International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 27

(09/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1054 – Supplement on best practice for governance of information security – Case of Burkina Faso

ITU-T X-series Recommendations – Supplement 27

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Supplement 27 to ITU-T X-series Recommendations

ITU-T X.1054 – Supplement on best practice for governance of information security – Case of Burkina Faso

Summary

To create value, the information should be governed within the organization so as to have a strategic alignment between the objectives of information security and those of the organization. Governance and management of information security should be conducted in complete synergy. The management should be responsible for the operation of information and reporting (idea of responsibility) to the governing body.

To achieve this, the organization can use standards, recommendations and other frameworks whose implementation will encourage its success.

It is in this spirit that Recommendation ITU-T X.1054 | ISO /IEC 27014 is implemented to the governance of information security of e-Council of Ministers in Burkina Faso.

This approach aims to be a case of best practice in the implementation of Recommendation ITU-T X.1054 | ISO /IEC 27014. Here it is used as part of a unifying project gathering all members of the Government of Burkina Faso (Presidency, Prime Ministry, General Secretariat of the government and the Council of Ministers, all ministries). However, this Supplement could be applied to any type of organization.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 27	2016-09-07	17	11.1002/1000/13072

Keywords

Governance of information security, Governance model, ITU-T X.1054 | ISO/IEC 27014.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 27 to ITU-T X-series Recommendations

ITU-T X.1054 – Supplement on best practice for governance of information security – Case of Burkina Faso

1 Scope

This Supplement describes a best practice case for the implementation of guidelines provided by [ITU-T X.1054].

[ITU-T X.1054] provides concepts and guidance on the principles and the processes for the governance of information security, by which organizations can evaluate, direct and monitor the management of information security.

This Supplement shows how [ITU-T X.1054] is implemented in an organization, in particular the government of Burkina Faso, to set up a model for the information security governance. It also provides a mapping between the model, principles and processes of [ITU-T X.1054].

2 References

[ITU-T X.1054] Recommendation ITU-T X.1054 (2012) | ISO/IEC 27014:2013, *Information technology – Security techniques – Governance of information security.*

3 Definitions

This Supplement uses the definitions given in [ITU-T X.1054].

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

A Assure

C Communicate

CIO Chief Information Officer

D Direct

E Evaluate

eCM e-Council of Ministers (e-Conseil des Ministres)

ICT Information and Communication Technology

IT Information Technology

M Monitor

5 Extracts from Recommendation ITU-T X.1054 | ISO/IEC 27014

This clause holds extracted portions from [ITU-T X.1054].

5.1 Objectives [ITU-T X.1054]

The objectives of governance of information security are to:

- align the information security objectives and strategy with business objectives and strategy (strategic alignment),

- deliver value to the governing body and to stakeholders (value delivery),
- ensure that information risk is being adequately addressed (accountability).

5.2 Desired outcomes [ITU-T X.1054]

The desired outcomes from effectively implementing governance of information security include:

- governing body visibility on the information security status,
- an agile approach to decision-making about information risks,
- efficient and effective investments on information security,
- compliance with external requirements (legal, regulatory or contractual).

5.3 Governance of information security/Principles and processes

Governance of information security involves applying rules adopted at principles level and perform the tasks described in processes. This clause describes the tasks required from the governing body to establish governance of information security.

5.3.1 Principles

Governance principles of information security are rules to be respected for the implementation of the governance. They constitute a sort of implementation guide. Each principle is characterized by what should happen (outcomes), but does not prescribe how, when (deadline) or by whom (responsible) the principle would be implemented.

There are six principles (actions to apply) to align information security with the goals of business. These include:

Principle 1 (P1): Establish organization-wide information security;

Principle 2 (P2): Adopt a risk-based approach;

Principle 3 (P3): Set the direction of investment decisions;

Principle 4 (P4): Ensure conformance with internal and external requirements;

Principle 5 (P5): Foster a security-positive environment;

Principle 6 (P6): Review performance in relation to business outcomes.

5.3.2 Processes

Governance processes for information security (i.e., Evaluate (E), Direct (D), Monitor (M), Communicate (C) and Assure (A)) describe a set of tasks to be performed to implement the governance of information security and the relationships between these tasks.

Every governance model is an integral component of the governance of an organization, which emphasizes the importance of alignment with the business objectives. It is usually beneficial for the governing body to develop a holistic and integrated view of its governance model, of which governance of information security should be a part.

In this Supplement, Burkina Faso's case is introduced. This case is based on the existing bodies to establish and implement the governance of information security of e-Council of Ministers (eCM).

6 Description of e-Council of Ministers

The aim of "e-Council of Ministers (eCM)" (*e-Conseil des Ministres*) or "Paperless Council of Ministers" is to ensure the total virtualization of document processing, from drafting in ministerial departments to final archiving after their adoption by the Council of Ministers.

6.1 Process of Council of Ministers documents

The process of Council of Ministers documents comprises the following eight steps:

- Step 1 – Producing documents by ministerial departments

Inputs	Actors	Outputs
1. Basic documents 2. Ideas	1. Minister 2. General Secretary 3. Chief of minister staff 4. Technical advisors	1. Reports on draft decrees 2. Reports on preliminary draft laws 3. Statements by council of ministers 4. Other reports

- Step 2 – Evaluate documents by the General Secretariat of the government and of the Council of Ministers

Inputs	Actors	Outputs
1. Reports on draft decrees 2. Reports on preliminary draft laws 3. Statements by council of ministers 4. Other reports	1. General Secretary of Government 2. Deputy-General Secretary of Government 3. Special advisers	1. Documents 2. Notes / remarks / comments

- Step 3 – Setting the agenda

Inputs	Actors	Outputs
1. Documents validated by the General Secretariat of Government 2. Draft agenda	1. Prime Minister 2. General Secretary of Government / Deputy-General Secretary of Government	1. Scheduled documents 2. Agenda

- Step 4 – Examination of documents tabled for discussion in the Council of Ministers

Inputs	Actors	Outputs
1. Scheduled documents 2. Agenda	1. Minister 2. General secretary 3. Chief of minister staff 4. Technical advisors	1. Scheduled documents 2. Agenda 3. Notes / remarks / comments made by each ministry

- Step 5 – Meeting with the Council of Ministers

Inputs	Actors	Outputs
1. Scheduled documents 2. Agenda 3. Notes / remarks / comments made by each ministry	1. President 2. Prime Minister 3. All ministers 4. General Secretary of Government	1. Scorecard or tracking sheet of the council by General Secretary of Government 2. Council report 3. Adopted texts 4. Withdrawn, rejected or renewed texts 5. Tracking sheet (by each minister)

- Step 6 – Finalization of texts adopted in the Council of Ministers

Inputs	Actors	Outputs
1. Agenda 2. Adopted texts 3. Tracking sheet of ministers council 4. Report of ministers council 5. Tracking sheet (by each minister)	1. Government members concerned with issues 2. General Secretary of Government 3. Deputy General Secretary of Government 4. Ministerial staff concerned with issues 5. Special advisors of General Secretary of Government	1. Finalized texts 2. Adopted draft laws

- Step 7 – Signature

Inputs	Actors	Outputs
1. Finalized texts 2. Passed laws	1. President 2. Prime Minister 3. Government members concerned with issues 4. General Secretary of Government	1. Signed texts 2. Passed laws

- Step 8 – Publication and archiving

Inputs	Actors	Outputs
1. Signed texts 2. Passed laws	1. Director of Legal Department (General Secretariat of Government) 2. Director of Department of ICT and archives (General Secretariat of Government) 3. Director of Library Department (General Secretariat of Government)	1. Official newspaper 2. Archives

In addition to these steps, inter-ministerial collaboration is also possible with regard to documents that concern decisions by more than one ministry.

Council of Ministers documents include the following:

- Reports on the preliminary draft laws
- Draft decrees
- Statements by the council of ministers
- Other types of reports (calls to tender, etc.).

6.2 Existing eCM administration and management bodies

The e-Council of Ministers is administered and managed by the following bodies:

- Steering committee
  - Steering committee's technical secretariat
- Users' group
- Project group.

Governance of information security covers confidentiality, integrity and availability of information. It should be handled by governance processes Evaluate, Direct and Monitor (EDM) and internal process "Communicate".

In [ITU-T X.1054], functions are described by processes which implement principles. Principles guide to action to be applied in order to achieve governance goals (strategic alignment, value delivery).

This approach starts from eCouncil of Ministers existing administration and management bodies to implementation principles and processes defined in [ITU-T X.1054] avoiding as much as possible creation of new bodies.

Functions are distributed in accordance with existing bodies while maintaining consistency with [ITU-T X.1054].

For example, the Audit committee implements principles P4, P5 and P6, and processes Monitor, Communicate and Assure. The implementation details of [ITU-T X.1054] to the case of governance of information security of e-Council of Ministers are described in clause 7.

7 Structure of information security governance for the e-Council of Ministers

Establishing a model of information security governance for the e-Council of Ministers involves a mapping between existing different administrative and management bodies and the processes identified in [ITU-T X.1054].

7.1 Functions

Figure 1 outlines the four major functions of the empirical governance model.

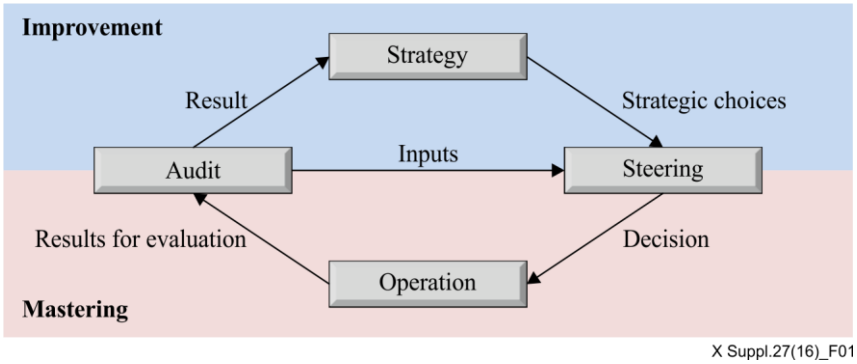

Figure 1 – Empirical governance model

The Strategy function feeds the results produced by the Audit function. The Steering function needs to know the strategic choices for deciding security options consistent with this strategy. Furthermore, the Steering function also needs the information provided by the Audit function. Overall, the Strategy, Audit and the Steering functions contribute to the improvement of the governance model.

The activities related to Operation function reflect (taking into account) the decisions taken by the Steering function and provide results that will be evaluated by the Audit function. There is no direct link between the Operation and the Strategy functions, as these functions are at distinct levels. Overall, the Audit, Steering and Operation functions contribute to the mastering of the governance model. Table 1 provides a summary description of the Strategy function.

Table 1 – Description of the Strategy function

Function	Strategy
Concerned by	Senior management
Period	As often as necessary to prepare senior management meetings. Every two months at ordinary meetings of senior management.
Objective	All activities aimed at ensuring that decisions relating to the information security of information systems take account of the strategic priorities of the e-Council of Ministers
Mandate	Define decisions regarding security strategy.
Agenda item	Decisions regarding security strategy.
Relates to	1 Audit function which provides input in the form of results. 2 Steering function which in the light of these strategic choices decides on the security options consistent with this strategy.

Table 2 provides a summary description of the Steering function.

Table 2 – Description of the Steering function

Function	Steering
Concerned by	1 Information technology (IT) manager 2 Security managers 3 Project manager
Period	As often as required to prepare steering meetings. Every month at ordinary steering meetings.
Objective	All activities to implement the strategy agreed by the senior management.
Mandate	1 To monitor closely the process of putting security procedures in place. 2 To steer the process of setting up procedures. 3 To steer the process of setting up security measures selected by the risk treatment plan.
Agenda items	1 Establishment of security procedures. 2 Establishment of security measures.
Related to	1 Strategy function which submits strategic decisions with a view to deciding on different security options consistent with that strategy 2 Audit function which provides input 3 Operation function which takes Steering function decisions into account.

Table 3 provides a summary description of the Operation function.

Table 3 – Description of the Operation function

Function	Operation
Concerned by	1 Operational management 2 Process managers
Period	Daily
Objective	All activities relating to provision of security services.
Mandate	Produce records to show that security processes work effectively and in accordance with information security governance policy.
Agenda items	Records produced.
Relates to	1 Steering function which passes on its decisions. 2 Audit function to which results are submitted for evaluation.

Table 4 provides a summary description of the Audit function.

Table 4 – Description of the Audit function

Function	Audit
Concerned by	Various hierarchical levels
Period	Monthly
Objective	All activities undertaken to ensure that governance model procedures produce effective outcomes that meet specifications.
Mandate	1 Monitor effectiveness of governance outcomes. 2 Verify compliance of the governance model with specifications.
Agenda items	1 Effectiveness of the governance outcomes. 2 Compliance of the governance model.
Linked to	1 Strategy function which uses the results produced. 2 Steering function to which it provides input. 3 Operation function assessing its results.

7.2 Principal bodies

The governance structure comprises four principal bodies: the **Steering committee** (which already exists); the **Security steering committee** (comprising some members of the existing Project group); **Operations group** (a subunit of the existing Project group); and the **Audit committee** (a subunit of the existing Users' group).

7.2.1 Steering committee

A decision was taken to expand the remit of the Steering committee to include questions of information security. The Steering committee already includes all those authorized to validate the tasks of the Strategy function. There is thus no need for a new body solely for information security issues, as it would only refer back to this one. Table 5 provides a summary description of the Steering committee.

Table 5 – Description of the Steering committee

Body	Steering committee: P1, P2
Members	Minister of ICT with a subset of General secretaries of ministries closely related with the steering of e-Council of Ministers.
Invited when necessary	1 Information security manager 2 Technical experts 3 Any other person likely to contribute to the discussions.
Chairman	Minister for the Development of the Digital Economy and Posts
Vice-Chairman	Secretary-General of the government and of the Council of Ministers
Period	Quarterly
Objective	Ensure that decisions on information security match the actual priorities of the eCouncil of Ministers: E, D
Mandate	1 Establish security priorities in align with eCouncil of Ministers strategy: P1, D 2 Establish risk acceptance criteria: P2, D 3 Approve residual risks: P2, D 4 Authorize setting up of the governance model 5 Authorize operation of the governance model 6 Establish information security governance policy: P1 7 Approve information security governance policy: P1, D 8 Define roles and responsibilities in the area of information security: P1, D
Agenda items	1 Approval of information security governance policy and perimeter 2 Setting up of risk acceptance criteria 3 Approval of residual risks as proposed by the Information security manager 4 Authorization to set up the information security governance 5 Authorization to operate the information security governance 6 Approval of eCouncil of Ministers security governance.
Relates to	1 The Audit committee, which reports annually on the state of compliance and effectiveness of the governance model 2 The Security steering committee, which proposes revisions of key points of the governance model once a year: C

7.2.2 Security steering committee

In addition to information technology (IT) aspects, the governance model also covers areas such as physical security, human resource management and a number of processes completely independent of IT. Instead of creating a new body, a subunit of the Project group has been taken as the basis of the Security steering committee. Table 6 provides a summary description of the Security steering committee.

Table 6 – Description of the Security steering committee

Body	Security steering committee: P3, P5, P6
Members	Information security manager IT systems security manager Information services dept. Managers of services (infrastructure service, development service, security service, service centre, training service).
Invited when necessary	Technical experts Project chief Key users.
Chairman	Information security manager
Period	Monthly
Objective	Ensure that security is sufficient to provide the level of confidence agreed by the Steering committee: E, D
Mandate	1 Monitor current projects 2 Propose solutions to problems encountered: P3, P5, P6
Agenda items	1 Communication and training in the area of security 2 Corrective and preventive measures under way: M 3 Analysis of requirements and expenses incurred in operating the governance model: D 4 Follow-up of current projects 5 Security incidents during the period in question: M
Annual agenda items	1 Review of information security governance policy and perimeter 2 Review of the governance model 3 Review of risk assessment 4 Examination of the annual audit report of the Audit Committee.
Relates to	1 Audit committee, to propose and follow-up on corrective and preventive measures if discrepancies are found in the audits 2 Operations group, to monitor production and steer the project 3 Steering committee, with proposals to the latter once a year regarding revisions of key points in the governance model.
Reports to	Steering committee: C

7.2.3 Operations group

The Operations group is responsible for the operational management of each service in the eCouncil of Ministers. Table 7 provides a summary description of the Operations group.

Table 7 – Description of Operations group

Body	Operations group: P4, P5, P6
Members	Operational managers Process managers Service managers (infrastructure service, development service, security service, service centre and training service).
Invited when necessary	Information security manager IT systems security manager Chief information officer (CIO)
Chairman	Service manager
Period	Daily
Objective	To ensure provision of security services agreed in the governance model
Mandate	1 Produce records to prove that the security processes operate effectively and in a manner consistent with the information security governance policy: P4, M 2 Take any necessary action to eliminate instances of non-compliance: P5, P6, M
Agenda items	1 Records produced 2 Security incidents
Weekly agenda items	1 Records produced 2 Security incidents 3 Current corrective and preventive measures.
Linked to	1 Steering committee, which ensures the level of confidence agreed 2 Audit committee, to which it submits results for evaluation.
Reports to	Security steering committee once a week, on the status of security services agreed in the governance model: C

7.2.4 Audit committee

Actions related to the Audit function is the responsibility of the Internal Audit committee, which decides on all questions pertaining to the Audit function of the governance model. The audit guidelines produced for this purpose will enable auditors to check the key points of the governance model. Decisions pertaining to governance model audits will be taken within the Audit committee, which is based on a subgroup of the Users' group, whose mandate will be expanded to include the following points as described in Table 8:

Table 8 – Description of the Audit committee

Body	Audit committee: P4, P5, P6
Members	Director of Legal department (General Secretariat of the government) Head of the Prime Minister's office Head of the department of Studies of the General Secretariat of Government A special secretary representing the Ministry of Territorial Administration and Security A representative of the Technical Inspectorate of Services of the Ministry for Development of the Digital Economy and Posts.
Invited when necessary	Information security manager IT systems manager.
Chairman	Director of Legal department (General Secretariat of Government)

Table 8 – Description of the Audit committee

Period	Every two months
Objective	Verify compliance and effectiveness of the governance model: P4
Mandate	1 Ensure that audits proceed smoothly: P4 , M 2 Follow-up on corrective and preventive measures: P5, P6, M
Agenda items	1 Review of audits undertaken since the previous meeting 2 Recorded instances of non-compliance 3 Approval of corrective and preventive measures: A 4 Current corrective and preventive measures.
Annual agenda items	1 Approval of the annual audit report to the Steering Committee 2 Approval of the audit programme for the following year.
Relates to	1 Security steering committee responsible for steering implementation of corrective and preventive measures where discrepancies are noted 2 Steering committee, reporting to the latter on compliance and effectiveness of the governance model 3 Operations group, evaluating the results of the latter: A
Reports to	Steering committee once a year on the state of compliance and effectiveness of the governance model: C

In [ITU-T X.1054], the process "Assure" is external. At the e-Council of Ministers, this process is performed by the Audit committee which is an internal body. However, it should be noted that it does not mean that this fact hinders the independence and objectivity of its opinions. The e-Council of Ministers is the top-level decision body of the country's executive. Information discussed at this level is sensitive. This information is confidential and strategic nature (sovereignty of a country). Therefore, it is decided that the process "Assure" should become an internal process.

8 Mapping between the e-Council of Ministers and ITU-T X.1054 | ISO/IEC 27014

The mapping between the information security governance of the e-Council of Ministers and the six principles and five processes indicated in [ITU-T X.1054] is provided in Table 9.

Table 9 – Mapping between the e-Council of Ministers and ITU-T X.1054 | ISO/IEC 27014

ITU-T X.1054 / Gov. eCM	Principles						Processes				
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**E**	**D**	**M**	**C**	**A**
Steering committee	X	X					X	X		X	
Security steering committee			X		X	X	X	X	X	X	
Operations group				X	X	X			X	X	
Audit committee				X	X	X			X	X	X

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019