issa

ISSA Guidelines

Information and Communication Technology

Extended edition 2016

The ISSA Guidelines for Social Security Administration consist of internationally-recognized professional standards in social security administration, and form part of the ISSA Centre for Excellence in Social Security Administration. The open access guideline documents are abridged versions of the complete ISSA Guidelines for Social Security Administration that are available to ISSA member organizations only. The latter are completed with information concerning the suggested operational structures for the functioning of individual guidelines and mechanisms for their implementation. Additional resources, references and links to good practice examples are also provided to assist comprehension. Within the practical framework of the ISSA Academy and Academy workshops, ISSA Guidelines for Social Security Administration offer a basis for learning and knowledge exchange among ISSA member organizations. For information on how to join the ISSA <www.issa.int>.

The ISSA Guidelines have been developed by the ISSA technical commissions and staff of the ISSA General Secretariat, based on a broad consultation with experts, international organizations and the worldwide ISSA membership.

English is granted precedence as the authoritative language for all ISSA Guidelines.

The ISSA Guidelines and related resources are available at <www.issa.int/excellence>.

First published in 2017

ISBN 978-92-843-1216-0

Contents

Introduction

The use of information and communication technology (ICT) in social security institutions represents a global trend. As institutions turn to ICT, the goal is the development of solutions that enable them to accomplish their mission, providing high-quality services, satisfying stakeholders and improving efficiency of key processes. Moreover, the challenges resulting from social security's permanent evolution require a more intensive and sophisticated use of technology in the social security domain. Over recent years, ICT has played a strategic role in the implementation of social security programmes. The application of ICT has enabled not only the automation of specific processes, but the transformation of operations and services, enabling improvements in the performance and service quality of social security institutions.

However, in spite of these generally encouraging results and the emergence of economically accessible products, ICT application remains a matter of concern for social security institutions. It is widely recognized that the complexities of ICT systems are increasing but do not always fulfil business results expectations. In addition, the quick evolution of products and their interrelationship can impact negatively on the stability of business processes. These elements have led to worries about the cost–result balance and have generated uncertainties about the better approaches to develop successful ICT applications.

Objectives of the *ISSA Guidelines on Information and Communication Technology*

There are three main aspects to corporate use of ICT) in social security institutions:

- **The governance and management of ICT-related activities**, which address the overall organization, implementation and operation of ICT systems, including a wide spectrum of related tasks, notably: defining principles, approaches and roles to governing ICT-related activities overall; elaborating ICT strategies and management processes; managing ICT investments; managing data and information infrastructure; and managing the continuity of the business, especially on citizen services.
- **The implementation of social security functions and required resources**, notably: benefit administration, contribution collection, financial management and compliance control, on the one hand; internal services such as human resources and internal audit on the other hand; and corporate information systems and ICT platforms as corporate resources to be used by the former.
- **The application of key technologies for social security systems**, which enables the implementation of integrated, safe and accessible ICT-based services. The application of these technologies, notably interoperability, data security and privacy, and mobile, plays a key role in the effective and efficient implementation of high-performance social security systems.

In addition, cutting across these aspects, the comprehension of international standards and practices on ICT (e.g. ISO, COBIT®, ITIL®, DAMA, CMMI, W3C, OASIS, Dublin Core, OMG, etc.) would enable social security institutions to apply comprehensive and rigorous approaches to managing the complexities of ICT application in large-scale and critical mission organizations.

The *ISSA Guidelines on Information and Communication Technology* address these issues and provide guidance to support social security institutions in carrying out ICT-related activities. Its main goals are

to promote the effectiveness and reliability of social security services, as well as their efficiency and standardization. It also aims to facilitate the adoption of international standards and practices on ICT in the context of the overall application of ISSA Guidelines for Social Security Administration.

These guidelines develop the aspects of ICT governance and management, and key technologies. They address the implementation of main social security functions and related resources, taking into account the range of social security scheme implementations as well as their dependence on institutions' mandates and organizational contexts. Given this diversity, the guidelines, which aim to be generically applicable to all institutions, are complemented by technical documentation, good practice and case studies. These will be further developed, taking into account the diversity of social security schemes and related administrative processes, among other factors. The relationship between social security functions and ICT-based implementation will be also considered in the corresponding guidelines.

It is important to highlight that carrying out the tasks related to these aspects involves not only ICT professionals and technical staff, but also units managing social security functions, contracts administration, staff, internal audit and the institutions' authorities (the board, chief executive, general manager, etc.).

As ICT is an indispensable enabler in the administration of social security systems, it is important for the board to work hand in hand with the management in ensuring that the institution has an adequate and efficient ICT platform. While the fundamentals of social security administration may remain the same – delivering the right benefits and services to the right person at the right time – the ways in which these benefits and services are delivered are evolving rapidly and dynamically. An institution that has a board and management who are attuned to and well informed about ICT trends and developments is in a much better position to appreciate not just what can be delivered but also the potential than can be achieved through ICT, all with a view to providing social security benefits and services in the most efficient, effective and equitable manner.

ICT Standards and Frameworks

The growing extent of ICT application globally has motivated the development of standards and frameworks, notably by the International Organization for Standardization (ISO), Control Objectives for Information and Related Technology (COBIT®), IT Infrastructure Library® (ITIL®), Data Management International (DAMA), Organization for the Advancement of Structured Information Standards (OASIS), World Wide Web Consortium (W3C), Object Management Group (OMG), Dublin Core Metadata Initiative and Capability Maturity Model Integrated (CMM/CMMI). These standards and frameworks are generic and cover a very wide range of activities, and so are applicable in all kinds of business areas.

It is widely accepted that the starting point for adopting ICT governance practices and developing an institutional framework is the standard ISO/IEC 38500, which defines six high-level principles for "good corporate governance of IT" and focuses on the role of the board and its responsibility concerning ICT governance. However, this standard does not address specific governance and management processes, which are covered by other standards and practices.

COBIT®, a generic, process-based framework which is increasingly accepted internationally, covers overall ICT governance and management. ITIL® is an integrated set of best practice recommendations which focuses on managing the ICT service lifecycle in line with the requirements of the business.

DAMA-DMBOK is a comprehensive guide which covers overall data management activities. Software application development has been addressed by CMM/CMMI, among others. In turn, OASIS, W3C, OMG and Dublin Core have focused on technical standards concerning interoperability, metadata and semantic and web-related technologies.

These international standards and frameworks provide social security institutions with comprehensive and rigorous approaches to managing the complexities of ICT application (e.g. in large and critical-mission organizations). In addition, as they are increasingly adopted worldwide, their application would enable institutions to take advantage of global knowledge, experience and trained human resources.

On the other hand, the corporate application of these standards requires significant administrative effort, and, frequently, changes in the organizational culture and processes. The burden of this transformation very often constitutes a barrier to adoption of these standards. Therefore, these practices should be adopted as medium-term capacity-building projects, focusing on selected areas which address the institution's priorities, especially those related to the implementation of social security programmes and services. Individually, these standards do not completely cover all aspects of social security administration.

The *ISSA Guidelines on Information and Communication Technology* aims at supporting social security institutions in the application of systematic and consistent ICT governance and management practices and providing a general framework for the application of standards in such institutions. They provide guidance to identify and apply general purpose frameworks and norms that are particularly relevant to social security.

Structure of the *ISSA Guidelines on Information and Communication Technology*

The following guidelines are organized in three parts:

Part A, ICT Governance and Management, incorporates five sections:

A.1. ICT Governance

A.2. ICT Management

A.3. ICT Investment and Value Management

A.4. ICT Service Delivery

A.5. Data and Information Management

Part B, Key Technologies, incorporates three sections:

B.1. Interoperability

B.2. Data Security and Privacy

B.3. Mobile Technologies

Part C, Social Security Components, incorporates two sections:

C.1. Master Data Management

C.2. ICT-based Implementation of Social Security Agreements

Within each part, specific guidelines are grouped according to particular elements of ICT. They are presented as follows:

Guideline. The guideline is stated as clearly as possible.

Structure. This is the suggested structure for the particular aspect of ICT that may support the application of the guideline and facilitate the promotion of the underlying principle. A sound structure is essential for the effective functioning of ICT. It should ensure an appropriate division of operational and oversight responsibilities as well as the suitability and accountability of the persons involved.

Mechanism. There are different ways in which a guideline may be implemented. The suggested mechanisms for ICT are designed to ensure appropriate controls, processes, communication and incentives which encourage good decision-making, proper and timely execution, successful outcomes, and regular monitoring and evaluation.

In these guidelines, the **ICT unit** refers to the institution's staff responsible for the specification, implementation and operations of ICT-based systems, regardless of organizational structure. Such tasks could be undertaken by internal staff or external contracted agents. To implement the suggested guidelines, the institution may further establish specialized units to conduct activities related to the application of ICT.

A. Governance and Management

Structure

The corporate application of ICT in social security institutions requires establishing policies and practices to carry out the wide spectrum of ICT-related activities in a consistent and systematic way. Such policies and practices are addressed by the disciplines of ICT governance and management, which aim to guide organizations (in particular, medium and large ones) to improve effectiveness and efficiency in their application of ICT.

ICT governance is a set of processes which ensure the effective and efficient use of ICT in enabling an organization to achieve its goals. It has two major aspects:

- ICT demand governance, to align ICT strategy with the business ("doing the right things");
- ICT supply-side governance ("doing things right").

Governance ensures that the institution's needs and goals are evaluated in order to determine and agree upon balanced objectives, set direction through prioritization and decision-making, and monitor performance and compliance against agreed objectives and direction.

ICT management is closely related to governance but focuses on planning, building, executing and monitoring activities aligned with the direction set through ICT governance, and on achieving its objectives.

ICT governance and management enable social security institutions to improve the performance of ICT-related processes and address the complexities of ICT systems through systematic and standard management approaches. These goals are shared with other large and citizen-service-oriented organizations, especially public ones. However, certain aspects of governance and management are particularly important for social security institutions because:

- The socio-economic impacts and increasing complexity of social programmes are driving the setting up of reliable and rigorously managed ICT services which aim to maximize their quality and continuity;
- The strategic role played by ICT in the implementation of high-impact social programmes motivates board and management involvement in the essential aspects of ICT application;
- The multiplicity of actors, products and services involved in the development and operation of social security software applications necessitates rigorous and standardized approaches to achieve adequate coordination and reach the required service quality;
- A standards-based approach is required to meet financial and technological dependency implications;
- The size and complexity of social security projects necessitates medium- and long-term perspectives on technologies and methodologies.

As an indispensable enabler in the administration of social security systems, ICT often spells the difference between services and processes that can or cannot be done, both within the institution and between the institution and its external partners. For this reason, the board and management should understand

the strategic implications of ICT application in social security functions and promote an efficient and adequate ICT platform to support the institution's operations.

The following guidelines are organized in five sections:

Section A.1, ICT Governance, begins with the definition of an ICT governance framework based on principles defined by the *ISSA Guidelines on Good Governance*, ISO/IEC 38500 and COBIT®, to guide the institution in setting up its own key governance principles. The guidelines then address the definition of ICT governance processes.

Section A.2, ICT Management, promotes the application of ICT management processes and highlights the importance of defining an ICT strategy and managing service continuity. It also introduces the identification of ICT-based solutions for implementing social security functions.

Section A.3, ICT Investment and Value Management, addresses the consideration of ICT investment proposals with appropriate care, diligence and soundness. It first addresses the value of projected outcomes, the cost–result relationship involved in ICT investment and evaluation of return on investment, and the processes of ICT investment, promoting a portfolio-based approach. It then highlights the importance of monitoring and evaluating investment results.

Section A.4, ICT Service Delivery, addresses issues related to software development and system operations, including the implementation of corporate mechanisms and systems to respond to user requests and deliver customer services – specific themes within mission-critical and user-oriented social security services.

Section A.5, Data and Information Management, addresses data governance and data quality, mechanisms to enable information retrieval and analysis, and the implementation of master data systems in social security.

A.1. ICT Governance

ICT governance can be defined as a "framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensure that the organization's IT supports and enables the achievement of its strategies and objectives".

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

ISO/IEC 38500 establishes six principles for good corporate governance of ICT. The principles express preferred behaviour to guide decision-making.

Principle 1: Responsibility. Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of and demand for ICT. Those with responsibility for actions also have the authority to perform those actions.

Principle 2: Strategy. The organization's business strategy takes into account the current and future capabilities of ICT; the strategic plans for ICT satisfy the current and ongoing needs of the organization's business strategy.

Principle 3: Acquisition. ICT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision-making. There is appropriate balance between benefits, opportunities, costs and risks, in both the short and long term.

Principle 4: Performance. ICT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.

Principle 5: Conformance. ICT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.

Principle 6: Human Behaviour. ICT policies, practices and decisions demonstrate respect for human behaviour, including the current and evolving needs of all the "people in the process".

Guideline 1. ICT governance framework

The institution defines a single, integrated framework for ICT governance that establishes responsibilities and duties at the highest levels.

The framework fosters the application of the *ISSA Guidelines on Good Governance* and ICT-related principles as defined in international standards.

Guideline 2. ICT governance processes

The institution establishes ICT governance processes linked to its governance objectives, which include evaluating strategic options, giving direction to ICT and monitoring outcomes.

Governance processes ensure that stakeholder needs, conditions and options are evaluated in order to determine and agree upon balanced institutional objectives, set direction through prioritization and decision-making, and monitor performance and compliance against agreed objectives and direction.

A.2. ICT Management

According to ISO/IEC 38500, management relates to "the system of controls and processes required to achieve the strategic objectives set by the organization's governing body. Management is subject to the policy guidance and monitoring set through corporate governance".

For COBIT®, ICT management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

This section of the guidelines provides a starting point for the application of ICT management processes overall and the ICT-based implementation of social security functions, and addresses the definition of ICT strategy and business continuity management.

The definition of an ICT strategy (Guideline 3) is especially relevant for social security institutions. On the one hand, the size and complexity of projects in social security necessitates a medium- and long-term perspective on technologies and products. First, fostering compatibility (interoperability) among ICT systems requires a prudent, forward-looking outlook and a definition of institutional standards to be followed in the long term. In addition, given the rapid obsolescence of ICT products, choosing those to be used in long-term projects requires a prospective analysis to identify those with as long a life as possible and which will enable easier evolution. On the other hand, the financial and technological dependency implications related to the selection of technologies and products necessitates medium- and long-term strategies for ICT portfolio management.

The ICT strategy aims at aligning ICT plans with the institution's strategic objectives and plans. It also builds on enterprise architecture building blocks and components, including external services and related capabilities, to enable nimble, reliable and efficient responses to strategic objectives. To achieve this, the strategy links into information technology and related service trends, ensures the identification of innovation opportunities and enables planning so that business needs benefit from innovation.

A key activity in social security institutions is operationalizing social security functions through ICT-based approaches (Guideline 4). This mainly consists of defining and implementing ICT-related plans and projects, based on the institution's goals and strategic plans and frameworks. The nature of implementation will ultimately depend on contextual factors, but some pointers are given here relevant to different types of social security functions.

The management of service continuity (Guideline 6) aims at ensuring the continued operation of key processes, especially those involving critical operations, and maintaining the availability of information at an acceptable level in the event of significant disruption. These topics have been addressed by international standards (ISO/IEC 22301, COBIT® and ITIL) as well as by the ISSA.

Guideline 3. ICT strategy and innovation prospective

The institution develops an ICT strategy and innovation prospective as the cornerstone of an integrated institutional view of the current business, the future direction for the ICT environment, and the initiatives required to reach the desired future environment.

Guideline 4. Operationalizing social security functions through ICT

The institution operationalizes its mission and general objectives into specific ICT-related plans and actions implementing social security functions.

Guideline 5. ICT management processes

The institution implements ICT management processes aligned to the planning, building, running and monitoring of ICT-related activities, and to full coverage of ICT services within the institution.

Guideline 6. Managing service continuity

The institution ensures the continuity of its services, especially those involving critical operations, and maintains the availability of information at an acceptable level in the event of significant disruption.

A.3. ICT Investment and Value Management

Taking into account the corporate impact and dynamics of ICT, investment proposals in ICT should be considered with appropriate care, diligence and soundness. Concerns of the board and management often arise not from the size of the investment per se but from issues that stem mainly from the *degree of confidence* that can be attached to, for example: the suitability of the recommended technology vis-à-vis the needs of the institution and its strategic plan; delivery of the promised capacities and services; anticipation of the impact on and interaction with existing ICT platforms; and any hidden and indirect costs attached to complementary or maintenance products and services.

Social security institutions have to face the challenges of managing investments in ICT-related elements, which consist of a complex mix of hardware, software licences, software applications and services. This includes not only the acquisition of the elements ("one-time" investment) but also periodic (e.g. annual) payments corresponding to software licence renewal, technical support services and contracts on ICT services in general.

All these ICT elements (hardware, software, services) provide the means to achieve the institution's mission and specific goals. Therefore, decision-making on the opportunity provided by ICT investment must take into account the expected return on investment (ROI) as well as cost–benefit ratios.

In order to better manage the return on investment and cost–benefit of ICT investments, the "value of the expected results" of ICT-based activities involving investment has to be analysed and defined.

This set of guidelines begins with definition of the concept of value for the main ICT-based activities and identification of approaches to optimize its realization (Guideline 7). The concept of value aims to measure the importance of (i.e. assign a value to) the outputs to be achieved by the institution through ICT-based activities. When these results are quantitative (e.g. number of persons, number of employers, number of transactions, amounts to be collected or paid), defining the value is relatively straightforward. However, value may also refer to achieving public policy outcomes, improvement in the quality of services provided to those whom the organization exists to serve, managing risks, and complying with legislation and regulations. While the concept of value relates to achievement of the institution's strategic plans with the resources used to do so, value delivery concerns executing the value proposition throughout the delivery cycle, ensuring that ICT-based activities deliver the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of the ICT elements (hardware, software, services).

The aim of ICT-related value management is to optimize value and enable an organization to:

- Clearly define and communicate its view of what constitutes value, and to whom;
- Select and execute investments;
- Manage its assets and optimize value with the affordable use of resources and an acceptable level of risk.

Other important characteristics of the ICT elements in which institutions invest are their diversity, interrelationships and life cycle features. In order to deal with them as consistently as possible, the overall set of ICT elements can be managed as a portfolio of enablers of ICT-based social security services. Thus, an ICT portfolio (Guideline 8) can be defined as the overall "objects of interest" (hardware and software, ICT services, ICT projects, other ICT assets or resources) managed and monitored to optimize business value. For social security institutions, managing the ICT portfolio in a systematic way is crucial

to achieving the expected return on investment for ICT-related investments and to satisfy cost–benefit relationships. Therefore, these guidelines recommend managing ICT investments by applying a portfolio-based approach. Managing ICT investments, through procurements and contracts, constitute challenges by themselves.

Finally, but no less importantly, managing ICT investments involves permanent monitoring and evaluation of results (Guideline 9). These guidelines recommend doing this at different levels: monitoring and evaluating the overall value of the ICT-enabled activities, the ICT-portfolio performance and the specific outcomes of ICT-based activities.

Guideline 7. Defining concept of value and approaches to optimize its realization

The institution clearly defines its own concept of value and the management practices devoted to generating the results expected from ICT-related investments (in ICT-enabled initiatives, services and assets) throughout their economic life cycle.

This involves defining the value of the outcomes to be achieved, analysing the cost-result of ICT investments and evaluating the return on investment of ICT-related initiatives.

Guideline 8. Managing ICT investments through a portfolio-oriented approach

The institution establishes processes to implement and manage ICT investments, acquisitions and contracts, taking into account (institutional and ICT-related) strategic plans, technology roadmaps and good governance principles, aiming at optimizing ICT value realization.

The purpose is to optimize the performance of the overall portfolio of ICT resources and related activities in response to programme and service performance and changing priorities and demands.

Guideline 9. Monitoring and evaluation of ICT-enabled investments

The institution monitors the performance of ICT-enabled investments and services, evaluates whether they generate the expected value and match the institution's goals, and determines whether adjustments are necessary.

The overall goal is to ensure that value is created and continues to be created throughout the investment life cycle.

A.4. ICT Service Delivery

This set of guidelines addresses the delivery and support of ICT services, covering the aspects related to the overall software and service life cycle (planning, development and software construction, operations and maintenance). The purpose of ICT service delivery is to provide agreed levels of service to users, and to manage the technology that supports the application of administrative procedures implemented by the institution.

It is only during this stage of their life cycle that services actually deliver value to the business, and it is the responsibility of ICT services staff to ensure that this value is delivered.

The objectives of ICT service delivery are to:

- Provide users with appropriate means to access the institution's services, particularly through multichannel online systems;
- Maintain business satisfaction and confidence in ICT through effective and efficient delivery and support of agreed ICT services;
- Minimize the impact of service outages on daily business activities;
- Ensure that access to agreed ICT services is only provided to those authorized to receive those services.

These guidelines address the issues related to system construction and ICT-based service delivery. The goal is to provide a systematic and standardized approach to managing software applications, technical issues, system operations, requests and incidents.

It is important to note that ICT service delivery has to deal with, and try to keep in balance, conflicting goals, such as stability versus responsiveness, quality versus cost of service, and reactive versus proactive approaches.

Guideline 10. Software development and application management

The institution establishes a systematic and standardized framework for developing and managing its software applications throughout their life cycle, including requirements, design, the build, deployment, operation and optimization.

Guideline 11. Implementing e-services

The institution implements electronic-based services (e-services) to improve service delivery by enabling users to interact with the institution remotely, and eventually autonomously.

Such e-services are multi-channelled, being based on different mechanisms (e.g. the Internet, mobile phones, call centres, kiosks).

Guideline 12. Managing technical support

The institution implements systematic and standard technical management practices to ensure the availability of resources to support the service life cycle.

Technical management activities involve planning, implementing and maintaining a stable technical infrastructure and ensuring that required resources and expertise are in place to design, build, transition, operate and improve information technology services and supporting technology.

Guideline 13. ICT operations management

The institution implements ICT operations management activities, which perform the daily operational activities needed to manage ICT services and the supporting ICT infrastructure following systematic and standard practices.

ICT operations management is responsible for the management and maintenance of the ICT infrastructure required to deliver the agreed level of ICT services to the institution. It consists of performing the daily operational activities, such as running the web-based systems for online citizen operations, benefit calculation and delivery processes, and the back-end systems that support both internal and web-based operations.

Guideline 14. Service desk and request fulfilment

The institution implements a service desk to provide a single, central point of contact for all users, enabling them to request standard services, and to provide information about services and procedures for obtaining them.

Guideline 15. Managing events, problems and incidents

The institution permanently monitors, analyses and treats ICT-related events and problems in order to prevent incidents. In turn, incidents are managed in order to restore normal services as quickly as possible and minimize the adverse impact on business operations.

A.5. Data and Information Management

Data and information are fundamental assets for social security institutions. The scale of social security institutions and relevance of the activities they develop increase the complexity of and risks related to data management. Institutions make key decisions based on data and information about people, including employees, employers and work activities.

Constructing social security corporate data is complex and costly as it usually covers a large proportion of the country's population and long life events. In addition, errors or misuse of this data could have important social and political impacts.

Therefore, data and information administration has to be based on an institution's corporate policies and practices. Systematic and standardized approaches to data and information management enable institutions to address these challenges and also take advantage of internationally developed knowledge.

This set of guidelines addresses issues of the effective and efficient planning, control and exploitation of data and information resources throughout their life cycle. They are based on standards and quality properties for data/information and processes to access and update data/information.

Guideline 16. Developing a data governance framework

The institution establishes a data governance framework to formalize the exercise of authority and control (planning, monitoring and enforcement) over the management of data assets.

The data governance function guides how all other data management functions are performed.

Guideline 17. Developing a master data model and system

The institution develops a unique master data model, which standardizes the definition of the core objects and relationships (e.g. persons, employers, enrolment periods, benefits). A corresponding ICT-based master data system fosters the consistency of such information.

The master data model should be of a highly stable specification covering information items used in most of the social programmes. The model can be viewed as the intersection of the sets of information items used in the social programmes. On the other hand, objects associated with specific programmes and their operations should not be included in the model (e.g. benefit payment information, variants on benefits).

Guideline 18. Data development and operations

The institution carries out data development and operation activities in a systematic and consistent way.

Data development concerns the analysis, design, implementation, deployment and maintenance of data and information systems. Data operations, which involve database and data technology administration, aim at managing the availability of data throughout its life cycle, optimizing the performance of database operations and protecting the integrity of data assets.

Guideline 19. Data quality management

The institution carries out unified and formalized data quality management, enabling it to improve the reliability of data and information used in the institution and, therefore, confidence in related processes.

As data is a key asset for social security operations, managing its quality becomes a required activity. The goal of data quality management is to formally and rigorously manage the data quality attributes that are relevant in social security operations.

Guideline 20. Mechanisms for information retrieval and analysis

The institution implements effective and efficient mechanisms for information retrieval and analysis which provide the means to exploit existing data assets, especially to support decision-making.

The effectiveness and efficiency of processes using information will, therefore, strongly depend on the mechanisms to retrieve and analyse the information.

B. Key Technologies

Structure

The following guidelines are organized in three sections:

Section B.1, Interoperability, focuses on implementing integrated ICT systems by ensuring the interoperability of the social security institution's own systems with independent ICT-based systems.

Section B.2, Data Security and Privacy, addresses the issues of providing data security and protecting data privacy when integrating data from social programmes.

Section B.3, Mobile Technologies, addresses mechanisms to implement ICT-based services for use through mobile devices (phones, tablets, etc.).

B.1. Interoperability

This section of the guidelines provides a high-level reference point for social security institutions applying interoperability techniques. The six guidelines which follow form a starting point from which institutions can develop their own policies and plans, and will assist in addressing the challenges of interoperability through a consistent and standards-based approach. The guidelines canvass the five dimensions of interoperability: political, legal, organizational, semantic and technical.

Guidance is based upon well-recognized principles and best practice related to interoperability, based on frameworks, models and interoperability recommendations. It has been drawn from several guidelines and reports, and input from public administrations, private industry, professionals in social security institutions, and standards and specifications bodies such as W3C, OASIS and the Open Group.

These six guidelines are oriented towards ICT staff, executives and managers accountable for interoperability between institutional systems. They must understand the different dimensions of interoperability to implement the proposed framework and application model. They are responsible for defining a service-oriented architecture (SOA) to implement interoperable systems by identifying the services to be connected, related business processes, the information structure and the data exchanged.

These guidelines may be applied at any stage of an activity, function, project, product or asset involving information. While, in general, interoperability techniques can be applied to complete information systems and facilities, they can also be directed to individual system components or services where this is practicable and useful.

Guideline 21. Institutional interoperability framework

The institution establishes an interoperability framework to formalize a systematic and standardized approach to the implementation of integrated social security systems.

The framework covers all levels of the organization and specifies the political and legal context, the business processes and concepts involved in interoperability operations, and the technologies used to implement them.

Guideline 22. Workplan for the implementation of interoperability-based social security programmes

The institution has a workplan to manage the overall implementation of interoperable social security programmes.

Implementation may depend on prior steps having been achieved, such as developing supporting information systems, signing agreements with other organizations and installing enabling technologies. The workplan should cover all required information resources and products and facilitate economies of scale in implementation.

Guideline 23. Institutional interoperability application model

The institution defines a service-oriented architecture (SOA)-based model to guide the application of interoperability in the implementation of integrated social security systems.

In order to provide practical benefits to implementation, the model comprises key components such as basic registries and interoperability services.

Guideline 24. Institutional semantic interoperability

The institution implements a strategy on developing information resources that fosters semantic interoperability and mainly consists of metadata systems.

Semantic interoperability concerns the non-ambiguous definition of core concepts used in the institution. It has a key impact on the success and quality of system interconnections as well as on the shared use of common information systems.

Guideline 25. Interoperable shared data services (basic registries)

The institution develops interoperable shared data services (basic registries) in accordance with the interoperability application model.

Shared data services play an essential role in the implementation of integrated social security systems. This includes the sharing of core social security data. Typically shared is data on benefits granted to beneficiaries, beneficiaries' family links, employees' worked periods, salaries and contributions, employers and contracted employees.

Guideline 26. Institutional technical standards on interoperability

The institution defines technical standards for interoperability technologies to foster the consistency and compatibility of ICT systems.

B.2. Data Security and Privacy

This section of the guidelines provides a high-level reference point for the management of information security and privacy in social security institutions. The eight guidelines which follow form a starting point from which institutions can develop their own policies and plans, and will assist in addressing the challenges of information security through a consistent and standards-based approach. They are also intended to raise awareness of the security risks to information assets and to indicate how to deal with them.

Guidance is based upon well-recognized principles and best practice related to planning, risk management and performance measurement. It has been drawn from several policy instruments, guidelines and reports from various jurisdictions, and input from private industry, professionals in social security institutions and standards bodies such as the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) and Information Systems Audit and Control Association (ISACA).

These eight guidelines are oriented towards ICT staff, executives and managers responsible for the security of information assets, and staff responsible for initiating, implementing and/or monitoring risk management and information security within their organizations. They may also be useful for departmental corporate risk managers, strategic planners, coordinators and other specialists who play an important role in helping to integrate security into corporate risk management, planning and performance measurement.

These guidelines may be applied at any stage of an activity, function, project, product or asset involving information. While information security management is usually applied to complete information systems and facilities, it can also focus on individual system components or services where this is practicable and useful.

Guideline 27. Management framework for information security

The institution establishes an information security management framework which defines the main procedures, duties and responsibilities in this domain.

Guideline 28. Data privacy policies and regulations

The institution establishes policies on data privacy management based on the corresponding regulations.

This refers not only to national regulations but also to requirements related to international data exchange.

Guideline 29. Security measures for data privacy

The institution establishes security measures to enforce data privacy policies for personal and sensitive data in particular.

This covers specific security issues affecting the implementation of a global system for the protection of privacy and personal data, and measures specifically related to privacy and personal data (covering both routine files containing personal data and sensitive personal data files).

Guideline 30. Comprehensive access control system

The institution implements a comprehensive system to control access to technological equipment and devices and software systems.

This includes mechanisms for data access control, endpoint access control, authentication and identification, user privilege management, network access control, password management and logs.

Guideline 31. Security in database systems

The institution incorporates security measures in its database systems, especially those storing critical data.

This involves: database administration procedures and practices; system accounts, privileges and roles; identification of users of applications; and database infrastructure.

Guideline 32. Security in networks and communication systems

The institution includes security measures in networks and communication systems, especially those linked with critical systems and information resources.

This involves the security of local area networks, the Internet, and wireless, FTP, email and mobile technologies and systems.

Guideline 33. Security in application development

The institution implements security measures in software application development, especially for Internet-based applications.

Guideline 34. Security in ICT operations

The institution establishes mechanisms to enforce security policies in ICT operations.

This includes software and patch management, protection against computer viruses and malicious codes, administration of operating systems and backups.

B.3. Mobile Technologies

This section of the guidelines covers the types of mobile services which social security institutions might offer, and their technological and organizational implications. These may vary according to the current level of deployment of mobile technologies in the country and institution concerned. The five guidelines which follow will assist those responsible for developing mobile services to focus on the technical decisions and choices to be made. They take account of success stories in both social security and other types of institutions, and of all existing technologies.

These guidelines are primarily intended to assist staff in the ICT unit of the social security institution. They focus on the specific features of each type of service according to the complexity and development stage of the institution's mobile services, and on evaluating system implementation, maintenance issues and costs, and opportunities to support new services within existing ones. The management of the institution must also consider the implications of these guidelines in view of their possible impact on the supply of services and maintenance costs. In addition, these guidelines may mean that the technical development and operational teams will have to adapt their skills, and they will help identify new skills requirements.

Three main elements are required to implement social security mobile services:

- User device. The potential users of these services are not only beneficiaries, but also social security managers and employers. The device characteristics and capabilities will be very important as they may limit the types of services to be accessed;
- Server infrastructure. As the core of the services deployed, the institution's servers must combine new mobile services with previously existing services and ensure data coherence and interaction with external servers and user devices;
- External service providers. The servers of external providers are needed to implement complex mobile services which are based on a combination of the capabilities of other providers.

These guidelines are applicable to institutions regardless of their level of use of technology, since they can be used to analyse what has been accomplished so far and guide the development of more advanced services.

While following these guidelines, each institution will need to prepare its own plan for the development of mobile services adapted to its specific needs, based on the judgements of experts in the technology and on the specificities of the institution.

Guideline 35. Institutional framework for the application of mobile technologies

The institution establishes a framework for the application of mobile technologies which defines the main procedures, duties and responsibilities, and technical standards, and includes an application strategy plan.

The application strategy could be a medium-term, three- to five-year plan.

Guideline 36. Variety of mobile services to be provided

The institution develops mobile-based services according to institutional plans, taking into account the main types of user interaction and system integration approaches.

Guideline 37. Mobile device-based user identification

The institution establishes a legally valid, efficient and secure means of maintaining an association between a user and a mobile device when a transaction is performed.

Such user identification will be required for several intermediate and advanced services.

Guideline 38. The mobile device as a gateway for payments and contributions

The institution evaluates the use of mobile devices for the collection of contributions and payment of benefits, taking account of the various methods of payment and technological options available.

Guideline 39. Using advanced hardware components included in mobile devices

The institution considers the use of advanced hardware components ("gadgets") in mobile devices to improve services, such as fingerprint readers for personal identification based on biometrics.

C. Social Security Components

Structure

The following guidelines are organized in two sections:

Section C.1, Master Data Governance and Master Data Management, addresses master data management concepts and activities, as well as organizational aspects to implementing master data in social security institutions.

Section C.2, ICT-based Implementation of International Agreements, addresses the implementation of the operational aspects of international agreements by using ICT, and focus on data exchange processes and related functions.

C.1. Master Data Governance and Master Data Management

Social security operations and strategic decisions are based on the mission-critical availability of data related to the individuals and stakeholders involved in social programmes managed by institutions. As a consequence, the reliability of these operations and adjudications are based strongly on the reliability of the used data. Among the large volumes of data managed by social security institutions there is a key subset that is common to social programmes, and its quality and management have a strong impact on the overall activities of social security institutions.

According to Allen Dreibelbis et al., "As companies struggle to become more agile by implementing information systems that support and facilitate changing business requirements, the management of core information, such as information about customers or products, becomes increasingly important. We call this information master data" (*Enterprise master data management: an SOA approach to managing core information*, Pearson Education, 2008). Master data has been described as "the authoritative, most accurate data available about key business entities, used to establish the context for transactional data. Master data values are considered golden" (Mark Mosley et al., *DAMA guide to the data management body of knowledge*, Technics Publications, 2010).

The master data in social security institutions consists of the subset of all the managed data that is required to carry out the social programmes. That data is also known as "corporate information systems" or "single registries". They are especially relevant because they provide a formalized and single institutional framework of the most relevant concepts used in the institution: employees, beneficiaries, families, contributors, employees' work history, and so on. Social security institutions require reliable information systems capable of supporting all master data and master data management operations. It is important that such information systems manage the quality of the data as regards completeness and accuracy to the greatest extent possible.

In turn, Master Data Management is defined in the *DAMA guide to the data management body of knowledge* as "the process of defining and maintaining how master data will be created, integrated, maintained, and used throughout the enterprise. The challenges of master data management are: 1) to determine the most accurate, golden data values from among potentially conflicting data values; and 2) to use the golden values instead of other less accurate data".

The following guidelines address master data management concepts and activities, as well as organizational aspects to implementing master data in social security institutions. They complement Guideline 17, Developing a master data model and system, Section A.5, Data and Information Management.

Background: Programmes and committees in MDGP and MDMP

Social security institutions need to manage data through clear lines of decision-making and authority from an organization-wide strategic perspective. This activity is known as *data governance*. When the data to be governed are master data, the activity is sometimes known as *master data governance*. When several actions related to master data governance are planned to bring about a specific implementation, it can be said that a *Master Data Governance Programme* (MDGP) is to be designed and executed. To bring a Master Data Governance Programme to tactical and/or operative levels, data stewards should be in charge of the data management operations by means of a *Master Data Management Programme* (MDMP). The group of staff in charge of the Master Data Governance Programme is commonly referred to as the *Master Data Governance Committee*. The group of staff in charge of the Master Data Management Programme is commonly called the *Master Data Stewardship Council* or *Master Data Management Committee*.

There is a close relationship between the Master Data Governance Programme (MDGP) and Master Data Management Programme (MDMP). The MDGP aligns the master data initiatives with the institutional goals in order to maximize the value of the master data and according to the Data Governance Programme; the MDMP implements and maintains the master data information systems in support of the master data operations.

To carry out the activities defined in these guidelines, social security institutions should create teams with the appropriate skills and mandate. It is particularly important that the Master Data Governance and Master Data Management Programmes be supervised to ensure that they are performed in a manner that is aligned with the social security institution's goals and objectives. For the purpose of these guidelines, we distinguish the following bodies:

- **Board and senior management**, who are responsible for the following aspects:
  - Establishing a strategic vision on the relevance of master data management for achieving the social security functions in the institution's mandate;
  - Driving organizational and cultural evolution towards corporate, institution-wide management of the institution's core data;
  - Supporting, among others, the Master Data Governance Programme institution wide, as a backbone for the institution's activities. This involves budgetary and organizational measures.
- The **Master Data Governance Committee** is the group of professionals in charge of the Data Governance Programme, and more specifically the Master Data Governance Programme (MDGP). This committee is responsible for:
  - Appointing high-ranking representatives of data-owning business functions who can make decisions about master data for the institution;
  - Appointing members of the Master Data Stewardship Council;
  - Approving the decisions of the Master Data Stewardship Council;
  - Approving policies related to master data.

- The **Master Data Management Committee** or **Master Data Stewardship Council** is the group of professionals in charge of the Master Data Management Programme (MDMP) at both technical and accountability levels. This Committee, or Council, is responsible for:
  - Carrying out development projects on the master data system;
  - Maintaining organizational expertise on the social security master data;
  - Maintaining the meaning and value of data;
  - Making recommendations on data decisions and writing data-related procedures.

Components of the master data architecture

In order to address the necessary issues, the following components of the master data architecture are identified:

- **Architecture of the master data system**, which is responsible for storing and supporting operations on the master data. The architecture has to provide the means of achieving both the functional and the non-functional requirements established in the institution, and may have to take into account interaction with external institutions to access data as well as to provide services to them.
- **Architecture for the master data management systems**, which should provide support to the specific master data operations, for example those related to master data quality cleansing, master data quality profiling, and master data management configuration (both entities and models).
- **Architecture for the master data governance system**, which should provide support for the various actions related to the Master Data Governance Programme. For instance, it should provide software components for monitoring and efficiency.

All these components are addressed in these guidelines with the aim of supporting social security institutions in their efforts to develop an integrated solution.

ICT standards and frameworks

To gain the widest possible understanding of all the concepts introduced in this document, the reader is encouraged to consult the following international standards – both *de jure* and *de facto* – that have been used as a background to support specific guidelines (listed in alphabetical order):

- COBIT® 4 and COBIT® 5
- DAMA DMBOK (2009) and/or (2015)
- ISO 20000 and ITIL®
- ISO 27000
- ISO 38500
- ISO 8000, parts 100–140

Principles

The six principles presented and defined in Section A.1 should also be observed by social security institutions when implementing master data systems. The following guidelines are intended to make

the implementation of such master data management systems easier, focusing always on optimizing the value of master data. The first step is to implement a Master Data Governance Programme.

Structure

Master data can be considered as among the most important assets for the adequate performance of social security institutions. It is important to highlight the fact that master data management is both an organizational/business-based and technological function. The most difficult part is to establish adequate links between these two functions.

The following guidelines are organized in four sections:

- **Section C.1.1, Master Data Governance and Master Data Management,** addresses the institutional decisions that must be taken to guide the design and implementation of master data projects as well as daily operations. The section begins with the design of the master data programmes aligned with the institutional ICT governance principles. The definition of a strategy and action plan follows, including the preliminary scope of the master data. The last guideline in the section addresses the issues of determining and optimizing the value of the master data and aims to provide elements relevant to investment decisions on master data systems.
- **Section C.1.2, Data Quality,** addresses the key issues of managing the quality and reliability of the master data. These guidelines focus on specific recommendations to manage quality in master data through preventive and corrective measures.
- **Section C.1.3, Design and Implementation,** addresses the activities involved in the implementation of master data systems, starting with the specification of architectures, continuing with implementation and change management, and finishing with the interoperability and security features to be considered in master data systems.
- **Section C.1.4, Master Data System Operations,** presents recommendations concerning ICT operations for master data systems in order to comply with service-level agreements (SLAs).

C.1.1. Master Data Governance and Master Data Management

Guideline 40. Master Data Management and Master Data Governance Programmes

The institution carries out a unique and integrated programme for master data governance aligned to ICT and organizational governance, as well as a Master Data Management Programme that implements the Master Data Governance Programme.

Guideline 41. Strategies, policies and roles

The institution establishes strategies, policies and plans for implementing the Master Data Governance and Master Data Management Programmes.

Guideline 42. Optimization of master data value

The institution determines the value of the master data and performs master data governance and master data management practices to optimize the results expected from ICT investments (services and authorized assets of ICT) throughout the master data life cycle.

This involves an estimation of the value of the results that have been achieved and cost–benefit results of investments in ICT for master data management and governance, as well as an evaluation of the return on investment of initiatives connected with the acquisition, storage, querying, import and export of data.

C.1.2. Data Quality

Should the master data not be of adequate quality, the functions involving these data will probably fail. In order to avoid the failure of key social security functions, it is necessary to carry out activities that ensure that the quality of the master data will be adequate for the tasks in which they will be used.

Guideline 43. Master data quality management

The institution manages the quality (e.g. completeness and accuracy) of the master data through a formalized and single institutional framework, with the aim of improving the reliability of the data used in the institution and, consequently, fostering confidence in related processes.

Since the master data are a key asset in social security operations, quality management is critical. The goal is to formally manage the quality attributes of the data which are relevant to social security operations through a single institutional framework. This includes verifying that the operations satisfy the business rules associated with the master models.

Guideline 44. Preventive measures to foster the quality of master data

The institution implements preventive measures to foster the quality of the master data, especially by communicating data quality requirements to development teams and to master data operations and personnel responsible for master data-related tasks.

Guideline 45. Improvement of master data quality

The institution implements measures to ensure adequate quality levels in the master data and to improve the quality when necessary.

These measures, which are based on data quality goals and indicators, typically consist of corrective master data profiling and master data cleansing operations. In order to be cost effective, the data quality goals have to be clearly defined.

C.1.3. Design and Implementation

Guideline 46. Architectures for master data systems

The institution defines architectures for the master data system, the master data governance system and the master data management system.

These three information systems should be adequately defined and conveniently integrated into the institutional architecture in order to better support the master data operations through the master data life cycle. This implies designing adequate architectural styles for the master data systems and the management information system in order to leverage maximum value for the institution's master data.

Guideline 47. Implementation of master data systems

The institution implements the master data systems taking into account the functional requirements of all involved business areas of the institution.

Guideline 48. Management of master data system evolution

The institution puts into practice specific processes to manage change, maintenance and the evolution of the master data system.

As the master data system is at the core of the institution's information systems and is used by a large number of systems, change and evolution have to be managed so as to minimize impacts and service disruptions. Therefore, the information model of the master data system should reflect the concepts used throughout the institution.

In addition, although the master data model and its implementation are considered to be stable, some maintenance operations will need to be executed. These operations should be part of the continuous improvements in the institution. Institutions should consider master data maintenance as part of the master data management activities. In turn, these activities will guarantee that the master data are updated, including integrity rules associated with the master data model.

Guideline 49. Master data system interoperability

The institution implements effective and quality-preserving interoperability mechanisms not only with other systems within the institution but also with external systems.

In addition to providing the means of interaction with other systems, interoperability mechanisms should keep track of the provenance of data obtained from other institutions.

Guideline 50. Security and privacy of master data

The institution establishes a framework for the management of the security and privacy of the master data based on the relevant regulations.

C.1.4. Master Data System Operations

The ICT operations of master data systems comprise the system administration activities that enable the use of the master data in the institution.

Given the critical nature of the master data system, the corresponding ICT operations have to ensure the service quality levels (e.g. availability, performance, etc.) required to carry out the social security operations using these data. Such quality levels are established in a service-level agreement (SLA).

Guideline 51. Operations to comply with SLAs on master data systems

The institution carries out ICT operations to enable the use of the master data system in compliance with the corresponding service-level agreements (SLAs).

The institution continuously monitors the availability and performance of the master data systems. Interruptions and malfunctioning of the master data systems should be prevented by setting up alarms that would warn the ICT team of an SLA violation (i.e. event, incident or problem).

C.2. ICT-based Implementation of International Agreements

International social security agreements make possible the portability of benefits for millions of insured people and generate the export of billions of dollars in cash benefits around the world among signatory countries. This involves significant cross-border data exchange and back-office information processing. The effective and reliable implementation of agreements therefore requires an intensive application of ICT to ensure the integrity of the process. In spite of the increasing application of ICT in social security, the ICT-based implementation of international agreements remains challenging, in large part because of a lack of standards.

International social security agreements constitute a key legal instrument that enable the portability of social rights to migrant workers by ensuring that periods of employment are taken into account for granting benefits in the signatory countries. International agreements also aim at preventing the "double contribution" of temporary workers in a host country, enabling costs savings without reducing social protection.

While most international social security agreements are bilateral – being concluded by two countries – there are some multilateral agreements allowing several countries to coordinate parts of their social security schemes.

These guidelines address the implementation of the operational aspects of international agreements by using ICT, and focus on data exchange processes and related functions.

The overall development of a social security agreement involves two streams of activities. First, it involves carrying out preliminary discussions and negotiations, preparing the agreement text, signing and ratifying the agreement, and defining when the agreement will start to be applicable (so-called *entry into force*). Second, it requires setting up the administrative procedures to respond to requests related to the agreement as well as defining the roles and responsibilities for these tasks. The latter are usually established in the so-called administrative arrangements attached to the social security agreement.

The implementation of international agreements requires reliable mechanisms for data exchange among the involved institutions. This includes, among other matters, defining the data to be exchanged, the authentication mechanism (e.g. electronic signature), the protocol for request-response exchanges specifying maximum delays, as well as implementing the ICT-based systems to support these operations. Moreover, it also involves carrying out the daily operation of the agreement, through automated processes to the greatest extent possible, which mainly consists of receiving and sending information and notifications of changes as well as processing benefits claims.

As the operational tasks involve cross-border data exchange and information processing, intensive usage of ICT is necessary to achieve effectiveness and reliability in the application of the agreement.

In spite of the increasing application of ICT in social security, the ICT-based implementation of international agreements remains challenging. The lack of standards on data and processes is the main reason. In addition, the complexity of developing inter-institutional and cross-border systems constitute a barrier for implementing ICT-based systems supporting international agreements.

While several recommendations, frameworks and guides have been developed to address the policy- and legal-related activities leading to the entry into force of the agreement, there are no similar materials supporting the operational implementation and the daily operations of international agreements. The

following guidelines support the ICT-based implementation of social security agreements by focusing on the operational aspects.

Definitions

The overall implementation of international social security agreements involves stakeholders whose roles are usually mentioned in the texts of the agreements. The following definitions provide the context in which they are used in these guidelines:

- *Competent authorities* refers to the ministries authorized under the social security legislation of a party participating in the agreement to administer that legislation. For example: the Minister of Labour and Social Affairs of Spain; the Secretary of Health and Human Services of the United States; the Minister of Employment and Social Development of Canada; the Minister of Overseas Indian Affairs; the Minister of Labour and Social Security of Uruguay; in Argentina, the Minister of Labour, Employment and Social Security and the Minister of Health; the Minister of Human Resources Development of the Republic of Korea; etc.
- *Liaison agencies (or liaison institutions)* refers to the organizations that ensure the coordination and exchange of information between the institutions of the parties participating in the agreement. Countries may define one or more liaison agency for all the different matters covered by an agreement. For example: the Federation of Administrative Bodies of Spanish Social Security; the Social Security System of the Philippines; the Japan Pension Service; Service Canada and the Revenue Agency for Detached Workers; the Social Security Administration of the United States; in France, the Centre for Social Security of Migrant Workers and the National Independent Social Security Fund for Miners; the Social Insurance Bank of Uruguay; in Argentina, the Superintendence of Health Services for health schemes, the National Administration of Social Security for pensions and family benefits, and the Superintendence of Labour Risks for workplace accidents; etc.
- *Competent institutions* refers to the institution(s) responsible for administering the legislation to which the agreement applies, particularly social security schemes. Many agreements use the generic phrases "the competent authority" and "the institution which is competent according to the legislation applicable". For example: the Minister of Employment and Social Development of Canada; the National Pension Service of the Republic of Korea; the Japan Pension Service; the National Social Security Fund of Morocco; the Employees' Provident Fund Organisation of India; the Social Insurance Bank of Uruguay; the Federation of Administrative Bodies of Spanish Social Security; the Social Security System of the Philippines; the National Old-Age Insurance Fund for Employees of France; etc.

Structure

The following guidelines address:

- The design and implementation of the operational processes and data exchange mechanisms using ICT, which includes the notification of changes to relevant information;
- The daily operation of the agreement, by applying the implemented processes and mechanisms to specific cases. This consists of receiving and sending information, notifying changes and processing benefit claims.

The guidelines are based on a number of assumptions in the context of the overall process of implementing an international agreement:

- The text of the agreement has been signed and has entered into force. The issues involving the socio-economic design and preparation of the text of the agreement, as well as negotiations for the agreement to be signed and entered into force, are out of the scope of these guidelines.
- There are well-defined national regulations on data protection as well as conditions established in the agreement. Although the guidelines may provide insights on these matters, they do not aim at influencing these elements.
- There are well-defined organizational structures at the international, national and institutional levels to manage the policy, regulatory and procedural aspects of the agreement as well as the relationships with other social security services. Therefore, these guidelines do not aim at designing such structures.

While some of the guidelines focus on institutional aspects, others address issues to be jointly defined at the international level by the institutions participating in the agreement.

The guidelines cover diverse scenarios and can be used in various ways according to the characteristics of the international agreements and the role the institution plays in their implementation. While implementing multilateral agreements requires taking into account all the recommendations, the implementation of bilateral agreements can be done by following a subset of the recommendations. In turn, institutions playing a liaison role should use those guidelines addressing features at the international and national levels, while those having the "competent institution" role would need to apply those guidelines focusing on the institutional level.

The following guidelines are organized in six sections:

- **Section C.2.1, Governance and Management,** begins with a definition of the mission, roles and governance structure for the ICT-based implementation of the agreements, and follows the establishment of a strategy and action plan. The last guideline in the section addresses the definition of the main administrative principles for the agreement.
- **Section C.2.2, Architectures,** addresses the specification of architectures at the international, national and institutional levels. The goal is to define the components enabling the implementation of effective and secure interactions among the institutions. Defining the architectures is one of the first and key steps in the implementation of an international agreement.
- **Section C.2.3, Interoperability for International Agreements,** addresses the key aspects of applying interoperability techniques for the implementation of international agreements. These guidelines, which further develop the related guidelines found in the current set of Guidelines, present the steps for defining an interoperability framework for the implementation of international agreements.
- **Section C.2.4, Security and Authentication for International Agreements,** addresses the key issues in the authenticating operations of the international agreement, complying with data protection regulations and putting into practice a secure environment for the institutions' interaction. These guidelines refine Section B.2, Data Security and Privacy, in this set of Guidelines.

- **Section C.2.5, Operational Processes and Information Models,** addresses the specification of the processes and information models involved in the implementation of international agreements.
- **Section C.2.6, ICT Operations of the International Agreements,** includes recommendations concerning ICT service delivery practices for the international agreements. These guidelines focus on the definition of service quality indicators (service-level agreements, or SLAs) and on setting up the system operations that will enable the carrying out of specific transactions in the context of the agreement.

C.2.1. Governance and Management

Guideline 52. Governance and management of the ICT-based implementation of international agreements

The institution defines its mission, roles and governance structure to implement the operations of the international social security agreements under its mandate in order to protect the social security rights of migrant workers.

If applicable, the institution participates in defining the governance structure for the international and inter-institutional levels.

Guideline 53. Strategy and action plan

The institution establishes a strategy and an action plan to implement the international social security agreements.

Guideline 54. Administrative principles for the main operations and resources of the agreement

The institution defines administrative principles to manage the main operations and resources of the international agreement.

The main operations include data exchanges based on requests/responses, notifications of changes and relevant information about persons covered by the agreement. The main resources comprise information models of the data exchanged, digital certificates and signatures, and the software systems to be used for the implementation.

C.2.2. Architectures

This section addresses the definition of architectures, specifying the main ICT components that enable the implementation of interaction between institutions putting into practice international social security agreements.

The implementation of agreements involves three architectures:

- International architecture, which addresses interaction at the international level between liaison agencies of different countries;
- National architecture, which addresses interaction at the national level between the liaison agency and competent institutions in the same country;
- Institutional architecture, which addresses the interaction of institutions' internal ICT systems with the other entities at the international and national levels.

The architectures to apply on specific agreements depend on the characteristics of the agreement.

While the international architecture of multilateral agreements requires common services and a "trusted third organization", bilateral agreements could be based on point-to-point connections between the liaison agencies (e.g. using Web Services protocols).

In turn, the national architecture applies only when there are several national institutions coordinating with each other; it is not necessary when there is only one institution involved in the agreement, which is a very frequent scenario. Table 1 summarizes the criteria.

Table 1. *Criteria for architectures of international agreements*

	Bilateral	**Multilateral**
Only one national institution participating in the agreement.	• Point-to-point connections between the only national institution and the other liaison agency(s).	• Full International architecture (including common services and a "trusted third organization") connecting the single national institution and the other liaison agency(s).
Several national institutions participating in the agreement.	• National architecture connecting the institutions using point-to-point mechanisms or using an integration middleware. • International point-to-point connections between the national liaison agencies(s) and the others.	• Full International architecure (including common services and a "trusted third organization") connecting the national liaison agencies. • Full National architecture connecting the national institutions.

Guideline 55. International architecture

The institution, in coordination with the other institutions participating in the agreement, defines an architecture enabling it to perform international data exchanges in an efficient and secure way.

In the case of multilateral agreements, the international architecture may include a "trusted third organization" storing key common information, such as a log of transactions, digital signatures and certificates.

Guideline 56. National architecture

If several national institutions participate in the agreement, they define an architecture covering national exchanges.

The national architecture focuses on the coordination between the liaison agency and the competent institutions in the country, enabling exchanges with cross-border institutions through the international architecture.

Guideline 57. Institutional architecture

The institution defines an institutional architecture specifying the mechanisms to perform an effective and secure interaction between the institution's systems and those at the national and international levels.

C.2.3. Interoperability for International Agreements

Interoperability techniques enable the connection of the systems of different institutions, particularly at the international level; they are therefore among the essential technologies for implementing international social security agreements.

Guideline 58. Interoperability framework for international agreements

The institution, in coordination with the others participating in the agreement, establishes an interoperability framework to implement international agreements.

Guideline 59. Semantic interoperability

The institution, in coordination with the other participants in the agreement, defines semantic interoperability resources at the international level in order to improve the automatization of data exchange operations among institutions involved in the agreement.

Using semantic interoperability in the implementation of international agreements would provide unambiguous definitions of the concepts used by the institutions involved. These mechanisms would be mainly based on metadata systems and vocabularies related to the exchanged data types.

Guideline 60. Interoperable services

The institution, in coordination with other participants in the agreement, implements interoperable services in accordance with the institutional model of interoperability for the implementation of international agreements.

The implementation of international agreements involves the development of a service-oriented architecture and includes the development and implementation of a set of services. These services must be properly orchestrated within a business processes model adequate to carry out the processes described in international agreements.

C.2.4. Security and Authentication for International Agreements

Security and authentication are critical features for systems implementing international social security agreements. First, given the interorganizational and cross-border nature of these systems, institutions have to apply security and data protection policies and regulations. Second, the ICT-based implementation has to provide the means to validate the authenticity of the operations and to replace the handwritten signature.

This section includes guidelines addressing these issues and providing recommendations to define an authentication framework at the international level as well as implementation measures at institutional level.

Guideline 61. Authentication framework

The institution, in coordination with the other participants in the agreement, establishes an authentication framework to provide legally valid, efficient and secure means for the transactions carried out in the social security agreement.

This framework replaces that based on handwritten signatures used in paper-based transactions and provides the means to validate the authenticity of the electronically exchanged data.

Guideline 62. Model for implementing authentication of transactions in the institutions

The institution implements an authentication model to identify, authenticate and sign digital transactions between institutions participating in the international agreement.

This model replaces the handwritten signatures used in paper-based transactions and enables validation of the authenticity of the data exchanged.

Guideline 63. Security policies and measures for transactions and digital certificates

The institution establishes ICT-related security policies and measures to protect transactions performed in the social security agreement as well as the digital certificates.

Guideline 64. Enforcing data protection in transactions and in digital certificates

The institution implements measures to enforce the applicable data protection regulations on transactions of the international agreement as well as on digital certificates.

These measures are based on the corresponding national regulations as well as the conditions established in the agreement.

C.2.5. Operational Processes and Information Models

This section addresses the definition of operational processes and information models related to operations between institutions implementing international social security agreements.

Information models may be based on the "data exchange forms" as usually defined.

While information models and notifications are defined at the international level, there may be operational processes (or sub-processes) to be defined at national and institutional levels.

Guideline 65. Operational processes related to the scope of the agreement

The institution, in coordination with the other institutions participating in the international agreement, specifies the processes enabling the application of the agreement in specific cases.

Guideline 66. Processes related to notifications of changes and concerning other relevant information

The institution, in coordination with the other institutions participating in the international agreement, specifies processes to notify changes and other relevant information related to individuals covered by the agreement.

Institutions agree on notifying changes concerning the personal and working status of persons covered by an agreement, as well as other relevant information within the scope of the agreement. This information includes: death, marriage, separation, birth, other benefits received in the host or origin country, income declarations, etc.

Guideline 67. Information models of the data exchanged

The institution, in coordination with the other institutions participating in the international agreement, specifies information models for data exchange according to requests, administrative communications and notifications.

These models, which correspond to the usually defined "forms" to exchange data, may include: personal data, labour records, death, marriage, separation, birth, other benefits received in the host or origin country, income declarations, expenses related to procedures on individual cases, etc.

C.2.6. ICT Operations of the International Agreements

The ICT operations of the international agreements comprise the system administration activities that enable the use of ICT systems to perform specific case transactions of the agreement.

Managing the ICT operations for the agreements involves the following main aspects:

- Defining a set of service quality indicators and goals to be complied with by the institutions participating in the agreement. This service-level agreement (SLA) would include indicators such as maximum delays in responding to requests and notifying changes, as well as the expected availability and response time of the ICT services required for performing inter-institutional transactions (e.g. submitting an information request to another institution, querying the log of operations/transactions, etc.).
- Defining SLAs at the national and institutional levels, which would establish service quality conditions corresponding to those defined at the international level for the national institutions, as well as to each of the internal systems.
- Putting into practice measures to implement the institutions' internal services, which will enable the carrying out of the transactions of the social security agreement complying with SLAs defined at the international and national levels. These measures should take into account that the institution may be operating several social security agreements.

Guideline 68. Service levels for the agreement

The institution, in coordination with the other participants in the agreement, defines service quality indicators and goals for the main operations in the agreement at the international level. In addition, the institution defines corresponding indicators and goals for its internal systems with the aim of ensuring the fulfilment of the goals established at the international level.

These service-level agreements (SLAs) with indicators and goals should be complied with by the participant institutions as part of their commitment to the signed international agreement.

Guideline 69. Setting up and managing the ICT operations for social security agreements

The institution puts into practice the ICT operations to implement international agreements complying with the corresponding SLAs. This is carried out in the context of the institution's ICT operations, starting with an evaluation of the implications and requirements generated by the systems implementing international agreements.

Acknowledgements

The ISSA Guidelines for Social Security Administration were prepared by the ISSA General Secretariat with the ISSA technical commissions.

The *ISSA Guidelines on Information and Communication Technology* were produced under the auspices of the ISSA Technical Commission on Information and Communication Technology chaired by Maria Eugenia Martin Mendizábal of the National Social Security Institute, Spain. The Guidelines were prepared by a team at the ISSA General Secretariat led by Raúl Ruggia Frick. Expert support and contributions were provided by Salvador Otón Tortosa, José Ramón Hilera González, José María Gutiérrez Martínez, José Javier Martínez Herraiz, José Antono Gutiérrez de Mesa, Roberto Barchino Plata, Luis de Marcos Ortega, Eugenio Fernández Vicente, Luis Fernández Sanz, Lourdes Jiménez Rodríguez, Carmina Pagés Arévalo, José Amelio Medina Merodio, Antonio Moratilla Ocaña, Antonio García Cabot and Eva García López of the University of Alcalá, Spain, as well as Ismael Caballero and Mario Piattini Velthuis of the University of Castilla-la-Mancha, Spain.

4 route des Morillons
Case postale 1
CH-1211 Geneva 22

T: +41 22 799 66 17
F: +41 22 799 85 09
E: issa@ilo.org | **www.issa.int**