its capacity to manage events, problems and incidents. It will be able to implement a systemic life-cycle outlook that will greatly enhance the institutional capacity to manage change and the demand for change, whether through development (internal or external) or acquisitions. All these elements will provide the information for decisions regarding investments and vendor management. The ICT governance and management processes will also enable service continuity and information security. These are complex and interconnected processes that must be orchestrated to ensure the operations that make policies become concrete, life-changing realities.

As the core of social protection activities, the MIS should also be the focus of most of the governance and management activities and processes. It is usually around the MIS that the institution is able to promote the all-important dialogue between those responsible for ICT and those responsible for the service-delivery business processes. This is one of the key enablers for responsible and effective decisions based on the understanding of the possibilities, needs and limitations of ICT in the organization and its strategic goals.

With regard to data, perhaps the most important element for implementing social policies is the implementation of a data-governance framework at the start of ICT procedures. This prepares the way for the continuous work of managing data quality and implementing the master data models that are key enablers for facing the challenge of data privacy and data analysis.

The capacity to analyse and adjust policy and management decisions based on the concrete data collected by the institution must be pursued. Having the data available and usable is the first step. This is followed by evolving the analytical capabilities and implementing the decision-making process and management procedures that will allow data-driven management and policy design.

The elements and procedures described in this module are not prescriptions that should be applied without consideration for the reasons why they are necessary and relevant. Contextualizing and prioritizing the governance and management recommendations are a constant necessity and a condition for effective outcomes. Appropriating this knowledge and applying these disciplines into each specific organizational context is certain to increase the potential for positive results. This is the invitation this module offers to all those involved in extending social protection for all.



▶ © Unsplash/RAEng

Bibliography

CRVS Systems Improvement Framework (Version 1.0), *Africa Programme for Accelerated Improvement of Civil Registration and Vital Statistics* (APAI-CRVS) et al. 2021.

"G-Cloud", *PowerPoint presentation on implementation of centralized cloud services for Belgian social security agencies*, 2019.

"Beyond Scale: How to Make Your Digital Development Program Sustainable", *Digital Impact Alliance (DIAL)*, 2017.

"Digital by Default: A Guide to Transforming Government", *McKinsey Center for Government*, 2016.

"Global Research on Governance and Social Protection", *ILO/UNDESA/Development Pathways*, 2021.

ISSA Guidelines for Good Governance, 2019.

ISSA Guidelines for Administrative Solutions for Coverage Extension, 2016.

ISSA Guidelines for Information and Communication Technologies, 2019.

ITIL, COBIT, LEAN, CMMI, DAMA-DMBOK. Various years. International norms, standards and conventions.

"Introducing openIMIS: An Open Source Solution for Universal Health", *Socialprotection.org/Blog*, *Ashleigh Slingsby*, 2018.

"Management Information Systems and Approaches to Data Integration: Manual for a Leadership and Transformation Curriculum on Building and Managing Social Protection Floors in Africa", *TRANSFORM*, 2017.

"Social Security Scotland: Digital and Technology Strategy" United Kingdom, *Social Security Scotland*, 2018.

"The European Commission Digital Strategy - A digitally transformed, user-focused and data-driven Commission European Commission", *European Commission*, 2018.

Governance of social protection systems: a learning journey

Module #2: Information and Communication Technologies & Data

This learning module is part of a series of working papers "Governance of social protection systems: a learning journey" developed in the context of the project "Achieving SDGs and ending poverty through Universal Social Protection", implemented from January 2019 until June 2021 under the 2030 Agenda for Sustainable Development sub-fund of the United Nations Peace and Development Trust Fund (UNPDF). The project is jointly implemented by the Division for Inclusive Social Development of the United Nations Department of Economic and Social Affairs (UN DESA), and the Social Protection Department (SOCPRO) of the International Labour Office (ILO), in the framework of ILO's Global Flagship Programme for Social Protection Floors and as part of the overall campaign for Universal Social Protection (USP 2030) launched in 2016. The project has pursued a two-fold strategy. In two focus countries, Pakistan and Cambodia, technical support was provided through the ILO offices to strengthen capacities of institutions and practitioners on different aspects identified as critical in social security governance. Simultaneously, at global level, the project has developed a knowledge base of good practices as well as learning modules in order to better support policy makers in their capacity to take strategic decisions in the field of social protection, the project has tried to identify and clarify, in a pragmatic and concrete way, the key drivers of different operational components inherent to all systems, starting with three core topics:

- **Coordination**
- **Information and Communication Technologies & Data**
- **Compliance and Enforcement of Legal Frameworks**

ilo.org

International Labour Organization
Route des Morillons 4
1211 Geneva 22
Switzerland