issa

ISSA Guidelines

Information and Communication Technology

Revised edition 2019

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 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>.

Revised and extended edition 2019

ISBN 978-92-843-1201-6

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, analytics 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, key technologies and the implementation of social security functions. They address the implementation of main social security functions and related resources as well as business processes, 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 Service Delivery

A.4. ICT Investment and Value Management

A.5. Data and Information Management

Part B, Key Technologies, incorporates four sections:

B.1. Interoperability

B.2. Data Security and Privacy

B.3. Mobile Technologies

B.4. Data Analytics

Part C, Social Security Components, incorporates four sections:

C.1. Master Data Management

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

C.3. eHealth – ICT Application in Healthcare

C.4. Implementation of social security business processes

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 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.4, 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.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. Application of the ICT governance framework

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

Established by recommendations of the *ISSA Guidelines on Good Governance*, the framework fosters the application of an institutional ICT Governance and related principles defined in international standards.

Structure

- The ICT Unit, in coordination with the ICT Governance Committee, should apply the ICT governance framework in all the ICT-related activities.
- The application of the ICT governance framework should be consistent with the institution's mission and governance structures.
- The application of ICT governance framework, established as recommended in the *ISSA Guidelines on Good Governance*, should follow international standards and practices on ICT (e.g. ISO/IEC 38500 and COBIT®).

Mechanism

- The board, with the assistance of the management, should issue a policy statement on the adoption of an ICT governance framework for the institution which establishes the main principles and governance approach. The framework should:
  - Enforce the principles of Responsibility, Strategy, Acquisition, Performance, Conformance and Human Behaviour, as defined in ISO/IEC 38500;
  - Cover the institution in its entirety, integrating the governance of ICT into the institution's general governance and covering all relevant functions and processes;
  - Enable the transformation of the institution's mission into an actionable strategy, by translating the institution's high-level goals into manageable, specific, ICT-related goals and mapping these to concrete processes and practices.
- The ICT unit, in coordination with the ICT Governance Committee, should apply the institutional ICT governance framework covering:
  - Strategic aspects that evaluate the current and future use of ICT, especially on innovative social programmes;
  - The preparation and implementation of plans and policies to ensure that use of ICT meets institutional objectives;
  - The definition of specialized roles with specific responsibilities to manage critical aspects, such as: investments, contracts and procurement of ICT products and services; data protection and security; and risk management and business continuity;
  - Monitoring of the conformance to policies, and performance against plans.
- The management should validate and communicate the ICT governance measures throughout the institution.

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.

Structure

- The board should commission the management and the ICT unit to establish ICT governance processes.
- A specialized organizational structure, reporting to or including the management, should be established to coordinate ICT governance processes. To establish accountability, the roles and responsibilities of units within that structure have to be well defined and documented.
- The ICT governance processes should follow the institution's ICT governance framework and be based on international standards and practices (e.g. ISO/IEC 38500 and COBIT®).

Mechanism

- The management, with the assistance of the ICT unit, should define ICT governance processes in order to:
  - Analyse and articulate the requirements for the governance of ICT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the institution's mission, goals and objectives;
  - Optimize the value provided to the institution's mission from business processes, ICT services and ICT assets resulting from investments;
  - Ensure that the institution's risk tolerance is understood, articulated and communicated, and that risk to the institution's value related to the use of ICT is identified and managed, especially concerning the operation of high-impact social programmes;
  - Ensure that adequate and sufficient ICT-related resources (people, processes and technology) are available to support the institution's objectives effectively at optimal costs;
  - Ensure the transparency of the performance and conformance measurement of ICT-related functions.
- The board should establish or delegate to the management the establishment of ICT governance structures, processes and practices.

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 5). 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. In this line, the implementation of e-services delivering a number of such functions constitutes nowadays a main activity of social security institutions (Guideline 6).

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.

Structure

- The management should commission the ICT unit to develop an ICT strategy and innovation prospective in line with the strategic directions established by the board and the management.
- Specialized roles should be established to manage processes concerning ICT strategy and innovation in the institution. To establish accountability, the responsibilities of the involved units have to be well defined and documented.
- The ICT governance processes should follow the institution's ICT governance framework and strategic plan, as well as institutional innovation strategies as recommended in the *ISSA Guidelines on Good Governance*, and be based on international standards and practices (e.g. COBIT®).

Mechanism

- The management, with the assistance of the ICT and specialized units, should establish processes to define and manage the ICT strategy and innovation prospective, which:
  - Define the strategic plan and roadmap for ICT developments in line with the strategic goals;
  - Establish an enterprise architecture consisting of business process, information, data, application and technology architecture layers for effectively and efficiently realizing institutional and ICT strategies;
  - Analyse opportunities for innovation or improvement which can be created by emerging technologies, services or ICT-enabled business innovation;
  - Establish institutional standards on ICT, defining system technologies and products to be used;
  - Establish an ICT-related investment mix, based on common understanding by the ICT unit and other business units of the potential opportunities for ICT to drive and support the enterprise strategy;
  - Maintain internal expertise required to keep a strategic control on the ICT products and services including carrying out appropriate training and professional development activities;
  - Maintain an awareness of information technology and related service trends, and identify innovation opportunities.
- The ICT strategy and innovation prospective should be included in the institution's strategic plan.
- The management should clearly communicate the institutional ICT strategy, to ensure that the objectives and associated accountabilities are understood throughout the institution and the ICT strategic options are identified, structured and integrated with the business plans.

Guideline 4. 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.

Structure

- The board should commission the management and the ICT unit to establish ICT management processes.
- A specialized organizational structure, reporting to or including the management, should be established to coordinate ICT management processes. To establish accountability, the roles and responsibilities of units within that structure have to be well defined and documented.
- The ICT management activities (planning, building, running and monitoring) should be aligned with the direction set by the board to achieve the enterprise objectives.
- The ICT management processes should follow the adopted ICT governance principles and ICT strategies, and be based on international standards and practices (e.g. COBIT®).

Mechanism

- The management, with the assistance of the ICT and specialized units, should define the ICT management processes covering the planning, building, running and monitoring of ICT-related activities and full coverage of ICT services within the institution.
- Management processes should cover the areas related to:
  - Aligning ICT elements with the institution's goals, as well as planning and organizing the overall ICT-related tasks. This includes:
    - Resource management, in particular budgeting and costs, human resources, suppliers, assets and service agreements;
    - Quality management, especially on key social security processes and assets;
    - Risk management, especially on key social security operations;
    - Security management;
  - Building, acquiring and implementing programmes, projects, ICT platforms and assets, including change management. This includes managing programmes and projects, managing requirements definition, and managing knowledge and assets;
  - Delivering, supporting and managing the continuity of ICT services;
  - Monitoring, evaluating and assessing the performance of ICT-based systems overall, and their conformity with the institution's goals and compliance with regulations.
- The management should define the organizational structure, optimizing the placement of ICT-related functions and establishing associated roles and responsibilities.

Guideline 5. 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.

Structure

- The management should commission the ICT unit to establish a systematic method based on business processes to operationalize the institution's mission and general objectives by identifying ICT-based approaches that enable their implementation.
- The management, through the ICT Governance Committee, should ensure that ICT-based solutions are implemented responding to users' needs, including but not limited to benefit administration, contribution collection, actuarial work, investments, programme design and evaluation, etc.
- The common architecture established in the ICT strategy and innovation prospective should be used as a framework to connect the social security and ICT elements.
- The method adopted to operationalize the institution's mission and general objectives should align with the institution's ICT governance as well as the ICT strategy. It should be based on the approaches recommended in this set of Guidelines for implementing social security business processes as well as other social security components.

Mechanism

- The ICT unit, with the assistance of the project managers and specialized units where applicable, should define and put into practice a systematic method to identify ICT-based approaches that enable the implementation of social security functions, taking into account:
  - Common characteristics of functions related to:
    - Policy and strategic definitions, which are usually carried out by the board and management;
    - Management of programmes and processes, which are developed by business units;
    - Service delivery, which focuses on users both internal and external (i.e. citizens) and on the mechanisms that facilitate applying procedures established by the institution, especially those implementing social security functions;
  - The implementation of cross-programme processes;
  - Integration between different systems and processes;
  - The implementation of corporate resources, such as master data or registries, which could play a key role in supporting the implementation of social security functions.
- The defined method could be based on a global map of social security functions and resources (e.g. the common architecture defined in the ICT strategy), from which connections to ICT-based solution approaches could be established.
- The outputs of this method should include implementation plans for ICT-related activities.
- The management should communicate the defined approach and related implementation plans throughout the institution.

Guideline 6. Implementing e-services

The institution implements online/digital services (e-services) 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) and cover all e-communication with customers.

Structure

- A strategy for improving the effectiveness, quality and efficiency of social security service delivery by providing multi-channel e-services should be adopted by the institution.
- The characteristics of the target public and, especially, constraints to access by specific population groups, should be taken into account. Standards on accessibility to e-services (web-based and mobile) should be followed.
- Regulations on data security and privacy should be taken into account when processing users' data and connections to the institution's systems.
- The institution's e-services should be articulated with national e-government platforms and frameworks where they exist.
- E-services should be based on institutional models and standards (ICT governance and management frameworks, data security and privacy frameworks, the institution's technical standards, W3C standards). They should be aligned with the implementation approaches for social security business processes as defined in the corresponding section of this set of Guidelines.

Mechanism

- The ICT unit should lead the design and implementation of multi-channel e-services, to enable users to interact with the institution through diverse mechanisms, such as web-based and mobile-oriented applications, phone connections and distributed kiosks.
- Web-based and mobile-oriented services may be based on "one-stop" portals to facilitate access and avoid the fragmentation of service sites.
- Implementation could be based on alternative strategies:
    - An improved services approach aiming at building individual services incrementally, focusing on short-term improvements in organizational efficiency;
    - A transformational approach aiming at building citizen-centric services which provide a broad possibility of self-guided access to information and operations, using collaborative front ends rather than an operations menu.
- Adaptation of the interaction methods to users' characteristics could be based on segmentation of the users' universe, as well as using advanced web technologies.

- The ICT and other relevant units should ensure service availability and quality of service, including access outside office hours and support for a large number of simultaneous connections. Techniques may consist of:
  - Service continuity practices to manage the high availability of the platform;
  - Asynchrony in back-end request processing, to better support the requests load.
- Using social web technologies and social networking approaches may be explored to improve interaction with specific user groups.
- Relevant units, including ICT and customer services, should continuously measure performance improvements and conduct service assessments through customer surveys, field studies, and transactions and usage analysis.

A.3. 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. In particular, the management of service continuity 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.

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 7. Strategy and processes to manage a portfolio of ICT services

The institution establishes a strategy and processes to define and manage a portfolio of ICT services responding to the institutional objectives. It should be based on business plans, ICT-related plans, technology roadmaps and good governance principles.

An ICT services portfolio includes ICT products and services which are already operational as well as others that are upcoming as part of institutional plans. The definition and management the ICT services portfolio has to rely on institutional strategies and processes connecting ICT Governance decisions and institutional business plans with specific ICT services to be provided.

Structure

- The board should commission the management to establish a strategy and processes to define and to subsequently manage a portfolio of ICT services considering the overall institutional needs and strategic plans. Such strategy and processes aim at optimizing the performance of the overall portfolio and related activities taking into account institutional business plans, ICT-related strategic plans, technology roadmaps and good governance principles.
- The ICT services portfolio should be developed taking as an input ICT Governance decisions as well as institutional objectives and plans related to the operationalization of social security functions through ICT.
- The ICT services portfolio should follow the adopted ICT governance principles, and the institution's strategic plans and Digital Governance strategies. They should be based on the ICT Governance guidelines as well as on international practices (e.g. COBIT®).

Mechanism

- The ICT Governance Committee and the ICT unit should define a portfolio of ICT products and services responding to the institution's needs and aligned with institutional strategies and plans. The portfolio should include all ongoing products and services as well as those in the pipeline which have been vetted by the competent areas.
- The portfolio should highlight the expected value-added of the products and services as well as their cost from a total life-cycle perspective. Service Level Agreements (SLAs) and related contracts should be consistent with the ICT product and services in the portfolio.
- The ICT unit should establish processes to manage the portfolio of ICT products and services across their entire lifecycle involving all the related areas. Agile portfolio management methodologies may be applied in order to reduce ICT services' "time to market" by establishing a close coordination with business areas.
- The ICT unit should establish processes to implement the different types of products and services in the portfolio matching with the corresponding objectives and requirements. In particular, it should establish appropriate project management and software development methodologies.

Guideline 8. Demand management process

The institution establishes a demand management process that aims to understand, anticipate and influence customer demand for products and services that are in the ICT portfolio.

As part of the service strategy stage, demand management rationalizes and optimizes the use of ICT resources. It ensures that the amount of technical and human resources that has been budgeted matches the expected demand for the service.

Structure

- The board should commission the management to establish management processes to rationalize and optimize the use of ICT resources.
- The management should establish a chain of responsibility and ownership. It should appoint a demand manager and demand user roles often called business relationship managers. Business relationship management creates and enhances the connection between the customer and the service provider and are responsible for the analysis of the customer demand cycle.
- The management should appoint stakeholders that have appropriate domain knowledge to evaluate demands related to each portfolio.
- The management should define metric categories and assessment metrics to develop and distributes assessment to appropriate audience.
- The demand management process should follow the adopted ICT governance principles, and the institution's strategic plans and digital governance strategies. They should be based on the ICT Governance guidelines as well as on international practices (e.g. COBIT®).

Mechanism

- The ICT unit should analyse the current customer usage of ICT services, in particular by analysing service desk data regarding incidents, requests, and problems.
- The ICT unit should anticipate future customer demands for ICT services notably by speaking with business users about forecasted needs and by making projections based on similar customer's trends.
- The ICT unit may influence consumption as necessary by financial or technical means. For instance, by charging excessive usages to offset the costs of the unforeseen demand if a customer uses more service than anticipated. In this way, demand management also makes sure that the appropriate costs are included in the service design.
- The ICT unit should carry out the main two processes involved in demand management:
    - Demand prognosis, in which the business relationship manager analyses ICT service usage in order to forecast future usage. A pattern of business activity (PBA) can be established in order to measure aspects of customer service usage: Frequency, Volume, Duration, and Location. The PBA may also include a user profile;
    - Demand control, which enables providers to control ICT service consumption. This may be carried out through technical or financial means. The control is performed until the capacity for greater demand is implemented into the service catalog.

Guideline 9. ICT service catalogue management

The institution establishes a service catalogue in order to enhance the visibility of the essential currently provided ICT products and services.

The service catalogue is a listing of the main products and services that are currently available for customer use. It includes hardware, software and applications as well as ICT-based services to be used internally by institution's staff and externally notably by contributors, beneficiaries and partners.

The service catalogue is different from the portfolio management as the portfolio will hold all current, previous and future services.

Structure

- The board should commission the ICT unit to design and establish a service catalogue based on the service portfolio but including only ICT products and services that are currently available for customer use.
- The ICT service catalogue should provide: (i) a customer view, which enables users to easily access the available products and services, and (ii) a Technical view, which includes the detailed information that is required for carrying out the administration tasks on the ICT products and services. In turn, the Customer view should differentiate products and services to be used by the institution's staff from the ones to be used by external users, notably contributors, beneficiaries and partners.
- To establish accountability, the role and responsibilities of service catalogue manager has to be well defined and documented.
- The implemented approach should follow the institution's ICT governance framework and ICT management processes, and be based on international standards and practices (e.g. ITIL v3–Service Operation and ISO/IEC 20000).

Mechanism

- The ICT unit should build an ICT service catalogue based on the service portfolio but including only ICT products and services that are currently available for customer use.
- The customer view should be implemented focusing on customers' requirements and accessibility needs and enabling an effective and intuitive access to ICT products and services:
    - It should enable to access and execute functionalities of the products and services as well as to report incidents and requests, i.e. as an entry-point to the service desk;
    - The user experience should be optimized. For instance, entries in the view should be categorized in meaningful ways for customers;
    - Descriptions of products and services should use a customer oriented vocabulary and not a technical one. In each case, customers' profiles have to be taken into account;
    - Security measures and access permissions for using the product/service should defined and appropriately explained.

- The technical view should include all the necessary information for performing administration tasks on products and services as well as for assessing their value/cost ratio.
- The catalogue should generate metrics and indicators about the usage of products and services, in particular those accessible to external users.

Guideline 10. Service level management

The institution establishes a service level management process (SLM) in order to measure and manage the quality of the ICT services provided with respect to service level agreements (SLAs).

Structure

- The board should commission the ICT unit to establish a service level management process in order to ensure that customers and the ICT unit have a clear and unambiguous expectation of the quality of the services to be delivered.
- To establish accountability, the roles and responsibilities of service level managers and service owners have to be well defined and documented:
  - Service level managers are responsible for negotiating service level agreements (SLAs) and ensuring that they are met;
  - Service owners are responsible for delivering a particular service within the agreed service levels. Typically, they act as the counterpart of the service level manager when negotiating operational/service level agreements (SLAs/OLAs).
- The implemented approach should follow the institution's ICT governance framework and ICT management processes, and be based on international standards and practices (e.g. ITIL v3–Service Operation and ISO/IEC 20000).

Mechanism

- The ICT unit should establish a service level management process in order to effectively define, document, agree, monitor, measure, and review the level of the provided ICT services. This involves the following activities for the services in the service catalogue and/or in the service portfolio:
  - Identify business-oriented quality of service requirements and translate them into ICT-based requirements. Update the entries in the service portfolio and service catalogue;
  - Establish the scope of services, timeliness and hours of operation, service performance and business continuity measures. Update the entries in the service portfolio and service catalogue;
  - Perform gap analysis between business requirements and available services. Determine the costs of bridging the existing gaps by increasing the existing service capacity, for instance the costs of hardware upgrades if the SLAs are not sustainable with the current platform;
  - Define and negotiate SLAs with the business units, ensuring the business requirements are met;
  - Implement SLAs, measure their performance and control the compliance.
- The ICT unit should ensure the monitoring of the agreed service levels and, more in general, of the quality of services focusing on improving them at an acceptable cost to the institution.
- The ICT unit should report regularly, in a standardized manner, the service level compliance and improvement plans when corresponds.

Guideline 11. Capacity management

The institution establishes a capacity management process in order to achieve an adequate infrastructure capacity to meet the business needs in a cost-effective manner. This comprises institution's infrastructure as well as on-demand based and cloud-based services (e.g. IaaS models).

The purpose is to determine the infrastructure capacity required to meet business availability and performance requirements. This involves a thorough understanding of how business demand influences demand for services, and how service demand influences demand on infrastructure.

Structure

- The board should commission the ICT unit to establish a capacity management process in order to define infrastructure configurations matching business needs in a cost-effective manner. Infrastructure configurations consist of hardware and software components supporting business services (e.g. servers, databases, application servers, etc.).
- The ICT unit is responsible for implementing services that meet the established service level agreements (SLAs) by using adequate infrastructure configurations. The capacity management process works closely with service level management to ensure that the business' requirements for capacity and performance can be met.
- Capacity management also supports the service desk and incident and problem management in the resolution of incidents and problems related to capacity.
- The implemented approach should follow the institution's ICT governance framework and ICT management processes, and be based on international standards and practices (e.g. ITIL v3–Service Operation and ISO/IEC 20000).

Mechanism

- The ICT unit should establish a capacity management process by carrying out the following activities:
  - Identifying and prioritizing institution's goals according to the needs of ensuring the availability and performance of certain critical services, reducing risks of not matching SLAs and containing costs;
  - Developing a capacity plan, which consists of different infrastructure configurations matching business needs at different times. For example a configuration supporting peeks of contribution submissions close to deadlines;
  - Continually reviewing the service capacity and performance.
- The ICT unit should implement the following capacity management sub-processes:
  - Business capacity management, which translates the business needs into ICT service requirements;
  - Service capacity management, which aims at ensuring that the provided end-to-end services meet the agreed service levels and SLAs. It focuses on the operation of services unlike component capacity management which focuses on infrastructure elements;

- Component capacity management, which focuses on the technology that provides the performance and capacity to the ICT service;
- Capacity management reporting, which provides with the information related to service capacity, service usage, and service performance.

Guideline 12. ICT service continuity management

The institution establishes a service continuity management (ITSCM) process to ensure 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. The ITSCM should focus on those events that the institution considers significant enough to be treated as a "disaster".

The risks of a loss of a business process, such as financial loss, damage to reputation or regulatory breach is measured through a joint exercise between functional team and ICT – called business impact analysis – , which determines the minimum critical requirements.

Structure

- A framework to respond to incidents and disruptions should be implemented in order to ensure the continued operation of critical processes and the required ICT services as well as to maintain the availability of information at a level acceptable to the institution.
- The board should commission the ICT unit to design and establish ICT service continuity management (ITSCM). A specialized organizational structure, reporting to the ICT management, should be established to manage IT service continuity.
- The ICT unit should appoint an ICT service continuity manager, who would be responsible for managing risks that could seriously impact ICT services:
    - A minimum agreed service level at the time of disaster should be guaranteed by reducing the risk to an acceptable level and planning for the recovery of ICT services. This involves a coordination with the risk manager and the availability manager;
    - Likewise, potential security threats to the service continuity should be assessed and preventive actions taken in coordination with the Information security management.
- The implemented ITSCM should follow the institution's ICT governance framework and strategic plan, and be based on international standards and practices (e.g. ISO/IEC 22301 and 24762, COBIT® and ITIL v3–Service Operation and ISO/IEC 20000.

Mechanism

- The management, with the assistance of specialized units where applicable, should define policies, objectives and scope for the continuity of critical social security processes and services (i.e. business continuity) aligned with the institution's objectives, notably including contribution collection and benefit delivery, e-services and citizen interaction, and operation of corporate resources, in the particular Master Data.
- The ICTSCM process has four stages or activities:
    - Initiation, which includes defining policy, scope, terms of reference, project planning and resource allocation;
    - Requirements and strategy, which involves performing business impact analysis and risk assessment for the different services as well as establishing priorities for the recovery;

  - Implementation, which includes the evaluation of recovery options, executing risk reduction measures, and testing the contingency plans;
  - Ongoing operation, which concerns testing, reviewing the ITSCM plans on a regular interval, and communicating them to the institution.
- The ICT unit, with the assistance of specialized units, should:
  - Define a service continuity strategy. This involves evaluating business continuity management options and choosing a cost-effective and viable strategy that will ensure enterprise recovery and continuity in the face of a disaster;
  - Develop and implement a business continuity response, based on a business continuity plan (BCP) according to the defined strategy;
  - Maintain the availability of business-critical information and services, implementing the appropriate contingency measures. Such measures should comprise systems, applications, data and documentation maintained or processed by third parties.
- The management should validate and communicate the ITSCM plans throughout the institution.

Guideline 13. Information security management

The institution establishes an information security management process in order to protect information resources against potential threats or losses.

The main goals are to ensure that information is available, reliable and usable only for the authorized users, and the systems that provide it can appropriately resist attacks and recover from or prevent failures.

Structure

- The board should commission the ICT unit to design and establish information security management.
- The ICT unit should appoint an information security manager, who should set up an information security management framework mostly done through ISO 27001.
- The implemented approach should follow the institution's ICT governance framework and ICT management processes, and be based on international standards and practices (e.g. ITIL v3–Service Operation and ISO/IEC 27001). A detailed description of data security and privacy practices is provided in a specific section.

Mechanism

- The information security manager should establish an ISM framework addressing five key elements:
  - Control, which consists of managing information security, preparing and implementing an information security policy, allocating responsibilities, and establishing and controlling documentation;
  - Plan: the planning phase of the framework involves gathering and fully understanding the security requirements of the organization and then recommending the appropriate measures to take based on the budget and the institutional context;
  - Implement, which involves putting the plan into practice enforcing the information security policies;
  - Evaluate, which consists of oversee policies and plans to ensure that the institution's systems are truly secure and your processes are running in compliance with your policies, SLAs, and other security requirements;
  - Maintain: an effective information security management system requires a continuous improving looking for opportunities to revise SLAs and the mechanisms in which they are monitored and controlled.
- The ICT unit should implement five different types of measures to minimize both threats and the impact of human errors:
  - *Preventive* measures, which focus on access management tasks such as assigning appropriate rights and permissions, verifying identification, and ensuring that unauthorized people cannot access the Institution information and systems;

- *Reductive* measures, which seek to reduce the impact of incidents, such as deploying contingency plans and performing automated backups of critical data and systems;
- *Detective* measures, which consist of controls to identify a risk or threat as quickly as possible usually through monitoring systems;
- *Repressive* measures, which consist of "counterattacks" such as automatically blocking connections from a suspicious IP address or temporarily locking usernames associated with suspicious login attempts;
- *Corrective* measures, which aim to repair damages caused by an error or incident. For example, restoring a backup.

Guideline 14. Application development management

The institution carries out application development through collaborative cross-functional teams in order to ensure quality while reducing deployment time by putting into practice shorter development cycles and faster innovation.

By applying the so-called Agile and DevOps approaches the institution may improve the coordination between the business, development and operations areas. This would enable to improve communication and collaboration and reduce deployment failures and time to recover.

Structure

- The board, with the assistance of the management and the ICT unit, should adopt a systematic and standardized framework for developing and managing software applications throughout their life cycle, including methodologies and a quality model.
- The board should commission the ICT unit to design and establish a DevOps approach for application development management by promoting the following capabilities:
  - DevOps culture, which is characterized by increased collaboration, decreasing silos, autonomous teams and increasing automation;
  - Permanent measurement in order to determine if DevOps is continuously improving processes;
  - Sharing knowledge and ideas between the involved stakeholders breaking the silos of business, development and operations.
- The scope of the framework should include all the institution's departments in which software development and application management activities are carried out (e.g. requirement specification, incident management, change management), and:
  - External services that carry out these activities on behalf of the institution (e.g. under software development contracts) should apply the framework in developing and managing software applications;
  - The contracts administration office should include the framework in requests for proposals (RFPs), contract documents and service level agreements;
  - The framework should ensure that the institution keeps the full control on the knowledge involving the systems and enforces that documentation is updated accordingly.
- The framework for developing and managing software applications should follow national regulations for public administration.
- The framework should follow the institution's governance frameworks, ICT governance framework and ICT management processes and be based on international standards and practices (e.g. CMMI; ISO/IEC 9126, 15504 and 20000; ITIL v3–Service Operation, and ISO/IEC 20000, CAMS).

Mechanism

- The ICT unit, with the assistance of specialized units, should establish a systematic and standardized framework for developing and managing software applications throughout their life cycle, including requirements, design, the build, deployment, operation and optimization. This includes software development methodologies, software project management methodologies and a software quality model.
- The ICT unit should put into practice an application development approach improving the "time to market" by fostering cross-area coordination and using DevOps and agile methodologies. This requires Product Owners to collaborate closely with Project Managers and to foster the following practices:
  - Working close to the business and seeking an active stakeholder participation in line with practices within the Agile community and Extreme Programming (XP) methodologies;
  - Continuous integration and deployment, which enable to quickly implement small changes, check in code to version control repositories frequently and deploy the application for production;
  - Automated testing in order to ensure quality at every stage in a context of a continuous development and deployment such as the promoted by DevOps-oriented methodologies.
- Development teams should provide production support by tackling serious production problems. The development team will often be referred to as "level three support" for the application because they will be the third (and last) team to be involved with fixing critical production problems.

Guideline 15. Change management

The institution establishes a change management process in order to perform the necessary business and technological evolutions as well as upgrades while minimizing risks and negative impact.

Changes are defined by ITIL as the addition, modification or removal of any authorized, planned, or supported service or service component that could have an effect on ICT services. ICT change management is a process designed to understand and minimize risks while making ICT changes. The main goals are to implement changes in the most efficient manner while minimizing the negative impact on customers when changes are implemented.

Structure

- The board should commission the ICT unit to design and establish a change management process.
- The ICT unit should appoint a change manager and set up a change advisory board for authorizing changes and further evaluating requests when the change manager determines that there is a high risk associated with these requests. The board takes into account the impact that a requested change may have on all affected parties.
- The implemented approach should follow the institution's ICT governance framework and ICT management processes, and be based on international standards and practices (e.g. ITIL v3–Service Operation).

Mechanism

- The change manager should define procedures to treat the diversity of types of changes, which may comprise urgent changes, standard changes, major and normal changes.
- The change manager should establish procedures for receiving change proposals and processing them comprising the following steps:
    - Creating a request for change: The request should include details about the reasons for the change, the scope of the change in terms of involved systems and business areas, a description of how the change would be implemented, and a preliminary cost assessment for the direct impact of the change;
    - Reviewing and assessing a request for change and determining if the request is reasonable and to give feedback related to the request: The impact of the change should be assessed taking into account all the involved systems and business services. A risk assessment should be carried out and a contingency plan should be established in case the change is not successful;
    - Creating a change proposal and associating a priority to the change request;
    - Planning the change: A change plan outlines the course that the change will take, the resources that are needed to complete the change, and a timeline for implementation.
    - Testing the change;
    - Implementing the change;

- Reviewing change performance, includes reviewing records to determine whether the change was successful or failed, and recording details about the time and expense of the change to determine the accuracy of estimates that were made before a request was fulfilled.

- The management should communicate the defined change management approach throughout the institution.

Guideline 16. 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.

Structure

- The management should commission the ICT unit to implement systematic and standardized practices to carry out ICT operations.
- A specialized organizational structure, reporting to the ICT management, should be established to manage ICT operations. To establish accountability, the roles and responsibilities of the units within that structure have to be well defined and documented.
- The implemented ICT operations practices should follow the institution's ICT governance framework and the ICT management processes, and be based on international standards and practices (e.g. ITIL v3–Service Operation and ISO/IEC 20000).

Mechanism

- The ICT unit, with the assistance of specialized units, should establish systematic and standardized practices to carry out ICT operations management. This includes two main functions:
  - ICT operations control, which provides centralized monitoring and control;
  - Facilities management, which is responsible for the management of data centres, computer rooms and recovery sites. It also coordinates large-scale infrastructure projects, such as data centre consolidation or server consolidation.
- The ICT unit, through specialized units, should carry out common service operation activities, including:
  - Monitoring and control: to detect the status of services and infrastructure elements and take appropriate corrective action;
  - Console management/operations bridge: a central coordination point for monitoring and managing services;
  - Management of the infrastructure: storage, databases, middleware, directory services, facilities/data centre, etc.;
  - Operational aspects of processes from other life-cycle stages: change, configuration, release and deployment, availability, capacity, knowledge, service continuity management, etc.

Guideline 17. 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.

Structure

- The management should commission the ICT unit to establish systematic and standardized practices to implement a service desk, including mechanisms for fulfilling requests.
- A specialized organizational structure, reporting to the ICT management, should be established to implement and manage a service desk and mechanisms for fulfilling requests. To establish accountability, the roles and responsibilities of the units within that structure have to be well defined and documented.
- The implemented service-desk practices and mechanisms for fulfilling requests should follow the institution's ICT governance framework and ICT management processes, and be based on international standards and practices (e.g. ITIL v3–Service Operation and ISO/IEC 20000).

Mechanism

- The ICT unit, with the assistance of the project managers and specialized units, should establish a service desk as a single, central point of contact for all users.
- Functions for fulfilling requests should be implemented, enabling users to request and receive standard services, and to assist with general information, complaints and comments.
- The service desk should carry out the following tasks:
  - Managing users' requests for information or advice, a standard change or access to an ICT service;
  - Logging, managing, categorizing and prioritizing incidents and requests;
  - Managing the life cycle of incidents and requests, escalating them as appropriate and closing them when the user is satisfied;
  - Keeping users informed of the status of services, incidents and requests;
  - Providing an interface for all other service operation processes and activities.
- All requests should be logged and tracked. The process should include appropriate approval before fulfilling the request.
- Possible approaches to implementing a service desk include having a:
  - Local service desk, physically close to the users;
  - Centralized, institutional service desk;
  - Virtual service desk, with staff in different locations but appearing to be a single team.

Guideline 18. 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.

Structure

- The management should commission the ICT unit to implement systematic and standardized practices to manage events, problems and incidents.
- A specialized organizational structure, reporting to the ICT management, should be established to manage events, problems and incidents. To establish accountability, the roles and responsibilities of the units within that structure have to be well defined and documented.
- The implemented practices for managing events, problems and incidents should follow the institution's ICT governance framework and ICT management processes, and be based on international standards and practices (e.g. ITIL v3–Service Operation and ISO/IEC 20000).

Mechanism

- The ICT unit, with the assistance of specialized units, should establish proactive and preventive practices to deal with events, problems and incidents.
- The ICT unit should continuously monitor and interpret events in order to determine the appropriate control action.
- The ICT unit should manage problems aiming at:
  - Analysing and resolving the root causes of incidents;
  - Proactively detecting and preventing future problems/incidents;
  - Maintaining information about problems and the appropriate workarounds and resolutions.
- The ICT unit should manage incidents in order to restore normal service as quickly as possible, and to minimize the adverse impact on business operations.

A.4. 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. To address these issues, a total life-cycle costs model for ICT products and services should be thorough applied in the institution as recommended in the *ISSA Guidelines on Good Governance*.

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. 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 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 and following a total life-cycle costs model. 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. 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 based on the institutional total life-cycle costs model.

Guideline 19. 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 based on an institutional total life-cycle costs model and evaluating the return on investment of ICT-related initiatives.

Structure

- The board should commission the management and the ICT unit to establish the institution's concept of value as well as approaches and practices to optimize its realization.
- A specialized organizational structure, reporting to the management and the ICT management, should be established to manage the institution's ICT-related values. To establish accountability, the roles and responsibilities of the units within that structure have to be well defined and documented.
- The management processes of ICT-related values should follow the adopted ICT governance principles and ICT strategies, and be based on international standards and practices (e.g. COBIT®).

Mechanism

- The management, with the assistance of the ICT, financial and other specialized units, should define the concept of value as well as the management principles and practices to enable optimal value realization from ICT-related investments throughout their economic life cycle based on an institutional total life-cycle costs model.
- The ICT and specialized units should continually evaluate the portfolio of ICT-enabled investments, services and assets to determine the likelihood of achieving institutional objectives at a reasonable cost. This involves:
    - Understanding stakeholder requirements – strategic ICT issues as well as capabilities regarding the actual and potential significance of ICT for the institution's strategy;
    - Understanding what constitutes value for the institution, and considering how well it is communicated, understood and applied throughout the institution's processes;
    - Evaluating how effectively the institution and ICT strategies have been integrated and aligned within the enterprise and with the institution's goals for delivering value;
    - Evaluating the portfolio of investments, services and assets for alignment with the institution's strategic objectives, taking into account: a total life-cycle perspective; risk evaluation; business process alignment; effectiveness in terms of usability, availability and responsiveness; and efficiency in terms of cost, redundancy and technical health.

- The ICT and specialized units should direct value management principles and practices to enable optimal value realization from ICT-enabled investments. This involves:
  - Defining and communicating portfolio and investment categories;
  - Directing the management to consider potential innovative uses of ICT that would enable the institution to respond to new opportunities or challenges.
- The board should communicate the institutional scope of the definition of value, and the principles to enable value realization, throughout the institution.

Guideline 20. 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 through a total life-cycle costs model.

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.

Structure

- The board should commission the management to establish management processes to implement and manage ICT investments, acquisitions and contracts.
- A specialized organizational structure, reporting to the management and the ICT management, should be established to manage ICT investments. To establish accountability, the roles and responsibilities of the units within that structure have to be well defined and documented.
- ICT investment management processes should follow national and institutional procurement regulations.
- The ICT investment, acquisitions and contracts processes should follow the principles of:
  - Being managed as a portfolio of resources;
  - Including the full scope of activities required to achieve business value;
  - Being managed throughout their economic life cycle – i.e. based on an institutional total life-cycle costs model;
  - Maintaining an internal expertise required to keep a strategic control on the ICT products and services;
  - Including risk assessments, in particular for external contracts and outsourcing.
- The ICT investment, acquisitions and contracts processes should follow the adopted ICT governance principles, and the institution's strategic plans, the institutional total life-cycle costs model, ICT strategies and defined ICT value concept. They should be based on international practices (e.g. COBIT®).

Mechanism

- The ICT and specialized units should follow the strategic direction set for investment, acquisitions and contracts in line with the enterprise architecture vision and the corresponding characteristics of the investment and related services portfolios. They should be based on the institutional total life-cycle costs model.

- The ICT and specialized units should implement processes to:
  - Manage the portfolios of ICT resources establishing the target investment mix, maintaining the portfolios to fulfil the institution's goals and managing the achievement of expected results;
  - Manage staff contracts, ensuring that they comply with the organization's policies and that contracted personnel meet contractual requirements;
  - Manage ICT assets through their life cycle by applying the institutional total life-cycle costs model to ensure that their use delivers value at optimal cost, they remain operational, and they are accounted for and physically protected;
  - Manage software licences to ensure that the optimal number are acquired, retained and deployed in relation to required business usage.
- ICT procurement approaches and practices should be defined to better address the different scenarios of ICT elements.
- The involved units should closely coordinate ICT investment management with processes for the management of budget and costs, human resources, service agreements and suppliers.

Guideline 21. 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 by applying the institutional total life-cycle costs model.

Structure

- The board should commission the management and the ICT unit to implement monitoring and evaluation processes on the performance of ICT-enabled investments and services based on the institutional total life-cycle costs model.
- A specialized organizational structure, reporting to the management and the ICT management, should be established to monitor and evaluate the performance of ICT-enabled investments and services. To establish accountability, the roles and responsibilities of the units within that structure have to be well defined and documented.
- The monitoring and evaluation processes on the performance of ICT-enabled investments and services should follow the adopted ICT governance principles and ICT strategies as well as the institutional total life-cycle costs model, and be based on international standards and practices (e.g. COBIT®).

Mechanism

- The ICT and specialized units should monitor the performance of ICT-enabled investments and services, evaluate whether they generate the expected value and match the institution's goals, and determine whether adjustments are necessary.
- The ICT and specialized units should implement processes to:
    - Define and monitor key metrics and respond quickly to any changes or deviations, monitoring the performance of different elements such as the overall portfolio, individual investments, ICT services and ICT assets, among others;
    - Monitor key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the institution from ICT-enabled investments and services, identify significant issues and consider corrective actions;
    - Monitor and optimize the performance of the investment portfolio and individual programmes on a regular basis throughout the investment life life cycle by applying the institutional total life-cycle costs model;
    - Monitor and control programme (solution delivery) and enterprise (value–outcome) performance against plans throughout the economic life cycle of each investment and report this performance to the programme steering committee and the sponsors.
- The established organizational structure should undertake evaluation throughout the entire life cycle of products and services.

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 22. 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.

Structure

- The board, with the assistance of the management, should issue a policy statement on the adoption of a systematic, clear and effective approach for the governance of data as a critical resource.
- The board and management should commission the ICT unit, in collaboration with business units, to define a data governance framework. Effective data governance depends on a partnership between business data stewards and data management staff.
- The data governance framework should take into account all the different scenarios of ICT services applicable in the institution (e.g. internal services, outsourced services, internal and external access to information).
- Data security and privacy aspects are addressed in the section on data security and privacy of these Guidelines.
- The ICT data governance framework should follow the institution's governance rules, ICT governance framework and strategic plan, and be based on international practices (e.g. ISO/IEC TR 10032 and DAMA-DMBOK).

Mechanism

- The ICT unit, with the assistance of specialized units, should specify and implement a framework defining processes, procedures and duties on data governance, comprising the following activities:
  - Defining data strategy and policies;
  - Specifying a corporate data architecture;
  - Defining data standards and procedures;
  - Defining the mechanisms to ensure regulatory compliance (e.g. national data protection regulations, Health Information Protection and Portability Act or equivalent);
  - Carrying out issue management.
- The ICT unit should address the implications of big data management and governance, in particular taking into account the "4 Vs" charactering the big data: Volume, Variety, Velocity and Veracity.
- The board and management might set up specialized organizational structures to carry out data governance processes. Special consideration should be given to business-oriented roles and data management activities.
- The management should validate the framework and communicate its scope throughout the institution.

Guideline 23. 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).

The implementation of a master data model and system is addressed in a specific section of this set of Guidelines.

Structure

- The management should commission the ICT unit to implement a master data model and information system covering the core objects for social security operations. Although it varies depending on the scope and characteristics of the social security system, this usually includes:
  - Persons' data, including family ties, role (e.g. employee, retired person, relative of worker);
  - Employers' data;
  - Social programmes;
  - Relationships between persons and employers, working periods, etc.;
  - Relationships between persons and social programmes (affiliation relationship), registration periods, characteristics of the affiliation, etc.
- A specialized organizational structure should be established to administer the master data model and information system. To establish accountability, the roles and responsibilities of the units within that structure have to be well defined and documented.
- The master data model and information system should be based on institutional models and standards: the institutional data governance framework; the service-oriented architecture (SOA)-based interoperability application model, interoperable shared data services (basic registries), and data security and privacy; and the institutional technical standards.

Mechanism

- The ICT unit should define and implement a master data model and implement a corresponding information system. The project should involve business experts in addition to ICT staff.
- The project should identify the core information items (for social security operations) in the institution and metadata should be developed.
- To ensure the accuracy of the specification, the master data model should be represented through a formal or semi-formal language (e.g. OWL, UML, Entity–Relationship Model).
- The implementation of a database including the referred information should be based on relational database management systems (RDBMS), ideally using the master data model as metadata. Given the importance of master databases, specialized technologies have been developed for them.

- ICT staff (in the main) should administer the master data system, and business staff should carry out data stewardship and data specification tasks.

Guideline 24. 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.

Structure

- The management should commission the ICT unit to define and implement systematic data development and operations.
- The management should establish duties and responsibilities to carry out data development and operations in accordance with the data governance framework.
- Business areas should participate in the elaboration of service level agreements concerning data development and operations.
- The framework for data and information quality should follow institutional standards (the data governance framework), international standards and practices (DAMA-DMBOK) and technical specifications for data to be used in social security studies.

Mechanism

- The ICT unit, taking service level agreements into account, should carry out data development activities in a systematic and formalized way, including:
  - Data modelling, analysis and design of information systems;
  - Data model and design quality management;
  - Database and information system implementation.
- The ICT unit, with the assistance of business managers and specialized units, and taking service level agreements into account, should elaborate and carry out data operations activities in a systematic and formalized way, including:
  - Information system administration;
  - Database administration;
  - Data issue management;
  - Data recovery management and operation.
- Data collection should take into account the diversity of scenarios: manual versus automatic; internal versus external (through partners); in the counter versus web-based systems.
- Data storage should cover long periods of working history (decades) and a diversity of social security records.

Guideline 25. 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.

Structure

- The board, with the assistance of the management, should issue a policy statement on the adoption of a systematic, clear and effective approach for the management of data and information quality.
- The management should commission the ICT unit to design a management framework for data and information quality, defining the procedures and duties involved.
- Specialized organizational structures should be established to manage data and information quality processes. To establish accountability, the roles and responsibilities of the units within that structure have to be well defined and documented.
- The contracts administration office should include these internal regulations and specifications in requests for proposals, contract documents and service level agreements.
- The framework for data and information quality should follow the institution's governance rules, ICT and data governance framework and strategic plan, and be based on international practices (e.g. ISO 8000 and DAMA-DMBOK).

Mechanism

- The ICT unit, with the assistance of specialized units, should specify and implement a framework defining processes, procedures and duties for managing data and information quality. All the different scenarios of ICT services applicable in the institution should be taken into account (e.g. internal services, outsourced services, internal and external access to information). This includes the following activities:
  - Specifying data quality requirements;
  - Profiling, analysing and assessing the quality of existing data;
  - Specifying a data quality measurement model (metrics, dimensions, etc.);
  - Specifying data quality business rules to be implemented in information systems;
  - Correcting data quality defects;
  - Continuously measuring data quality;
  - Defining procedures for managing data quality issues.
- Preventive measures should be implemented, especially by communicating data quality requirements to the data development and operations teams and data entry staff.

- Specific data quality assurance measures should be implemented to ensure the availability of sufficient and reliable data to perform actuarial work. A specialized data quality assurance model should include the dimensions of completeness, correctness, and consistency with master social security data as well as through time.

Guideline 26. 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. In particular, the application of analytics technologies is addressed in a specific section of these Guidelines.

Structure

- The management should commission the ICT unit to implement mechanisms for information retrieval and analysis also known as Business Intelligence.
- Mechanisms for information retrieval and analysis should take into account regulations and guidelines on data security and privacy.
- Mechanisms for information retrieval and analysis should take into account the availability and technical characteristics of data hosted by external partners, along with interoperability aspects.
- Mechanisms for information retrieval and analysis should follow the institution's governance rules, ICT and data governance framework and strategic plan, and the SOA-based interoperability application model, and be based on international practices (e.g. DAMA-DMBOK).

Mechanism

- The ICT unit should implement mechanisms enabling effective and efficient information retrieval and analysis, including the following activities:
  - Analysis of information requirements;
  - Definition of a corporate architecture for document and content management;
  - Definition of a corporate architecture for decision support systems and the information involved; data warehousing approaches should be used;
  - Implementation of DSS, separated decision support system (DSS), but connected with transactional systems; data warehousing and business intelligence tools (e.g. databases, ETL, OLAP, data mining) should be taken into account.
- The business units should incorporate the systematic use of information exploration and analysis within the business process, especially in decision-making processes.
- The ICT and specialized units should develop a communications plan to provide appropriate information to social security service areas of the institution about the available mechanisms for information retrieval and analysis.

Guideline 27. Information retrieval and analysis for actuarial work

The social security institution ensures the availability of the data necessary to perform actuarial work as defined by the *ISSA-ILO Guidelines on Actuarial Work for Social Security* by providing relevant support and appropriate financial and staff resources.

The institution designs and maintains decision support systems (DSS) capable to accommodate, and ease extraction and sorting of data and/or information for the purpose of actuarial work

Structure

- The board should provide effective oversight to ascertain that management produces statistical report enabling the actuary to satisfy applicable professional standards described in section on regulatory issues, standards and professional guidance of the *ISSA-ILO Guidelines on Actuarial Work for Social Security*.
- The board and the management should commission the ICT unit to implement, directed by a project manager and in coordination with the actuarial unit, Information Systems capable to accommodate, and ease extraction and sorting of data and/or information for actuarial work.
- The social security institution supports training and professional development on advanced tools for information analysis to be used by actuarial staff. ICT specialists to ensure the understanding of data needed for the actuarial work. Reference should be made to guideline of the *ISSA-ILO Guidelines on Actuarial Work for Social Security* on developing and maintaining professional expertise).
- The institution will ensure that the information collected from external actors is complete for the purpose of the actuarial work.
- The ICT unit and the project manager should ensure that DSS are designed to:
    - Permit the extraction of relevant and sufficient data for specific purposes including but not limited to policy formulation, decision-making, actuarial valuations, benefit calculations, policy appraisal and redesign;
    - Safeguard the accuracy and completeness of historical data over a reasonably long time horizons;
    - Ensure that the data quality requirements for actuarial purposes are fulfilled.
- Approaches for providing the required data and/or information for actuarial work should be based on the institutional data governance framework as well as on the mechanisms for information retrieval and analysis as in the corresponding guideline in this section, and should respond, in particular, to the requirements of guidelines of the *ISSA-ILO Guidelines on Actuarial Work for Social Security* on data, projection model and determination of benefit entitlements.

Mechanism

- The institution should define the roles of different stakeholders in the data management process and, in particular, the interaction between those carrying out the actuarial work and ICT unit.

- The ICT unit should implement a DSS to enable the uptake of basic biographical data and assign unique identifiers to each insured person at the initial registration stage. More concretely:
  - Biographical data should include but not limited to: date of birth, gender, marital status – including date of birth and sex of spouse, date of marriage, number of children including sex and date of birth, date of death;
  - Occupational history should include but not limited to employment date, type of employment, amount of earnings per year, amount of contributions, contributory service, contribution density, etc.;
  - Benefits history should include but not limited to effective date of benefits, type of benefits, amount of benefits, end date of benefits, etc.;
  - A connection with the institutional Master Data should be established.;
  - Validity checks should be implemented to avoid record duplications.
- The project manager should ensure that DSS allow the pickup of complementary and/or modified information under the same unique identifier upon validation by the competent authority. In particular, it should ensure that:
  - DSS allow the portability of unique identifiers from one employer to another (in case of change of employment), from one category of insured to another (mandatory or voluntary) and/or from contributor to beneficiary (change of status) and vice versa;
  - Unique identifiers are usable by the principal insured and secondary insured person(s) for health and family and maternity benefits schemes;
  - Unique identifiers from the principal insured to the secondary insured are appropriately connected for survivors' benefits.
- The ICT unit should ensure that information on declaration and payment of contributions and/or insurance premiums is readily attributed to each individual's records through the unique identifiers detailing the amount apportioned to each covered contingency and/or branch.
- The ICT unit should ensure that information on number of claims, type and amount paid per benefit and/or use of services per branch/contingency are readily attributed to each individual record's through the unique identifiers and apportioned to the respective beneficiaries.
- In respect to the establishing a new scheme, the social security institution should put in place mechanisms for data collection and analysis. The ICT and actuarial units should work together to establish such mechanisms. Reference should be made to guideline of the *ISSA-ILO Guidelines on Actuarial Work for Social Security* on valuation and costing of a new social security system.
- The ICT unit should ensure that DSS systems are designed to permit the extraction and sorting of data of insured persons (number of births, deaths, new entrants, new claims, benefits paid, accrued rights, insured earnings etc.) by single age and sex.
- The ICT unit should ensure that DSS systems are designed to guarantee the availability and reliability of historical data.

B. Key Technologies

Structure

The following guidelines are organized in four 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.).

Section B.4, Data Analytics, presents techniques to understand the past, explain them the cause of events, inform them what is likely to happen and suggest actions to take.

B.1. Interoperability

This section of the guidelines provides a high-level reference point for social security institutions applying interoperability techniques. 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 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 eight 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 28. 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.

Structure

- The board and management should establish a policy on the application of interoperability as a key technology to implement integrated social security systems.
- The board and management should commission the ICT management to elaborate an institutional interoperability framework which defines processes, models and technologies for applying interoperability techniques.
- The board and management may establish specialized structures to manage interoperability processes within the institution, with well-defined and documented roles and responsibilities to ensure their accountability.
- The institutional interoperability framework should be based on mainstream interoperability models (e.g. SEI, EIF) and on standards such as those proposed by W3C, OASIS and the Open Group.

Mechanism

- The board and management should establish internal policies and regulations on information sharing and exchange, and on the reuse of services, i.e. ICT-based services complying with service-oriented architecture (SOA), by internal units and external institutions.
- The ICT unit should specify and implement the institutional interoperability framework, which should define the institutional approach across five dimensions:
    - The political and legal dimensions of the framework should include both external (i.e. government defined) and internal policies and regulations; agreements should also be established wherever necessary to avoid any discrepancy that may jeopardize the application of interoperability in social security systems;
    - The organizational dimension should specify the interoperable processes and operations within the institution, defining the corresponding service interfaces and service-level agreements;
    - The semantic dimension should be based on metadata, which consists of a model of the main business concepts involved in interoperable operations (e.g. data sharing, data exchange, service invocation) and relationships among them, to define a unique meaning for these concepts throughout the institution to facilitate the automatic treatment of data. If the interoperability operations involve different institutions, the corresponding inter-institutional metadata should be specified;
    - The technical dimension should define the technologies to be used for implementing interoperable operations in order to ensure adequate technical integration of information

and systems; this technical specification should constitute an internal standard to be applied in any institutional development.

- Interoperability-based systems operating jointly with other institutions should be covered by formal agreements established prior to the beginning of any project.
- The management should communicate the scope of the framework throughout the institution.

Guideline 29. 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.

Structure

- The management should commission the ICT unit to elaborate a workplan for the implementation of interoperable social security applications in line with the institution's strategic plan; it should include all the elements required by the main social security applications and all necessary precursor elements and tasks.
- The management, in accordance with the institutional framework on interoperability, should establish duties and responsibilities to carry out the workplan of interoperability-based projects.
- The institutional workplan of interoperability-based projects should be based on the institutional models and standards, such as the institutional interoperability framework, the SOA-based interoperability application model and the institutional technical standards.

Mechanism

- In elaborating the workplan, the ICT unit, with the assistance of project managers and specialized units where applicable, should identify:
  - Projects involving the integration of social services and applying interoperability mechanisms, and categorize them according to one or more of the following: (i) social protection and social services; (ii) integrated health insurance systems; (iii) integrated compliance and contribution collection; (iv) improving institutional efficiency and quality of information and services; and (v) implementation of international agreements;
  - Agreements to be established with other institutions or partners prior to the implementation of interoperable social security applications;
  - Information resources required by interoperable social security applications (this may involve the implementation of information systems and/or the collection of data to be stored in the system);
  - Technologies and products required to implement interoperable social security applications (this may involve the selection, acquisition and installation of new software products).
- The management should approve, adopt and communicate the workplan to all units involved.

Guideline 30. 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 shared data services or basic registries and interoperability services.

Structure

- The ICT unit should define a model which includes the main elements required for the overall implementation of interoperable applications within the institution.
- The management should establish duties and responsibilities to specify and manage the institutional interoperability application model.
- The model for applying interoperability in the institution should be based on the institutional models and standards, such as the institutional interoperability framework, the workplan for implementing interoperability-based social programmes and the institutional technical standards.
- A generic model proposed in the ISSA technical documents may be taken as a reference point and refined to develop the desired institutional model.

Mechanism

- The ICT unit should elaborate a service-oriented architecture (SOA)-based model for applying interoperability in the institution, including:
  - Shared data services, which are information systems including core social security data. They would be shared internally and with other institutions to promote data reusability;
  - Interoperability services, to connect interoperable applications and information systems following the service-oriented architecture. They would consist of protocols (e.g. SOAP), tools (e.g. XSLT) and integration platforms (e.g. ESBs);
  - External services provided by third parties participating in interoperable solutions (e.g. basic registries, financial services for contribution collection or benefit payments);
  - Secure data exchange mechanisms providing a common secure environment for interoperable operations (e.g. mechanisms to authenticate operations and data);
  - Aggregate services built using other basic services (e.g. combining several basic registries and external services connected through interoperability services and using appropriate secure mechanisms).
- The ICT unit, with the assistance of specialized units where applicable, should establish service level agreements covering participant services, especially external ones. This may involve formal agreements with other institutions.
- The ICT unit may take the generic model proposed in the ISSA technical documents as a reference point and refine it to develop the desired institutional model. This generic model includes specified components (defined above) and aims at reducing the complexity of developing an institutional model as well as providing a common tool for ISSA member institutions.
- The management should approve, adopt and communicate the model to all units involved.

Guideline 31. E-government services

The institution defines a strategy for implementing e-government services in order to coordinate public e-services with other organizations.

Structure

- The ICT unit should define a strategy to implement e-government services in order to enable the systematic development of coordinated inter-institutional social services. The strategy may involve using national e-government platforms as well as implementing joint inter-institutional services with specific organizations.
- The management, with the assistance of the ICT unit and business areas, should establish agreements with national e-government authorities and other organizations involved in joint public services, in particular concerning service level agreements (SLA) and data protection requirements.
- The management should establish duties and responsibilities to manage the coordination with e-Government services as well as with other organizations.
- The approach for implementing e-government services should be based on national e-Government and Interoperability standards and frameworks, as well as on the institutional Interoperability framework and the guidelines in this section.

Mechanism

- The ICT unit in coordination with the business areas should define and put into practice a strategy concerning the implementation of institutional e-government services comprising:
  - The identification, prioritization and specification of e-government services and related processes to be implemented. They should be added to the institutional workplan of interoperability-based social programmes;
  - The specification of a service-oriented architecture (SOA) for the e-government services;
  - Approaches to enforce compliance with regulations and standards within the inter-institutional services.
- The integration strategy should establish the e-government layers in which the institution's processes and services will be integrated:
  - Access layer, which includes the channels through which users will access public services (e.g. mobile, web, kiosks, etc.);
  - E-government layer, which consists of one stop shop portals with single-sign-on integrating different websites and e-services provided by government agencies as well as by other partners;
  - E-business layer, which includes shared data systems (e.g. Master Data, Reference Data, etc.), web services endpoints, Middleware platforms and technologies, and generic software tools (e.g. CRM, ERP, Groupware, document management systems, geographic systems, etc.);
  - Infrastructure layer, including network and support technologies.

- The implementation of e-government services should comprise the following technical features:
  - Specialized techniques according to how institution's processes participate in e-Government and inter-institutional services, differentiating producer vs. consumer and reading-only data vs. reading and writing;
  - The Middleware technologies to be used, such as ESBs, web services, etc.;
  - The security model, including the authentication, access control and authorisation to the business process operations involving multiple organizations;
  - Enforce quality of services (QoS) of processes involving multiple organizations and according to established SLAs;
  - Metadata management for common concepts and data, especially for shared data systems.
  - The data consistency model of distributed transactions among institutions, which may range from strict consistency models to eventual consistency ones.

Guideline 32. 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.

Structure

- The management, with the assistance of the ICT and specialized units, should establish and implement a strategy to develop semantic interoperability resources in order to foster interoperability by providing unambiguous data descriptions.
- The management, in accordance with the institutional framework on interoperability and the workplan for implementing interoperable social security applications, should define duties and responsibilities to carry out a strategy on semantic interoperability resources.
- The strategy on semantic interoperability should be based on the institutional models and standards, such as the institutional interoperability framework, the workplan for implementing interoperability-based programmes, the service-oriented architecture (SOA)-based interoperability application model and the institutional technical standards.

Mechanism

- In implementing the strategy to develop semantic interoperability resources, the ICT unit, with the assistance of specialized units where applicable, should:
  - Establish a development plan for semantic resources based on the work plan for interoperable social security programmes, prioritizing the semantic resources necessary for selected applications;
  - Develop an institutional metadata schema including the main concepts and relationships between them, and a metadata management system common to all interoperating institutions;
  - Include data quality characteristics in the metadata to enable data consumers to improve the effectiveness of their data use;
  - Use standard languages to specify the metadata (i.e. XML for documents and data objects, OWL to specify semantic relationships between concepts);
  - Address the impacts on business and services within the implementation plan.
- The ICT unit should use a maturity model for medium- and long-term strategy on metadata management to improve the quality and effectiveness of the semantic resources.
- The ICT unit should develop a communications plan to provide appropriate information on the implementation of metadata systems to social security service areas within the institution.

Guideline 33. Interoperable shared data services

The institution develops interoperable shared data services 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.

Structure

- The ICT unit should establish and implement shared data services to ensure the consistency of core data within the institution and foster data reusability.
- The management should establish duties and responsibilities concerning the implementation and operation of shared data services.
- The interoperable shared data services should be based on the institutional models and standards, such as the institutional interoperability framework and workplan, the SOA-based interoperability application model and the institutional technical standards.

Mechanism

- In implementing shared data services (or basic registries), the ICT unit should:
  - Establish project implementation teams and ICT specialized units to analyse, design and implement the required shared data services;
  - Generate a technical specification including, for each candidate shared data service, the information model of objects and relationships (i.e. the metadata schema), service-oriented characterization (i.e. service-oriented-architecture (SOA) interfaces) and non-functional requirements (i.e. performance, security, etc.);
  - Base the implementation of shared data services on the methodologies and technologies adopted by the institution. The main technical approaches to foow are shared files, shared databases, service-oriented-architecture (SOA) data services and master data solutions;
  - Address the impacts on business and services within the implementation plan.
- The ICT unit should develop a communications plan to provide appropriate information on the implementation of shared data services to social security service areas within the institution.

Guideline 34. Data exchange

The institution implements standardized data exchange mechanisms in accordance with the interoperability application model.

Structure

- The ICT unit should establish and implement standardized data exchange mechanisms in order to achieve economy of scale on implementing business data exchange enforcing data protection regulations. In particular, the design and implementation should foster institutional mechanisms and prevent fragmented specific data exchange business applications.
- The management should establish duties and responsibilities concerning the implementation and operation of standardized data exchange mechanisms in particular concerning the enforcement of data protection regulations and the coordination with other organizations.
- The standardized data exchange mechanisms should leverage on international standards and models such as the ones provided by the ISSA.
- The standardized data exchange mechanisms should be based on the institutional models and standards, such as the institutional interoperability framework and workplan, the SOA-based interoperability application model and the institutional technical standards.

Mechanism

- In implementing standardized data exchange mechanisms, the ICT unit should:
  - Establish project implementation teams and ICT specialized units to analyse, design and implement the required data exchange mechanisms;
  - Generate a technical specification including, for each candidate data exchange channel: The information model of data to be exchanged (i.e. the metadata schema and validation rules), service-oriented characterization (i.e. service-oriented-architecture (SOA) interfaces), Operational data exchange models (data packages) using standard languages and formats (e.g. XML, JSON, etc.), technical interoperability mechanisms, and non-functional requirements (i.e. performance, security, etc.).
- The ICT unit should base the implementation of secured data exchange mechanisms on the methodologies and technologies adopted by the institution, in particular:
  - Technical Interoperability mechanisms supporting asynchronous and response-less invocations by using advanced Web Services (WS) (i.e. WS-Discovery, WS-Addressing, WS-Eventing, WS-Notification, WS-ReliableMessaging, WS-Reliability, and WS-Policy);
  - Secured data exchange based on encrypted secured communication channels, which may consist of private ones as well as of Internet channels using TSL and secured Web Services (i.e. using WS-Security, WS-Federation and WS-Trust).

- To facilitate enforcing data protection, exchange of protected personal data should be minimized and encrypted, and should be only accessible to the corresponding organizations in the data exchange.
- The ICT unit should develop a communication plan providing appropriate information to social security service areas within the institution on the implementation of data exchange systems.

Guideline 35. Institutional technical standards on interoperability

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

Structure

- The management should ensure that the institution adopts ICT standards, including standards for interoperability.
- The management should specify relevant duties and responsibilities to specify and manage the institutional technical interoperability standards.
- Institutional standards on ICT should be based on international standards (e.g. W3C, OASIS), the institutional interoperability framework and the service-oriented-architecture (SOA)-based interoperability application model.

Mechanism

- In elaborating the institutional standards for technical interoperability, the ICT unit, with the assistance of specialized units where applicable, should cover:
  - Standard technologies on networking and data communications, covering data transport and related protocols such as TIC/IP, HTTP, FTP, SMTP, SOAP and others used in Internet-based applications;
  - Data integration and interoperability, covering technologies to describe data structure and formatting which improve the effectiveness of data exchange operations. Some of the main standards are Unicode, XML, XML Schema, XSL, S/MIME, RDF (for web resource description) and OWL (for semantic relationships of concepts);
  - Enterprise services, which enable data exchange between business applications and implementation of reusable services and shared processes. Reusable services should be implemented using web services and should follow the standards of WSDL, UDDI, SOAP, WS-* and the interoperability-oriented recommendations of WS-i. Service composition and orchestration should be implemented using WSBPEL. Enterprise platforms, which enable integration of heterogeneous applications, should be based on ESB systems. The overall integration architecture should be service-oriented architecture (SOA);
  - The presentation layers of applications, which include data which should be accessed from different utility software (such as web browsers or text viewers). Data representation standards include the file formats TXT, PDF, JPEG, PNG, HTML, XHTML and XML;
  - User interaction, especially web- and portal-based applications. Standards include Portlets (JSR 286), Microsoft Webparts, WSRP and Google gadgets/widgets.
- The management should approve, adopt and communicate the institutional standards for technical interoperability to all units involved.

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 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 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 36. Management framework for information security

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

Structure

- The board and management should establish a policy on the adoption of a systematic, clear and effective approach for the management of information security.
- The board and management should commission the ICT unit to design a management framework for information security which defines procedures and specifies related duties and responsibilities.
- The board and management may establish specialized structures to manage information security processes within the institution, with well-defined and documented roles and responsibilities to ensure their accountability.
- The contracts administration office should include these internal regulations and specifications in requests for proposals, contract documents and service level agreements.
- The framework for information security management should follow the international standard ISO/IEC 27002:2005 Information technology – Security techniques.

Mechanism

- In elaborating the framework to protect data and reduce security risks, the ICT unit should:
  - Include an inventory of information assets, specifying the respective owners;
  - Take into account all possible ICT service scenarios applicable to the institution (e.g. internal services, outsourced services, internal and external access to information, etc.);
  - Establish information security policies and protocols to govern interaction between human resources and institutional data, emphasizing security prior to, during and following termination of employment. These protocols should apply to all staff: internal, external consultants, contractors and temporary staff;
  - Establish physical security measures for the platforms storing institutional data;
  - Develop business impact analysis and contingency management plans, including information technology business continuity and disaster recovery plans.
- The management should communicate the scope of the framework throughout the institution.

Guideline 37. 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.

Structure

- The board and management should establish a policy on data privacy and protection in accordance with the legal and regulatory environment.
- The board and management should define the legal and regulatory environment of the institution, taking into account not only national regulations but also agreements with external organizations concerning mutual respect of data privacy.
- The management should designate responsibility (e.g. to a specialized unit) to develop a strategic plan to implement data privacy policies. An organizational structure (e.g. a unit or a committee) should coordinate measures and report to the management.

Mechanism

- The management should analyse the legal and regulatory environment, taking into account all instruments which could affect the institution's activities, including both national regulations and those governing the implementation of international agreements.
- The board and/or management should formalize agreements with external organizations on the mutual respect of data privacy regulations during collaboration between institutions.
- The internal audit office should carry out a detailed audit of files containing personal data and classify them according to their level of sensitivity.
- The unit responsible for data privacy ("specialized unit") should establish procedures to ensure the appropriate treatment of personal data, i.e. to minimize the amount of data collected and ensure that data is accurate, up to date and used solely for defined purposes. The unit should implement adequate security measures for personal data files. The usage of personal data in analytics applications, particularly for profiling, should be specifically assessed and ruled.
- The specialized unit should implement data collection mechanisms in compliance with the applicable data privacy policies and regulations.
- The specialized unit should implement mechanisms which protect personal rights concerning data. Such mechanisms should enable people to access their personal data stored by the institution and ensure that proper consent is obtained when necessary.
- The specialized unit should establish data transfer mechanisms to third parties which comply with the applicable data privacy policies and regulations.

- The public relations unit should carry out information campaigns and training activities explaining the scope and impact of the data privacy regulations and policies, for both the staff of the institution and other members of the social security system.
- The internal audit office should periodically audit and monitor the data privacy measures and mechanisms in place.

Guideline 38. 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).

Structure

- The ICT unit should define and implement security measures to protect the privacy of data.
- The management should define relevant duties and responsibilities for the enforcement of security policies concerning data privacy based on the information security management structure.
- Security measures for data privacy should be based on the institutional information security management framework as well as on international standard ISO/IEC 27002:2005 Information technology – Security techniques.

Mechanism

- The ICT unit should establish security measures for the protection of personal data files in order to ensure data privacy. These measures should be compiled in a master guide and should include:
  - Security measures for routine personal data files, explicitly defining access rights and implementing rigorous mechanisms to both control access and log all operations;
  - Security measures for sensitive personal data files which apply in addition to those for routine personal data. They should include cryptography mechanisms, restrictions on the movement of sensitive data outside the data centre and strict procedures for sensitive data management;
  - Security measures for data access and manipulation. The treatment of personal data should follow an established protocol to restrict data access and manipulation to authorized cases.
- The management should approve, adopt and communicate the security measures to all units involved.

Guideline 39. 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.

Structure

- The ICT unit should design and implement a comprehensive access control system.
- The management should define relevant duties and responsibilities concerning the control of access based on the information security management structure.
- The system for the control of access should be based on the institutional information security management framework and the international standard ISO/IEC 27002:2005 Information technology – Security techniques.

Mechanism

- In elaborating the comprehensive access control system, the ICT unit should:
  - Take into account both the information security structure and the technologies and products used in the institution;
  - Establish a unique authentication and identification system based on a robust user account mechanism, covering all the software systems operating in the institution. The user accounts system should be based on roles and profiles and follow the principle of minimum privileges for accounts in all the systems;
  - Establish a robust password mechanism by determining rules on password format and encrypting passwords when transmitted over an insecure communication network;
  - Establish measures to restrict access to information to users with the appropriate rights on a need-to-know basis. Access rights should be clearly defined and reviewed periodically;
  - Establish measures to control the connection of external devices to internal devices by controlling data access to endpoints with portable electronic storage devices and controlling the use of the different ports;
  - Establish procedures and mechanisms for access to operating systems based on secure log-on procedures;
  - Establish procedures and mechanisms for controlling access to web pages, which may be under a specific authentication and access control system;
  - Establish procedures and mechanisms to manage the connection of external information systems to the internal network, based on an authentication procedure and including the requirement for approval from the ICT unit;
  - Define policies and establish procedures and mechanisms for the management of activity logs concerning access to information systems, based on business needs and data classification requirements.

Guideline 40. 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.

Structure

- The ICT unit should develop and implement a plan to ensure security in database systems; in addition to general database security issues, the plan should take into account data privacy and data protection regulations which impose compulsory data security measures for protected data.
- The management should define relevant duties and responsibilities to enforce security policies in database systems.
- The contracts administration office should include these internal regulations and specifications in requests for proposals and contract documents.
- The ICT unit should ensure that the database security measures are included in disaster recovery plans, especially in backup mechanisms.
- Security mechanisms for database systems should be based on the institutional information security management framework and on international standard ISO/IEC 27002:2005 Information technology – Security techniques.

Mechanism

- In elaborating and implementing the database security plan, the ICT unit should:
  - Structure the plan around three main aspects: the data requiring protection, the rationale for protecting it and the protection mechanisms applied;
  - Establish database user accounts which are separate from those used in business applications, and particularly for when applications are accessed anonymously. These accounts should have the minimum privileges required to carry out the operations, and database administrators and administration accounts should be strictly monitored;
  - Include security measures in the database infrastructure, specifically concerning user authentication mechanisms, server protection, DBMS configuration and vulnerability control and communications encryption (if necessary for sensitive data);
  - Establish and audit development practices for applications accessing databases, to reduce the risks concerning applications and backend systems.

Guideline 41. 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.

Structure

- The ICT unit should develop comprehensive security measures for networks and communication systems to protect computer networks, information exchange systems and e-services, and monitor information processing facilities.
- The management should define duties and responsibilities to enforce security policies for networks and communication systems.
- Internal policies and procedures on security for networks and communication systems should be based on the institutional information security management framework, the international standard ISO/IEC 27002:2005 Information technology – Security techniques, and recommendations issued by the National Institute of Standards and Technology (NIST).

Mechanism

- In elaborating comprehensive security measures for networks and communication systems, the ICT unit should:
  - Introduce network measures to control external access to data resources, especially by configuring firewalls to allow access only through previously defined ports and protocols; other access should be restricted;
  - Establish security measures to control access to internal resources through wireless communication, especially by implementing IEEE 802.1x at access points and using various authentication mechanisms (not only based on MAC address);
  - Establish security measures for FTP-based communication systems in order to avoid risks related to this protocol (avoid using this protocol to transfer sensitive data);
  - Establish measures in order to avoid risks related to e-mail protocols (use SMTP protocols with external systems only when the institution's equipment is adequately configured);
  - Establish measures for accessing the Internet which enable control of access to data resources through the Web, ideally through centrally managed gateways;
  - Establish security measures to protect mobile devices in order to avoid illegal access to internal resources through this channel.

Guideline 42. Public-key infrastructure

The institution assesses the adoption of public-key infrastructure means (PKI) enabling the application of cryptographic mechanisms, such as digital certificates, to ensure integrity, identification, authentication, and non-repudiation of data exchanged with other entities and individuals.

Structure

- The management, with the assistance of the ICT unit, should assess the adoption of public-key infrastructure (PKI) means in order to support the integrity, identification and authentication, and non-repudiation of exchanged data. The main goal is to enable the implementation of electronic transactions with a legal value by using electronic authentication methods to verify the identity of the sender as well as to ensure the integrity of electronic content.
- The management, with the assistance of specialized areas, should ensure that the institutional use of PKI is in line with regulatory frameworks establishing the legal standing of electronic signatures and the use of PKI. This may involve establishing agreements with other entities.
- The institutional use of PKI should be based on the institutional information security management framework, the international standard ISO/IEC 27002:2005 Information technology – Security techniques, and recommendations issued by the National Institute of Standards and Technology (NIST).

Mechanism

- The ICT unit, with the assistance of specialized areas, should use PKI to cover the security services: integrity, confidentiality, identification and authentication, and non-repudiation. In order to achieve confidentiality, symmetric keys can be distributed using either key transport or key agreement.
- The management, with the assistance of the ICT unit and other specialised areas, should establish policies and rules concerning the components of the adopted PKI:
    - Defining valid Certification Authorities (CA) and the digital certificates they issue as well as Registration Authorities (RA);
    - Ensuring that digital certificates are based on the X.509 standard;
    - Establishing the mechanisms and frequency to access the Certificate Revocation Lists (CRLs), which are published by the CAs to communicate the certificates that have been revoked, as well as the procedures to control revoked certificates involved in operations with the institution;
    - Defining what staff will have digital certificates and the physical container (e.g. tokens, smart cards, etc.).
- The management should establish the business operations and administrative procedures using PKI means in particular digital certificates and electronic signature.
- The ICT unit should deploy software tools to enable a practical usage of digital certificates and PKI services, notably to sign and authenticate documents and emails. Training activities should be carried out to support the PKI application.

Guideline 43. Digital identities management

The institution manages digital identities for individuals in order to support secured operations through the institution's e-services.

Structure

- The management should commission the ICT unit implementing digital identity measures in order to manage unique representations of individuals involved in online operations with the institution and enable to perform a strong enough authentication.
- The institution's digital identity environment should support the following principles for trusted e-services: electronic signature, electronic seal, time stamping, electronic registered delivery, and website authentication.
- The institution may use digital identities issued by an external credential service provider (CSP), which performs the enrolment and digital identity issuance. Alternately, if the institution carries out the CSP role, sufficient resources have to be allocated to cover the required infrastructure and staff.
- The management of digital identities should comply with data protection regulations, in particular concerning the individuals' information managed during identity proofing, authentication, authorization, and federation.
- The management should establish agreements with relevant organizations such CSP and other entities involved in the Digital Identity management.
- The management of Digital Identities should be based on the institutional information security management framework, the international standard ISO/IEC 27002:2005 Information technology – Security techniques, and recommendations issued by the National Institute of Standards and Technology (NIST).

Mechanism

- The ICT Unit should implement digital identity management with the following features:
  - Authentication based on three factors: something the user knows (e.g. password); something the user has (e.g. cryptographic key); and something the user is (e.g. biometric data);
  - Federated architecture enabling to use a common digital identity system with other agencies. Although using federated digital identities requires coordinating with other organizations, it could facilitate providing joint services as well as reducing costs through an economy of scale.
- The ICT unit, in coordination with business areas, should perform a risk assessment for the online services provided to citizens in order to identify the digital identity features required in a cost-effective implementation. The risk assessment should include:
  - Risks of identity proofing, authentication errors and federation errors;

  - Specific impact categories, such as: financial, institution liability, reputation, fraud, unauthorized release of sensitive information, etc.;
  - Potential impacts for each category according to the three levels: low, moderate and high.
- Based on the risk assessment, the ICT unit, in coordination with business areas, should implement effective mechanisms for deploying and controlling digital identities in order to respond to the identified risks accordingly to the impact. They should provide different levels of assurance according to the risk assessment and the implementation costs.
- The management should communicate to the concerned users the characteristics of the implemented digital identity mechanisms and the application rules in the institution's e-services.

Guideline 44. Security in application development

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

Structure

- The board and management, with the assistance of specialized units, should establish internal security policies for software applications, especially those accessed through the Internet.
- The ICT unit should design and implement an internal guide to enforce the systematic application of information security practices in software applications.
- The contracts administration office should include these internal regulations and specifications in requests for proposals and contract documents.
- The internal audit office should monitor compliance with the established internal regulations.
- Policies and procedures on security in application development should be based on the institutional information security management framework, the international standard ISO/IEC 27002:2005 Information technology – Security techniques, and recommendations issued by the National Institute of Standards and Technology (NIST).

Mechanism

- In elaborating and implementing the software application security system, the ICT unit should:
  - Develop and issue an internal manual to enforce information security in software applications, especially those accessed through the Internet;
  - Ensure the implementation of preventive measures prior to application development; the measures should pay special attention to the separation of application execution environments (development, testing and operation) and the assignment of staff responsibilities;
  - Ensure that security rules to be included in application development and maintenance processes are specified and, especially, oriented to reduce risks of intrusion and disruption of services;
  - Implement security measures concerning the configuration and administration of web servers, especially those providing access to internal and critical information systems.
- The internal audit office, and specialized units if they exist, should establish standard procedures to monitor compliance with security protection rules in business applications.

Guideline 45. 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.

Structure

- The ICT unit should design and implement comprehensive security measures for ICT operations.
- The management, based on the information security management structure, should define duties and responsibilities for the enforcement of security policies in ICT operations.
- Internal policies and procedures on security in ICT operations should be based on the institutional information security management framework, the international standard ISO/IEC 27002:2005 Information technology – Security techniques, and recommendations issued by the National Institute of Standards and Technology (NIST).

Mechanism

- In elaborating and implementing security measures for ICT operations, the ICT unit should:
  - Implement measures covering administration of operating systems; procedures for backup management, software and information exchange, physical media transportation, removable media management, and information and storage handling; and protection against computer viruses and malicious codes (see below);
  - Establish specific measures related to software and patch installation and updates, focusing on permanent protection against reported risks as well as on the authenticity of software installed;
  - Establish specific protection against viruses and malicious codes on all local area network servers and personal computers, taking into account computers connecting to the internal network via remote access channels and wireless networks;
  - Establish security measures related to operating system operations, especially concerning remote access services, system account privileges and password management;
  - Implement specific and comprehensive backup and recovery measures, addressing not only information recovery but also the protection of backup media against unauthorized access, misuse or corruption during transportation.

Guideline 46. Cybersecurity measures

The institution puts into practice cybersecurity measures in line with national frameworks in order to protect critical information infrastructure and services

Structure

- The board and the management, with the assistance of the ICT and business units, should issue a policy statement on the adoption of cybersecurity measures in order to protect critical institution's information infrastructure and social security services.
- The management should commission the ICT unit and other relevant areas to put into practice cybersecurity measures coordinated with national cybersecurity authorities as well as with other organizations with which the institution shares information and services.
- The management, with the assistance of the relevant areas, should establish policies to prioritize information resources and services to be protected against cybersecurity risks.
- Cybersecurity measures should follow the *ISSA Guidelines on Good Governance*, especially the guidelines on risk management and on ICT governance, and they should be based on the institutional information security management framework, on international standards from the International Telecommunications Union (ITU) as well as on recommendations issued by the National Institute of Standards and Technology (NIST).

Mechanism

- In elaborating and implementing the cybersecurity measures, the ICT unit and relevant business areas should cover the concurrent and continuous functions:
  - *Identify*, which focuses on understanding the business context, the resources that support critical functions, and the related cybersecurity risks. It also comprises prioritizing efforts according to the institution's risk management strategy and business needs. Some key activities are:
    - Establishing dependencies and critical functions for delivery of critical services as well as resilience requirements;
    - Establishing cybersecurity roles and responsibilities for the entire institution and partners;
  - *Protect*, which focuses on implementing appropriate protection measures to ensure the delivery of critical services and to limit or contain the impact of a cybersecurity incident:
    - Limit access to physical and logical assets and associated facilities;
    - Protect the confidentiality, integrity, and availability of institution's data as well as against data leaks;
    - Implement an overall systems architecture comprising defensive approaches to prioritize the integrity of critical information and institution's services;
  - *Detect*, which focuses on implementing mechanisms to timely identify cybersecurity incidents;

- *Respond*, which focuses on implementing the appropriate actions to contain the impact that a cybersecurity incident may have on the institution's information infrastructure and services;
- *Recover*, which focuses on implementing plans for resilience and to timely restore to normal operations institution's capabilities and services impacted by a cybersecurity incident.

- The management should communicate the defined cybersecurity measures and related roles and responsibilities throughout the institution and partners. Training activities should be carried out to support the cybersecurity measures and plans.

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 47. 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.

Structure

- The board and management should develop a strategic framework for the adoption of mobile technologies with the aim of making significant improvements in the quality of the institution's service and the effectiveness of its administration; the framework should include a medium-term plan for the application of mobile technologies and describe the scope of resulting services and their benefits, as well as the required level of investment.
- The management may set up specialized organizational structures to develop, maintain and audit mobile services deployment processes, with well-defined and documented roles and responsibilities to ensure accountability.
- The contracts administration office should include institutional technical standards in requests for proposals, contract documents and service level agreements.
- The ICT unit should specify institutional technical standards on mobile technologies, and determine duties and responsibilities regarding their application and management.

Mechanism

- In developing an operational framework for the implementation of services based on mobile technologies, the ICT unit, together with the business units, should include:
    - Analysis of mobile technologies available in the institution and the country, the extent of their utilization among target groups, their costs (infrastructure and communications contracts) and other requirements;
    - A medium-term plan for the implementation of mobile services which takes account of the technical and economic potential and complexity of incorporating the technologies; adopts a gradual approach to services and technologies to achieve their rapid implementation at lowest cost; takes account of the capacities of potential users, the technology and the institution; and considers different management options (e.g. internal services, market publishing, outsourced services, internal and external access to information);
    - A plan for the incorporation of mobile technologies and products within the institution, including the maintenance of mobile systems and integration with services on other platforms, in accordance with the service plan. In the absence of applicable international standards, internal standards on mobile technologies should be based on available technological specifications and ongoing investigation and follow-up of technological developments; the plan should also include performance evaluation procedures on the effectiveness and efficiency of the implemented services.

- The ICT unit, with assistance from specialized units, should prepare a training plan for all those involved in the provision of the services.
- The management should communicate the operational framework throughout the institution, emphasizing the new services and their advantages to internal and external users.

Guideline 48. 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.

Structure

- The management, with the assistance of the ICT and business units, should establish priorities for mobile-based services of interest to the institution.
- The management should consider underlying user interaction and system integration approaches to mobile-based services, including:
  - Unidirectional and notification services, without state or session maintenance;
  - Bidirectional and interactive services, with state or session maintenance on a server;
  - Mobile office services, with state or session maintenance on a server and the client combining multiple applications in an integration environment.
- The management should take into account infrastructure and communication services available to users, as a key aspect in selecting the type of interaction.
- Based on the medium-term plan developed under the operational framework, the management should establish policy for the allocation of responsibilities and resources for the implementation of mobile services.
- The implementation of mobile-based services should proceed in accordance with the operational framework, in particular by conforming with the technological standards.

Mechanism

- The management, with the assistance of the ICT and business units, should identify the (user) services to be offered as a priority, commissioning the specialized units to design them. They should take account of the technological parameters and costs. In addition, they should ensure coordination with the work units responsible for non-mobile services so as to reuse existing data sources.
- The management should appoint the internal and external work teams responsible for the creation, maintenance and use of mobile services.
- The ICT unit should ensure that design of mobile services takes account of unidirectional, bidirectional and mobile office modalities and the need to integrate them with other services. Concrete services may be based on a combination of these approaches.
- The ICT unit should ensure that implementation of services maintaining a session or state take into account data consistency issues. When data is exposed in clients' mobile devices, consistency and security should be extended to those devices.
- It should be borne in mind that the training of the human resources involved and follow-up on the quality of the services will be crucial to their success.

Guideline 49. 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.

Structure

- The management should establish the relevance and priority for the institution of utilizing mobile device-based user identification methods.
- The management should entrust to the ICT unit or another specialized unit the selection of services likely to utilize device-based identification.
- The management should review and, as appropriate, update institutional definitions of valid forms of user identification, establishing policies and rules for their coexistence.
- The management should establish policy on the privacy of information stored for identification purposes, based on current legislation.
- The management should conclude the necessary agreements with telecommunications companies for the maintenance of the various forms of identification.
- The implementation of mobile-based identification mechanisms should proceed in accordance with the operational framework, in particular by conforming with the technological standards.

Mechanism

- The ICT and business units should draw up a list of the services in which to utilize user identification methods, based on the range of mobile devices in use.
- The ICT unit should develop the technical design for the user identification mechanism based on institutional technical standards and the operational framework, and coordinate its implementation.
- The management should ensure technical and operational coordination with telecommunications companies within the framework of existing agreements; this includes defining the necessary protocols for access to user identification data so as to associate such data with that held by the institution.
- The management, with the assistance of specialized units, should organize security audits so as to guarantee compliance with policies on the protection of personal data.
- The management should ensure the necessary human resources training, service disclosure and follow-up on service quality, which are crucial elements to success, in accordance with the operational framework.

Guideline 50. 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.

Structure

- The management should establish the priority to be attached to the use of mobile-based payment gateways.
- The management should review and, where necessary, update institutional definitions of valid forms of payment, establishing policies and rules for their coexistence.
- The management should establish policy on the privacy of information stored for the purpose of collecting contributions and implementing payments, in accordance with data protection regulations.
- The management should conclude the necessary agreements with banking entities and telecommunications companies to permit such operations.
- The implementation of mobile-based payment gateways should be conducted as set out in accordance with the operational framework, in particular by conforming with the technological standards.

Mechanism

- The ICT and business units should identify the services that could benefit from a mobile-based payment gateway.
- The ICT unit should draw up the technical design for the payment gateway based on institutional technical standards and the operational framework, and coordinate its implementation.
- The management should ensure technical and operational coordination with banking entities and telecommunications companies within the framework of existing agreements; this includes defining the necessary protocols for accessing user data for use in payment gateways.
- The management, with the assistance of the specialized units, should organize security audits to guarantee compliance with policies on personal data protection and the security of operations.
- The management should ensure the necessary human resources training, service disclosure and follow-up on service quality, which are crucial elements to success, in accordance with the operational framework.

Guideline 51. 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.

Structure

- The management, with the assistance of the ICT and business units, should establish the priority attached to the use of functions provided by advanced hardware gadgets in mobile devices.
- The management, with the assistance of the ICT unit, should conclude the necessary agreements with telecommunications companies to support the use of such gadgets.
- The use of gadgets in mobile devices should be in accordance with the established framework, in particular as regards technological standards.

Mechanism

- The ICT and business units should identify the services capable of utilizing gadgets in mobile devices.
- The ICT unit should draw up the technical design for the use of gadgets based on institutional technical standards and the operational framework.
- During implementation, the ICT unit should ensure that special attention is paid to the integration of devices from different manufacturers (with their specific drivers), and should follow up to ensure the quality of integration.
- The management, with the assistance of the specialized units, should organize security audits to guarantee compliance with policies on the protection of personal data and the security of operations.
- The management should ensure the necessary human resources training, service disclosure and follow-up on service quality, which are crucial elements to success, in accordance with the operational framework.

Guideline 52. Securing mobile applications

The institution secures mobile applications taking into account not only security requirements of the concerned business applications but also device-related protection measures notably tackling vulnerability breaches.

Mobile application security describes the amount of protection an application on a mobile device has from malware, phishing, and other harmful hacker crimes. All the components of a mobile application make them vulnerable to security breaches. Because identity theft and financial hacks are becoming more and more common, it's for the institutions utterly important to take extra security precautions to protect mobile apps and the people using them.

Structure

- The board should commission the ICT unit to design and establish a Secure Mobile Application Strategy taking into account relevant risks in the scenarios in which the mobile applications will be used.
- The ICT unit should include security considerations in the mobile application portfolio as well as in the development and testing tools.
- The implemented solution should follow the institution's ICT governance framework, ICT management processes, the guidelines in the section on data security and privacy, and be based on international standards and practices such as ISO 27XXX and OWASP.Org .

Mechanism

- The ICT unit should address mobile application security assuming that all mobile devices are insecure, all the applications can be compromised, and that data moving to and from the mobile application can be captured.
- The protection of mobile applications should be based on the measures described in the section on data security and privacy as well as on the following specific approaches:
    - Establish a security checklist with standardized best practices at the inception phase in order to oversee and map possible scenarios during the development and deployment of the app. This would also enable developers to assess the potential data threats and attacks;
    - Implement strong user authentication and authorization covering key features of user privacy, identity management, session management and device security features. The mechanisms should implement 2FA (two-factor authentication) and/or MFA (multi-factor authentication) and to take advantage of proven security technologies such as OpenID Connect protocol and OAuth 2.0 authorization framework;
    - Encrypt all the credentials. It is crucial to secure the access to apps' data as well as to functionalities deployed in the mobile applications;
    - Secure app data on Device, considering encryption methods like 256-bit Advanced Encryption Standard symmetric-key algorithm standards to store data on a device in the form of files, databases, and other data sources;

- Assess security features of development frameworks as well as OS vulnerabilities leveraging the latest platforms in order to mitigate the security risks. Deploying the mobile apps on legacy platforms and operating systems can increase the likelihood of security attacks.

- The ICT unit should prepare informative material for customers using mobile applications explaining the security measures and providing channels for support.

B.4. Data Analytics

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

Data analytics is mainly based on institution's data and potentially external one, which, after preparation, is analyzed to derive insights using various analytic approaches, in particular:

- **Descriptive analytics**, which tries to answer "what has happened". It provides an understanding of the past transactions that occurred in the organization;
- **Diagnostic analytics**, which tries to answer the question "why or how did it happen". It involves an understanding of the relationship between relatable data sets and identification of specific transactions along with their behaviour and underlying reasons;
- **Predictive analytics**, which tries to predict "What, When, where will it happen" based on past data. Forecasting techniques can be used to predict, to a certain extent, the future outcome of an activity;
- **Prescriptive analytics**, which allows to "prescribe" a range of possible actions as inputs such that outputs in future can be altered to the desired solution. In prescriptive analytics, multiple future scenarios can be identified based on different input interventions.

In turn, big data analytics leverages on very large volumes of data usually beyond institutions' transactions. Big data is characterized by the "4 Vs": Volume, Variety, Velocity and Veracity. For instance, a potential source of big data could be medical home devices monitoring patients' vital signs. Big data analytics requires a revisit of data analysis techniques in fundamental ways at all stages from data acquisition and storage to data transformation and interpretation. In particular, the task of collecting and analyzing data – which is at the heart of the big data analytics pipeline.

Concerning the support to decision making through Machine Learning, the main types of techniques are:

- **Inductive learning** in which models are built from the generalization of examples;
- **Deductive learning** in which deduction is applied to obtain generalizations from a solved example and its explanation;
- **Genetic learning** in which algorithms are inspired in the theory of evolution are applied to find general description to groups of examples;
- **Connexionist learning** in which generalization is performed by the adaptation mechanisms of artificial neural networks.

The main goals of the section are to support social security institutions on applying data analytics as well as on adopting emerging technologies.

These guidelines are primarily intended to provide orientations to the ICT unit on implementing and providing adequate enabling tools and services to the business areas. They also aim at providing guidance to the institution's management on applying cutting-edge and emerging technologies. 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.

Guideline 53. Institutional framework for applying data analytics

The institution establishes a framework for the application of data analytics, which defines the main procedures, duties and responsibilities, as well as technical standards.

Structure

- The management should commission the ICT and business units to develop a framework for adopting data analytics technologies. The goal is to deploy a trusted analytics strategy to improve social programmes and services through a comprehensive and systematic use of available data. The framework should enable to bridge the gap between decision-makers, data scientists and business managers.
- The board and management may establish specialized structures to manage data analytics application within the institution with well-defined and documented roles and responsibilities to ensure their accountability.
- The management should establish policy on the privacy of information used through data analytics in accordance with data protection regulations.
- The data analytics framework should follow the institution's governance rules, and the ICT governance framework and strategic plan. It should be based on ISO/IEC 10032, DAMA/DMBOK, ISO 19731:2017, ISO 9001, CRISP-DM. It should also follow recommendations in the section on data management within the current set of Guidelines.

Mechanism

- The ICT Unit should develop a framework for data analytics including the following phases:
  - Data lifecycle management, which comprises: data identification, data acquisition and filtering, data extraction, data validation and cleansing;
  - Developing metadata mapping databases to business concepts;
  - Data modelling aligned with business objectives;
  - Managing the data repository and data warehouses accessible to business users;
  - Data analysis and model development responding to business needs;
  - Performance measurement evaluating business-oriented outcomes of data analytics;
  - Interoperability with institutional Master Data and business information systems.
- The data analytics framework and the trusted analytics strategy should be based on the following data management disciplines:
  - Data quality: Ensure an accurate and correct data;
  - Data integration: Integrate your data systems together for optimal usage;
  - Data federation: Link data from heterogeneous data sources into a single, combined unit;
  - Data governance: Policies and procedures for data management and usage;

    - Master data management: Cover institution's core business data, reference data and the analytical data that supports decision making.
- The management, with the assistance of the ICT unit, should develop and train new staff profiles, notably chief data officer (CDO) and data scientists in order to cover the human resource needs on analytics application.
- Data analytics projects should involve ICT and business staff as well as the specialized profiles in order to ensure complementary contributions. All the staff should be aware of the data protection regulations.
- The management, assisted by the ICT unit, should ensure an adequate data processing capabilities. Given that many applications may not led to permanent systems, cloud-based platforms could provide adequate solutions to a highly variable context. Security and data protection should be included in infrastructure and cloud-based contracts.
- The management should communicate the framework throughout the institution, emphasizing the advantages to internal and external users.

Guideline 54. Descriptive analytics – Understanding the past

The institution applies descriptive analytics to look at data and to analyze past events for insight as to how to approach future decisions.

Structure

- The management, with the assistance of the ICT and business units, should identify areas of interest and establish a medium-term plan with priorities for the application of descriptive analytics in order to analyze past events. Descriptive analytics examine institution's data and past performance. The most robust use of descriptive analytics is programming logic into the platform to issue alerts when certain criteria or trends begin to emerge.
- The management should commission the ICT unit to carry out descriptive analytics applications based on business goals and complying with data protection regulations.
- The application of descriptive analytics should be based on the institutional framework for data analytics and should follow recommendations in the data management section within the current set of Guidelines.

Mechanism

- The business areas should describe the phenomenon or pattern to analyze, define requirements as clearly as possible, and determine in the end how the result should be presented and what the target audience will be.
- The data analytics team, including the ICT unit and business areas, should carry out the following activities:
  - Establish the most salient features of the phenomenon and which aspects, concepts, or categorizations are necessary to describe the phenomenon;
  - Identify the constructs (i.e. measures) that best represent the most salient features and would be most effective in order to systematically observe relevant features of the phenomenon;
  - Establish types of data and data collection methods that will produce the appropriate level of abstraction and quantification for analysis. Subsequently, collect the required data;
  - Identify patterns and relationships that describe the key concepts of the phenomenon by applying statistical methods and exploratory data analysis on the collected data. Pattern identification efforts should not be limited to a pre-existing hypothesis;
  - Communicate the identified patterns that describe the phenomenon of interest through the best suited presentation depending on the intended audience and by taking advantage of data visualisation techniques. The type of data presentation should be the best suited. It should be distilled and targeted to succinctly capture the essences of the phenomenon;
  - Iterate on the process as needed reviewing hypothesis, definitions and data used for the analysis.

Guideline 55. Diagnostic analytics – Explain the cause of it all

The institution applies diagnostic analytics to look towards the processes and causes of an event, instead of the result.

Structure

- The management, with the assistance of the ICT and business units, should identify areas of interest and establish a medium-term plan with priorities for the application of Diagnostic Analytics in order to explain causes of past events. Diagnostic analytics can provide an answer to questions such as "How can we avoid this problem?" and "How can we replicate this solution?".
- The management should commission the ICT unit to carry out diagnostic analytics applications based on business goals and complying with data protection regulations.
- The application of diagnostic analytics should be based on the institutional framework for data analytics and should follow recommendations in the data management section within the current set of Guidelines.

Mechanism

- The data analytics team, including the ICT unit and business areas, should carry out the following activities:
  - Identify anomalies or phenomena to explain. Based on the results of descriptive analysis, analysts should identify areas that require further study because they raise questions that cannot be answered simply by looking at the data;
  - Drill into the analytics (i.e. discovery). This step requires analysts to look for patterns outside the existing data sets, and it might require pulling in data from external sources to identify correlations and determine if any of them are causal in nature. Analysts should identify the data sources that will enable them explain the targeted phenomena;
  - Determine causal relationships. Hidden relationships are uncovered by looking at events that might have resulted in the identified phenomena. Techniques include: probability theory, regression analysis, filtering, and time-series data analytics;
  - State the conclusion clearly and provide supporting evidence by detecting phenomena of interest, anomalies, surfacing 'unusual' events, and identifying drivers of key performance indicators (KPIs):
    - This requires application of different analytical techniques to determine causation and identify independent variables that institutions can adjust to effect positive change;
    - Advanced solutions for diagnostic analytics may use machine learning techniques to increase the analysis capacity. Enabled by machine learning, diagnostic analytics serve an important function in reducing unintentional bias and misinterpretation of correlation as causation. Nevertheless, diagnostic analytics should be governed by users. Just as machines can be used to help increasing efficiency and reducing the bias in human decision making, so should people be used to contextualize the outputs of machine decision making.

Guideline 56. Predictive analytics – What is likely to happen

The institution applies predictive analytics to develop preventive approaches and related measures based on predictive models at strategic, operational and tactical levels.

Structure

- The management, with the assistance of the ICT and business units, should identify areas of interest and establish a medium-term plan with priorities for the application of Predictive Analytics in order to make predictions based on data.
    - The term "predictive analytics" describes the application of statistical or machine learning techniques to create a quantitative prediction about the future through a predictive model. Predictive models alone do not create business value, but rather need to be effectively deployed either into a business decision-making process.
    - Potential areas of application are: preventing error and fraud, proactive launch of social programmes and services based on preventive approaches targeting vulnerable population groups, and predicting service demands including budgeting, etc.
- The management should commission the ICT unit to carry out predictive analytics applications based on business goals and complying with data protection regulations.
- The application of predictive analytics should be based on the institutional framework for data analytics and should follow recommendations in the data management section within the current set of Guidelines.

Mechanism

- The business areas should describe the phenomenon or pattern to analyse, define requirements as clearly as possible, and describe unambiguously the business decisions that will be made using outputs of the predictive model.
- The data analytics team, including the ICT unit and business areas, should carry out the following activities:
    - Create a clear scope. Each model should be developed for its own specific purpose;
    - Choose the right predictive model type among different options, such as: machine learning, linear regression, naïve bayes, etc.;
    - Plan the model starting by assembling the datasets that will be used for training. Afterwards, formulate clear objectives, cleanse and organize the data, perform data treatment including missing values and outlier fixing, make a descriptive analysis of the data with statistical distributions, and create data sets used for the model-building;
    - Prepare the dataset covering the necessary variables for the expected prediction. Focus on the behavioural-oriented information;
    - Build the model, calculate scores, and validate the data:
        - Built the model using a sample from the data set;
        - Calculate a score, which represents the likelihood of what the model is predicting;

  - Validate the model, typically against datasets not used in the model development;
  - Define the information output and reporting;
  - Take into account that simplicity is a good feature. The fewer assumptions there are in a predictive model, the greater will be the predictive power.
- Implement the model defining the access storage and mechanisms to use the data.
- Manage the continuous improvement of the model.

Guideline 57. Prescriptive analytics – What action to take

The institution applies prescriptive analytics to obtain decision options on how to take advantage of a future opportunity or to mitigate a future risk.

Structure

- The management, with the assistance of the ICT and business units, should identify areas of interest and establish a medium-term plan with priorities for the application of Prescriptive Analytics, which differs from predictive analytics in that it doesn't stop at showing a likely outcome, but continues to present suggested actions. Prescriptive analytics incorporates a feedback loop in which descriptive and predictive models are combined to influence one another and direct the trends instead of simply detecting them.
- The management should commission the ICT unit to carry out prescriptive analytics applications based on business goals and complying with data protection regulations.
- Management should be aware that, although the high potential business-impact of prescriptive analytics, it can quickly become complex. A close collaboration between analytics teams and business management as well as developing a comprehensive view and high-level sponsorship are crucial, particularly in large institutions, because an optimal solution at the institution's level may be sub-optimal at departmental levels.
- The application of Prescriptive Analytics should be based on the institutional framework for data analytics and should follow recommendations in the Data Management section within the current set of Guidelines.

Mechanisms

- Business areas should describe the phenomenon or pattern to analyse, describe the prescriptive objective as clearly as possible for valid and actionable results, and define the variables, control factors and constraints to be analysed.
- The data analytics team, including the ICT unit and business areas, should carry out the following activities:
    - Create a clear scope. Each model is developed for its own specific purpose;
    - Choose the right optimization model type among options such as: linear optimization non-linear optimization, integer optimization, and stochastic optimization;
    - Create a business rules database, which are called "constraints" in the optimization terminology;
    - Build the model, calculate scores, validate the model and data, and define the information output and reporting.
- The prescriptive analytics environment should be integrated into the overall systems environment as fully as possible.
- The technology platform should scale and offer high levels of performance. While initial projects may be comparatively modest the scale and scope will rapidly grow.

- Monitor and manage prescriptive analytics projects using effective reporting mechanisms so that changes in the business environment can be responded to in an adequate manner, and changes in business strategy quickly implemented.

Guideline 58. Analytics of big data

The institution assesses the adoption of big data analytics, which consists in applying analytics techniques on such very large sets of data.

Structure

- The management, with the assistance of the ICT and business units, should identify areas of interest and establish a medium-term plan with priorities for the application of big data analytics in order to obtain outcomes from very large volumes of data characterised by the 4Vs (i.e. Volume, Variety, Velocity, and Veracity):
  - The types of available data may fall into various categories, notably: Internet of things, medical devices for long-term care (LTC), personal and home devices, social web content, geo-referenced data, environmental data, and social security transactions, etc.;
  - As data is often fragmented across many sources it may require transformations between data formats;
  - The most common big data analytics techniques are: association rule learning, classification tree analysis, genetic algorithms, machine learning, regression analysis, sentiment analysis, and social network analysis.
- The management should establish organizational structures, to address the issues related to Big Data Analytics:
  - The management may appoint a chief data officer to manage the concerned data and generated information over the long term;
  - The management may establish a research ethics board (REB) responsible for the ethical and regulatory compliance of big data applications.
- The application of big data analytics should be based on the institutional framework for data Analytics and should follow recommendations in the section on Data Management within the current set of Guidelines.

Mechanisms

- The data analytics team, including the ICT unit and business areas, should take into account several major issues concerning big data:
  - Missing and unreliable data. Data collection processes should detect potential incompleteness as well as inaccuracies and quantify their impact on the data analysis;
  - The speed at which data is generated, particularly from devices.
- The data analytics team should carry out the following activities:
  - Data collection taking into account data protection regulations and managing low data quality;
  - Data integration:
    - Ensure that the record linkage procedure used is accurate to fulfil the purposes of the project;

  - Enforce data protection regulations by de-identifying the linked data sets, ensuring that integrated data sets don't result in a permanent database of personal information and destroying data sets copies with personal information;
- Data analysis:
  - Ensure that the information analyzed is accurate, complete and up to date as well as representative of the target population to fulfil the purposes of the project;
  - Be aware of potential spurious correlations and ensure that all patterns discovered in the analysis are meaningful;
  - Assess potential variables correlating with protected personal characteristics and prevent data protection violations;
  - Focus on analytics not reporting;
- Data profiling, which should comprise verifying the results of decisions based solely on profiling in cases where the decisions significantly affect individuals.

Guideline 59. Machine learning on big data – Supporting decision making

The institution assess the application of machine learning techniques on big data to support decision making.

Structure

- The management, with the assistance of the ICT and business units, should identify areas of interest and establish a medium-term plan with priorities for the application of machine learning techniques in order to make decisions more accurate, effective and efficient. The goals are:
  - Reducing the time between the three steps: data collection, analysing it for relevant information, and using the outcome to take well informed decisions;
  - Machine learning algorithms are quite adaptive in nature. The more data you feed, the more they learn and their predictive modules become more precise and the results become more accurate. Therefore, big data and machine learning may support social security managers planning new social programmes.
- The main types of machine learning to be considered for application are: inductive learning, deductive learning, genetic learning, connexionist learning.
- The application of machine learning techniques should be based on the institutional framework for data analytics and should follow recommendations in the data management section within the current set of Guidelines.

Mechanisms

- The data analytics team, including the ICT unit and business areas, should carry out the following activities:
  - Define a business problem statement;
  - Identify machine learning use cases focusing on analytics problems well suited for self-teaching algorithms and checking data availability to assess feasibility;
  - Define the dataset, comprising sources and data update frequency;
  - Define data preparation requirements differentiating between Historical machine learning and real-time use cases. Define imputation rules to replace missing data and establish the right data profiling and quality measures to assess false positives and data skew;
  - Define the logical data usage patterns. Users should define how they intend to use the data – i.e., the decisions the machine learning algorithm will make, the necessary input data types, the temporality of those decisions, data to transform, etc.;
  - Architect a data pipeline for each use case both for model training and production;
  - Select your data platforms taking into account data sources and processing requirements. Consider data lakes and map reduce technologies as well as cloud-based processing;

- Plan for fast growth with significant buffer capacity in the processing power, storage, and network bandwidth that each data pipeline requires;
- Streamline data flows using change data capture (CDC) technology, which copies data and metadata real-time updates from sources by sending only incremental data updates;
- Carefully consider requirements for model testing. Models should be tested to optimize results repeatedly both before and after going into production;
- Plan for fast and frequent iterations to your production environment including data input changes, replacing algorithms, and trying new algorithm combinations;
- Monitor and refine data flows.

C. Social Security Components

Structure

The following guidelines are organized in four 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 Social Security Agreements, addresses the implementation of the operational aspects of international agreements by using ICT, and focus on data exchange processes and related functions.

Section C.3, eHealth – ICT Application in Healthcare, presents approaches for developing technological capabilities in social security institutions to manage health-related information and services.

Section C.4, Implementation of Social Security Business Processes, addresses the issues of putting into practice a process-based approach in social security institutions.

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: I) to determine the most accurate, golden data values from among potentially conflicting data values; and ii) 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

This section addresses the institutional decisions that must be taken to guide the design and implementation of master data projects as well as daily operations.

Guideline 60. 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.

Structure

- The board should appoint a committee of directors – Master Data Governance Committee – in charge of the Master Data Governance Programme, and a committee for stewardship – Master Data Stewardship Council – in charge of the Master Data Management Programme.
- The board, the management and the Master Data Governance Committee, with the assistance of the ICT governance, should issue a statement on what master data governance means for the institution.
- The Master Data Governance Programme should apply the six principles of ICT governance and should be consistent with the mission, vision and goals of the institution.
- The Master Data Management Programme should be aligned to the Master Data Governance Programme in order to implement and maintain the corresponding master data management information systems to support master data management operations throughout the master data life cycle.
- The Master Data Governance Committee should develop indicators to monitor the level of implementation of the Master Data Governance Programme.
- The Master Data Stewardship Council should develop indicators to monitor the performance of the master data management information systems and the quality levels of the master data.
- The Master Data Governance Programme should follow the current set of Guidelines and the *ISSA Guidelines on Good Governance*, as well as standards and international practices on ICT (e.g. ISO/IEC 38500, COBIT®).
- The Master Data Management Programme should follow the current set of Guidelines, particularly the section on data and information management, as well as standards and international practices on master data management (e.g. ISO 8000, parts 100–140; DAMA).

Mechanism

- The board should establish the corresponding Master Data Governance (MDG) and Master Data Management (MDM) Committees.
- The Master Data Governance Programme should:
    - Cover the institution as a whole, integrating master data governance into data governance and ICT governance as well as governance of the institution in general, encompassing all functions and all relevant processes;
    - Cover the need to exchange master data with other institutions;

  - Follow the principles of Responsibility, Strategy, Acquisition, Performance, Conformance and Human Behaviour as determined in ISO/IEC 38500, through defining corresponding policies.
- The board should validate and communicate the Master Data Governance Programme for the entire institution through appropriate actions.
- The board should leverage the Master Data Management Programme. This implies carrying out activities to:
  - Appoint staff with appropriate skills to be in charge of the Master Data Stewardship Council;
  - Identify the ICT resources and their corresponding capabilities to support the master data management activities;
  - Lead the deployment projects of the master data management infrastructure;
  - Assess the performance of the master data management infrastructure to account to senior management.

Guideline 61. Strategies, policies and roles

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

Structure

- The Master Data Governance Committee should:
  - Derive a strategy for master data governance from the organizational strategy. The strategy should be based on business goals related to using master data in social security and should be described by means of policies;
  - Implement plans in order to carry out the master data governance and master data management processes linked to the governance objectives;
  - Identify the roles required to execute the various master data management operations across the master data life cycle;
  - Identify the responsibility chains in order to track accountability on the master data actions. This can be done by using the RACI Matrix;
  - Appoint staff to be responsible for the master data governance activities required, as well as data stewards;
  - Define a structure for documenting, storing and communicating a set of policies which cover all six principles defined by ISO/IEC 38500.
- The Master Data Governance Programme should include an assessment of the needs, conditions and options of the institution's areas of concern in order to define institutionally balanced objectives. It should establish priorities and monitor performance and compliance with agreed objectives.
- A specialized organizational structure should be established to coordinate the master data governance processes. To provide accountability, the roles and chains of responsibility among persons and units appointed to carry out the various tasks should be clearly defined. Roles for master data governance may be based on the data governance roles identified in COBIT®.
- The master data governance processes should follow the institution's framework of data governance as well as standards and international practices (e.g. ISO/IEC 38500, COBIT® 4.1, COBIT® 5).
- The defined strategy and action plans should be based on the institutional ICT governance and management processes recommended in this set of Guidelines.

Mechanism

- The Master Data Governance and Master Data Management Committees should define the criteria and a preliminary scope concerning the data types to be included in the master data:
  - The criteria may establish that the master data should include the data types required by software applications implementing the main social security functions. They can also be based on a risk analysis of inconsistencies due to multiple versions of the same data. These criteria may lead to the inclusion, for instance, of personal basic data and family links, employee–employer links, etc.;

- A preliminary scope may include: personal basic data according to the various relations with social security functions (employee, beneficiary, contributor, etc.), family and household-related links, employers, labour records (employee–employer relationship), and employees' monthly salary;
- Master data items should be classified according to the degree of requirement (e.g. critical, necessary, recommended, optional, etc.). This classification has to be updated systematically.

- The Master Data Governance Committee should define the master data governance processes with the aim of:
  - Analysing and articulating the requirements for master data governance, and establishing and maintaining structures, principles, processes and best practices with clear responsibilities and authority;
  - Optimizing the value provided to the mission of the institution's business processes and ICT services for the government and management of the data and the data assets that are derived from the investment;
  - Managing the risks related to using unreliable data in social programmes;
  - Allocating adequate resources (staff, processes and technologies) for the master data programmes to support the objectives of the institution effectively with optimal costs;
  - Ensuring transparency of the performance and measurement of compliance with the government and management of the data-related functions;
  - Defining and maintaining an inventory of the responsibilities required for each of the activities and operations in the master data life cycle;
  - Identifying the training programmes required to improve the skills of the staff involved in master data operations and activities.
- The Master Data Governance Committee should establish structures, processes and practices for governance and management of the data.

Guideline 62. 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.

Structure

- The board should appoint the Master Data Governance Committee to establish the value of master data for the institution, as well as the most suitable approaches and practices to optimize performance.
- The management should appoint a specialized unit to manage the values of the institution relating to ICT and master data management and governance.
- The Master Data Governance Committee should identify the best means of estimating the value of the master data.
- The process of determining the value of the master data should be based on the institutional ICT governance and management processes recommended in in these Guidelines, as well as on COBIT® (ValueIT).

Mechanism

- The Master Data Governance Committee, with the assistance of the ICT unit and other competent units, should define the value of the master data. This involves:
  - Understanding the requirements of the various interest groups – the strategic ICT issues as well as the capacities relating to the actual and potential significance of the master data for business and the institution's ICT strategy;
  - Determining the value of master data for the institution and communicating this information throughout all the organizational processes of the institution. For instance, determining:
    - How it enables the implementation of compliance controls in order to prevent errors and fraud;
    - How it enables the automation of business processes;
    - The impacts on time, effort and costs of accessing fragmented information systems and of using unreliable data in social programmes;
    - The value of implementing new social programmes with short delays by reusing the master data;
  - Assessing how effectively the strategies to implement master data management operations have generated the desired value;

    - Optionally classifying master data items according to their value. This classification would be updated systematically.

- The ICT and specialized units should continuously assess the portfolio of ICT-related investments in master data, services and licensed ICT assets, to determine the probability of achieving institutional goals at a reasonable cost.
- The ICT and specialized units should address the principles and practices of data value management, to allow the achievement of optimal value from agreed ICT investments. This implies encouraging the management to consider potential innovative uses of ICT which allow the institution to respond to new challenges and opportunities.
- The Master Data Governance Committee should communicate the institutional scope of the definition of value and principles that allow the value of the data to be realized in the social security institution as a whole.

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 63. 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.

Structure

- The board and the Master Data Governance Committee should issue a policy statement on the adoption of a systematic, clear and effective management approach for the quality of master data.
- The Master Data Governance Committee should commission the ICT unit to design a framework for master data quality management, defining the functions and procedures to be involved.
- Specialized organizational structures may be established to manage the quality of the master data. Accountability, roles and responsibilities should be clearly defined and documented.
- The Master Data Stewardship Council should identify the most representative data quality measures for master data.
- The management measures for the quality of the master data should follow the institutional data management frameworks recommended in this current set of Guidelines in the section on data and information management, as well as the international practices defined in ISO 8000 and the DAMA DMBOK.

Mechanism

- The ICT unit and the master data management implementation team, with the assistance of specialized units, should specify and implement a framework that defines processes, procedures and functions for the management of the quality of data and information. Different scenarios of the applicable master data services in the institution (e.g. internal services, outsourced services, access to internal and external information) should be taken into account. This includes the following activities:
  - Specification of the requirements related to the quality of the master data;
  - Specification of a model for evaluating the quality of the master data (metrics, dimensions, etc.);
  - Specification of the "business rules" on the quality of the master data that must be implemented in the master data management systems. This activity should involve coordination with business areas and customer services;
  - Definition of rules for fixing the non-conformities to master data quality;

- Definition of a strategy for the continuous improvement of master data quality, taking into account the different categories of the master data:
  - Data quality goals and indicators for specific categories of master data;
  - Strategies for achieving cost-effective quality levels in the master data (preventive versus corrective, defining acceptable risks, etc.);
- Definition of procedures for the management of incidents relating to the quality of the master data.

Guideline 64. 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.

Structure

- The Master Data Governance Committee should institutionalize practices related to the implementation of the preventive measures to foster the quality of the master data.
- The Master Data Stewardship Council should:
  - Identify the causes of relevant problems related to poor data quality in master data and assess the risks of such problems;
  - Define preventive actions to reduce poor data quality problems, focusing on their root causes.
- The preventive measures to foster the quality of the master data should follow the institutional data management frameworks recommended in Section A.5, Data and Information Management, as well as international practices defined in the DAMA DMBOK.

Mechanism

- The Master Data Stewardship Council should:
  - Identify relevant risks due to poor levels of data quality;
  - Identify root causes of poor levels of data quality and the related problems;
  - Evaluate the possible impact of the risks and prioritize based on the possible impact.
- The Master Data Stewardship Council and the ICT unit should implement preventive measures fostering the consistency of master data, including:
  - Preventing poor-quality and non-validated data from being inserted in the master data system, especially when exchanging data with other organizations;
  - Maximizing the use of already validated data, especially in data entry software applications;
  - Systematically monitoring the quality of master data.
- Software applications performing operations on the master data should include components to carry out preventive quality controls.

Guideline 65. 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.

Structure

- The Master Data Governance Committee should institutionalize practices related to the management and improvement of the master data quality.
- The Master Data Stewardship Council should:
  - Define relevant goals and indicators for the quality of master data;
  - Implement practices to ensure adequate quality levels and to improve them when necessary;
  - Design and coordinate the assessment and improvement actions.
- The quality improvement measures on the master data should follow the institutional data management frameworks recommended in this set of Guidelines, section on data and information management, as well as international practices defined in the DAMA DMBOK.

Mechanism

- The Master Data Stewardship Council should define goals and indicators concerning the quality of the master data. These goals and indicators:
  - Provide the means to carry out permanent quality control and improvement;
  - Should be defined in coordination with business areas and customer services.
- The Master Data Stewardship Council should implement monitoring mechanisms on the quality levels of the master data.
- The Master Data Stewardship Council should implement measures to improve quality levels of the master data:
  - These measures may consist of master data profiling and master data cleansing operations;
  - They may be applied periodically and on an ad hoc basis.

C.1.3. Design and Implementation

This section 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.

Guideline 66. 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.

Structure

- The Master Data Governance Committee should appoint the Master Data Stewardship Council and the ICT unit to specify the architectures for the master data system, the master data governance system, and the master data management system.
- The Master Data Stewardship Council should specify requirements for architectures of the master data, the master data governance and the master data management information systems in order to achieve their goals.
- The ICT unit should ensure that the three information systems will be adequately integrated into the institutional ICT infrastructure covering all aspects, such as security, performance, quality, etc.
- The Master Data Management Committee may use the principles introduced in ISO 2000, ISO 8000, parts 100–140, and DAMA to design the exchange-oriented master data system architecture.
- The architecture for the master data-related systems should be based on the institutional architectures as well as the recommendations of the current set of Guidelines, particularly in the sections on management and on key technologies.

Mechanism

- The Master Data Governance Committee should specify requirements for the architecture of the master data governance system.
- The Master Data Stewardship Council should specify requirements for the architecture of the master data management system.
- The Master Data Stewardship Council should specify requirements for the architecture of the master data system.
- The ICT unit, with the assistance of ICT architects, should specify the architecture for the master data system in order to achieve the goal of an institutional master data system providing validated core social security data to the whole institution. Among others, the following aspects should be taken into account:
    - The architecture should follow a design based on SOA (service oriented architecture) and cover the Metadata in addition to the master data model;

- The architecture should support transactional CRUD (Create, Read, Update, Delete) operations as well as provide information for decision-support systems (e.g. Data Warehouse and Business Intelligence);
- The architecture should be integrated into the institutional one, establishing interactions with the other business applications in the institution;
- The architecture may combine styles such as registry, repository, local distribution, remote distribution, etc., possibly involving external institutions;
- The architecture should follow a service-oriented approach;
- The architecture may support master data exchange with external institutions.

Guideline 67. 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.

Structure

- The board and the management should commission the Master Data Governance Committee, the Master Data Management Committee and the ICT unit to define a project aimed at implementing a master data system.
- The project should take into account:
  - Functional requirements of all involved business areas of the institution, especially those managing core social security functions such as enrolment, benefits, contribution collection and payment;
  - Non-functional requirements of the ICT unit and other competent areas. This should include service-level agreements (SLAs) for the operations of the master data systems.
- Component development may be based on processes for software development described in ISO 12207 or CMMI-DEV. In the case of acquiring the software components, the institution may apply processes for software acquisition described in ISO 12207, ISO 20000 or CMMI-ACQ.
- The implementation of the master data system should be based on the institution's project and development frameworks and models.

Mechanism

- The Master Data Governance Committee, the Master Data Management Committee and the ICT unit should set up a project with organizational structure and resources adequate to implement the institution's master data system.
- The Master Data Management Committee should specify the requirements for the master data system. The following considerations should be taken into account:
  - Concerning architectural aspects, the implementation should follow the defined architecture and an SOA approach. The system should provide service-oriented interfaces and use SOA-oriented middleware to facilitate access across and outside the institution;
  - Concerning the contents, the system should use reliable identifiers, especially for persons, as well as reference data (e.g. activity and geographic codes, etc.). The system should manage data versions, keeping the values for slowly changing objects, such as persons changing family status and address, or companies changing sector of activity. In turn, the criteria for moving active data to historic databases should be defined;
  - Concerning operations, the system should implement data management operations including CRUD and should support online transactions and provide master data to decision-support systems (i.e. data warehouses and business intelligence tools).
- The scope of the data objects to include in master data constitutes one of the main types of functional requirements. Based on the preliminary scope, defined as recommended in

Guideline 2, IT governance processes, the following data types may be included in the master data:

- Persons, including basic data and specific data corresponding to their different relations with the social security functions (employee, beneficiary, contributor, etc.), family and household-related links;
- Employers, including basic data and the contribution collection balance if relevant for other areas of the institution;
- Labour records (employee–employer relationship, employee's monthly salary).

- The ICT Governance Committee, with the assistance of the ICT unit, may conduct the elaboration of a detailed design of the master data model and the metadata.
- The ICT Governance Committee, with the assistance of the ICT unit, should conduct the corresponding buy-or-develop analysis to choose the most appropriate option.

  Several master data products are available on the software market, which should be customized to the social security domain.

Guideline 68. 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.

Structure

- The Master Data Governance Committee should establish change management practices on the master data system which minimize the impact on other systems as well as disruptions in operations.
- Processing change requirements on the master data system should start with an impact analysis on master data operations, as well as on the other systems, in order to determine overall costs and potential disruptions.
- The Master Data Stewardship Council should:
  - Implement a configuration management system that can help to maintain the baseline of the master data sets;
  - Execute the corresponding activities in order to implement continuous improvement of master data, paying special attention to the concepts included in the master data as well as the business rules associated with the master data model.
- The Master Data Management Committee can use the principles on master data quality provided in ISO 8000-60.
- The implementation of change and evolution of management practices should be based on the institution's project and development frameworks and models defined in the master data system.

Mechanism

- The Master Data Stewardship Council should manage requested changes to the master data by means of the configuration management system.
- The Master Data Stewardship Council should put into practice measures to improve the master data sets.
- Procedures to carry out an impact analysis should cover:
  - The master data system, establishing whether the change implies disruptions in services;
  - The systems using the master data, assessing the consequences in terms of disruptions in services as well as in making changes to these systems.

- Concerning change management, the Master Data Stewardship Council should:
  - Identify the set of actions in a continuous way so that master data can be improved when necessary. It should make a plan to assess the viability of the actions;
  - Determine approaches to carry out the changes in order to minimize costs and system disruptions;
  - Define a change work plan so that several changes may be carried out at a time.

Guideline 69. 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.

Structure

- The Master Data Governance Committee should issue an interoperability-related policy and should commission the Master Data Stewardship Council and the ICT unit to implement the related measures. These policies should foster a common understanding of the meaning of master data throughout the institution's processes.
- The Master Data Stewardship Council and the ICT unit should implement interoperability mechanisms for the master data system covering system interaction as well as data provenance aspects when other institutions are involved.
- The Master Data Stewardship Council can use ISO 8000, parts 100–140, to leverage master data provenance and semantic interoperability.
- The interoperability mechanisms for the master data system should follow the institutional framework and technical standards on interoperability recommended in the current set of Guidelines, section on interoperability.

Mechanism

- The Master Data Stewardship Council should define interoperability requirements to integrate the master data system with other systems (both within and outside the institution). It should:
  - Identify and characterize other systems to interact with;
  - Develop the necessary mechanisms to add the data provenance to the master data. A data dictionary may enable better management of the master data when the systems interoperate. ISO 8000, parts 100–140 could be used.
- The ICT unit and the Master Data Stewardship Council should implement interoperability mechanisms for the master data system, including:
  - System interaction based on technical interoperability techniques, such as enterprise middleware and web services. These techniques should comply with non-functional requirements defined for the master data system;
  - Definition of the formats of input and output data to the master data system;
  - Definition of semantic links between pieces of data;
  - Components to provide information about the data provenance of the master data when it is exchanged between organizations.

Guideline 70. 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.

Structure

- The Master Data Stewardship Council should establish policies and responsibilities for the adoption of master data security based on the institution's security framework and on the relevant regulations. It should highlight when laws and regulations oblige the institution to carry out data governance procedures (integrity, storage and maintenance, data protection, "right to be forgotten", etc.).
- The Master Data Stewardship Council should design a framework observing the master data security policies and relevant data protection regulations as well as privacy requirements generated by individual consents.
- The framework should cover all relevant data security aspects, involving not only corporate access control and databases, but also security in networks and communications as well as physical security.
- The management should establish roles and responsibilities on the enforcement of data security and privacy rules and regulations.
- The defined data security and privacy framework should follow the institutional data security framework, as well as this set of Guidelines, particularly in the section on data security and privacy, and the international standard ISO/IEC 27000.

Mechanism

- The master data management team and the ICT unit should implement the security and privacy framework for the master data system, including the following measures:
  - Include an inventory of master data assets, specifying the respective owners and the access rights;
  - Classify master data items according to the institutional model and applicable regulations for public, private and sensitive information;
  - Consider relevant risk scenarios for the master data systems' security and privacy;
  - Establish policies and protocols of master data security that govern the interaction between human resources and institutional data, highlighting privacy before, during and after the termination of employment. These protocols should apply to all staff: internal, external, consultants, contractors and temporary staff.
- Data protection regulations on master data should be enforced taking into account data exchange with other institutions.
- The security measures should also be applied to all business applications using the master data.

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 71. 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).

Structure

- The Master Data Stewardship Council and the ICT unit should establish the infrastructure required to support the master data operations as well as to respond to eventual master data system interruptions or malfunctioning. This includes analysis and assessment of the economic and technical implications as well as those related to human resources.
- The management, based on the assessment of the ICT unit, should define roles and responsibilities involving the operation of the master data system.
- The implementation of master data system operations should follow institutional ICT management and operations processes, in the section on ICT service delivery, and underlying international practices such as ITIL® and ISO 2000 to design the business continuity of the master data operations.

Mechanism

- The Master Data Governance Committee should put into practice the necessary measures to ensure the business continuity of the master data operations.
- The Master Data Stewardship Council should:
  - Determine the threshold for the system performance indicator according to the SLA in order to ensure the business continuity of the master data operations;
  - Establish continuous monitoring and alarms on SLA-related indicators for the master data operations;
  - Define prevention plans such as high-availability configurations on different sites and redundancy of the most critical resources;
  - Define contingency plans such as activation of hot sites to enable the continuity of the master data operations.
- The ICT unit should analyse the implications and requirements of operating the master data system. Some aspects to take into account are:
  - Intensive use of the system by a large number of software applications in the institution, some of which are critical;
  - Eventual 7-day and 24-hour operations due to e-services accessing the master data.
- The ICT unit should carry out the master data system operations as part of the institution's ICT operations management and service delivery activities. This also includes: managing technical support, service desk and request fulfilment, as well as events, incidents and problems.

C.2. ICT-based Implementation of International Social Security 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 the section on 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

This section 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

Guideline 72. 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.

Structure

- The board should establish the institution's mission and roles for the operational implementation of international social security agreements that are within the mandate of the institution.
- The board and the management should establish the internal governance structure to implement the international agreements as defined in its mission. This may cover the eventual participation of the institution in the interorganizational bodies, committees and working groups that manage the agreement at the international and national levels.
- The board and the management should define specialized structures to manage the processes in the implementation of international agreements, defining roles and responsibilities.
- The management should define and use appropriate procedures to achieve effectiveness and document control. Document control may be carried out according to the ISO 9001 guidelines, section 4.2.3, Control of Documents, and section 4.2.4, Control of Record.
- The defined mission, roles and governance structure to implement the operations of the international social security agreements should be based on the institutional ICT Governance and Management processes recommended in this set of Guidelines.

Mechanism

- The board should establish the mission and roles of the institution concerning the implementation of international agreements. Such mission and roles may concern participation as a "competent institution" in certain social security branches, or as the "liaison agency" for the country.
- The board and the management should establish the internal governance structure, including management and operational roles, to implement the international agreements:
    - The main units involved may be the international relations unit, benefits administration units and the ICT unit;
    - The institution may join committees and working groups at the national and international levels, such as the Contact Group that manages the general aspects of the agreement, the committee defining the data to be exchanged, working groups for data protection aspects, the Responsible Technical Team (RTT) in charge of the ICT aspects, and other specialized groups;
    - In order to maximize the alignment of ICT developments with the social security goals, the ICT and other relevant units should establish a preliminary set of key principles.

Guideline 73. Strategy and action plan

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

Structure

- The board and the management should establish a strategy for implementing the operational activities of international agreements. This strategy should be included in the institution's strategic plan.
- The management, in accordance with the defined strategy, should establish an action plan to implement the operational activities of international agreements. This includes defining roles and responsibilities based on the defined governance structures.
- The strategic plan for implementing international agreements should follow the principles defined in the *ISSA Guidelines on Good Governance*.
- The defined strategy and an action plan to implement the international social security agreements should be based on the institutional ICT Governance and Management processes recommended in the current set of Guidelines.

Mechanism

- The strategy for the implementation of the operational activities of the international agreements may include some of the following elements:
  - The institution's goals on improving the effectiveness related to the operations of the agreements. These may include increasing the integrity of the programme, minimizing errors and undue payments, reducing delays in operations, reducing disputes with other institutions, etc.;
  - The institution's policies on ICT security and data protection, as well as on the authentication of operations;
  - Incremental development of the international project, starting with a subset of functions and branches, and implementing pilots;
  - Carrying out parallel training activities for the staff to be involved in the ICT-based operations of the agreement.
- The management, with the assistance of the competent units, should define an action plan for the implementation of international agreements.
- The board should approve and communicate the strategic plan for the implementation of international agreements in conformance with the institutional strategic plan. The management should approve, adopt and communicate the action plan.

Guideline 74. 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.

Structure

- The management, with the assistance of the ICT and other competent units, should define principles to manage key operations and resources, such as data exchange operations, notifications, information models of the data exchanged, digital certificates and signatures, and the software systems to be used.
- These definitions should comply with the terms and arrangements in the international agreements to be implemented as well as with institutional policies and technical standards.
- The defined administration principles for the main operations and resources should be based on the institutional ICT management processes recommended in the current set of Guidelines.

Mechanism

- The principles on which to manage the main operations and resources may involve:
  - The internal authorization procedures required to process requests from other institutions as well as delivery responses (e.g. certain requests must be validated prior to being processed in the internal system, all responses granting benefits require a special authorization, etc.);
  - Periodicity and procedures to send notifications to the other institutions in the agreement (e.g. automatically when a change occurs, on a pre-established periodicity, etc.);
  - Reciprocity rules concerning expenses involved in the application of the agreement;
  - Information models used in the institution concerning employees and beneficiaries, their working periods and benefits received, as well as their family status, etc.;
  - Persons' identification mechanisms used by the institution and in the country (e.g. national personal ID, passport number, internal ID issued by the institution, etc.);
  - Data protection and ICT security considerations that may lead to applying case-by-case approaches to processing requests;
  - Traceability requirements on the operations to facilitate the follow-up (i.e. keeping a record of relevant operations, particularly between institutions);
  - Usage of digital signatures in the institution and how to manage the authorizations for performing different operations in the agreement;

- Characteristics of the software systems to use in implementing the agreements' operations (e.g. components that would be common to several agreements, reusing other existing components, etc.).

- The management should approve, adopt and communicate principles, goals and a framework to manage the main operations and resources related to implementing international agreements.

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 C.2.1 summarizes the criteria.

Table C.2.1. *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 agencies.	• Full International architecture (including common services and a "trusted third organization") connecting the single national institution and the other liaison agencies.
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 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 75. 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.

Structure

- The management should commission the ICT unit and the institution's delegates in the working committees of the agreement to establish an international architecture in coordination with the other participant institutions.
- To enable efficient and secure international data exchanges, the architecture should include interoperability mechanisms, security features, authorization and non-repudiation functions, as well as traceability services for the transactions.
- The international architecture should comply with the terms and administrative arrangements of the agreement.
- The management, with the assistance of the ICT unit, should appoint members of the institution's staff to the Responsible Technical Team (RTT) of the international agreement, which manages the ICT aspects of the agreement at the international level.
- The international architecture should be the most compatible possible with the institutional architectures and models recommended in the current set of Guidelines, particularly the section on ICT management, and Part B on key technologies.

Mechanism

- The Responsible Technical Team (RTT) should define an international architecture for the international social security agreement, enabling it to perform international data exchanges in an efficient and secure way.
- The scope and features of a specific international architecture would strongly depend on the characteristics of the agreement:
    - Architectures for bilateral agreements may be based on a liaison-to-liaison pattern, having the key resources on the liaison agencies' sites;
    - Architectures for multilateral agreements may require additional components to support multi-liaison interactions and additional common resources (e.g. directory of liaison agencies, log of transactions, etc.). In addition, an organization may play the role of a "trusted third organization" to manage the key common resources;
        - Distributed architectures based on standards have the advantages of reducing the requirements for a central hub system as well as the risks of single point of failure. Nevertheless, a centralized hub-oriented approach would be appropriate for common

services with a single validation point. Distributed architectures and centralized hub-oriented approaches are compatible;

- A variant of an international architecture for multiple bilateral agreements may be considered in order to reuse software applications and key resources.

- The international architecture should include a Common Reference Service (CRS), which works as a data broker between institutions. Some of the main goals of a CRS are to:
  - Provide service-oriented interoperability mechanisms to perform efficient and secure data exchange operations between institutions;
  - Manage the verified signatures of institutions' staff as well as their corresponding authorizations to perform operations in the agreement;
  - Manage metadata and semantic resources on the data to be exchanged;
  - Provide the means to manage service quality indicators, especially concerning service-level agreements (SLAs) established for the agreement's operations;
  - Provide the means to manage transaction logs, keeping track of all operations in order to provide traceability functions.
- The RTT should oversee the implementation and management of the CRS, including the tasks of:
  - Defining the technological infrastructure required for the CRS, particularly the interoperability mechanisms;
  - Defining the data, metadata, processes and services the broker will use to serve as a common reference service;
  - Defining metrics, performance indicators and monitoring mechanisms;
  - Defining requirements concerning security vendors, security policy and key management, and identifying external service providers for the generation of digital certificates.
- The RTT, in coordination with the institution's ICT unit, should define technical requirements and configurations to connect the institution to the CRS.
- The ICT unit, in collaboration with the RTT and following the institution's interoperability policies, should develop the gateways necessary to connect the institution to the CRS.

Guideline 76. 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.

Structure

- The management should commission the ICT unit and institution's delegates in the working committee of the agreement to establish, in coordination with the other national institutions, a national architecture.
- The main purpose of the national architecture is to coordinate the interaction of several competent institutions in the same country with the country liaison agency, which performs the cross-border exchanges based on the international architecture.
- The national architecture should comply with national standards and frameworks for e-government.
- The national architecture should be the most compatible possible with the institutional architectures and models recommended in the current set of Guidelines, particularly the sections on ICT management, and on key technologies.

Mechanism

- The Responsible Technical Team (RTT) for the national institutions should define a national architecture to connect institutions of the same country to the international social security agreement.
- The scope and features of a specific national architecture would strongly depend on the national configuration of competent institutions administering the social security branches covered by the agreement.
- The national architecture corresponds to a national hub connected to the international CRS. The main goals of the components in the national architecture are to:
    - Redirect incoming international requests to the national institutions concerned, possibly generating multiple specific requests for each one;
    - Generate outgoing international data packages to be sent through the international architecture, using as input requests or replies from the national institutions.
- The proposed architecture should be able to maintain a repository of relevant local data as well as replicas of CRS data. This may include logs of transactions, digital certificates, etc.
- The national architecture will include a National Exchange System (NES), which may be implemented based on the paradigm of asynchrony message processing:
    - The implementation of asynchrony message processing may be based on message queues using an appropriate middleware system;

- To implement the hub-oriented operations, the NES may have specialized dispatchers to process messages from a cross-border liaison agency and from the competent national institutions;
- The NES should maintain an operation log for transactions, notifying the CRS of the new state when any change occurs. Such notification may be made asynchronously if the international agreement allows it to do so.

Guideline 77. 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.

Structure

- The management should commission the ICT unit to define and implement an institutional architecture to manage requests and responses exchanged with other institutions participating in the agreement.
- The institutional architecture should be in conformance with the institutional principles defined to manage the main operations and resources involved in the agreement, as recommended in Guideline 3.
- The institutional architecture should comply with institutional security and data protection policies and measures.
- The institutional architecture should be based on the institutional architectures as well as the recommendations of the current set of Guidelines, particularly the section son ICT management, and on key technologies.

Mechanism

- The ICT unit should define an institutional architecture to perform interaction with other institutions, enabling international data exchanges in an efficient and secure way.
- The institutional architecture should include an Institutional Exchange System (IES) that implements mechanisms for managing requests and responses interacting with the NES (National Exchange System) and with the international CRS (Common Reference Service). The main functions of the IES include:
    - Providing an effective and secure connection between the institution's ICT systems, the NES and the CRS;
    - Providing transaction flow management capabilities that enable the institution to accept, suspend or reject individual case transactions;
    - Generating requests to other institutions participating in the agreement;
    - Validating incoming requests prior to their being processed by the institution's information systems;
    - Generating response messages to requests;
    - Validating outgoing messages prior to sending them to the NES and CRS;
    - Providing timely information on the status of each request sent by the institution, as well as mechanisms for maintaining service-level agreements (SLAs) accordingly.
- The IES may be implemented based on the paradigm of asynchrony message processing:
    - The implementation of asynchrony message processing may be based on message queues using an appropriate middleware system in order to manage the SLA message control parameters;

- The IES may include a data transformation component to adapt the requests received for its own institution's information system schemes. This component may be implemented using standard technologies such as the XSLT language transforming XML data packages;
- This approach may enable the implementation of a case-by-case processing approach for requests and responses.

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 78. Interoperability framework for international agreements

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

Structure

- The management should commission the ICT unit and institution's delegates in the working committee of the agreement to define an interoperability framework at the international level for the international agreements in coordination with the other participating institutions.
- The management may establish specialized structures to manage interoperable processes in the implementation of international agreements. To establish accountability, the roles and responsibilities must be well defined and documented.
- The interoperability framework for the implementation of international agreements should be based on the institutional interoperability framework recommended in this set of Guidelines, section on interoperability.

Mechanism

- The Responsible Technical Team (RTT) should define an interoperability framework at the international level to implement international social security agreements, covering the following five dimensions:
  - The **political and legal dimensions** of the framework should mainly consist of the international agreement itself as well as other relevant laws and regulations. Additional arrangements may be established wherever necessary to avoid any discrepancy that may jeopardize the application of interoperability in the implementation of the international agreement;
  - The **organizational dimension** should specify the interoperable processes and operations involved in the implementation of international agreements;
  - The **semantic dimension** should be based on metadata that consist of a model of the main business concepts involved in the implementation of international agreements (e.g. data sharing, data exchange, service invocation) and relationships among them, to define a unique meaning for these concepts throughout the institutions to facilitate the automatic treatment of data. As the operations in the implementation of international agreements involve different institutions, the corresponding inter-institutional metadata should be specified;
  - The **technical dimension** should define the technologies to be used for implementing interoperability in order to ensure adequate technical integration of information and systems.
- The management should communicate the scope of the framework throughout the institution.

Guideline 79. 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.

Structure

- The management should commission the institution's delegates in the liaison committee of the agreement, and the ICT unit, to define semantic interoperability resources at the international level for the international agreements, in coordination with the other participating institutions.
- The management may establish specialized structures to manage semantic interoperability resources. To establish accountability, the roles and responsibilities have to be well defined and documented.
- The semantic interoperability strategy for the implementation of international agreements should be based on the institutional model for semantic interoperability recommended in the current set of Guidelines, section on interoperability.

Mechanism

- The Responsible Technical Team (RTT) should define semantic interoperability resources at the international level. This involves:
  - Establishing a development plan of semantic resources for the implementation of international agreements;
  - Developing institutional metadata schema including the main concepts and the relationships between them, and a metadata management system common to all interoperating institutions;
  - Including data quality characteristics in the metadata to enable data consumers to improve the effectiveness of their data use;
  - Using standard languages to specify the metadata (i.e. XML for documents and data objects, DC to define metadata records, OWL to specify semantic relationships between concepts).
- The semantic interoperability may be implemented in the Common Reference Service (CRS), in order to facilitate managing a single copy of this common resource. Alternatively, they may be implemented in the institution's Institutional Exchange System (IES).
- The RTT and the ICT unit should use a maturity model for medium- and long-term strategy on metadata management to improve the quality and effectiveness of the semantic resources for the implementation of international agreements.
- The ICT unit should develop a communications plan to provide appropriate information on the implementation of metadata systems for the implementation of international agreements in areas of social security service within the institution.

Guideline 80. 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.

Structure

- The management should commission the institution's delegates in the liaison committee of the agreement, and the ICT unit, to implement interoperable services at the international level for the international agreements, in coordination with the other participating institutions.
- The management should commission the ICT unit to implement interoperable services at the institutional level.
- The interoperable services should be based on the defined architectures (international, national and institutional).
- The interoperable services for the implementation of international agreements should follow the institutional technical standards on interoperability recommended in the current set of Guidelines, section on interoperability.

Mechanism

- In order to develop interoperable services for the implementation of international agreements, the Responsible Technical Team (RTT) and the ICT unit should:
  - Establish project implementation teams and ICT specialized units to analyse, design and implement the necessary services in the implementation of international agreements;
  - Generate a technical specification including, for each candidate, data exchange operation, the information model of objects and relationships (i.e. the metadata schema), service-oriented characterization (i.e. SOA interfaces) and non-functional requirements (i.e. performance, security, etc.);
  - Design a business processes model for the implementation of international agreements and identify those processes that can be automated by invoking the services developed;
  - Assess the impacts on business within the implementation plan.
- Interoperable services executed in the Common Reference Service may consist of loosely-coupled message exchange, for example using web services.
- Interoperable services executed in the National Exchange System may use, ideally, e-government platforms implemented in the country, or loosely coupled message exchange, for example using web services.

- Interoperable services executed in the Institutional Exchange System to implement system integration within an institution, may consist of message queues using SOA-oriented middleware, for example Enterprise Service Bus, and also web services.
- The ICT unit should establish and implement interoperable services at the institutional level to put into practice interaction with the other institutions.
- The RTT and ICT unit should carry out communications plans to convey the relevant information on the development of services for the implementation of international agreements in the areas of social security in the institutions.

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 81. 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.

Structure

- The management should commission the ICT unit and the institution's delegates in the working committees of the agreement to define, in coordination with the other participating institutions, an authentication framework to be used in the agreement in order to manage the authenticity of the messages exchanged and to prevent repudiations.
- The authentication framework should comply with national and international legislation and should take into account the political and legal context, business processes and concepts involved in authenticating operations.
- The adoption of the authentication framework at the international level should be formalized in the context of the social security agreement, for instance through administrative arrangements.
- The authentication framework should follow the institutional data security framework, as well as the recommendations of the current set of Guidelines, particularly the section on data security and privacy.

Mechanism

- The Responsible Technical Team (RTT), with the assistance of specialized groups, should establish an authentication framework to provide legally valid, efficient and secure means by which to perform the transactions specified in the social security agreement.
- The key principles that underpin the authentication framework are: Transparency, Risk Management, Consistency, Interoperability, Responsiveness and Accountability, Trust and Confidence, Privacy, Choice, Flexibility, and Cost Effectiveness and Convenience.
- The authentication framework should include approaches that maintain a balance between mitigating identity-related risks in transactions and usability, affordability and feasibility of implementation.
- To promote reuse, the authentication framework may be based on mainstream authentication models used in existing agreements as well as on existing authentication credentials already used in the participant institutions.
- The authentication framework should include a standardized criterion for determining the level of security required for a particular electronic transaction.
- The scope of the authentication framework:
    - Covers the types of operations of the agreement that require a signature. There may be operations that do not have this requirement (e.g. consulting local information and the log of transactions may require only an authorized access to the system);

  - Covers staff of institutions who: (i) would perform operations requiring electronic signature; and (ii) would use electronic certificates for authentication into the systems;
  - Provides the way to implement a future trusted electronic environment where social security institutions can transact with each other as well as with other stakeholders.
- Authentication may be implemented following different approaches, particularly:
  - Paired (applicable only for two institutions), where each institution implements and manages its own authentication solutions, including the definition of authorized signatures;
  - With a "trusted third organization" (recommended for multilateral agreements), where institutions participating in the agreement commission a third organization to manage the set of authorized signatures.
- The implementation of the authentication framework requires:
  - Authentication solution components with the capacity to meet the security levels required for transactions;
  - Authentication models implementing the framework in each institution participating in the agreement. This is addressed in the guideline on Implementing e-services;
  - A repository of signatures and the authorization level associated with different types of operation (e.g. make a request, provide personal data of a person, grant a benefit, etc.);
  - Using standards, such as X.509.
- The competent authorities involved in the social security agreement formalize the adoption of the authentication framework for the transactions in the agreement.

Guideline 82. 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.

Structure

- The management should commission the ICT unit to implement an authentication model enabling authentication and digital signature for transactions between institutions participating in the international agreement.
- The authentication model should provide the means to achieve authentication, data integrity, confidentiality, and non-repudiation. It should be based on the authentication framework established for the agreement at the international level.
- The management should establish roles and responsibilities to put into practice the authentication-related functions in the institution.
- The implementation of a model based on digital certificates should include all aspects related to the acquisition, use and management of digital certificates.
- The institutional authentication model should be consistent with the institution's standards on ICT.
- The model for implementing the authentication of transactions should follow the institutional data security framework, as well as the recommendations of the current set of Guidelines, particularly the section on data security and privacy.

Mechanism

- The ICT unit should implement an authentication model based on the authentication framework established for the agreement at the international level as well as on institutional standards.
- The model should enable users to identify, authenticate and sign electronic transactions between institutions participating in the international agreement.
- The implementation of the authentication model includes:
    - Defining the types of electronic transactions to which the model will be applied and the associated security measures (enquiries, information provision or instruction, declarations, statements, financial transactions, etc.);
    - Selecting the appropriate authentication mechanism (e.g. password, biometric authentication, digital certificate) for the different types of transactions;
    - Defining the credential life-cycle management system (issuance, activation, deactivation, etc.) that meets the required security level.

- Obtaining certificates could be based on alternative strategies, such as:
  - Certificates from a private Certificate Authority (CA), free or with payment, such as VeriSign, DigiCert, Entrust, StartCom, etc.;
  - Certificates from a National Public Certificate Authority (CA);
  - Owning and operating a local CA to issue private certificates for users and applications.
- The ICT unit should choose between the use of internal or external certificates based on a number of factors, such as maintenance (time and resources), control of certificates, costs, etc.

Guideline 83. 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.

Structure

- The board and management, with the assistance of the ICT unit, should establish security policies for transactions performed in the social security agreement as well as for digital certificates.
- The board and management should commission the ICT unit to implement data security policies related to transactions and digital certificates.
- The security policies and measures to protect transactions and digital certificates should follow the institutional data security framework, as well as the international standard ISO/IEC 27002:2005 Information technology – Security techniques, and the recommendations of the current set of Guidelines, particularly the section on data security and privacy.

Mechanism

- The ICT unit should implement specific measures of security in access control systems related to transactions and digital certificates:
  - Only authorized staff should be able to access the software application(s) managing the operations implementing the agreement system as well as the related information;
  - Access control may be based on the digital certificates used to sign the exchanges.
- The ICT unit should implement an inventory of certificates, specifying the respective owners.
- The ICT unit should implement specific security measures in database systems, networks and communication systems related to electronic transactions and digital certificates:
  - Database access rights should be granted to business users according to their duties and responsibilities;
  - Networks and communication systems should be configured to use secured protocols, especially for internet-based exchanges (e.g. using HTTPS).
- The ICT department should implement security measures concerning the access and manipulation of digital certificates, as well as physical security measures in the infrastructure involved. The access to these objects should be highly restricted.
- The ICT unit should establish information security policies and protocols to govern interaction between human resources and certificates, emphasizing security prior to, during and following termination of employment. These protocols should apply to all staff: internal, external consultants, contractors and temporary staff.

Guideline 84. 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.

Structure

- The management should commission the ICT and other competent units to implement measures enforcing the applicable data protection regulations on transactions of the international agreement as well as on digital certificates. Such data protection regulations include national regulations as well as conditions established in the agreement.
- It is important to highlight that regulatory frameworks oblige institutions to carry out data governance procedures (e.g. integrity, storage and maintenance, data protection, "right to be forgotten", etc.).
- A common legal framework regarding data protection for the transfer of information between countries could be defined at the international level. The principles may be based on the OECD Privacy Framework and guidelines for trans-border flows of personal data.
- The management should define roles and responsibilities on implementing and managing data protection measures related to transactions and digital certificates.
- The defined data protection policies and measures should follow the institutional data security framework, as well as the recommendations of the current set of Guidelines, particularly the section on data security and privacy.

Mechanism

- The units responsible for enforcing data protection regulations should establish procedures to ensure the appropriate treatment of personal data in transactions of international agreements as well as in managing digital certificates.
- The units responsible for enforcing data protection should implement:
  - Mechanisms for collecting and storing digital certificates in compliance with the applicable data privacy policies and regulations;
  - User access mechanisms to protect personal data in certificates. Such mechanisms should enable users to access their personal data stored in certificates, and should ensure that proper consent is obtained when necessary.
- The unit responsible for data protection should establish:
  - Certificate transfer mechanisms to third parties, compliant with the applicable data protection regulations;
  - Certificate cancellation mechanisms compliant with the applicable data protection regulations.

- The unit responsible for data protection should communicate technical specifications and measures to the unit defining the metadata schema for information to be exchanged, in order to enforce them by design as much as possible.
- The internal audit office should periodically audit and monitor the data protection measures and mechanisms in place.

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 85. 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.

Structure

- The management should commission the institution's delegates in the liaison committee of the agreement to specify the main operational processes of the agreement in coordination with the other participant institutions.
- The operational processes of the agreement should comply with the terms and administrative arrangements of the agreements involved, particularly the data protection conditions.
- Processes may have an international part involving the other parties to the agreement and a national part that specifies operations within the institution and other national institutions.
- The implementation of the operational processes related to the scope of the agreement should be based on the architectures, frameworks and models defined for the agreement at the international, national and institutional levels, as well as on this set of Guidelines.

Mechanism

- The technical committees working at the international level of the agreement should specify the main operational processes of the agreement.
- One of the key processes to be specified concerns the accurate identification of the persons covered by the agreement in the different countries where they have lived:
  - This may be based on personal identifications (IDs) used in each country for social security procedures;
  - These personal IDs may be requested when an operation of the agreement is performed (e.g. claiming a benefit, registering a detached worker, etc.).
- Other frequent processes include the following:
  - Collecting relevant personal data of persons covered by the agreement;
  - Registering a detached worker;
  - Claiming a benefit in the scope of the agreement;
  - Requesting past labour history/records (for pensions);
  - Inquiring about current employee status (for detached workers);
  - Inquiring about rights to receive medical services in a host country;
  - Granting or rejecting a benefit claim.
- Benefit payment or service delivery may be based on existing processes in the institution.

- Processes may consist of two sub-processes:
  - A request sub-process, which corresponds to operations requesting data;
  - A response sub-process, which corresponds to the result of a request.
- The specification should include the input, output, procedure and expected delays, and the roles involved in each process.
- While the international part of the processes has to be jointly defined by all the parties to the agreement, national and institutional parts are specified by each institution. Efficiency may be improved by defining common processes for different agreements.
- All the processes, especially those involving a request to another institution, may generate a record for traceability purposes. The content of these records should comply with the data protection conditions established in the agreement.
- The exchanges involve security controls as follows:
  - Outgoing packages (requests and data) should be electronically signed in order to embed the identification of the staff person issuing the message;
  - Incoming packages should be authenticated by validating their electronic signature.
- These processes should be included in the administrative arrangements associated with the agreement.

Guideline 86. 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.

Structure

- The management should commission the ICT unit and institution's delegates in the working committees of the agreement to specify, in coordination with the other participant institutions, processes related to notifications of changes and to providing relevant information within the scope of the agreement.
- The processes related to notifications of changes and to providing relevant information within the scope of the agreement should comply with the terms and administrative arrangements of the agreement involved, particularly the data protection conditions.
- The implementation of processes concerning notifications of changes and other relevant information within the scope of the agreement should be based on the architectures, frameworks and models defined for the agreement at the international, national and institutional levels, as well as on the current set of Guidelines.

Mechanism

- The technical committees working at the international level of the agreement should specify the main notification processes of the agreement.
- Some of the main types of notification relevant to international social security agreements are:
  - Death of beneficiaries. This notification may be implemented through so-called "deaths data matching", which consists of: (i) an institution of country A sending a list of beneficiaries living in country B; (ii) institutions in country B cross-checking the list with their databases and registries; (iii) institutions in country B notifying the institution of Country A of differences between the list and their databases enabling to identify beneficiaries who have died;
  - Changes in family status of beneficiaries (marriage, divorce, birth of children, etc.).
- Other types of data relevant to international social security agreements are:
  - Pension amounts: exchange of pension of mutual pensioners with a Minimum Supplement or a Residency Supplement to check their right to such a supplement;
  - Other benefits being received in each country, to implement rules preventing undue accumulation of benefits;

- Data related to rights to health benefits (e.g. residence country, etc.);
- General income, for income-dependent benefits;
- Validation of the identification of a person who has been reported as having changed his/her status.

- These processes should be included in the administrative arrangements associated with the agreement.

Guideline 87. 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.

Structure

- The management should commission the ICT unit and institution's delegates in the working committees of the agreement to specify information models related to the data exchanged, in coordination with the other participant institutions.
- The information models should comply with the terms and administrative arrangements of the agreements involved, particularly the data protection conditions and the reciprocity rules for expenses.
- The implementation of the information models related to the data exchanged in the agreement should be based on the architectures, frameworks and models defined for the agreement at the international, national and institutional levels, as well as on the current set of Guidelines.

Mechanism

- The technical committees working at the international level of the agreement should specify the information models covering the main packages of data exchanged.
- Data exchanged usually includes:
  - Personal data;
  - Labour history/records;
  - Declaration of detached workers.
- Data exchanged should have common personal identification (ID) attributes to connect the different exchanged packages as well as to follow up a person's events. These attributes may consist of the personal IDs used in each country for social security procedures.
- Depending on the reciprocity rules for expenses defined in the agreement, the amounts corresponding to individual cases (e.g. administrative fees, medical fees, etc.) could be included in the exchanged data as an input for the application of these rules.
- Traceability data may be specified to keep track of the exchanges. This should include only a transaction identification and the involved institutions but not business and personal data.
- A conceptual representation of the information models should be provided by using standard languages such as UML, as well as through a connection with the metadata and semantic resources (e.g. vocabulary, etc.).
- The metadata should enforce, as much as possible by design, data protection and other relevant regulations.

- The ICT-based implementation of the data exchange should use standard languages such as XML to represent the data packages to be exchanged, as defined in Section B.1, Technical Interoperability, of the current set of Guidelines.
- These information models should be formally supported by the administrative arrangements associated with the agreement.

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 88. 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.

Structure

- The management should commission the ICT unit and the institution's delegates in the working committees of the agreement to define service quality indicators and goals (i.e. SLAs) for the main operations in the agreement, in coordination with the other participant institutions.
- If applicable, the national institutions in the country should establish a corresponding national SLA in order to comply with the service quality indicators defined at the international level.
- The management, with the assistance of the units involved, should establish an internal SLA in order to comply with the SLAs defined at the international and national levels in line with the objectives of the social security agreement.
- The management should establish organizational structures to manage the processes that evaluate and enforce the SLAs of the international agreement. Roles and responsibilities should be well defined and documented.
- The defined SLAs should follow the institutional ICT management and operations processes, as well as those of the section on ICT service delivery.

Mechanism

- The board and management should commission the institution's working groups participating at the international level of the agreement to define service quality indicators and goals (i.e. SLAs) for the main operations. This should be done with the assistance of the ICT unit and in coordination with the other institutions.
- Typically, the SLA may include "business-oriented" indicators, such as the maximum delay in:
  - Responding to an information request;
  - Responding to a benefit request;
  - Paying benefits granted;
  - Notifying deaths and changes in the personal status of beneficiaries.
- The SLA may include "ICT-oriented" indicators on the ICT services required for performing inter-institutional transactions, such as:
  - Availability of the ICT services (e.g. 24 hours/7 days, 24/5, 8/5, etc.);
  - Maximum response time for the ICT services.

- The management should commission business and ICT units to define:
  - An internal SLA based on the international and national SLAs;
  - A set of processes to evaluate and enforce the internal SLA.
- The management should approve, adopt and communicate the SLAs.

Guideline 89. Setting up and managing the ICT operations for international 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.

Structure

- The management should commission the ICT unit to set up and manage the ICT operations of social security agreements as part of the institution's operational processes. This includes analysis and assessment of the economic and technical implications as well as implications related to human resources.
- The management, based on the assessment of the ICT unit, should define roles and responsibilities involving the operation of the ICT systems implementing international agreements.
- The ICT operations practices implemented should follow the institutional ICT management and operations processes, as well as those of Section A.4, ICT Service Delivery, and underlying international practices such as ITIL®.

Mechanism

- The ICT unit should analyse the implications and requirements of operating ICT systems that implement international agreements. Some aspects to take into account are:
  - Interaction with external entities, involving interaction with staff and systems of other institutions;
  - The possibility of 24-hour operations, given the time differences between the countries involved.
- The ICT unit should carry out the ICT operations of international agreements as part of the institution's ICT operations management and service delivery activities. This also includes managing technical support, service desk and request fulfilment, and managing events, incidents and problems.
- Given the interorganizational implications, dedicated ICT staff may be appointed to interact with the international liaison agency and with similar staff in the other institutions.
- The ICT unit should permanently provide information on the SLA internally and to the RTT, establishing an alarm policy to manage any exceptional case that may arise.

C.3. eHealth – ICT Application in Healthcare

In an increasingly digital world, there is growing recognition that information and communication technologies (ICT) must be integrated into the health sector. ICT is inevitable for cost-effectiveness of healthcare services and to improve efficiencies of health systems. Alike the World Health Organization (WHO), this document uses the term 'eHealth' to describe the use of all forms of ICT for health. EHealth has been often described as a means to ensure the provision of the correct health information and services to the right person at the right place and time in a secure, electronic manner to optimize the quality and efficiency of health care delivery, research, education and knowledge. The daily business of health relies on information and communication and, increasingly, on the technologies that enable it, at every level and in every context. The strategic deployment of eHealth can support improving the ability of systems to plan, budget and deliver services, as well as planning and coordinating decentralized health systems. There is an increasing trend in governments' recognition of the importance of eHealth and gradual efforts to develop and adopt national policies, strategies and regulatory frameworks for eHealth. This is consistent with the announcement of WHO that universal health coverage is achievable with the diffusion of eHealth.

The following guidelines address key aspects for developing eHealth capabilities in social security institutions. They take into account the diversity of mandate and services provided in the health and medical areas. While this section focuses on specific eHealth matters, the application of ICT for implementing general social security processes and ICT capabilities are covered by the overall *ISSA Guidelines on Information and Communication Technology*. Given that these guidelines are cross-cutting with other ISSA Guidelines, references are made where deemed relevant and necessary.

These guidelines are primarily intended to provide orientations to the ICT unit on implementing and providing adequate eHealth-enabling tools and services to the business areas. They also aim at providing guidance to the institution's management and business areas on the main eHealth aspects to cover. 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.

Guideline 90. Framework on eHealth: ICT policy, strategy, and regulations for healthcare

The institution establishes a framework on eHealth complying with the national eHealth strategy, policies and legal frameworks as they lay out the vision, objectives, action plan, and monitoring framework of the national system for eHealth. The institution follows the national eHealth regulations in order to adhere to the national elements of governance and standards.

The national legal framework for eHealth includes regulations for the transfer and use of information between healthcare workers and patients, meanwhile addressing issues of privacy and confidentiality, and rules on access and sharing rights.

Structure

- The board, with the assistance of the management, the ICT unit and business areas, should establish an institutional eHealth framework that is consistent with the institution's mission and its governance structures, and is coherent with the national ICT policies, strategy, regulations and legal framework for healthcare.
- The management should commission the ICT and Health Units to develop the eHealth framework comprising a medium term plan for the various application of ICT in healthcare should be prepared taking into account infrastructure and communication services available, and should describe the scope of resulting services and their benefits, as well as the required level of investments.
- The eHealth framework should follow the guidelines for governance and management of ICT and on data decurity and privacy. The guideline on specific data protection and privacy considerations in this section should also be observed.

Mechanism

- The ICT unit and the Health business areas should develop an eHealth framework with endorsement from the board, and communicate this framework throughout the institution with the assistance of the management. The communication could be via a policy statement which establishes the main principles and governance approach of the framework.
- The management, under the directions from the board, should lay out an implementation roadmap with achievable goals, concrete processes and practices. It structures activities over the medium term, while building a foundation for the long term.
- The management should elaborate on duties and responsibilities of specialized units where applicable to ensure the implementation of the roadmap while ensuring accountability and conformance with the governance framework.
- The management should communicate the framework throughout the institution highlighting that it:
    - Follows national eHealth regulations in order to adhere to the national elements of governance and to comply with the national health standards;

- Enables transformation of the institution's vision of ICT application in healthcare into an actionable strategy;
- Allows the system to operate in a way that protects public health, including by preventing development of illicit markets of medicines, medical devices and unauthorized health products and services.

Guideline 91. ICT-based implementation of healthcare services in management and support functions

The institution systematically applies ICT to improve quality of healthcare and efficiency of services for the benefit of the institution and beneficiaries in various institutional processes. This includes but not limited to the use of ICT in healthcare planning, decision making, delivery of patients' services, claim reimbursement, e-prescriptions, e-sickness leave certificates, fraud detection, procurement, stock management and facility performance evaluation.

Structure

- The management, through the institutional strategic plan, should select and communicate the particular services that will deploy eHealth based on the needs of the institution and beneficiaries, and provide fund for rolling out such services.
- The management should commission the ICT and health-related units to prepare and implement specific plans, while it should provide the necessary means for effective implementation of eHealth by signing agreements with infrastructure providers, and purchasing required software and hardware equipment from suppliers.
- The ICT unit should provide technical support for the kick-off, implementation, maintaining and sustaining the services.
- The institution eHealth services delivery should be aligned with Part A of these Guidelines on ICT service delivery as well as with the *ISSA Guidelines on Service Quality*; meanwhile, observing the relevant guidelines of this section.

Mechanism

- The ICT unit and the business areas, particularly those managing health-related services, should define and implement a work-plan for systematically applying ICT in health-related services such that:
  - ICT-based health services are well integrated within the existing ICT systems and mainstream institution's business processes so they are easily accepted and used by staff;
  - ICT-based health services interact with the institution's Master Data for managing the core information;
  - Web and mobile technologies are used to facilitate customers' accessibility and complying with accessibility standards for persons with disabilities;
  - The systems monitor the facility's performance indicators in order to report on current trend and future projections to support decision making.
- The ICT unit should carry out an infrastructure deployment plan in order to ensure the availability of software and hardware required for operating eHealth services.
- The ICT unit should provide the necessary support for electronic management of stock of medical supplies and equipment in order to prevent shortage and ensure continuous supply.

- The management should ensure the necessary human resources are deployed for service delivery, and follow-up on service quality, in accordance with its operational framework.
- The institution should introduce a training system suited to health service users and its professionals in order to ensure that ICT-based services are used efficiently, safely and protectively.

Guideline 92. Electronic health record system

The institution has an electronic real-time, patient-centred records (EHR) that provide immediate and secure information to authorized users, and the EHR system operates within the relevant national policies and legal framework and is well-integrated within other health information systems such as the national EHR system, and with the social security information system.

The EHR is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, diagnoses and treatment, medications, allergies, immunizations, as well as radiology images and laboratory results.

Structure

- The management should adopt a strategy to improve effectiveness, quality and efficiency of healthcare services delivery by utilizing EHR system.
- The management should commission the ICT and health Units the implementation of an EHR system.
- The institution's EHR system should be interoperable with national health records to make a patient's medical history accessible – upon authorization – to health professionals in health care facilities. It also provides relevant linkages to related services; such as pharmacies, laboratories, specialists, and emergency and medical imaging facilities.
- EHR information should be codified and classified in such a way as to ensure interoperability at regional, national and international levels.
- The management should commission the ICT Unit to implement specific data quality assurance and data management measures for the EHR.
- Through the ICT unit, the institution should ensure the service continuity and technical support of EHR system.
- The institution's EHR system should conform to the guidelines of the section Data and Information Management and relevant guidelines of this section namely: on data security and evaluation.
- The EHR system should follow the International Organization for Standardization regarding privacy and security requirements of EHR systems (ISO/TS 14441:2013).

Mechanism

- The ICT and health Units should implement an EHR system as part of its internal system. The EHR should include the patient's health and medical history.
- The EHR system should follow common terminology and clinical coding systems (e.g. SNOMED Clinical Terms, NOMESCO 46 for classification of surgical procedures, ICD-11 International Classification of Diseases).
- The ICT Unit, with the resources made available by the management, should provide the necessary hardware and software for EHR system operation along with the technical support and human resources required.

- The ICT Unit should implement specific data quality assurance measures for the EHR.
- The institution should train designated staff on the use of the EHR system to allow smooth implementation.
- The management should enforce rules that cover all guarantees given to patients for the protection of privacy and safeguarding their digital data.

Guideline 93. eHealth interoperability at institutional, national and international levels

The institution's various electronic health applications are interconnected through standardized interoperability mechanisms with consistent flow of information to ensure complementarity of services and no contradiction or duplication of data. All operates in harmony with the social security information system, disability benefits whenever relevant, and with the national health services and/or national health insurance architecture.

eHealth interoperability covers institutional, national and international system interaction.

Implement proven and established international standards and coding systems from the beginning of any development and deployment. HL7 international standards guide information package, communication from one party to another, setting the language, structure, and data types for seamless integration between systems. DICOM (Digital Imaging and Communications in Medicine) is the international standard to transmit, store, retrieve, print, process, and display medical imaging information. LOINC is the universal standard for identifying health measurements, observations, and documents. SNOMED CT is a systematized nomenclature of clinical terms. These capabilities enable the institution to be integrated within national health services and/or to national health insurance systems.

Structure

- The board and management should establish a policy on adopting health interoperability standards in accordance to national strategies and standards.
- The board and management should establish roles and responsibilities on defining and managing interoperable processes and standards for eHealth involving ICT and health areas.
- The board should formalize the participation of the institution in national health services and/or health insurance systems involving interconnection and data exchange. It should also establish agreements for interoperability and exchange of health data with organizations outside the national systems. Attention should be given to health-related interoperability conditions that are included in the administrative arrangements of international agreements involving health services and medical certifications.
- The interoperability mechanisms should comply with data protection regulations, medical confidentiality regulations and standards as well as data security and privacy standards and institutional measures.
- The institutional eHealth interoperability mechanisms should be based on the institutional interoperability framework recommended in this set of Guidelines, in the sections on Interoperability, on Data Security and Privacy, on Master Data Governance and Master Data Management, on ICT-based Implementation of International Agreements as well as on International Health Interoperability Standards HL7, DICOM, LOINC, and SNOMED CT.

Mechanism

- The ICT unit, together with the related business units, should:
  - Define reference architectures specifying actors (e.g. sub-systems, departments, institutions, etc.), types of data (e.g. EHR, administrative health data, etc.) and the standards used in intra-institution and cross-institution interoperability scenarios;
  - Define approaches (using health interoperability standards) for implementing cross-department and cross-institutional processes involving health data;
  - Establish and manage institutional capacity and implementation plans on relevant international interoperability standards.
- The ICT unit should implement eHealth interoperability mechanisms to support the interconnection of health applications at national and international levels: The implementation of national health services may require:
  - Exchanging personal Electronic Health Records (EHR) with other institutions;
  - Developing gateways and data transformation mechanisms enabling the interoperability between health-related information system and others, notably related to other social security benefits.
- The implementation of national health insurance systems comprise health and administrative social security data and may require interconnecting different types of organizations, such as:
  - Insurance administration;
  - Medical service providers;
  - Social security administrations.
- International data exchange systems involving health-services and medical certificates should be based on using health interoperability standards agreed by the involved parties.
- The implementation of interoperable mechanism with a main master data should be in line with the section on master data governance and master data management.

Guideline 94. The application of mHealth

The institution defines an implementation strategy for mobile ICT applications in order to support its healthcare system and services.

mhealth is the medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants, and other wireless devices. Mhealth has been shown to increase access to health information, services and skills, as well as promote positive changes in health behavior to prevent the onset of acute and chronic diseases. mhealth capitalizes on the use of mobile phone's core utility of voice and short messaging service (SMS) as well as more complex functionalities and applications including general packet radio service (GPRS), third and fourth generation mobile telecommunications (3G and 4G systems), global positioning system (GPS), and Bluetooth technology.

Structure

- The board and management should defines a strategy concerning the adoption of mobile technology with the aim of improving the quality of the institution's service and the effectiveness of its administration.
- The management, with the assistance of the ICT and business units, should establish priorities for mobile-based services of interest to the institution taking into account infrastructure, communication services available to users, and cost.
- The ICT unit should specify institutional technical standards on mobile technologies, and determine duties and responsibilities regarding their application and management.
- The management should conclude the necessary agreements with telecommunication companies for the maintenance of the various forms of identification.
- Communications security should be ensured through measures in the section on data security and privacy.
- The implementation of mHealth applications should be based on the institutional framework for eHealth, on the data protection mechanisms and permanent evaluation practices recommended in this section as well as in the section on mobile technologies.

Mechanism

- The ICT unit and the health-related business areas should develop a workplan, in line with the management strategy for the adoption of mobile technologies for health applications. The plan should include a set of identified services and their advantages to internal and external users.
- The plan takes account of the technological parameters and costs and envisage standards and tools for the comparative assessment of functionality, scalability and comparative value of mHealth solutions.
- The ICT unit should ensure that the design of mobile services takes account of unidirectional, bidirectional and mobile office modalities and the need to integrate them with other services; a combination of these approaches may be considered.

- The ICT unit, with assistance from specialized units, should prepare a training plan for all those involved in the provision and maintenance of the services.
- The management should ensure technical and operational coordination with telecommunications companies within the framework of existing agreements.

Guideline 95. Provision of telehealth – The practice of medicine at a distance

The institution defines a strategy for providing telehealth services in at least one discipline; including but not limited to: teleradiology, teledermatology, telepathology, telepsychiatry, and remote patient monitoring.

Telehealth is an interaction between a health care provider and a patient when the two are separated by distance. Telehealth services are deployed either synchronously or asynchronously in order to exchange information for the diagnosis, follow up, and treatment of diseases and injuries; research and evaluation; and for the continuing education of health professionals.

Structure

- The board and management should establish a strategy concerning the adoption of Telehealth/ telecommunication either synchronously or asynchronously.
- The management, with the assistance of the ICT and business units, should establish priorities of telehealth application of interest to the institution taking into account infrastructure, communication services available to users, and cost.
- The management concludes the necessary agreements with telecommunications companies for the maintenance of the various forms of infrastructure and technology required.
- The ICT unit should specify institutional technical standards on relevant technologies, and determine duties and responsibilities regarding their application and management.
- Communications security should be ensured through measures in the section on data security and privacy, while interoperability standards should be enforced particularly through the DICOM (Digital Imaging and Communications in Medicine) standard whenever relevant.
- The institutional telehealth application complies with other relevant guidelines of this section.

Mechanism

- The management, in collaboration with the ICT and health units, should develop and communicate a plan for incorporating telehealth within the institution while identifying set of applications with their advantages to internal and external users. They should take account of the technological parameters and costs.
- The ICT unit in collaboration with the health unit should carry out an implementation plan for the Telehealth services and the required products and infrastructure.
- The ICT unit, with assistance from specialized units, should prepare a training plan for all staff involved in the utilisation and maintenance of telehealth application.
- The ICT unit should provide the technical support to telehealth application and frequent trainings to users whenever needed.
- The management should ensure technical and operational coordination with telecommunications companies within the framework of existing agreements.

Guideline 96. The use of social media to communicate on health related matters

The institution uses social media to improve dissemination of knowledge to and from the health workforce in order to: promote health education messages, raise awareness, ensure equal access to workplace health promotion messages; disseminate information in case of health emergencies; run community-based health campaigns; generate interactive platforms to share and discuss health related issues and concerns; and to receive feedback.

Structure

- The board and management should adopt the strategic use of social media in communicating with the public for the purpose of health education and dissemination of information as well as seeking feedback on services. This adoption should include a thorough analysis of opportunities, risks, challenges, and mitigating measures.
- The management to identify certain social media platforms to be utilised by the institution with policies to carry out the objectives of this utilization and observe the best interest of the institution and beneficiaries.
- The institution's deployment of social media should be in accordance with the *ISSA Guidelines on Communication by Social Security Administrations,* in the sections on communication unit and on external communication.
- The institution's deployment of social media should conform with relevant guidelines in this section.

Mechanism

- The management, in collaboration with the ICT and health units, should develop and communicate a plan for the use of social media in communicating with beneficiaries with an assigned set of responsibilities to the ICT unit and administrators of the social media platforms to be used.
- A set of guiding rules is put in place, with the support of the legal unit, for the proper use of social media to ensure the best interest of the institution and prevent any perceived harmful, incorrect, misleading, or inappropriate communication to the public; similarly to screen and reject any communication that is perceived as inappropriate or entails potential harm.

Guideline 97. Potential uses of emerging technology, big data and new data sources

The institution develops appropriate technical capacities as well as robust governance structure and regulations enabling an effective and safe use of emerging technology in healthcare, and in particular data generated by the various applications of ICT and personal devices in health services. This governance structure follows the national policy or strategy regulating the use of big data in the health sector.

The recent development of ICT applications in healthcare services shows concurrent advances of new personal devices commonly known as internet of things (IoT), and medical devices and application that are connected to the healthcare IT system known as internet of medical things (IoMT). All have high potential and are new data sources of an unprecedented scale and velocity. Big data analysis is to identify priorities and policies to improve health care, develop preventive strategies, support decision making and planning strategies. In turn, based on big data, artificial intelligence mechanisms enable to automate procedures.

Structure

- The management commissions the ICT Unit and the health management to establish a work-plan of initiatives for applying emerging technology such as IoT, IoMT, and personal devices to improve health services as well as for building the required institutional capacity.
- The management to develop a governance framework around the development of statistics and research for evidence-based decision making. This is to ensure that the data are not misused and that individuals' privacy remains protected throughout the process.
- The institutional use of big-data should follow the International Organization for Standardization (ISO) regarding security of electronic health records communications (ISO/TS 13606-4:2009) and the ISO regarding data protection to facilitate trans-border flows of personal health data (ISO 22857:2011).
- The institutional use of big-data should conform with the section in this set of Guidelines on data security and privacy as well as the relevant guidelines in this section.

Mechanism

- The management, in collaboration with the ICT and health-related units, should identify initiatives for applying tools of new technologies such as big data, analytics, artificial intelligence, IoT, IoMT, and personal devices to improve health services that may include preventive measures and home monitoring for long-term care.
- The management should encourage the use of personal devices and IoMT to serve the institution's vision and establish partnerships with telecommunication providers for this purpose.
- The management should establish capacity building activities for ICT and health staff besides generating new staff profiles such as health data analysts, etc.

- With the support of the legal unit, the institution should conform to data de-identification standards and data sharing agreements and contracts in order to bind data recipients to follow data protection requirements.
- The ICT Unit together with the health-related units should ensure adherence to standards in health data and technology in order to achieve a secure, timely and accurate exchange of data for health decision-making.
- The management should establish support systems for patients to register complaints, and delegate the legal unit to pursue criminal penalties and/or fines for data misuse.

Guideline 98. Specific data protection and privacy considerations

The institution implements eHealth complying with specific data protection regulations and setting-up strict data protection mechanisms given the highly private and sensitive nature of personal health data and the pertaining medical confidentiality. The institution implement healthcare data security solutions that will protect important assets while also satisfying healthcare compliance mandates.

The electronic collection, storage, processing and transmission of personal health data, and medical information adhere to the highest standards of data protection that completely safeguards confidentiality of medical and administrative records.

Structure

- The board and the management adopt policy on health related data privacy, security and observation of medical confidentiality with zero tolerance to breaches.
- ICT-based health systems should comply with national regulations as well as with the terms established by international agreements involving cross-borders health data exchange.
- The management should invest in appropriate safeguards and security measures to enforce data privacy and security policies.
- The ICT unit should ensure secure online management of health data and secure data access centres and remote systems.
- The management, with the assistance of specialized units, should organize security audits so as to guarantee compliance with policies on the protection of personal health data, and medical records.
- The management to communicate a consent management policy based on the national health regulation for the utilisation and sharing of data.
- The institution should conform to the sections on data and information management and on data security and privacy in this set of Guidelines. Similarly, the International Organization for Standardization regarding security of electronic health records communications (ISO/TS 13606-4:2009) should be observed as well as the national standards of medical record confidentiality.

Mechanism

- The ICT unit, in collaboration with health business areas, should implement appropriate security and data protection measures as a precondition to the deployment of eHealth systems, in particular:
    - Authentication of users and securing access to corporate networks, protecting the identities of users, and ensuring that a user is who he claims to be;
    - Data encryption preventing unauthorized access of sensitive data. The encryption scheme should be efficient and easy to use;

- Data masking for data anonymization, replacing sensitive data elements with an unidentifiable value so the original value cannot be returned from the masked value;
- An access control policy for users utilising the information system, in particular based on the privilege and right of each practitioner authorized by patient or a trusted third party.

- The management should establish an active regulation to seek a patient's consent for collecting, processing, or sharing health related information that guarantee the requirements of protection and medical confidentiality as well as the necessary practicability and flexibility of the system.

Guideline 99. Permanent evaluation of ICT health applications and services

The institution implements permanent evaluation and improvement mechanisms of ICT health applications and services in order to estimate whether they generate the expected results and if they match the institution's objectives while achieving return on investments, thus determining relevant adjustments when deemed necessary.

In order to achieve continuous improvement, permanent and systematic evaluation should be based on performance indicators and service quality evaluation involving the main stakeholders and the public. Using a standard model increases the institution's ability to compare its performance against institutions in other countries with similar ICT-based health applications as well as the same applications' performance over time.

Structure

- The management designs and implements a permanent evaluation mechanism aligned with the institutional strategies that enables the institution to track and assess the results of implementing the eHealth services and applications.
- The institution should follow the section of these Guidelines on ICT investment and value management as well as the section of the *ISSA Guidelines on Service Quality* on continuous improvement.

Mechanism

- Management should assign responsibilities and accountability (who), and should determine the approach (how) and timing (when) for measuring the results and the proper reporting mechanism to the management.
- Those responsible for evaluation should solicit users and staff feedback to identify problem areas for further investigation and explore potential solutions.
- Those responsible for evaluation should deliver regular reports on performance results and service quality evaluation to the management with recommendations of improvement.
- The health unit should define performance and service quality indicators that provide insight into the adoption of eHealth and the tangible results for health and non-health stakeholders.
- Identifying indicators' baselines and target measures to allow monitoring and evaluation of progress over the duration of implementation.
- Indicators should be aligned with the institutional performance system and contribute to calculating global indicators.

C.4. Implementation of Social Security Business Processes

Generally speaking, business processes describe end-to-end processing paths including tasks and information flows. Often crossing departmental and even organizational boundaries, business processes usually starts with a customer request/need and ends with an outcome for the customer and the organization. In turn, a Business Process Model specifies several related business processes and defines the ways in which operations are carried out to accomplish the intended organizational objectives.

A process-based approach in social security administration relies on best practices to provide a common way of describing the activities of a social security institution. The overall management of social security business processes involves its business areas, notably: registration, contribution collection, accounting and finance, payment, appeals and complaints management, planning and evaluation areas, and cash benefits administration for pensions, sickness, health insurance, unemployment, maternity, and family benefits.

This section addresses these issues and provides recommendations on implementing a process-based approach in social security institutions. The key advantage of this approach is that it allows for the identification of business process similarities across various programmes which allows for economies of scale in the development and maintenance of systems as well as simplifying operations both for the user/customer and for the staff responsible for the various functions through standardization.

The core operational business processes are:

- Registration of all categories of contributors and beneficiaries.
- Contribution collection for all categories of contributors, which includes collecting declarations/payroll, collection of contributions and apportionment of contributions/premiums.
- Management of cash benefits:
  - Receiving benefit applications for all the schemes;
  - Control and adjudication, including eligibility and other controls as well as decisions on entitlement and computation of payment amounts.
- Payment of cash benefits.
- Managing appeals, complaints and redress.
- Permanent evaluation of the operational processes by computing key performance indicators.

The main goals of this section are to:

- Provide recommendations on implementing core social security business processes taking into account schemes' specificities and, at the same time, preventing fragmented implementations by promoting common processes when it corresponds.
- Promote a standardized business process framework for the ICT developments as well as for other functions (e.g. service delivery) enabling to address schemes' and business requirements.
- Promote good practices on the design and implementation of social security processes in particular for strengthening security and data quality assurance mechanisms.

The section takes into account specificities of the targeted core processes in the different social security schemes and programmes, which are grouped as follows:

- Short term income replacement benefits providing an income replacement for a limited time period during which the insured person is not able to work due to sickness, maternity and unemployment.
- Long-term benefits payable for life or for a considerable number of years, such as: old-age, disability and survivors pensions.
- Hybrid benefits such as family allowances and health insurance. The former provides additional income for families with young children, often with conditionality such as means-testing and/or school attendance and receiving medical care. The latter covers health services to workers and their dependants. The benefits may consist of covering beneficiaries' enrolment to medical services provided by external health and/or, reimbursement-based cash benefit for medical expenses incurred.

The Table C.4.1 summarizes the business process considered in this section as well as the ICT-implementation approach.

These guidelines are primarily intended to provide orientations to the ICT unit on implementing software systems responding to requirements of business areas. They also aim at providing guidance to the institution's management and business areas on the main social security business processes.

In addition, these guidelines may mean that technical development and operational teams will have to adapt their skills, and they will help identify new skills requirements.

Table C4.1. *Schemes and business processes*

<table>
<tr><th colspan="2" rowspan="2">Business processes</th><th colspan="7">Schemes</th></tr>
<tr><th colspan="2">Long-term benefits</th><th>Hybrid benefits</th><th>Health insurance</th><th>Short-term benefits for income replacement</th><th>Unemployment</th><th>Maternity</th></tr>
<tr><th colspan="2"></th><th>Pensions</th><th>Disability</th><th>Family</th><th></th><th>Sickness</th><th></th><th></th></tr>
<tr><td colspan="2">Registration</td><td colspan="7">Common implementation in all schemes</td></tr>
<tr><td colspan="2">Contribution collection</td><td colspan="7">Common implementation in all schemes</td></tr>
<tr><td rowspan="4">Benefit Management</td><td>Applications receipt</td><td colspan="7">Common implementation in all schemes with potentially automatic activation based on life events known by the institution</td></tr>
<tr><td rowspan="3">Eligibility and other controls</td><td colspan="7">Main common controls: Enrolment, worked periods, compliance with contributions, proof of life</td></tr>
<tr><td colspan="2">Cessation of work due to age or contingency</td><td rowspan="2">Child birth
Family status
Conditionalities: schooling vaccination</td><td rowspan="2">Proof of expenses if based on reimbursement</td><td colspan="3">Cessation of work due to contingency</td></tr>
<tr><td>Worked periods</td><td>Medical certificate (proof of disability)</td><td>Medical certificate (proof of sickness)</td><td>Compliance with unemployment regulations</td><td>Medical certificate</td></tr>
<tr><td>Adjudication</td><td colspan="2">Based on working history and salary.</td><td>Base benefit amount
Family status Household income</td><td>Proof of expenses for reimbursement</td><td colspan="3">Based on current salary</td></tr>
<tr><td colspan="2">Payment</td><td colspan="7">Common implementation in all schemes</td></tr>
<tr><td colspan="2">Appeals and Complaints</td><td colspan="7">Common implementation in all schemes</td></tr>
<tr><td colspan="2">Process and programme evaluation</td><td colspan="7">Common implementation in all schemes</td></tr>
</table>

Guideline 100. Institutional business process model for social security processes covering different schemes

The institution specifies a business process model for the main social security processes covering the schemes in the institution's mandate.

Structure

- The management should commission the ICT and other competent units to define and implement a business process model for the main social security processes covering the schemes in the institution's mandate.
- The management should define roles and responsibilities on specifying and implementing social security business processes, in particular involving the ICT unit and business areas.
- The business process model should be aligned with institutional strategies on social service delivery and it should follow the practices recommended in this current set of Guidelines, particularly on ICT governance and strategy.

Mechanism

- The ICT unit and the business areas should specify a business process model covering core business processes according to the institution's mandate, notably: registration, contribution collection, receiving benefit applications, performing eligibility and other controls, calculations and adjudication, payment, appeals and complains management:
  - The model should take into account and may include other relevant processes for the institution, such as: compliance enforcement and fraud detection, administration of non-cash benefits, accounting processes, budget management and planning, etc.;
  - Processes specifications should include information flows between each other and in with the Master and Reference Data.
- The implementation of the business processes should:
  - Lead to an integrated software and prevent system fragmentation and siloes while taking into account scheme specificities;
  - Improve effectiveness and efficiency through automation;
  - Where legislation allows, put into practice the "ask-once" policy for interacting with users by using data in the institution's information systems and already provided evidences;
  - Include security controls and preventive measures to minimize error, evasion and fraud, notably using institutions' data, pre-filling declarations and performing early validations;
  - Performing rigorous data quality controls aligned with preventive measures to foster the quality of master data as well as to ensure the adequate delivery of benefits.
- The following design and security features should be taken into account in the implementation of the business processes:
  - The front-end should be implemented as e-services (e.g. my-socialsecurity) with robust security measures for authentication and access control;

  - To improve flexibility and evolutivity, systems should be based on a Service Oriented Architecture (SOA) including specific software components by scheme and calculation formulas should be parametric according to schemes, types of benefits and contribution categories.
- The management should permanently improve the model and the involved processes.
- The board, with the assistance of the management, should validate and communicate the business process model throughout the institution.

Guideline 101. Registration as a common process to all schemes

The institution implements registration as a common process to all the schemes in the institution's mandate with variants and specialized channels for different population groups and employers.

Structure

- The management should commission the ICT and other competent units to implement the registration process based on the institutional business process model:
  - It should be a common process to all the schemes with specialized channels for the different population groups and employers;
  - The main goals are to facilitate the registration of all individuals and entities related to social security services and to cover their relevant life events.
- The registration process may have to interact with other institution's processes and external entities, notably civil registries, social and labour registries.
- The registration process should enforce data protection regulations in particular concerning the management of sensitive personal data.
- The implementation should be aligned with social security coverage strategies and follow recommendations in the *ISSA Guidelines on Service Quality* and the *ISSA Guidelines on Communication by Social Security Administrations.* It should also follow the guidelines in the current set, particularly on data quality, data security and privacy, master data, interoperability, and mobile technologies.

Mechanism

- The ICT unit and the business areas should implement the registration process as a common system to all the schemes comprising the main registration tasks (i.e. first time registration, record update and deletion) and with the following features:
  - Follow a multi-channel approach providing user interfaces tailored to different customer groups. It includes middleware mechanisms for interacting with external systems;
  - Include software specialized components for registration scenarios, such us registering: (i) employers, (ii) employees including their employer as well as dependants and family links, (iii) self-employed workers, and (iv) beneficiaries of social assistance and non-contributory programmes.
- The registration process should interact with the Master and Reference Data related to employers and to employees as well as to beneficiaries.
- An e-services implementation for the registration (i.e. e-registration) should comprise secured self-services functionalities with a robust authentication mechanism enabling:
  - All customers to update and validate their records where appropriate;
  - Employers to manage employees' registration.

- The ICT Unit should take into account the design, security and performance considerations previously described in the guideline concerning the design of an institutional business process model.

Guideline 102. Contribution collection as a common process to all schemes

The institution implements contribution collection as a common process to all schemes in the institution's mandate but with approaches specialized on different types of persons and enterprises.

Structure

- The management should commission the ICT and other competent units to implement the contribution collection process based on the institutional business process model:
  - It should be a common process to all the schemes with specialized channels for the different types of contributors (i.e. employers, employees, self-employed);
  - The main goals are: fostering voluntary compliance by facilitating the contribution payment and aiming at overcoming barriers for difficult-to-cover groups as well as maximizing efficiency through electronic submissions and automatic processing.
- The contribution collection process may have to interact with other institution's processes and external entities, notably: the institution's accounting and benefit management systems, other agencies' contribution collection processes, and external partners involved in collecting payments (e.g. banks, telecommunication companies for mobile payment, small shops and post offices supporting decentralized presence-based contributions payments, and organizations contracted by government to deliver aspects of social security).
- The contribution collection process should enforce data protection regulations in particular concerning the management of personal, sensitive and protected data (e.g. salary, etc.).
- The implementation should be based on the business processes established in the *ISSA Guidelines on Contribution Collection and Compliance* and aligned with institution's compliance strategies in particular for difficult to cover groups as established in the *ISSA Guidelines on Administrative Solutions for Coverage Extension*. It should also follow the guidelines in the current set, particularly on data quality, data security and privacy, master data, interoperability, and mobile technologies.

Mechanism

- The ICT unit and the business areas should implement the contribution collection process as a common system to all the schemes comprising the main contribution collection sub-processes with the following features:
  - Follow a multi-channel approach providing user interfaces tailored to the different types of contributors, particularly differentiating employers from self-employed. It includes middleware mechanisms to interact with external systems notably employers' and payment partners';
  - Include processing variants according to contribution periodicity as well as to the type of contributor, notably employers paying contributions on behalf of employees, and self-employed workers.

- The contribution collection process should interact with Master and Reference Data on Contribution bases and employees' salaries and income declarations.
- An e-services implementation should comprise self-services functionalities enabling the submission and follow-up of social security contributions digitally signed and enabling the legal authentication of the submitted documents.
- The ICT unit should take into account the design, security and performance considerations previously described in this section as well as the following ones:
  - Enable contributors to perform electronic submissions using a predefined data format and pre-filled with the institution's data;
  - Perform validations and contribution calculations through potentially asynchronous back-end process to manage peaks of submissions;
  - Perform an account reconciliation and activate contributors' rights for the related benefits after receiving the corresponding payment.

Guideline 103. Receiving benefit applications through a common process

The institution implements the receiving benefit applications process, differentiating according to different types of benefits.

Structure

- The management should commission the ICT and other competent units to implement the receiving of benefit applications process based on the institutional business process model:
  - It should differentiate according to different types of benefits taking into account the urgency for receiving the benefit especially in for short-term income replacement (sickness, maternity, and unemployment);
  - The main goals are: facilitating the submission of benefit applications by a wide diversity of beneficiaries as well as nominees or trustees acting on behalf of a social security applicant, facilitating access to persons with disabilities and from vulnerable groups, performing preventive controls, and anticipating new operations and appointments such as medical controls.
- The reception of benefit applications should enforce data protection regulations in particular concerning the management of sensitive personal data.
- The process may have to interact with other institution's processes and external entities, notably: Registration, medical services and operations traceability.
- The implementation should follow recommendations in the *ISSA Guidelines on Service Quality* and in the *ISSA Guidelines on Communication by Social Security Administrations*. It should also follow the practices recommended in this current set of Guidelines, particularly on data quality, data security and privacy, master data, interoperability, and mobile technologies.

Mechanism

- The ICT unit and the business areas should implement the receiving benefit applications process as a common system to all the schemes comprising the main benefit applications tasks with differentiated software components for different types of benefits and with the following features:
  - Follow a multi-channel approach providing user interfaces tailored for interacting with different applicant groups, in particular with vulnerable and difficult to reach groups;
  - Perform systematic controls of all the required evidences using, wherever possible, available institution's data.
- An e-services implementation should comprise self-services functionalities enabling the submission and follow-up of a benefit application as well as the attached documentation. The submitted documentation may be digitally signed and enable a legal authentication. Benefit applications should be pre-filled with the institution's data and existing required documentation should be automatically attached.

- The process should interact with the Master and Reference Data on employees as well as their beneficiaries.
- The ICT Unit should take into account the design, security and performance considerations previously described in the guideline concerning the design an institutional business process model.

Guideline 104. Control and adjudication of long-term benefits

The institution implements the control and adjudication process of long-term benefits including the processing of provisional pensions, new effective pensions, and the revision of pensions. If the institution manages other schemes, these processes would be part of a common process comprising the other benefits processing.

Long-term benefits include pensions for old-age, disability and survivors.

Structure

- The management should commission the ICT unit and other competent units to implement the control and adjudication process for long-term benefits based on the institutional business process model:
  - It should include the eligibility and other controls as well as ensure the accuracy of benefits calculation;
  - The main goals are: implementing the programme , performing rigorous eligibility controls, accurately computing benefits' amounts based on the parameters and adjudication rules, and efficiently generating payment orders.
- The process should enforce data protection regulations in particular concerning the management of sensitive personal data.
- The control and adjudication of long-term benefits may have to interact with other processes and external entities, notably: medical services and operations traceability.
- The implementation should be aligned with institutional compliance and with service delivery strategies as recommended in the *ISSA Guidelines on Service Quality* and in the *ISSA Guidelines on Communication by Social Security Administrations,* in particular with difficult-to-cover groups. It should also follow the guidelines in the current set, particularly on data quality, data security and privacy, master data, interoperability, and mobile technologies.

Mechanism

- The ICT unit and the business areas should implement the Control and adjudication process for long-term benefits as a system with specific software components for the control and calculation functions and with the following features:
  - High flexibility by managing parametric formulas and the history of versions of conditions and calculation rules for legacy purposes;
  - Manage insured's' medical files for disability benefits;
  - Take into account changes in the pension status (i.e. ongoing, stopped, and suspended);
  - Combine rules and a service-oriented architecture (SOA).
- The calculation function should include:
  - The main parameters for pension calculation: age, person's salaries, general salary base calculation base, arrears and regularisations;
  - Formulae and calculation rules for the different variants as well as for the increases.

- The control and adjudication process should interact with the Master and Reference data related to insured persons, worked periods and salaries, medical records for disability pensions, and living status.
- The ICT Unit should take into account the design, security and performance considerations previously described in the guideline concerning the design of an institutional business process model.

Guideline 105. Control and adjudication of hybrid benefits

The institution implements the control and adjudication process of hybrid benefits, which include family benefits and health insurance.

If the institution manages other schemes, these processes would be part of a common process comprising the other benefits processing.

Structure

- The management should commission the ICT and other competent units to implement the Control and adjudication process of hybrid benefits based on the institutional business process model:
  - It should include the eligibility and other controls as well as ensure the accuracy of benefits calculation;
  - The main goals are: implementing the programme , performing rigorous eligibility controls, accurately computing benefits' amounts based on the parameters and adjudication rules, and efficiently generating payment orders.
- The control and adjudication process should enforce data protection regulations in particular concerning the management of sensitive personal data.
- The process may have to interact with other processes and external entities, notably: operations traceability, education and medical services.
- The implementation should be aligned with institutional compliance and with service delivery strategies as recommended in the *ISSA Guidelines on Service Quality* and in the *ISSA Guidelines on Communication by Social Security Administrations*, in particular with regard to difficult-to-cover groups. It should also follow the practices recommended in this current set of Guidelines, particularly on data security and privacy, master data, interoperability, and mobile technologies.

Mechanism

- The ICT unit and the business areas should implement the Control and adjudication process for hybrid benefits as a system with specific software components for the control and calculation functions and with the following features:
  - High flexibility by managing parametric formulas and the history of versions of conditions and calculation rules for legacy purposes;
  - Manage insured's' medical files concerning benefits' conditionalities and disability conditions;
  - Take into account changes in the benefit status (i.e. ongoing, stopped, and suspended);
  - Combine rules and a service-oriented architecture (SOA).
- The calculation function should include the formula and calculation rules for the different variants as well as for the increases taking into account household composition and income data.

- The control and adjudication processes should interact with Master and Reference data related to insured persons, salaries and income declarations, medical records and medical control assessment, and school and education records.
- The ICT unit should take into account the design, security and performance considerations previously described in the guideline concerning the design of an institutional business process model.

Guideline 106. Control and adjudication of short-term benefits

The institution implements the control and adjudication process of short-term benefits for income replacement. Short-term benefits for income replacement include maternity, sickness and unemployment cash benefits.

If the institution manages other schemes, these processes would be part of a common process comprising the other benefits processing.

Structure

- The management should commission the ICT and other competent units to implement the control and adjudication process for short-term benefits for income replacement based on the institutional business process model:
  - It should include the eligibility and other controls as well as ensure the accuracy of benefits calculation;
  - The main goals are: implementing the programme , performing rigorous eligibility controls, accurately computing benefits' amounts based on the parameters and adjudication rules, and efficiently generating payment orders.
- The benefits control and adjudication process should enforce data protection regulations in particular concerning the management of sensitive personal data.
- The process may have to interact with other processes and external entities, notably: medical services, unemployment and operations traceability.
- The implementation should be aligned with institutional compliance and with service delivery strategies as recommended in the *ISSA Guidelines on Service Quality* and in the *ISSA Guidelines on Communication by Social Security Administrations*, in particular with regard to difficult-to-cover groups. It should also follow the practices recommended in this current set of Guidelines, particularly on data security and privacy, master data, interoperability, and mobile technologies.

Mechanism

- The ICT unit and the business areas should implement the control and adjudication process short-term benefits for income replacement as a system with specific software components for the control and calculation functions and with the following features:
  - High flexibility by managing parametric formulas and the history of versions of conditions and calculation rules for legacy purposes;
  - Take into account changes in the benefit status (i.e. ongoing, stopped, and suspended);
  - Combine rules and a service-oriented architecture (SOA).
- The calculation function should include:
  - The main parameters for the benefit amount calculation: type of benefit, economic sector, worked periods, household data, arrears and regularisations;
  - Formulae and calculation rules for the different variants as well as for the increases.

- The control and adjudication processes should interact with the Master and Reference data related to insured persons, salaries and income declarations, medical records and medical control assessments, employment status, periods previously declared.
- The ICT unit should take into account the design, security and performance considerations previously described in the guideline concerning the design of an institutional business process model.

Guideline 107. Payment as a common process to all the schemes

The institution implements the payment of benefits as a common process to all the schemes in the institution's mandate with specific delivery methods according to payment periodicity and to types of beneficiaries in order to overcome barriers and difficulties to reach population groups.

Structure

- The management should commission the ICT and other competent units to implement the payment of benefits process as a common process based on the institutional business process model:
  - It should be a common process to all schemes with delivery methods specialized on the different population groups;
  - The main goal is facilitating the payment of all types of benefits to all categories of beneficiaries through specialized and targeted service delivery methods tailored to different population groups as well as different payment periodicities.
- The payment process may have to interact with other institution's processes and external entities, such as: the institution's benefit payment records, accounting system, insured persons payment accounts, traceability system, banks, shops other public services, and telecommunication companies providing mobile services.
- The payment process should enforce data protection regulations in particular concerning the management of personal and payment data.
- The implementation should recommendations in the *ISSA Guidelines on Administrative Solutions for Coverage Extension, ISSA Guidelines on Service Quality* and *ISSA Guidelines on Communication by Social Security Administrations*. It should also follow the practices recommended in this current set of Guidelines, particularly ondata security and privacy, master data, interoperability, and mobile technologies.

Mechanism

- The ICT unit and the business areas should implement the payment of benefits process such that:
  - It consists of a common system to all the schemes comprising the main payment tasks with parametric formulas and software components for the specific processing, notably the differential periodicity;
  - It includes validations of conditions which may lead to stopping payments (e.g. death, changing family status, changing income level, etc.);
  - It includes traceability functions, especially for payments made by external partners;
  - It combines rules, event-based activation of payments, and service-oriented architecture (SOA)-based interaction with other subsystems.

- The implementation of the payment of benefits process should support diversified delivery methods adapted to different population groups and potentially involving external partners, notably:
  - Bank transfer involving banks;
  - Pre-paid cards involving financial and card administrators;
  - Mobile money involving telecommunication companies;
  - Decentralized presence-based payment delivery through partners' networks (e.g. small shops, post offices, etc.).
- The process should interact with Master and Reference data related to beneficiaries and insured persons.
- The ICT unit should take into account the design, security and performance considerations previously described in the guideline concerning the design of an institutional business process model.

Guideline 108. Appeals and complaints management as a common process to all schemes with specialized approaches for different types of users

The institution implements the appeals and complaints management process as a common process to schemes in the institution's mandate with approaches specialized on the different types of users, in particular contributors and beneficiaries.

Structure

- The management should commission the ICT unit and other competent units to implement the appeals and complaints management process based on the institutional business process model:
  - It should be a common process to all the schemes with variants and specialized channels for different population groups and employers;
  - The main goals are: facilitating the collection and processing of appeals and complaints for all branches and institution's services involving all type of persons and employers and improve the efficiency, effectiveness and accuracy especially if involves re-processing a case.
- The appeals and complaints management process may have to interact with other institution's processes and external entities, notably benefit transactions, traceability system, external partners providing payment collection and delivery.
- The implementation should follow recommendations in the *ISSA Guidelines on Service Quality* and *ISSA Guidelines on Communication by Social Security Administrations*. It should also follow the practices recommended in this current set of Guidelines, particularly on data security and privacy, master data, interoperability, and mobile technologies.

Mechanism

- The ICT unit and the business areas should implement the appeals and complaints management process such that:
  - It consists of a common system to all the schemes comprising the main appeals and complaints management process tasks to avoid system fragmentation;
  - Follows a multi-channel approach providing user interfaces tailored for interacting with different population groups;
  - Manages different types of appeals and complaints, in particular related to the quality of services, rights to a benefit, application case and delay, medical control and assessment, and benefit amount.
- To be adaptable to different operational scenarios, the appeals and complaints management process should comprise all files on complaints and the history of interactions with the institution.

- An e-services implementation should comprise self-service functionalities enabling the submission and follow-up of complains.
- The process should interact with the Master and Reference data related to insured persons.
- The ICT unit should take into account the design, security and performance considerations previously described in the guideline concerning the design of an institutional business process model.

Guideline 109. Permanent evaluation through a connection between business processes and key performance indicators

The institution designs and implements permanent evaluation mechanisms for the main social security functions and processes through a connection between business processes and key performance indicators (KPI).

Structure

- The management should establish a quality evaluation and permanent improvement model for the social security business processes based on key performance indicators indicators (KPI), which can be quantitative and qualitative. A standard model should be used in order to facilitate the implementation and to increase the institution's ability to compare its operational performance against other institutions.
- The management should commission the ICT unit and other competent units to implement permanent evaluation mechanisms for the social security business processes. In particular, systems implementing the business processes should generate data to compute key performance indicators.
- Indicators should be aligned with the institutional performance system and contribute to calculate different type of indicators, such as production indicators, quality indicators, internal control indicators, indicators by branch, and related to social outcomes.
- The implementation should follow the institution's strategic plan, established goals and evaluation frameworks (e.g. balanced scorecard) as recommended in the *ISSA Guidelines on Good Governance* as well as on the continuous improvement principles recommended in the *ISSA Guidelines on Service Quality*. It should also follow the practices recommended in this current set of Guidelines, particularly on ICT investment and value management, data management, and on interoperability.

Mechanism

- The management should establish permanent evaluation mechanisms including the identification of indicators' baselines and target measures to allow monitoring and evaluation of progress over the duration of implementation.
- To measure processes' operations through key performance indicators, the ICT unit and the business areas should implement connections between the business processes and information systems computing performance indicators (e.g. balanced scorecard system). These connections should not undermine the performance and quality of services to be provided by the operational processes.
- The management may use the evaluation to assess the performance of external partners as well as the fulfilment of contracts and service level 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.

This revised version was prepared by Dalya Elziniy, Jamal Chentouf, Sven Hutse and Raúl Ruggia Frick with the support from the ISSA Technical Commission on Information and Communication Technology chaired by Gloria Redondo Rincon. Review, commentary and other inputs were generously provided by ISSA member institutions.

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**