NATIONAL INFORMATION TECHNOLOGY AUTHORITY-DIRECTORATE OF PLANNING RESEARCH AND DEVELOPMENT – STANDARDS CATALOGUE

June 2017

DISCLAIMER

Whereas NITA-U has employed all reasonable means and care in the creation of this document, this document is provided to the reader as is without any warranty (express or implied) as to accuracy or completeness and NITA-U cannot be held liable for any errors or omissions in this document, nor any losses, damages or expenses arising consequent to the use of this document by the reader.

CHANGE HISTORY

Document Control

Level	Name	Signature	Date

Version Control

Issue Date	Version	Summary of Changes
21/09/2015	0.1	Initial Draft
16/12/2016	0.2	Second Draft
30/06/2017	0.3	Final

Circulation List

Role	Name

TABLE OF CONTENTS

NATIONAL FOREWORD

National Information Technology Authority, Uganda (NITA-U) is a parastatal organization under the Ministry of Information Communication Technology established under Act 4 of 2009 of the laws of Uganda. NITA-U is mandated to:

a) provide high quality information technology services to government;
b) promote standardization in the planning, acquisition, implementation, delivery, support and maintenance of information technology equipment and services, to ensure uniformity in quality, adequacy and reliability of information technology usage throughout Uganda;
c) provide guidance and other assistance as may be required to other users and providers of information technology;
d) promote cooperation, coordination and rationalization among users and providers of information technology at national and local level so as to avoid duplication of efforts and ensure utilization of scarce resources;
e) promote and be the focal point of cooperation for information technology users and providers at regional and international levels; and
f) promote access to and utilization of information technology by the special interest groups.

In line with b) above, NITA is charged with the role to:

a) set, monitor and regulate standards for information technology planning, acquisition, implementation, delivery, support, organization, sustenance, disposal, risk management, data protection, security and contingency planning;
b) regulate and enforce standards for information technology hardware and software equipment procurement in all government ministries, departments, agencies and parastatals; and
c) protect and promote the interests of consumers or users of information technology services or solutions.

The work of development, coordinating and elaboration of Information Communication Technology (ICT) standards is carried out through Technical Committees. A Technical Committee is established to deliberate on standards in a given field or area and consists of representatives of users, the business community, manufacturers, government and other stakeholders. Draft ICT Standards adopted by the Technical Committee are widely circulated to stakeholders and the general public for comments. The committee reviews the comments before recommending the draft standards for approval and declaration as Uganda Standards by the NITA-U Board or the National Standards Council of Uganda National Bureau of Standards.

1 INTRODUCTION

This document contains a complete list of NITA-U standards available in the standards library. These standards have been developed through consensus by industry, consumers, government departments, research organizations, universities and private institutions.

The tables in this document show the standards currently available on the NITA-U website and library and some key information relating to each standard.

For each standard, the following information is provided where appropriate:

- Reference number: Unique identifier of the standard
- Name: Title of the standard as listed in the standards library
- Date : Date this version of the standard was published by Uganda
- Edition Version of the standard
- Description: Brief description of the standard

The standards are classified according to broad subject areas for easy retrieval. This standards catalogue is a living document and shall undergo regular updating whenever new standards are developed or existing standards are withdrawn or whenever need arises.

2 CLASSIFICATION OF STANDARDS

2.1 IT SECURITY TECHNIQUES

The IT security techniques broadly refer to mechanisms which are relevant to the provision of the security features such as confidentiality of data, confidentiality for the user identity in transmission, entity authentication, integrity for data and non-repudiation among others. They include generic methods, techniques and guidelines to address both security and privacy aspects. These measures include the following:

a) Security requirements capture methodology;

b) Management of information and ICT security, in particular information security management systems, security processes, security controls and services;

c) Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;

d) Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;

e) Security aspects of identity management, biometrics and privacy;

f) Conformance assessment, accreditation and auditing requirements in the area of information security management systems; and

g) Security evaluation criteria.

Purpose

These standards are developed for the protection of information and ICT.

Reference number	Name	Date	Edition	Description
US ISO IEC 27010:2015	Information security management for inter-sector and inter-organizational communications	2014-10-15	First	Both public and private sectors dealing with exchange and sharing of sensitive information and protection of an organization or nation state's critical infrastructure
US ISO IEC 27001: 2005	Information technology - Security techniques - Information security management systems - Requirements	2012-12-18	First	Specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. Specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.
US ISO IEC 27003: 2010	Information technology - Security techniques - Information security management system implementation guidance	2012-12-18	First	Focuses on the critical aspects needed for successful design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005. Describes the process of ISMS specification and design from inception to the production of implementation plans.
US ISO IEC 27002: 2005	Information technology - Security techniques - Code of practice for information security management	2012-12-18	First	Establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization.
US ISO IEC 27004: 2009	Information technology - Security techniques - Measurement	2012-12-18	First	Provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls as specified in ISO/IEC 27001.
US ISO IEC 27005: 2011	Information technology - Security techniques - Information security risk management	2012-12-18	First	Provides guidelines for information security risk management. Supports general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.
US ISO IEC 27006: 2011	Corporate governance of information technology -Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management system	2012-12-18	First	Specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accre18028-ditation of certification bodies providing ISMS certification.

Reference number	Name	Date	Edition	Description
US ISO IEC 27007: 2011	Information technology - Security techniques - Guidelines for information security management systems auditing	2012-12-18	First	Provides guidance on managing an information security management system (ISMS) audit program, on conducting audits and on the competence of ISMS auditors in addition to the guidance contained in ISO 19011. Applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit program.
US ISO IEC 27032: 2012	Information technology - Security techniques - Guidelines for cybersecurity	2012-12-18	First	Provides an overview of cybersecurity, an explanation of the relationship between cybersecurity and other types of security, provides a definition of stakeholders and a description of their roles in cybersecurity, guidance for addressing common cybersecurity issues and a framework to enable stakeholder to collaborate on resolving cybersecurity issues.
US ISO IEC 27035: 2011	Information technology - Security techniques - Information security incident management	2012-12-18	First	Provides a structured and planned approach to: detect, report and assess information security incidents; respond to and manage information security incidents; detect, assess and manage information security vulnerabilities and continuously improve information security and incident management as a result of managing information security
US ISO IEC 24762:2008	Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services	2012-12-18	First	Provides guidelines on the provision of ICT disaster recovery services as part of business continuity management. It specifies requirements for implementing, operating, monitoring and maintaining ICT DR services and facilities. Specifies capabilities which outsourced ICT DR service providers should possess and the practices they should follow so as to provide basic secure operating environments and facilitate organizations' recovery efforts. Provides guidance for selection of recovery site and guidance for ICT DR service providers to continuously improve their ICT DR services.
US ISO/IEC 27039:2015	Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems	2015-02-11	First	Provides guidance for an organization that decides to include an intrusion detection capability within its IT infrastructure. Provides information that will facilitate collaboration among organizations using IDS. Provides an overview of the intrusion detection process.
US ISO /IEC 27033-4:2014	Information technology - Security techniques - IT network security - Part 3: Securing	2014-02-21	First	Provides an overview of security gateways through a description of different architectures. It outlines the techniques for security gateways to analyze the network traffic. Provides guidelines for the selection and configuration of security gateways and provides

Reference number	Name	Date	Edition	Description
	communications between networks using security gateways			guidance for choosing the right type of architecture for a security gateway which best meets the requirements of an organization
US ISO IEC 18028-4: 2005	Information technology - Security techniques - IT network security - Part 4: Securing remote access	2012-12-18	First	Provides guidance for securely using remote access. Introduces the different types of remote access including the protocols in use. Discusses authentication issues related to remote access and provides support when setting up remote access securely.
US ISO IEC 18028-5: 2006	Information technology - Security techniques - IT network security - Part 5: Securing communications across networks using virtual private networks	2012-12-18	First	Provides detailed guidance on the security aspects of the management, operation and use of IT networks, and their inter-connections. It defines techniques for securing inter-network connections that are established using virtual private networks (VPNs). It is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example IT network managers, administrators, engineers, and IT network security officers).
US ISO 21188:2006	Public key infrastructure for financial services - Practices and policy framework	2014-10-15	First	Provides a framework for managing a PKI through certificate policies, certification practice statements, control objectives and supporting procedures.

2.2 INFORMATION TECHNOLOGY SERVICE MANAGEMENT AND INFORMATION TECHNOLOGY GOVERNANCE

Information technology management refers to a broad set of capabilities and processes to direct and control the service provider's activities and resources for design, transition, delivery and improvement of services to fulfill the service requirements. IT governance in this context is used to broadly refer to the system by which the current and the future use of IT is directed and controlled. These standards cover best practices for IT management and governance including areas of IT activity such as audit, digital forensics, risk management, outsourcing, service operations and service maintenance.

Purpose:

In general, these standards are developed to standardize IT management and IT governance. The standards specify requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve a service management system, they also provide guiding principles for members of governing bodies of organizations (owners, directors, partners, executive managers) on the effective, efficient and acceptable use of information technology (IT) within their organizations. They also provide guidance to those advising, informing, or assisting governing bodies.

Reference number	Name	Date	Edition	Description
US ISO IEC 20000-1: 2011	Information Technology - Service Management - Part 1: Service Management System Requirements	2014-10-15	Second	Specifies requirements for the service provider to plan establish, implement, operate, monitor, review, maintain and improve a service management system (SMS). The requirements include the design, transition, delivery and improvement of services to fulfill agreed service requirements.
US ISO IEC 20000-3: 2012	Information Technology - Service Management - Part 3: Guidance on Scope Definition and Applicability of ISO/IEC 20000-1	2014-10-15	First	Useful for service providers, consultants and assessors. Offers practical guidance on scope definition, applicability, and demonstration to the requirements in ISO/IEC 20000-1. Provides guidance on different types of conformity assessment and assessment standards.
US ISO IEC TR 20000-4: 2010	Information Technology - Service Management - Part 4: Process Reference Model	2014-10-15	First	Facilitate the development of a process assessment model according to ISO/IEC 15504 process assessment principles
US ISO IEC TR 20000-5: 2013	Information Technology - Service Management - Part 5: Exemplar Implementation Plan for ISO/IEC 20000-1	2014-10-15	Second	Provides an exemplar implementation plan providing guidance on how to implement a service management system (SMS) to fulfill the requirements of ISO/IEC 20000-1:2011.
US ISO IEC 38500: 2008	Corporate governance of information technology	2012-12-18	First	ISO/IEC 38500:2008 provides guiding principles for directors of organizations (including owners, board members, directors, partners, senior executives, or similar) on the effective, efficient, and acceptable use of Information Technology (IT) within their organizations.

2.3 TELECOMMUNICATIONS AND INFORMATION EXCHANGE BETWEEN SYSTEMS

This broad category of standards refers to the exchange of information over a given distance by electronic means and refers to all types of voice, data and video transmission. It includes a wide range of information technologies such as telephones, microwave communications, fiber optics, satellites, radio and television broadcasting, the internet and telegraphs.

Purpose:

The standards are used to standardize exchange of information between open systems, including system functions, procedures, parameters as well as the conditions for their use. They also help in the standardization of protocols and services of lower layers including physical, data, link, network and transport as well as those of upper layers.

Reference number	Name	Date	Edition	Description
US ISO IEC 9594-8:2008	Information Technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate Frameworks	2014-02-25	Seven	Defines a framework for public-key certificates. The framework includes specification of data objects used to represent the certificates themselves as well as revocation notices for issued certificates that should no longer be trusted. Provides the foundation upon which full PKIs and their specifications would be built. Provides a framework for attribute certificates and provision of authentication services by the Directory to its users.

2.4 PROJECT PROGRAM AND PORTFOLIO MANAGEMENT

This category of standards deals broadly with the management of portfolio components (project, program or other related work) grouped together to facilitate their management to meet, in whole or in part an organization's strategic objectives.

Purpose:

The standards are used to;

a) Help executives and senior managers responsible for setting and implementing organizational strategies and business planning

b) Decision makers responsible for selecting, authorizing and governing projects, programs and portfolios

c) Teams and individuals responsible for implementing and managing the project and program portfolios

d) Help project and program managers and other stakeholders

Reference number	Specification	Date	Edition	Description
US ISO 21500:2012	Guidance on Project Management	2014-10-15	First	Provides guidance for project management. Provides high level description of concepts and processes that are considered to form good practice in project management.
NITPMM2013	National Information Technology Project Management Methodology	2013-05-15	First	Provides project management best practices for planning and management of government information technology projects. It provides concepts, tools, and techniques to enhance implementation of information technology projects.

2.5 DATA MANAGEMENT AND INTERCHANGE

These standards cover reference models and frameworks for the coordination of existing and emerging standards, definition of data domains, data types and data structures and their associated semantic languages, services and protocols for persistent storage, concurrent access, concurrent update and interchange of data, methods, languages, services and protocols to structure, organize and register metadata and other information resources associated with sharing interoperability including electronic commerce.

Purpose:

Standards for data management within and among local and distributed information system environments provide enabling technologies to promote harmonization of data management facilities across sector specific areas.

Reference number	Name	Date	Edition	Description
US ISO IEC 9075-2: 2011	Information Technology - Database Languages - SQL - Part 2: Foundation (SQL/Foundation)	2014-10-15	Four	Defines the data structures and basic operations on SQL - data. It provides functional capabilities for creating, accessing, maintaining, controlling and protecting SQL -data.
US ISO IEC 9075-11: 2011	Information Technology - Database Languages - SQL - Part 11: Information and Definition Schemas (SQL/Schemata)	2014-10-15	Three	Specifies an information schema and a definition schema that describes the structure and integrity constraints of SQL -data, the security and authorization specifications relating to SQL -data and the features supported by an SQL implementation together with other sizing information.
US ISO IEC 9075-14: 2011	Information Technology - Database Languages - SQL - Part 14: XML -Related Specifications (SQL/XML)	2014-10-15	Four	Defines ways in which SQL can be used in conjunction with XML. It defines ways of importing and storing XML data in an SQL database manipulating it within the database and publishing both XML and conventional SQL data in data in XML form.

2.6 INFORMATION AND DOCUMENTATION

These standards cover the broad areas of technical interoperability, quality, that is with regard to statistics and performance evaluation, identification and description, requirements for document storage and conditions for preservation and archives and record management.

Purpose:

These standards lead to the harmonization of practices relating to libraries, documentation and information centers, publishing archives, records management, indexing and abstracting services and information science.

Reference number	Name	Date	Edition	Description
US ISO IEC 15489-1:2016	Records Management - Part 1: General	2016-04-07	Second	Ensures that appropriate attention and protection is given to all records, and that the evidence and information they contain can be retrieved more efficiently and effectively, using standard practices and procedures.
US ISO 13008:2012	Digital Records Conversion and Migration Process	2017-06-20	First	This standard specifies the planning issues, requirements and procedures for the conversion and/or migration of digital records (which includes digital objects plus metadata) in order to preserve the authenticity, reliability, integrity and usability of such records as evidence of business transactions. These digital records can be active or residing in a repository.
US 1717:2017	Implementation Guidelines for Digitization of Records	2017-06-20	First	This standard establishes guidelines for creating and maintaining records in digital format only. It sets out best practice guidelines for digitization to ensure the trustworthiness and reliability of records and enable consideration of disposal of the non-digital source records. The guidelines may have impact on the legal admissibility and evidential weight of digitized records. It also establishes best practice guidelines for the accessibility of digitized records for as long as they are required and specifies strategies to assist in creating digitized

				records fit for long term retention. The standard establishes best practice guidelines for the management of non-digital source records following digitization.
US ISO 8439:1990	Forms Design – Basic Layout	2017-06-20	First	The standard specifies overall sizes, image areas, their division and data fields for forms intended for use within administration, commerce and industry.
US ISO 16175-1:2010	Principles and Functional Requirements for Records in Electronic Office Environments – Part 1: Overview and Statement of Principles	2017-06-20	First	The Uganda standard establishes fundamental principles and functional requirements for software used to create and manage digital records in office environments.
US ISO 16175-2:2011	Principles and Functional Requirements for Records in Electronic Office Environments – Part 2: Guidelines and Functional Requirements for Digital Records Management Systems	2017-06-20	First	This Uganda Standard is applicable to products that are often termed 'electronic records management systems' or 'enterprise content management systems'. This standard articulates a set of functional requirements for digital records management systems. These requirements apply to records irrespective of the media in which they are created and/or stored. The requirements are intended to: • Set out the processes and requirements for identifying and managing records in digital records management systems • Set out the records management functionality to be included in a design specification when building, upgrading or purchasing digital records management systems software • Inform records management functional requirements in the selection of commercially available digital records management systems; and • Review the records management functionality of, or assess the compliance of, an existing digital records management system

2.7 HEALTH INFORMATICS

Health informatics is the interdisciplinary study of the design, development, adoption and application of IT based innovations in healthcare services delivery, management and planning. Health informatics describes the acquiring, storing, retrieval and use of healthcare information to foster better collaboration among a patient's healthcare providers. It links information technology communications and healthcare to improve the quality and safety of patient care.

Purpose:

To meet the need for standardization in the field of health informatics in order to facilitate the coherent and consistent interchange and use of health-related data, information and knowledge to support and enable all aspects of the health system.

Reference number	Name	Date	Edition	Description
US ISO 17090-1:2013	Public key infrastructure - Part 1: Overview of digital certificate services	2014-10-15	Second	Defines basic concepts underlying the use of digital certificates in health care and provides a scheme of interoperability requirements to establish digital certificate enabled secure communication of health information
US ISO 17090-2:2008	Public key infrastructure - Part 2: Certificate Profile	2014-10-15	Second	Provides health care specific profiles of digital certificated based on the international standard X.509
US ISO 17090-3:2008	Public key infrastructure - Part 3: Policy management of certification authority	2014-10-15	First	Deals with management issues involved in implementing and using digital certificates in healthcare. It defines a structure and minimum requirements for certificate policies and a structure for associated certification practice statements.

2.8 SYSTEMS AND SOFTWARE ENGINEERING

These standards cover the processes, supporting tools and supporting technologies for the engineering of software products and systems. Systems engineering is an interdisciplinary approach governing the total technical and managerial effort required to transform a set of customer needs, expectations and constraints into a solution and to support the solution throughout its life.

Purpose:

These standards provide guidance on the development of process models and good practice. They provide methods and techniques independent of the application domain.

Reference number	Name	Date	Edition	Description
US ISO IEC 25010:2011	Systems and Software Quality Requirements and Evaluation (SQuaRE) - System and Software Quality Models	2014-10-15	First	Provides a means for defining and measuring the quality characteristics related to the software system and data. The Quality models in this standard can be used to identify relevant quality characteristics that can be further used to establish requirements, their criteria for satisfaction and the corresponding measures.
US ISO IEC 25051:2014	Systems and Software Quality Requirements and Evaluation (SQuaRE) - Requirements for Quality of Ready to Use Software Product (RUSP) and Instructions for Testing	2014-10-15	First	Provides a set of requirements for ready to use software product (RUSP) and requirements for testing a ready to use software product against its requirements.
US ISO IEC 25062: 2006	Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing	2006-03-31	First	ISO/IEC 25062:2006 provides a standard method for reporting usability test findings. The format is designed for reporting results of formal usability tests in which quantitative measurements were collected, and is particularly appropriate for summative/comparative testing. The CIF does not indicate how to perform a usability test but provides guidance on how to report the results of a usability test. The CIF targets two audiences: usability professionals and stakeholders in an organization. Stakeholders can use the usability data to help make informed decisions

Reference number	Name	Date	Edition	Description
				concerning the release of software products or the procurement of such products.
US ISO IEC 15504-1: 2004	Software Engineering - Process Assessment - Part 1: Concepts and Vocabulary	2014-10-15	First	Provides a general introduction to the concepts of process assessment and a glossary for assessment related terms.
US ISO IEC 15504-2: 2003	Software Engineering - Process Assessment - Part 2: Performing an Assessment	2014-10-15	First	Sets the minimum requirements for performing an assessment that ensure consistency and repeatability of the ratings.
US ISO IEC 15504-3: 2003	Software Engineering - Process Assessment - Part 3: Guidance on Performing an Assessment	2014-10-15	First	Provides guidance on meeting the minimum set of requirements for performing an assessment contained in ISO/IEC 15504-2.
US ISO IEC 15504-4: 2004	Software Engineering - Process Assessment - Part 4: Guidance on Use for Process Improvement and Process Capability Determination	2014-10-15	First	Identifies process assessment as an activity that can be performed either as part of a process improvement initiative or as part of a capability determination approach.
US ISO IEC 15504-5: 2004	Information technology – Process assessment – Part 5: An exemplar software life cycle process assessment model	2014-10-15	Second	Provides an example of a Process Assessment Model for use in performing a conformant assessment in accordance with the requirements of ISO/IEC 15504-2. Provides a statement of conformance of the process assessment model to the requirements defined in ISO/IEC 15504-2. Selected characteristics for typical work products to assist the assessor in evaluating the capability level of processes. Style guides for defining base practices, work products and generic practices for adjusting the process assessment model and guidance explaining how to expand or adapt the model.
US ISO IEC 25022:2016	Systems and software quality requirements and evaluation (SQuaRE) – Measurement of quality in use	2017-06-20	First	This Uganda Standard defines quality in use measures for the characteristics defined in ISO/IEC 25010 and is intended to be used together with ISO/IEC 25010. It can be used in conjunction with the ISO/IEC 2503n and the ISO/IEC 2504n standards or to more generally meet user needs with regard to product or system quality. This standard contains the following: a basic set of measures for each quality in use characteristic; an explanation of how quality in use is measured. This standard provides a

Reference number	Name	Date	Edition	Description
				suggested set of quality in use measures to be used with the quality in use model ISO/IEC 25010.
US ISO IEC 25023:2016	Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of system and software product quality	2017-06-20	First	This Uganda Standard defines quality measures for quantitatively evaluating system and software product quality in terms oof characteristics and sub characteristics defined in ISO/IEC 25010. It can be used in conjunction with ISO/IEC 2503n and the ISO/IEC 2504n or to more generally meet user needs with regard to software products or system quality.

2.9 CLOUD COMPUTING

Cloud computing is defined as a paradigm for enabling network access to a scalable elastic pool of shareable physical or virtual resources with self-provisioning and administration on-demand. Examples of resources include servers, operating systems, networks, software applications and storage equipment.

The cloud computing paradigm is composed of key characteristics, cloud computing roles and activities, cloud capabilities types and cloud service categories, cloud deployment models and cloud computing cross cutting aspects.

The key characteristics of cloud computing are: broad network access, measured service, multi-tenancy, on-demand self-service, rapid elasticity and scalability and resource pooling.

Purpose:

To achieve standardization in the area of cloud computing and distributed platforms including but not limited to service oriented architecture, service level agreements, interoperability and portability and data and its flow across devices and cloud services.

Reference Number	Name	Date	Edition	Description
US 1649:2016	Information technology – Distributed Application Platforms and Services (DAPS) – General technical principles of service oriented architecture	2016-12-13	First	ISO/IEC TR 30102:2012 describes the general technical principles underlying Service Oriented Architecture (SOA), including principles relating to functional design, performance, development, deployment and management. It provides a vocabulary containing definitions of terms relevant to SOA. It includes a domain-independent technical framework, addressing functional requirements and non-functional requirements.
US ISO/IEC 17203:2011	Information technology – Open Virtualization Format (OVF) specification	2016-12-13	First	ISO/IEC 17203:2011 specifies an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines

Reference Number	Name	Date	Edition	Description
US ISO/IEC 17789:2014	Information technology – Cloud computing – Reference architecture	2016-12-13	First	ISO/IEC 17789:2014 specifies the cloud computing reference architecture (CCRA). The reference architecture includes the cloud computing roles, cloud computing activities, and the cloud computing functional components and their relationships.
US ISO/IEC 17826:2012	Information technology – Cloud data Management Interface (CDMI)	2016-12-13	First	ISO/IEC 17826:2012 specifies the interface to access cloud storage and to manage the data stored therein. It is applicable to developers who are implementing or using cloud storage.
US ISO/IEC 17963:2013	Web Services for Management (WS-Management) Specification	2016-12-13	First	ISO/IEC 17963:2013 describes a Web services protocol based on SOAP for use in management-specific domains. These domains include the management of entities such as PCs, servers, devices, Web services and other applications manageable entities. Services can expose only a WS-Management interface or compose the WS-Management service interface with some of the many other Web service specifications. A crucial application for these services is in the area of systems management. To promote interoperability between management applications and managed resources, ISO/IEC PAS 17963:2012 identifies a core set of Web service specifications and usage requirements that expose a common set of operations central to all systems management.
US ISO/IEC 17788:2014	Information technology – Cloud computing – Overview and vocabulary	2016-12-13	First	ISO/IEC 17788:2014 provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards. ISO/IEC 17788:2014 is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).

2.10 OFFICE EQUIPMENT

These standards cover standardization of basic characteristics, test methods and other related items of products such as 2D and 3D Printers/Scanners, copiers, projectors, fax and systems composed of their combinations. They also cover accessibility guidelines to be considered when planning, developing and designing electrographic copying machines, page printers and multifunction devices.

Purpose:

The purpose of these standards is to provide interoperability, ease of use and particularly to improve accessibility required when primarily older persons, persons with disabilities and persons with temporary disabilities need to use office equipment.

Reference Number	Name	Date	Edition	Description
US ISO/IEC 10779:2008	Information technology – Office equipment accessibility guidelines for elderly persons and persons with disabilities	2016-12-13	First	ISO/IEC 10779:2008 specifies accessibility guidelines to be considered when planning, developing and designing electro-photographic copying machines, page printers and multi-function devices. These guidelines are intended to improve accessibility required when primarily older persons, persons with disabilities and persons with temporary disabilities use office equipment.

USER INTERFACES

These standards cover standardization in the field of user-system interfaces in information and communication technology (ICT) environments and support for these interfaces to serve all users including people having accessibility or other specific needs, with a priority of meeting the requirements for cultural and linguistic adaptability. This includes:

- User interface accessibility (requirements, needs, methods, techniques and enablers);

- Cultural and linguistic adaptability and accessibility (such as evaluation of cultural and linguistic adaptability of ICT products, harmonized human language equivalents, localization parameters, voice messaging menus);
- User interface objects, actions and attributes;
- Methods and technologies for controlling and navigating within systems, devices and applications in visual, auditory, tactile and other sensorial modalities (such as by voice, visual, movement, gestures);
- Symbols, functionality and interactions of user interfaces (such as graphical, tactile and auditory icons, graphical symbols and other user interface elements);
- Visual, auditory, tactile and other sensorial input and output devices and methods in ICT environments (for devices such as keyboards, displays, mice);
- User interfaces for mobile devices, hand-held devices and remote interactions.

Purpose

Reference Number	Name	Date	Edition	Description
US ISO/IEC 24786:2009	Accessible User Interface for Accessibility Settings	2017-06-20	First	This standard specifies requirements and recommendations for making accessibility settings accessible. It provides guidance on specific accessibility settings. It specifies how to access and operate the accessibility setting mode, and how to directly activate specific accessibility features. It applies to all operating system user interfaces on computers, but can also be applied to other types of information/communication technology, where appropriate. The standard does not apply to the user interface before the operating system is loaded and active.

GEOGRAPHIC INFORMATION / GEOMATICS

These standards cover standardization in the field of digital geographic information. Standardization in this area aims to establish a structured set of standards for information concerning objects or phenomena that are directly or indirectly associated with a location relative to the earth.

Purpose:

These standards may specify, for geographic information, methods, tools and services for data management (including definition and description), acquiring, processing, analyzing, accessing, presenting and transferring such data in digital / electronic form between different users, systems and locations.

The standards may be linked to appropriate standards for information technology and data where possible and provide a framework for the development of sector specific applications using geographic data.

Reference Number	Name	Date	Edition	Description
US ISO 19101-1:2014	Reference Model – Part 1: Fundamentals	2017-06-20	First	This Uganda Standard defines the reference model for standardization in the field of geographic information. This reference model describes the notion of interoperability and sets forth the fundamentals by which this standardization takes place. Although structured in the context of information technology and information technology standards, this part of US ISO 19101 is independent of any application development method or technology implementation approach.
US ISO/TS 19101-2:2008	Reference Model – Part 2: Imagery	2017-06-20	First	This Uganda Standard defines a reference model for standardization in the field of geographic imagery processing. This reference model identifies the scope of the standardization activity being undertaken and the context in which it takes place. The reference model includes gridded data with an emphasis on imagery.

				Although structured in the context of information technology and information technology standards, this Technical Specification is independent of any application development method or technology implementation approach.
US ISO 19103:2015	Conceptual Schema Language	2017-06-20	First	This Uganda Standard provides rules and guidelines for the use of a conceptual schema language within the context of geographic information. The chosen conceptual schema language is the Unified Modeling Language (UML). This standard provided a profile of the UML. The standardization target type of this standard is UML schemas describing geographic information.
US ISO 19104:2016	Terminology	2017-06-20	First	This Uganda Standard specifies requirements for the collection, management and publication of terminology in the field of geographic information. The scope of this document includes the selection of concepts, harmonization of concepts and development of concept systems, structure and content of terminological entries, term selection, definition preparation, cultural and linguistic adaptation, layout and formatting requirements in rendered documents and establishment and management of terminology registers.
US ISO 19105:2000	Conformance and Testing	2017-06-20	First	This Uganda Standard specifies the framework, concepts and methodology for testing and criteria to be achieved to claim conformance to the family of ISO geographic information standards. It provides a framework for specifying Abstract Test Suites (ATS) and for defining the procedures to be followed during conformance testing. Conformance may be claimed for data or software products or services or by specifications including any profile or functional standard. Standardization of test methods and criteria for conformance to geographic information standards will allow verification of conformance to those standards. Verifiable conformance is important to geographic information users, in order to achieve data transfer and sharing.

US ISO 19106:2004	Profiles	2017-06-20	First	This Uganda Standard is intended to define the concept of a profile of the ISO geographic information standards and to provide guidance for the creation of such profiles. Only those components of specifications that meet the definition of a profile contained herein can be established and managed through the mechanisms described in this standard, This document also provides guidance for establishing, managing and standardizing at the national level (or in some other forum).