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

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/.

Table of Contents

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*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

3.1.1 application [ITU-T Y.2261]: A structured set of capabilities, which provide value added functionality supported by one or more services, which may be supported by an application programming interface (API).

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 application-to-network interface (ANI): An interface that results from the connection between an application and a network.

3.2.2 detection point (DP): The detection point, which is located in each service provider, network provider, and user terminal, is capable of collecting sophisticated metrics related to risk.

3.2.3 disaster surveillance sensor network (DSSN): The network that performs surveillance of disasters based on a sensor network.

3.2.4 network-to-network interface (NNI): An interface that results from the connection of two networks.

3.2.5 risk analysis function (RAF): The function that analyses and processes data from the risk search functional entity.

3.2.6 risk analysis functional entity (RAFE): The entity that performs identification, analysis and prioritization of risks which come from the risk search function.

3.2.7 risk analysis service (IRAS): The service that is implemented to facilitate the prevention or reduction of risk to which users or organizations subscribed to an NGN are exposed.

3.2.8 risk classification functional entity (RCFE): The entity that classifies the received risk events as being associated with either internal or external risk.

3.2.9 risk detection functional entity (RDFE): The entity that performs monitoring and tracing of risk relevant events from detection points.

3.2.10 risk mitigation functional entity (RMFE): The entity that is to prevent a risk and to reduce the impact of a risk incident.

3.2.11 risk search function (RSF): The function that is used to detect risk events that are obtained from the detection point.

3.2.12 risk service profile (RSP): The repository that stores the various risk patterns and the individual's user data.

3.2.13 service management function (SMF): The function that provides session management and controls the risk search function, risk service profile and risk analysis function.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

ANI Application-to-Network Interface

API Application Programming Interface

DP Detection Point

DSSN Disaster Surveillance Sensor Network

IRAS Risk Analysis Service

NGN Next Generation Network

NNI Network-to-Network Interface

NP Network Provider

RAF Risk Analysis Function

RAFE Risk Analysis Functional Entity

RCFE Risk Classification Functional Entity

RDFE Risk Detection Functional Entity

RMFE Risk Mitigation Functional Entity

RSF Risk Search Function

RSFE Risk Search Functional Entity

RSP Risk Service Profile

SMF Service Management Function

SNI System Network Interface

SP Service Provider

TE Terminal Equipment

UNI User Network Interface

5 Conventions

None.

6 Overview

The term "risk analysis service" means a service which is implemented to facilitate the prevention or reduction of risk to which users or organizations subscribed to an NGN are exposed. The risk analysis service classifies the risk into one of two types, viz. internal or external risk, as shown in Figure 6-1. Each of these types of risk is discussed below.

6.1 Internal risks

Internal risks are risks which are related to potential failures of the network provider, service provider or user terminal. These risks can be associated with items such as hardware failures, software errors affecting service features and integrity, network outages, data centre failures, network congestion, inefficient software code, inadequate capacity and malicious calls.

The risks related to the network provider are associated with network failures, network congestion, and inadequate network capacity or provisioning. Risks of this sort can be evaluated to determine their potential impact, e.g., causing transactions to be abandoned and reducing customer, partner and client satisfaction.

The risks related to the service provider are associated with incorrect or unreliable information such as insecure data, incorrect service contents, inadequate service data and malware. Service provider risks must also include the risk associated with the use of data that may be stolen. Risks of this sort can be evaluated to determine their potential impact: breach of client confidentiality and trust, loss of service availability, identity theft and theft of financial property.

The risks related to the user terminal are associated with the failure due to improper user fault, terminal loss and malicious operation. Risks of this sort can be evaluated to determine their potential impact: material losses, property damage and leakage of private information.

6.2 External risks

External risks are risks related or due to forces that are external to the network. External risks can be associated with items such as disasters like earthquakes, volcanoes, typhoons, tsunamis and floods, serious accidents such as fire, nuclear disasters, and attacks of various kind such as cyber attacks, security incidents and mass deception, as well as terrorist attacks on important facilities. Risks of this sort can be evaluated to determine their potential impacts: extent of potential physical damage to a network, extent of potential service loss and extent of potential loss of life and property.

6.3 Conceptual model for an IRAS function

Figure 6-1 shows a conceptual model for an IRAS function.

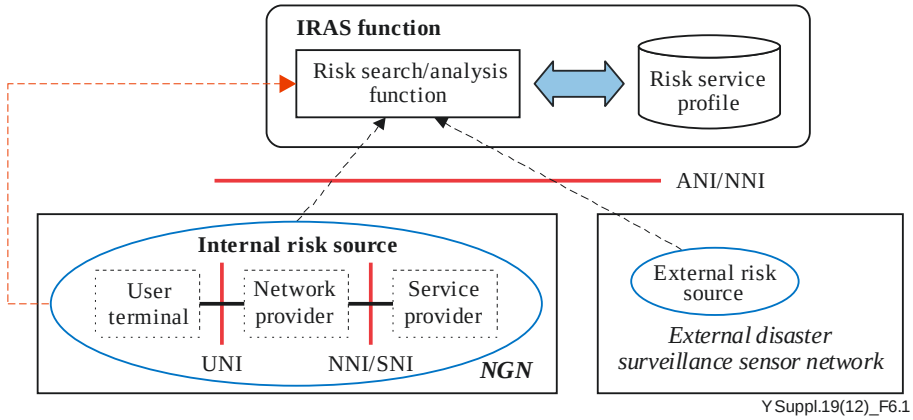

Figure 6-1 – Conceptual models of IRAS

The IRAS performs the following functions:

– detection of internal and external risk information, which comes from the internal and/or external environment;

– analysis of the obtained internal and external risk information and grouping of risk information into its various types and sources;

– evaluation of the risks associated with each risk category, which are network performance failures, user actions and terminal failures, service feature failures, security failures and disaster failures;

– generation of an assessment of all the risks to produce a resultant risk grade;

– use of the results of the risk assessment to propose an action plan on how to mitigate risk.

7 IRAS function

The IRAS function is intended to be implemented in networks whose operational frameworks are configured similar to those shown in [ITU-T Y.2012]. Figure 7-1 shows a functional model for the IRAS function.

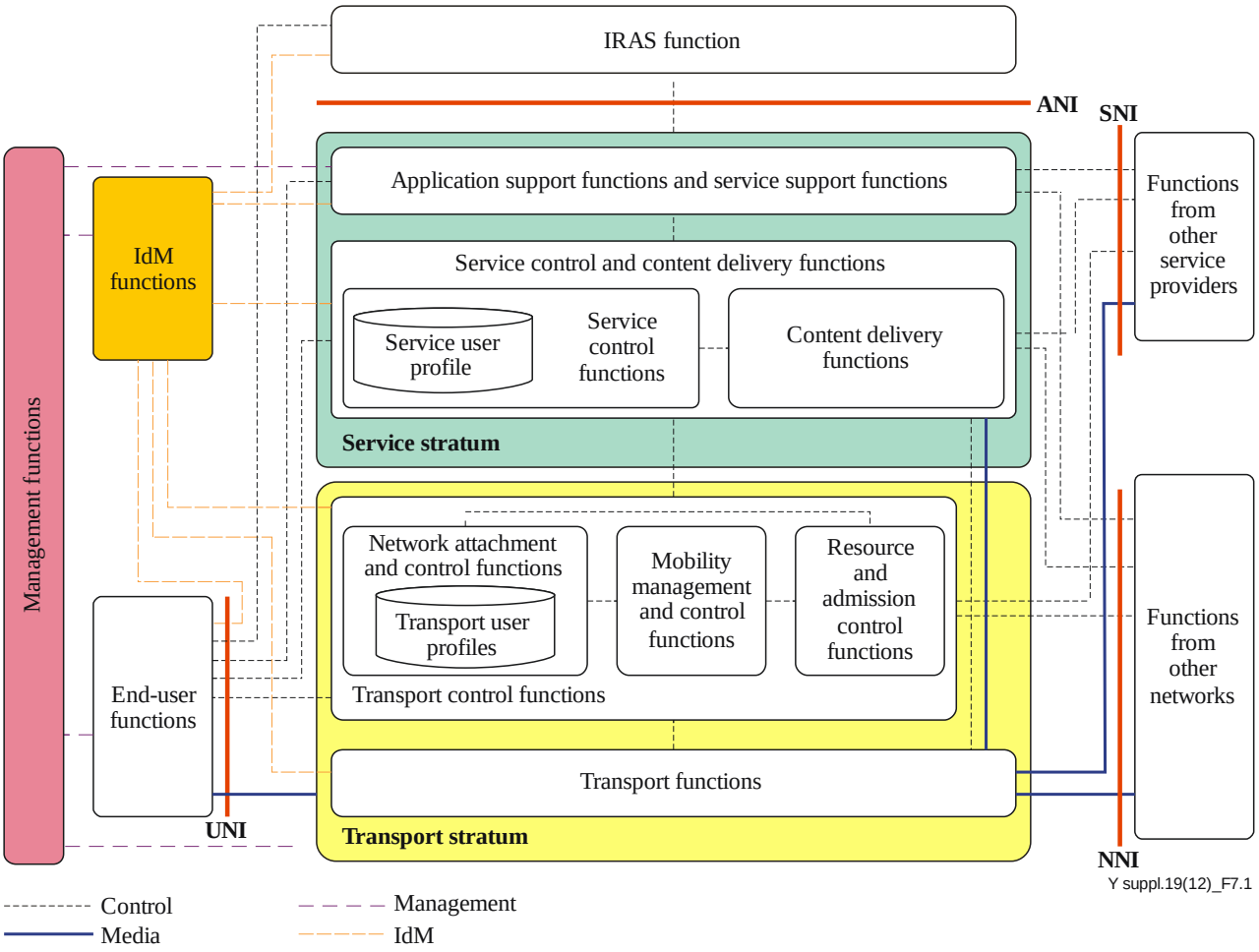

Figure 7-1 – Generic network IRAS functional model

The IRAS functions include detection points (DPs), risk analysis function(s), a risk search function(s), risk service profile(s) and a service management function(s). An IRAS may manage one or more domains and will collect measurement data from the detection points. The DPs of the service provider, network provider and users/terminals are considered to be located in the service provider's domain, network provider's domain, and users/terminals' domain, respectively. The DPs have capabilities that are a function of the domain in which they are located and thus DPs in different domains have different capabilities. Each DP collects information and measurement data from the domain in which it is located.

When risk data are received from a DP via an application support function which uses the NGN, the IRAS can start its analysis process. The IRAS can separate internal risk data from external risk data. Internal risk data are defined as data received from a DP that are received through an ANI, and possibly an UNI as well, but not through an NNI. On the other hand, external risk data are defined as data received from a DP that are received through an ANI as well as an NNI. The IRAS function model is presented in Figure 7-2.

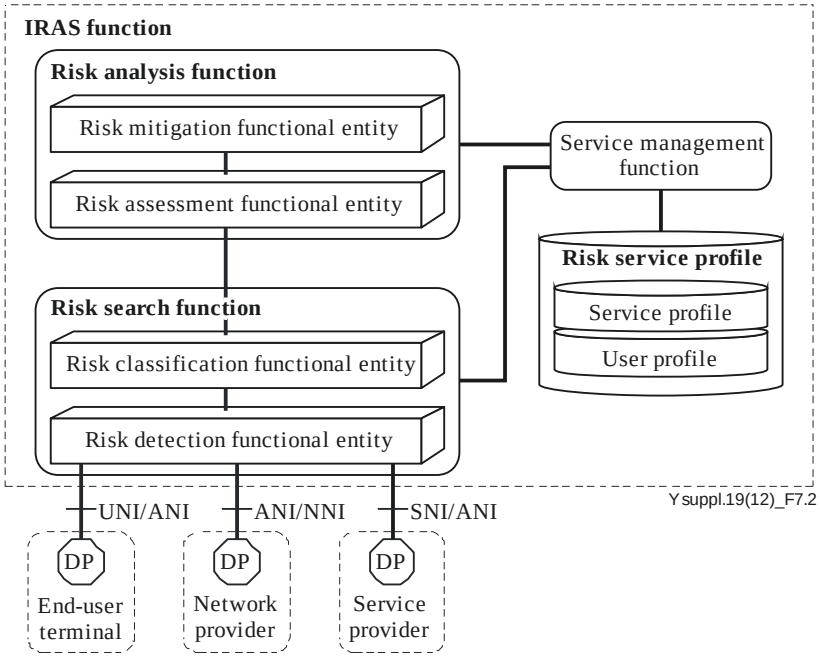

Figure 7-2 – IRAS functional model

The following clauses provide additional information about each of the IRAS functions.

7.1 Application service management function

The IRAS application service management function performs registration, deletion and information updates for both the service and users. It provides session management and controls the risk search function, risk service profile and risk analysis functions.

7.2 Risk search function

The IRAS risk search function (RSF), as shown in Figure 7-2, is used to detect risk events which are obtained from detection points. The search function should be able to categorize each risk event that is detected as being either an external or an internal risk. Some of the data generated by the RSF are provided to the risk analysis function (RAF), while the remainder are provided to the service management function (SMF). The RSF is considered to be composed of a risk classification functional entity (RCFE) and a risk detection functional entity (RDFE). Further information on each of these entities is provided in the following clauses.

7.2.1 Risk detection functional entity

The RDFE performs periodic monitoring and tracing of risk relevant events from DPs located in the network provider, service provider and user terminal domains.

7.2.2 Risk classification functional entity

The RCFE classifies the relevant received risk events as being either associated with external or internal risk.

7.3 Risk analysis function

The RAF analyses and processes data received from the RSFE and then passes the processed data to the SMF. Figure 7-3 shows the steps related to the performance of a risk analysis. The risk analysis function is considered to be composed of an RAFE and a risk mitigation functional entity (RMFE) as shown in Figure 7-2. Further information on each of these entities is provided in the following clauses.

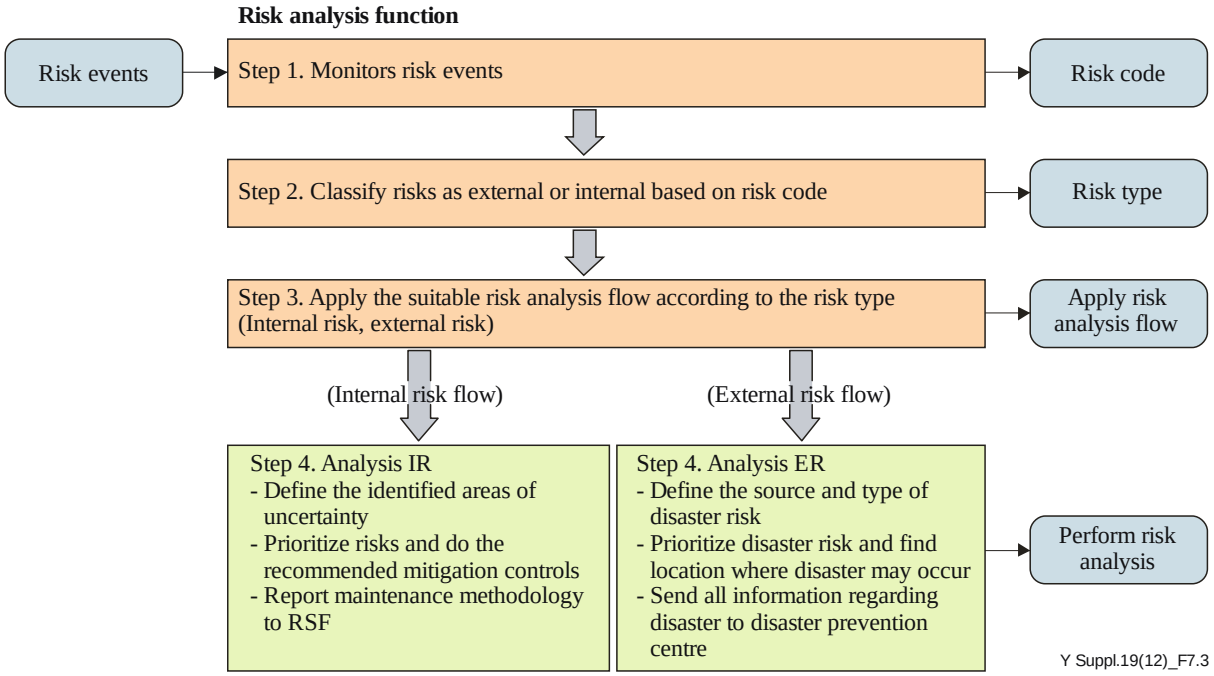

Figure 7-3 – Risk analysis service function

7.3.1 Risk assessment functional entity

The RAFE analyses and processes data from an RSF. It acts on the received data to perform three basic functions, viz. identification, analysis and prioritization of risk as follows.

- The role of the identification function is to identify the area of uncertainty/risk.
- The role of the analysis function is to define how the identified areas of uncertainty/risk could affect the user and organizations subscribed to the network.
- The role of the prioritization function is to prioritize the risks. Specifically, it identifies those risks that must be completely eliminated due to their extreme impact; those that are important enough to demand regular monitoring and review; and those that are deemed to have a minor impact. Risks that have minor impact do not require detailed monitoring. However, it should be recognized that just because risks could have a minor impact they should not be totally ignored, but rather they will require less attention than those risk events/situations that could have greater impact.

7.3.2 Risk mitigation functional entity

The RMFE receives data from the RAFE, which has already prioritized the risk. This mitigation function is now required to evaluate the data and identify a set of actions which would result in mitigating the risk. Risk identification, analysis and prioritization are only beneficial if actions are defined and executed to mitigate the risk. This Supplement does not address the execution of actions to eliminate risk. Risk mitigation actions must be defined individually for each risk. In some cases, immediate action is recommended. Mitigation actions are intended to be proactive so as to prevent a risk from becoming a risk incident and impacting the user and organization subscribed to network or so as to reduce the impact of a risk incident. Risk can be mitigated not only by eliminating the events or situations that contribute to risk but also by reducing the probability of risk associated with certain events or situations. Accordingly, risk mitigation can be divided into risk elimination and risk reduction functions.

Risk elimination requires carrying out the actions necessary to completely remove the events or situations that contribute to risk. Therefore, a risk would no longer be considered during a risk assessment subsequent to its mitigation.

Risk reduction, on the other hand, does not completely remove the events or situations that contribute to risk but it does cause the impact of the risk event to be reduced.

Risk mitigation activity, if invoked at an early stage, will reduce the likelihood of the technology environment causing a problem, as risk-contributing factors will have been addressed prior to the risk-related events actually occurring.

7.4 Risk service profile

The risk analysis service stores the various risk patterns based on risk state information derived from past communications. It should be updated periodically with the most recent information. Risk state information generally describes whether the event data are part of a new service or part of a continuing service. Risk states could include the state of network performance, user actions and terminal performance, and service features.

The risk service profile stores the individual's user data which is the user ID, password, user preferences, the status of sessions by log-in services to be used, connection status and duration and device types, including model number(s) and terminal attributes that have been activated.

8 Execution of IRAS functions

Users subscribed to a network provider who wish to avail themselves of an IRAS will have to register their attributes via an application service management function and be authorized by an IRAS identification and authentication procedure. After registration, users will have the opportunity to use a service application that can perform a risk analysis. Figure 8-1 presents a functional model for execution of IRAS functions when the IRAS is invoked by a user device.

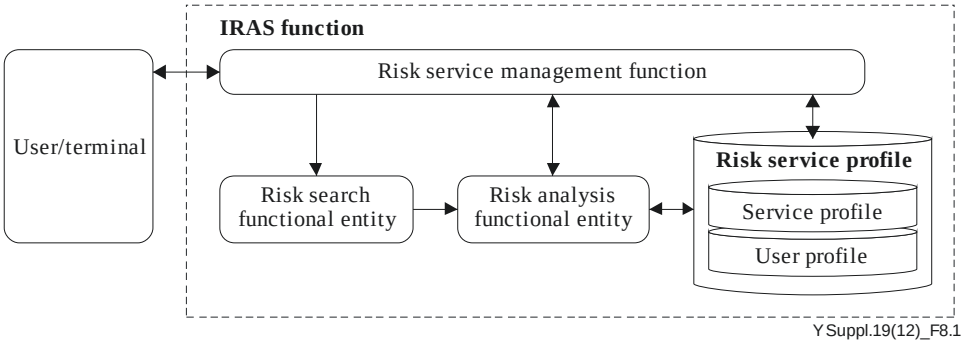

Figure 8-1 – Functional model for an execution function when the IRAS is invoked by a user terminal

8.1 Risk analysis service and user registration

8.1.1 User registration

The user inputs his/her ID number and password, and other prerequisite information for registration into an IRAS function according to an established registration procedure. The IRAS automatically checks to see if this registration could be authorized. If the received information is valid, the user is registered into the IRAS risk service profile. The user entity function models a user. The user model record has many attributes and properties one would expect of a user, such as name, address and ID. IRAS can add IDs and passwords as well as update them – and even delete registered users.

8.1.2 Risk analysis service registration

The registration process of a risk analysis service is executed by the application service management function. The IRAS service management function registers the service and when doing so enforces the collection of information that is required to complete the registration process.

In particular, it captures the relevant information about a service such as the service code, service type and service name. The IRAS service management function can perform 'add service', and 'delete service' functions to registered services.

8.2 Log-in session process

The user executes an IRAS log-in process by entering a user ID and password. The session log-in process checks the identification and authenticates the user and makes the requested service available to the authorized user. Once the user is authorized to use the service, the application service management function provides the risk analysis service to the authorized user.

8.3 Risk analysis service execution

Risk analysis service is executed in the risk analysis function by the application service function management. When the risk event information is received from a DP, the risk analysis function starts to analyse it and evaluates the likelihood of the risk and impact of the risk, should the risk event occur. Risk can be categorized as being one of the following types.

– High likelihood and high impact: These are critical risk events that are likely to occur and which would have severe material impact if/when they do occur.

– Low likelihood and high impact: These are significant risk events that are not likely to occur but which would have severe material impact if/when they do occur.

– High likelihood and low impact: These are critical risk events that are likely to occur and which would not have a significant material impact to the user if/when they do occur.

– Low likelihood and low impact: These are risk events that are unlikely to occur and which would not have a significant material impact to the user if/when they do occur. It is suggested that although these risks should be monitored to ensure that they do not change category, the effort devoted to monitoring should be proportionate to their likelihood of occurrence and impact.

Once the evaluation of the risk event information is completed, it is possible to initiate the risk mitigation service. The risk mitigation service identifies the risk and suggests the proper action to be taken.

9 Risk analysis service procedure

9.1 General risk analysis service procedure

Risk events caused by users/terminals, network providers and service providers connected to the network can be identified as internal risk sources, whereas those caused outside the network (such as natural disasters) can be identified as external risk sources. If a risk event is detected by a risk search function (RSF), it is classified as either internal or external risk. The RSF is considered to exist in the risk search functional entity (RSFE). The RSF delivers the information about the risk event to the risk analysis function (RAF). The RAF is considered to exist in the risk analysis functional entity (RAFE). The information flows and actions associated with a risk analysis service procedure are depicted in Figure 9-1.

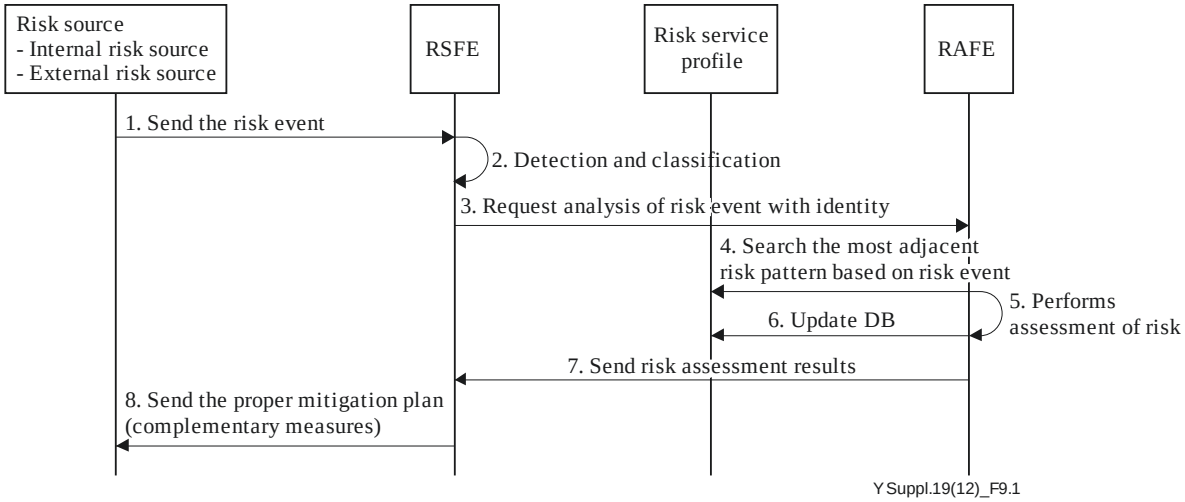

Figure 9-1 – Information flows and actions associated with a risk analysis service procedure

The information flows and actions related to the risk analysis service procedures are as follows.

1) The DP detects a risk event and sends it to the RSFE.
2) The RSFE detects the risk event from the DP and immediately classifies it as an internal or an external risk.
3) The RSFE requests analysis from the RAFE.
4) The RAFE searches the most adjacent pattern stored in the service profile with the risk data.
5) The RAFE performs an assessment using the most adjacent pattern to be searched.
6) The RAFE updates the data currently stored in the risk service profile.
7) The RAFE reports the analysis results to the RSFE
8) The RSFE sends the proper mitigation plan.

9.1.1 Risk assessment function procedure

The risk assessment function procedure is the process used to determine the likelihood of risks. The results obtained from this procedure will help identify appropriate measures for reducing or eliminating risk. The various phases associated with a risk assessment function procedure are shown in Figure 9-2. The risk assessment procedure encompasses the following phases.

Phase 1 – Characterization of risks: This phase defines the scope of the risk assessment and the boundaries of risk, which provides information regarding the type and sources of risk to be characterized. Internal risks are risks to network performance, hardware, software and security, which are acquired from the user terminal, network provider and service provider. External risks are disasters – natural risks which result from flooding, high winds, severe storms, tornados, fires, snow storms, etc.

Phase 2 – Risk source recognition: This phase identifies a threat location that has the potential of being a particular risk source. A risk source does not present a risk when there is no vulnerability that can be exercised. Risk source recognition involves identifying potential risk sources and compiling a risk statement, which lists the potential threat sources that are applicable to the application service being evaluated. A risk source is defined as an event point or threat location.

Phase 3 – Vulnerability recognition: This phase identifies whether vulnerabilities are present, whether they vary depending on the nature of risk source and type such as unauthorized users, system failure and natural disaster. The technical and non-technical vulnerabilities associated with an application service environment can be identified via information gathering techniques, which gather information from internal and external risk sources.

Phase 4 – Likelihood decision: This phase determines an overall likelihood rating that indicates the probability that a potential vulnerability, due to a risk source, may be exercised within the construct of the associated threat environment. The governing factors that should be considered include the threat risk source motivation and capability, nature of the risk and existence and effectiveness of current service controls. The likelihood that a potential vulnerability could result from a found-risk source type can be described as high, medium or low.

Phase 5 – Risk impact analysis: This phase determines the adverse impact resulting from a risk source. An impact analysis can identify the anticipated impact level such as high, medium and low based on a qualitative and/or quantitative assessment of the sensitivity and criticality. The assessment identifies and prioritizes sensitive and critical information.

Phase 6 – Risk determination and assessment: This phase assesses the level of risk resulting from internal and external risk sources, and determines if the level of risk is acceptable. The determination of impact for a particular risk and vulnerability can be expressed as a function of the likelihood of threat sources. The magnitude of the impact should be estimated by exercising the vulnerability and the adequacy of plans for reducing or eliminating the risk.

Phase 7 – Risk mitigation and removal: This phase identifies an action plan that could be implemented to eliminate risk or decrease risk to an acceptable level, with minimal adverse impact on the user's resources.

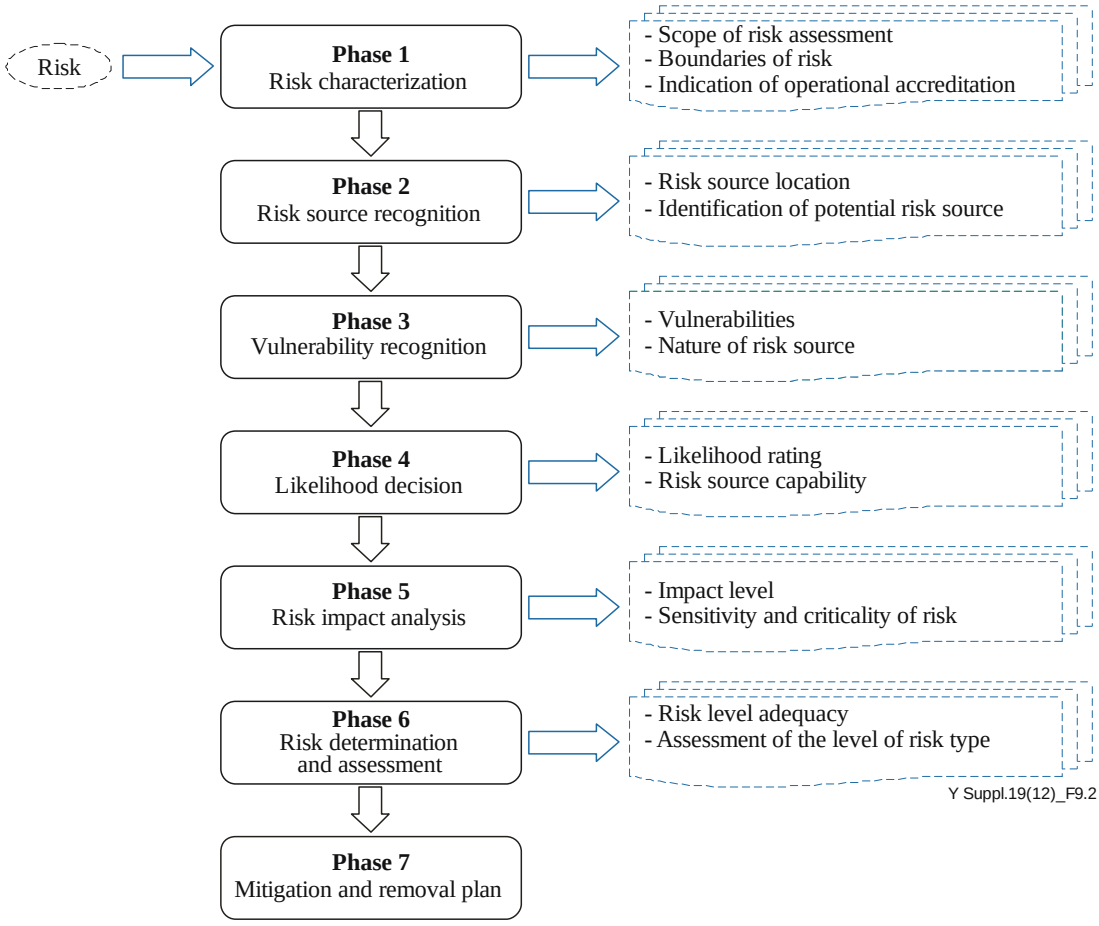

Figure 9-2 – Risk assessment phase

9.1.2 Risk mitigation service

The risk mitigation service takes proactive measures to eliminate risk or to reduce risk so as to either prevent risk events from occurring or to reduce the impact of risk events. Risk identification, analysis and prioritization are only beneficial if actions are defined and executed to mitigate risk. Risk mitigation actions must be defined individually for each risk. Risk mitigation should not be confused with counter measures. Risks can be mitigated not only by risk removal but also by reducing the degree of risk occurrences to users or organizations subscribed to the network. Risk mitigation and removal services involve prioritizing, evaluating and implementing the appropriate risk-reducing and risk removal actions recommended from the risk assessment process. The various phases associated with a risk mitigation service flow are shown in Figure 9-3. The risk mitigation service encompasses the following phases.

Phase 1 – Prioritizing risk rank: This phase uses information obtained from the risk assessment reports and the application prioritizes the needed actions based on the risk assessment results. Top priority should be given to addressing risk items having the highest rank.

Phase 2 – Evaluating feasibility and effectiveness of control options: This phase evaluates the control options recommended in the risk assessment process, as they may not be the most appropriate and feasible options for a specific user or organization. The objective is to select the most appropriate control option for minimizing risk.

Phase 3 – Selecting control options: In this phase the risk analysis function determines the most effective control for reducing risk by selecting the most appropriate control option produced during phase 2.

Phase 4 – Developing mitigation plan: In this phase the action plan is developed.

Phase 5 – Action mitigation plan: This phase involves carrying out the developed control actions associated with the mitigation plan. Depending on the individual situation, the implemented controls may eliminate the risk or lower the risk level but not eliminate it.

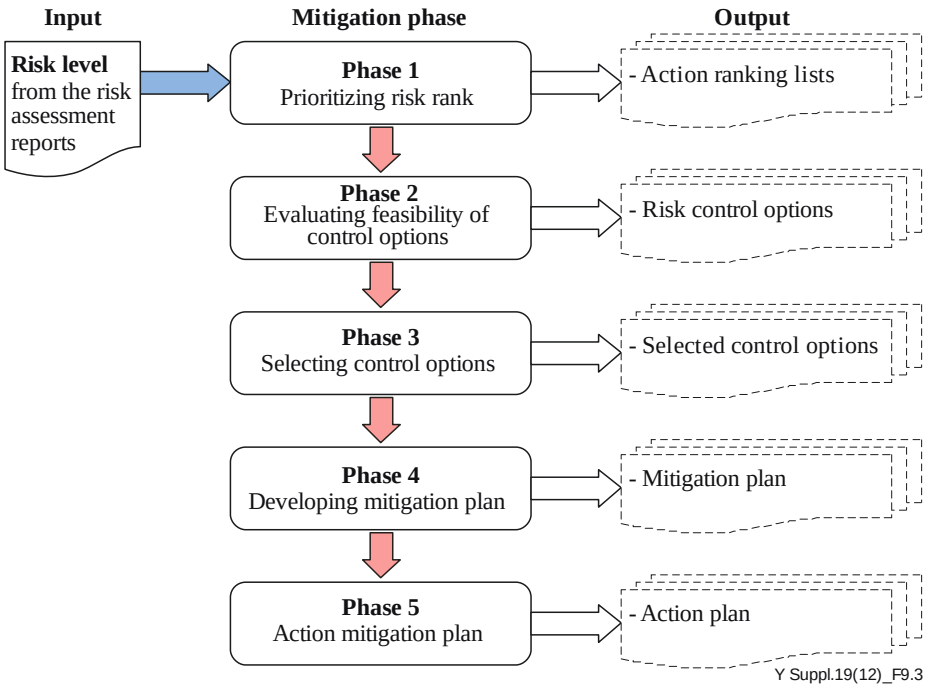

Figure 9-3 – Risk mitigation service flow

10 Service scenarios

Service scenarios for external and internal risks are presented in this clause. The service scenario for external risks includes consideration of earthquakes, volcanic disasters, typhoons, tsunamis, floods and serious accidents such as large fires. The service scenario for internal risks includes consideration of phishing, lost terminals, user operation failures, network failures, delayed service and malicious operation. The procedures associated with the external and internal risk analysis service scenarios are shown in Figures 10-1 and 10-2, respectively.

10.1 Service scenario related to external risks

In this service scenario related to external risks the IRAS identifies risks from messages that are generated by a DP and which then pass via a network, connected to disaster prevention centre, and across an NNI and an ANI. The procedures associated with the external risk analysis service scenario are pictorially presented in Figure 10-1.

The information flows and actions related to the external risk analysis service scenario via an external network such as a disaster surveillance sensor network (DSSN) is as follows.

1) The external sensor network initiates a registration request to the IRAS.
2) The IRAS places the registration information into the risk service profile.
3) The IRAS sets up the risk analysis service.
4) The IRAS sends an 'acknowledge' signal to the DSSN.
5) The IRAS monitors the risk event via the risk analysis service support function.
6) It generates the external risk.
7) The IRAS executes an analysis of detected risk.
8) The IRAS sends an appropriate mitigation actions plan to the DSSN.
9) The DSSN takes appropriate measures based on the mitigation actions plan proposed by the IRAS.
10) The DSSN reports action results to the IRAS.

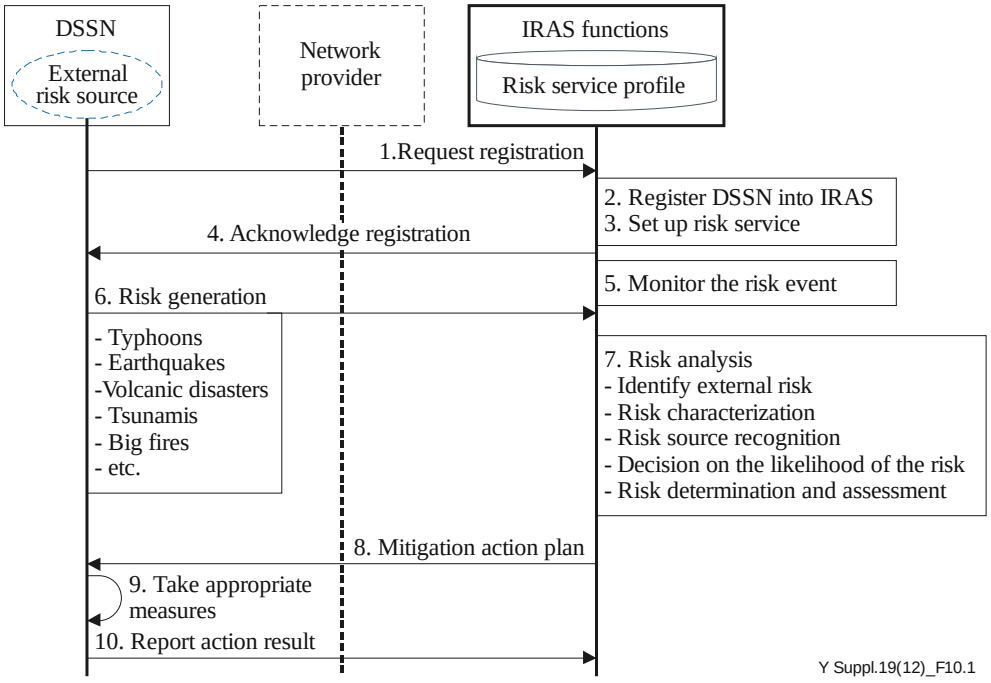

Figure 10-1 – External risk analysis service scenarios

10.2 Service scenario related to internal risks

In this service scenario related to internal risks, the IRAS identifies risks from messages that are generated by a DP and across an ANI. The procedures associated with the internal risk analysis service scenario are pictorially presented in Figure 10-2.

The information flows and actions related to the internal risk analysis service scenario are as follows.

1) The user initiates a registration request to the IRAS.
2) The IRAS places the registration information into the risk service profile.
3) The IRAS sets up the risk analysis service.
4) The IRAS sends an 'acknowledge' signal.
5) The IRAS periodically monitors the risk event via the risk analysis service support function.
6) It generates the internal risks.
7) The IRAS executes an analysis of detected risk.
8) The IRAS sends an appropriate mitigation action plan to the internal source.
9) The internal source takes appropriate measures based on the mitigation action plan proposed by the IRAS.
10) The internal risk sources (terminal errors, network provider, service provider) report action results to the IRAS.

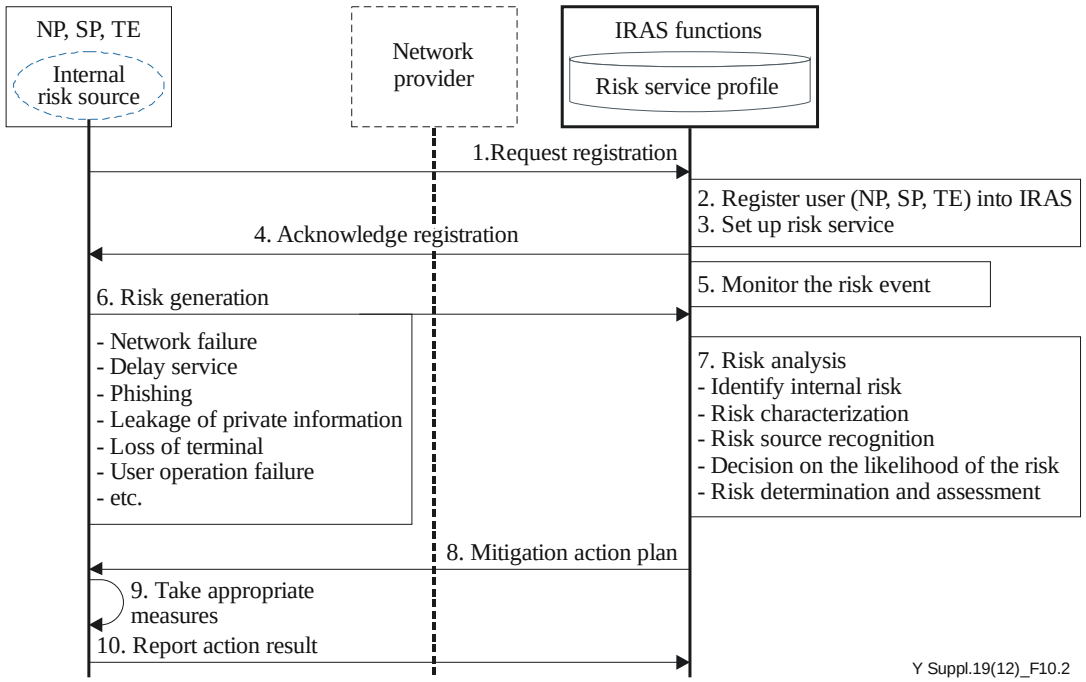

Figure 10-2 – Internal risk analysis service scenarios

11 Security consideration

While no specific guidance is provided in this Supplement in regards to security, implementers of an IRAS should be aware of the security considerations provided by [ITU-T Y.2701] and [ITU-T Y.2702].

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, 2013