

Standardizations on IT Risk analysis service in NGN

Heechang Chung*, **Sok Pal Cho, Yongseon Jang *

*NIA, Bldg 77, Mugyo-Dong, Jung-Gu, Seoul, Korea,

** Sungkyul University-ro 53, Manan-gu, Anyang-si, Korea

heechang@nia.or.kr, spcho@sungkyul.edu, jangys@nia.or.kr

Abstract—Information technology (IT) risk analysis service is a service which is capable of identifying risk, assessing the risk, and then invoking process which can identify the proper actions which should be taken to reduce damage that could affect users or organizations subscribed to an Network. Provided that a risk situation exists, the risk analysis function performs the analysis and assessment of the risk event data with an algorithm which applies the most recent pattern according to procedures, and reports the analysis results and the proper complementary measures which, if invoked, will reduce risk.

Keywords—IT risk analysis, internal risk, external risk, Identifying risk, assessing risk, mitigation risk

I. INTRODUCTION

The information technology(IT) risk service must contend with internal risks, which are risks related to potential network providers, service providers, and user/terminal failures, and with external risks, which are risks related to forces external to the network. Internal risks can be associated with such items 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 such items as disasters resulting from –earthquakes, typhoons, tsunamis and floods. An invoked IT risk analysis service will identify proper actions to take reduce risk and, which if taken, would reduce the risk of critical NGN service failures. Failure to invoke an IT risk service, especially one that can deal with risk sources, could result in serious events which could affects users subscribed to NGN.

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

- Analysing the risk sources based on detected information
- Assessment of risks so as to calculate the risk grade
- Determine actions necessary to mitigating risk.

II. GENERAL FUNCTION OF IT RISK

The risk analysis service classifies the risk into one of two types, viz. internal or external risk, as shown in figure 1. Each of these types of risks is discussed below.

1. Conceptual model for Internal risks and External risks

Internal risks are risks which are related to potential network provider, service provider, and user terminal failures. These risks can be associated with such items as hardware failures, software errors affecting service features and integrity, network outages, data centre failures, network congestion, inefficient software code, inadequate capacity, malicious calls. External risks are risks which are related or due to forces that are external to the network. External risks can be associated with such items as disasters which are earthquake, volcanoes, typhoons, tsunamis and flood, serious accident such as fire, nuclear disasters, and attacks of various kind such as cyber-attack, security incidents, and mass deception, and terrorist attacks on important facilities. Risk of this sort can be evaluated to determine their potential impacts which are extent of potential physical damage to a network, extend of potential service loss, and extent of potential loss of life and property.

Figure 1 below shows a conceptual model for an IRAS function.

2. IRAS Function

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 which 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.

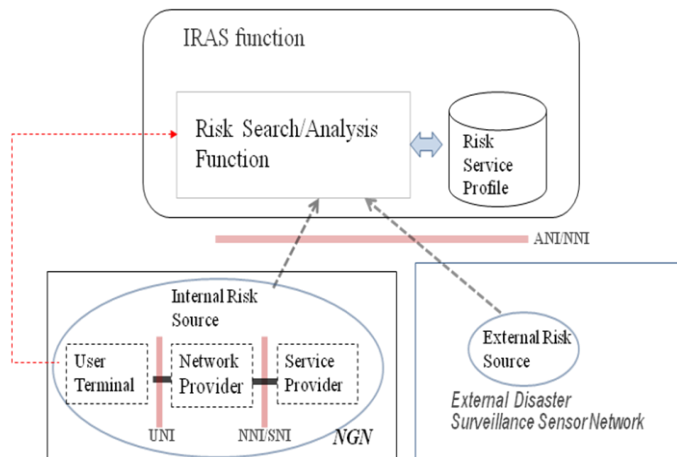


Figure 1 Conceptual models of IRAS.

When risk data is 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 is defined as data received from a DP which is received through an ANI, and possibly a UNI as well, but not through an NNI. On the other hand external risk data is defined as data received from a DP which is received through an ANI as well as an NNI. The IRAS function model is presented in Figure 2 below.

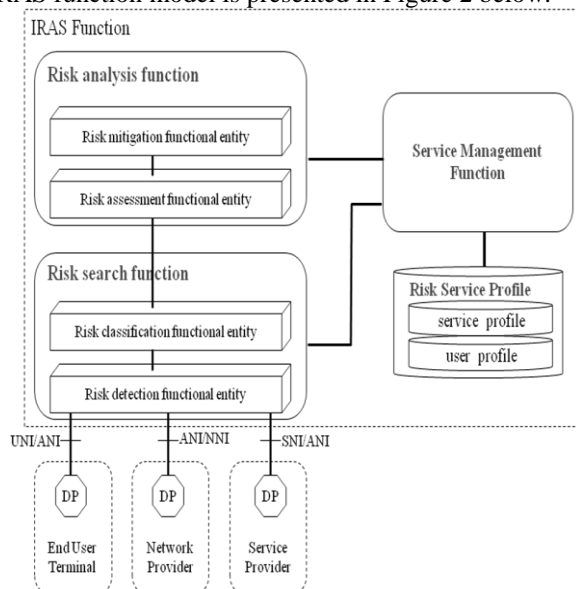


Figure 2 IRAS functional model.

3. General risk analysis service procedure

Risk events caused by users /terminals, network providers, and service providers connected to network can identified as internal risk source, whereas those caused by the outside network such as disaster can be identified as external risks source. If a risk event is detected by a risk search function (RSF), it is classified whether it is internal or external risk. The RSF is considered to exist in the risk search function 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 3.

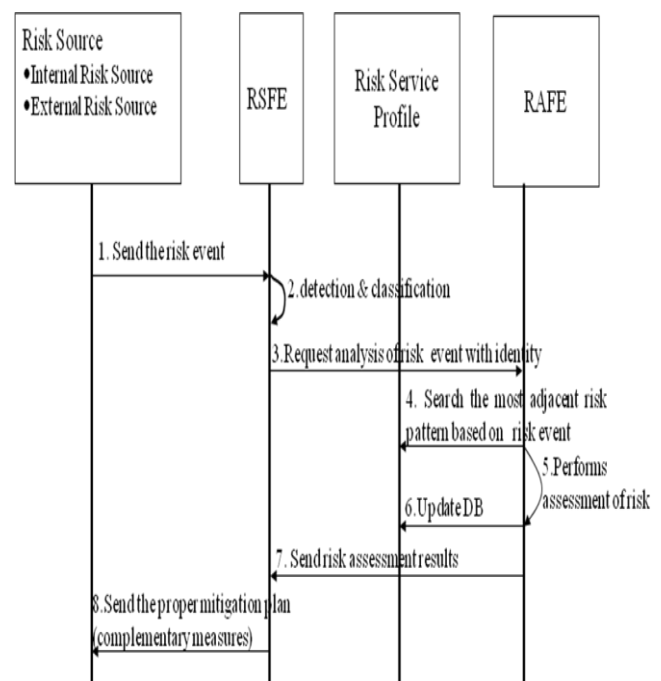


Figure 3 Information flows and actions associated with a risk analysis service procedure.

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

- 1) The DP detects a risk event and send it to the RSFE
- 2) The RSFE detects the risk event from DP and immediately classifies it whether it is an internal or an external risk.
- 3) The RSFE requests analysis to 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 send the proper mitigation plan.

III. CONCLUSIONS

The risk analysis service must contend with internal risks, which are risks related to potential network providers, service providers, and user/terminal failures, and with external risks, which are risks related to forces external to the network. Internal risks can be associated with such items 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 such items as disasters resulting from – earthquakes, typhoons, tsunamis and floods. An invoked risk analysis service will identify proper actions to take reduce risk and, which if taken, would reduce the risk of critical 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 affects users subscribed to NGN.



(1986~1999,KT and STI)

Yongseon Jang received B.S degree from Kyungpook National University, Korea in 1986, M.S degree from Hanyang University, Korea in 2001. He has worked for planning Korea's BcN(Broadband converged Network) project and developed services in rural areas (2010-2013). and worked for KII(Korea Information Infrastructure) Project (2010-2005). He was in charge of communication network planning and services, optical transmitting systems and mobile networks

REFERENCES

- [1] [ITU-T Y.2011] Recommendation ITU-T Y.2011 (10/2004) General principles and general reference model for Next Generation Networks
- [2] [ITU-T Y.2012] Recommendation ITU-T Y.2012 (09/06) Functional requirements and architecture of next generation networks
- [3] [ITU-T Y.2201] Recommendation ITU-T Y.2201 (09/2009) *Requirements and capabilities for ITU-T NGN*
- [4] [ITU-T Y.2234] Recommendation ITU-T Y.2234 (09/2008) *Open Service Environment Capabilities for NGN*
- [5] [ITU-T Y.2261] Recommendation ITU-T Y.2261 (09/2006) *PSTN/ISDN evolution to NGN*
- [6] [ITU-T Y.2701] Recommendation ITU-T Y.2701 (04/207) *Security requirements for NGN release 1*
- [7] [ITU-T Y.2702] Recommendation ITU-T Y.2702 (09/208) *NGN authentication and authorization requirements for NGN release 1*
- [8] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) [b-ITU-T E.106] Recommendation ITU-T E.106 (03/2000) Description of an international emergency of preference scheme (IEPS)



Heechang Chung received B.S degree from Korea University, Korea in 1980, M.S and P.H degree from Aju University, Korea in 1989 and 1997. He was a principal researcher at ISDN Center, ETRI from April 1980 to November 2000. His current research interests include future service management, service creation and standardization. Currently he is a special fellow in NIA, a Rapporteur in ITU-T SG13 Standardization.



Sok Pal Cho received a Ph.D.(1992) from the Kyung Hee University, Seoul Korea. He was a computer system engineer at Control Data Corp. since 1976. He was a senior researcher at R&D Center, Sam Sung Co., from April 1984 to February, 1994. He was an assistant professor in the Division of Information and Data Communication at Nam Seoul University, Korea in 1994. He joined the department of Computer Communication Engineering, the Sungkyul University,

