

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y
Supplement 19
(06/2012)

SERIES Y: GLOBAL INFORMATION
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS
AND NEXT-GENERATION NETWORKS

ITU-T Y.2200-series – Supplement on the risk analysis service in next generation networks

ITU-T Y-series Recommendations – Supplement 19



International
Telecommunication
Union

Document Sharing Hub

ITU-T Y-SERIES RECOMMENDATIONS
**GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-
GENERATION NETWORKS**

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

FUTURE NETWORKS

Y.3000–Y.3499

CLOUD COMPUTING

Y.3500–Y.3999

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

Supplement 19 to ITU-T Y-series Recommendations

ITU-T Y.2200-series – Supplement on the risk analysis service in next generation networks

Summary

Supplement 19 to the ITU-T Y-series Recommendations deals with the risk analysis service, which is a service that is capable of identifying risks, assessing them and then invoking processes to identify the proper actions that should be taken to reduce damage that could affect users or organizations subscribed to a next generation network (NGN). Provided that a risk situation exists, the risk analysis function performs the analysis and assessment of the risk event data with an algorithm that applies the most recent pattern according to procedures, and reports the analysis results and the proper complementary measures which, if invoked, will reduce risk.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y Suppl. 19	2012-06-15	13

Keywords

Risk analysis service.

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/>.

© ITU 2013

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Supplement	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Overview	3
	6.1 Internal risks	3
	6.2 External risks	4
	6.3 Conceptual model for an IRAS function	4
7	IRAS function.....	4
	7.1 Application service management function	6
	7.2 Risk search function	6
	7.3 Risk analysis function.....	6
	7.4 Risk service profile.....	8
8	Execution of IRAS functions.....	8
	8.1 Risk analysis service and user registration.....	8
	8.2 Log-in session process.....	9
	8.3 Risk analysis service execution	9
9	Risk analysis service procedure.....	9
	9.1 General risk analysis service procedure	9
10	Service scenarios	13
	10.1 Service scenario related to external risks	13
	10.2 Service scenario related to internal risks	14
11	Security consideration	14

Introduction

The risk analysis service must contend with internal risks, which are risks related to potential network providers, service providers and user/terminal failures, as well as with external risks, which are risks related to forces external to the network. Internal risks can be associated with items such as hardware failures, software errors affecting service features and integrity, network outages, poor change management, data centre failures, network congestion, inefficient software code, inadequate capacity and malicious calls. External risks can be associated with items such as disasters resulting from earthquakes, typhoons, tsunamis and floods. An invoked risk analysis service will identify proper actions to take to reduce risk, which if taken, would reduce the risk of critical next generation network (NGN) service failures. Failure to invoke a risk analysis service, especially one that can deal with risk sources, could result in serious events which could adversely affect users subscribed to an NGN.

Supplement 19 to ITU-T Y-series Recommendations

ITU-T Y.2200-series – Supplement on the risk analysis service in next generation networks

1 Scope

Risk analysis service (IRAS) is a service that is capable of identifying risk, assessing the risk and then invoking a process to identify the proper actions that should be taken to reduce damage that could have an effect on users or organizations subscribed to an NGN. Invocation of a risk analysis service will result in identification of a set of positive actions that could be taken to reduce the current risk level for users or organizations subscribed to an NGN. A risk analysis service will be capable of performing the following functions:

- identification and capture of the risk information, which will be used as the input to the IRAS;
- analysis of the risk sources based on detected information;
- assessment of risks so as to calculate the risk grade;
- determine actions necessary to mitigating risk.

2 References

- [ITU-T E.106] Recommendation ITU-T E.106 (2003), *International Emergency Preference Scheme (IEPS) for disaster relief operations*.
- [ITU-T G.8001] Recommendation ITU-T G.8001 (2012), *Terms and definitions for Ethernet frames over transport*.
- [ITU-T Y.1308] Recommendation ITU-T Y.1308 (2004), *Ethernet UNI and Ethernet NNI*.
- [ITU-T Y.1910] Recommendation ITU-T Y.1910 (2008), *IPTV functional architecture*.
- [ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.
- [ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.
- [ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.
- [ITU-T Y.2234] Recommendation ITU-T Y.2234 (2008), *Open Service Environment Capabilities for NGN*.
- [ITU-T Y.2261] Recommendation ITU-T Y.2261 (2006), *PSTN/ISDN evolution to NGN*.
- [ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.
- [ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.