Risk Analysis Methodology for New IT Service

IT Infrastructure Protection Division
IT Infrastructure Protection Planning Team
Korea Information Security Agency

KISA 한국정보보호진흥원
Korea Information Security Agency

Content

◆ Related research

- Analyses of major domestic and foreign risk analysis techniques
- ITU-T X.805

◆ New IT service information protection risk management methodology

- **Proposed frame of the methodology**

◆ Example

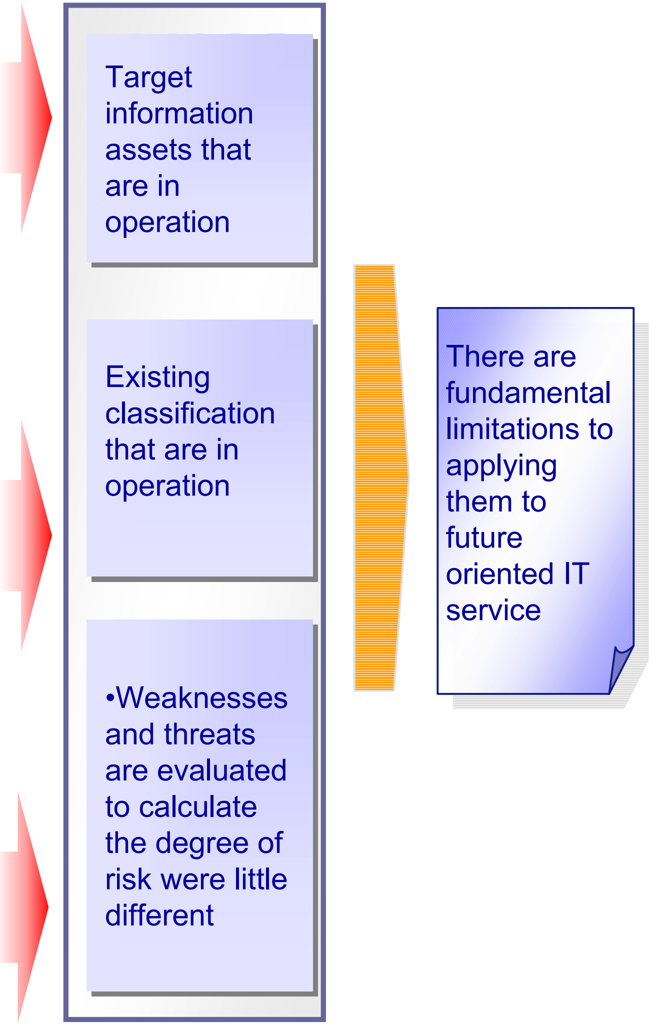
- BcN VoIP Service

◆ Conclusion

- **Concept, characteristics & advantages of the methodology being presented**

Analyses of major domestic and foreign risk analysis techniques

Methodology	NIST	GMITS	BS7799	CSE	OCTAVE	KISA
Classification of assets	■hardware ■software ■system interphase ■information & data ■human ■system	■information & data ■hardware ■software ■telecommunications equipment ■palmware ■documents ■capital ■manufactured products ■service ■confidence and trust in service ■environmental equipment ■manpower ■organization image	■information ■software ■physical equipment ■service ■documents ■human ■company image, reputation	■information ■process ■platform ■interface ■human ■environment ■material asset ■immaterial asset	■information ■system ■software ■hardware ■human	■information & data ■documents ■hardware ■software
Classification of weaknesses	-	■environment and basic facilities ■hardware ■software ■telecommunications ■documents ■human ■general weaknesses	■employee security ■physical environment security ■management of computer & networks ■Maintain system access control & development	■external ■systems ■Objects ■manpower	■server ■network ■security system ■desktop ■PC ■notebook ■storage device ■wireless LAN, mobile phone ■etc	■Management ■policy, organization, human resources ■building, facilities, etc. ■Technical
Classification of threats	■threat from nature ■threat from humans ■consideration of intention of threat ■threat from environment	■planned ■coincidental ■environmental ■human	■'infected/bad' software not allowed to access the system or network ■software operation malfunction ■Sending of not allowed message ■re-sending of message by 3rd party ■fire ■burglar ■employee mistake	■non-human ■ random (navure) ■planned (human) ■Artificial ■Internal ■External	■human ■System ■Hardware ■software ■Etc ■natural disaster ■communication obstacle ■physical environmental obstacle	■Executor ■Human ■non-human ■access route ■Network ■phical ■Intention ■Coincidence ■intentional ■result of damage ■Change ■Vulnerability ■Destruction ■Inturruption
Calculation method of degree of risk	■standard matrix for calculating degree of risk ■Asset → frequency of threat → severity of threat → level of threat	■standard matrix for calculating degree of risk ■Asset → weakness → threat → degree of risk	■standard matrix for calculating degree of risk ■Asset → weakness → threat → degree of risk	■scenario of threat ■Asset -> threat (motive, ability to execute) -> weakness (severity, vulnerability) -> degree of risk	■risk evaluation standard established by situation ■Important assets->threat profile->weakness ->threat (degree of damage, frequency of threat)	■standard matrix for calculating degree of risk ■Asset → weakness → threat → degree of risk



Target information assets that are in operation

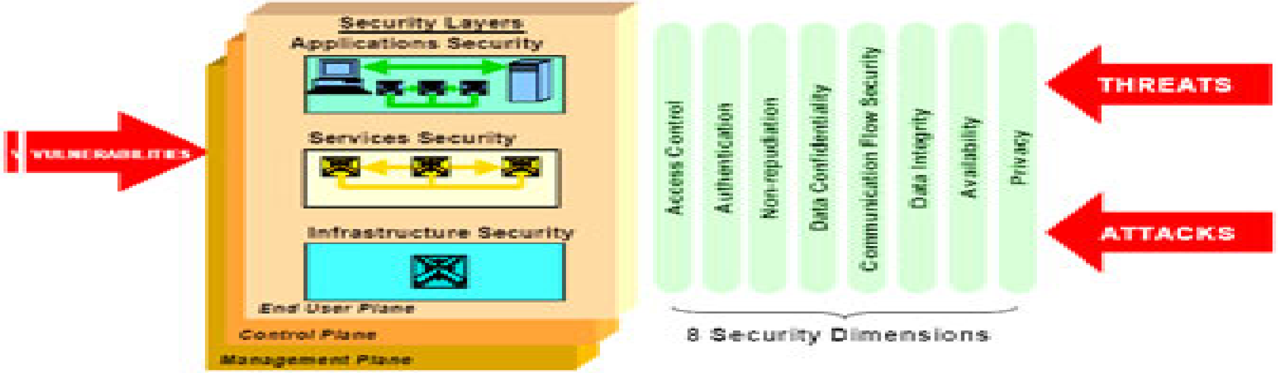
Existing classification that are in operation

•Weaknesses and threats are evaluated to calculate the degree of risk were little different

There are fundamental limitations to applying them to future oriented IT service

ITU-T X.805

ITU-T X.805

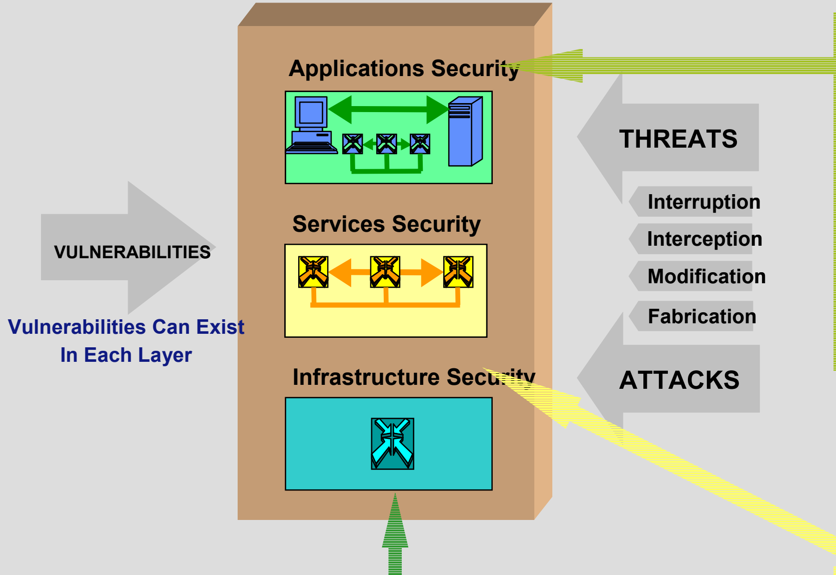


	Infrastructure Layer	Service Layer	Application Layer
Management Plane	Module One	Module Four	Module Seven
Control Plane	Module Two	Module Five	Module Eight
User Plane			

Module 2: Infrastructure Layer, Control Plane

Security Dimension	Security Objectives
Access Control	Ensure that the network device will only accept control information messages from authorized network devices
Authentication	Verify the identity of the person or device observing or modifying control information resident in the network device.
Non-repudiation	Provide a record identifying each individual or device that observed or modified control information in the network device and the action that was performed. This record can be used as proof of access to or modification of the control information.
Data confidentiality	Protect control information resident in a network device or in offline storage from unauthorized access or viewing
Communication Flow Security	Ensure that control information being transported across the network only flows between the source of the control information and its desired destination. The control information is not diverted or intercepted as it flows between these endpoints
Data Integrity	Protect control information resident in network devices, in-transit across the network, or stored
Availability	Ensure that network devices are always available to receive control information from authorized sources
Privacy	Ensure that information that can be used to identify the network device or communications link is not available to unauthorized personnel or devices

ITU-T X.805 Security Layers



Applications Security Layer:

- Network-Based Applications Accessed by End-Users
- Includes:
  - Fundamental Applications (e.g., Web Browsing)
  - Basic Applications (e.g., Directory Assistance and Email)
  - High-End Applications (e.g., E-Commerce)

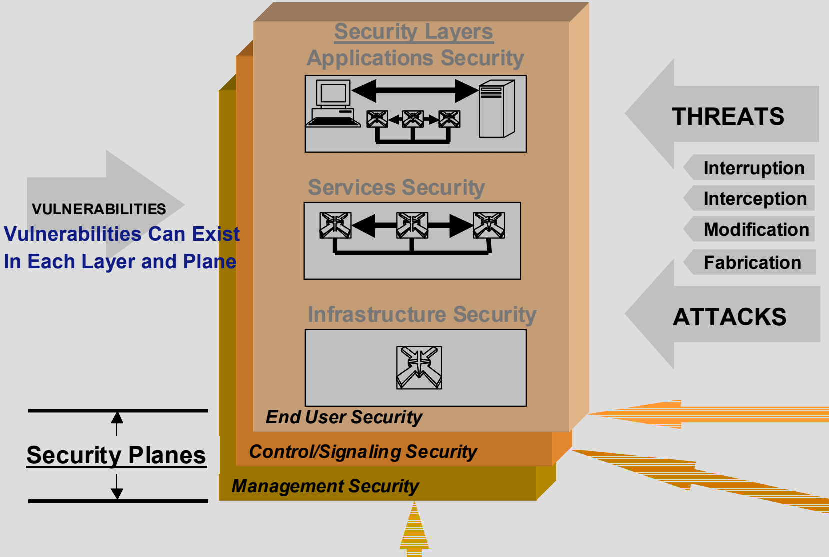
Infrastructure Security Layer:

- Fundamental Building Blocks of Networks, Services, and Applications.
- Individual Network Elements and the Interconnecting Communications Facilities
- Examples:
  - Individual Routers, Switches, Servers
  - Point-to-Point WAN Links
  - Ethernet Links

Services Security Layer:

- Services Provided to Customers or End-Users
- Range from Basic Transport to High-End, Value-Added Services.
- Examples:
  - Carrier Facilities (DS-1, DS-3, etc.)
  - Frame Relay, ATM, IP Connectivity
  - VoIP, QoS, IM, Location Services
  - 800-Services

ITU-T X.805 Security Planes



End-User Security Plane:

- How Customers Access and Use the Network
- Represents End-User Data At Rest and In Motion
- End-Users May Use the Network For:
  - Basic Connectivity/Transport
  - Value-Added Services (VPN, VoIP, etc.)
  - Access to Network-Based Applications (e.g., Email).

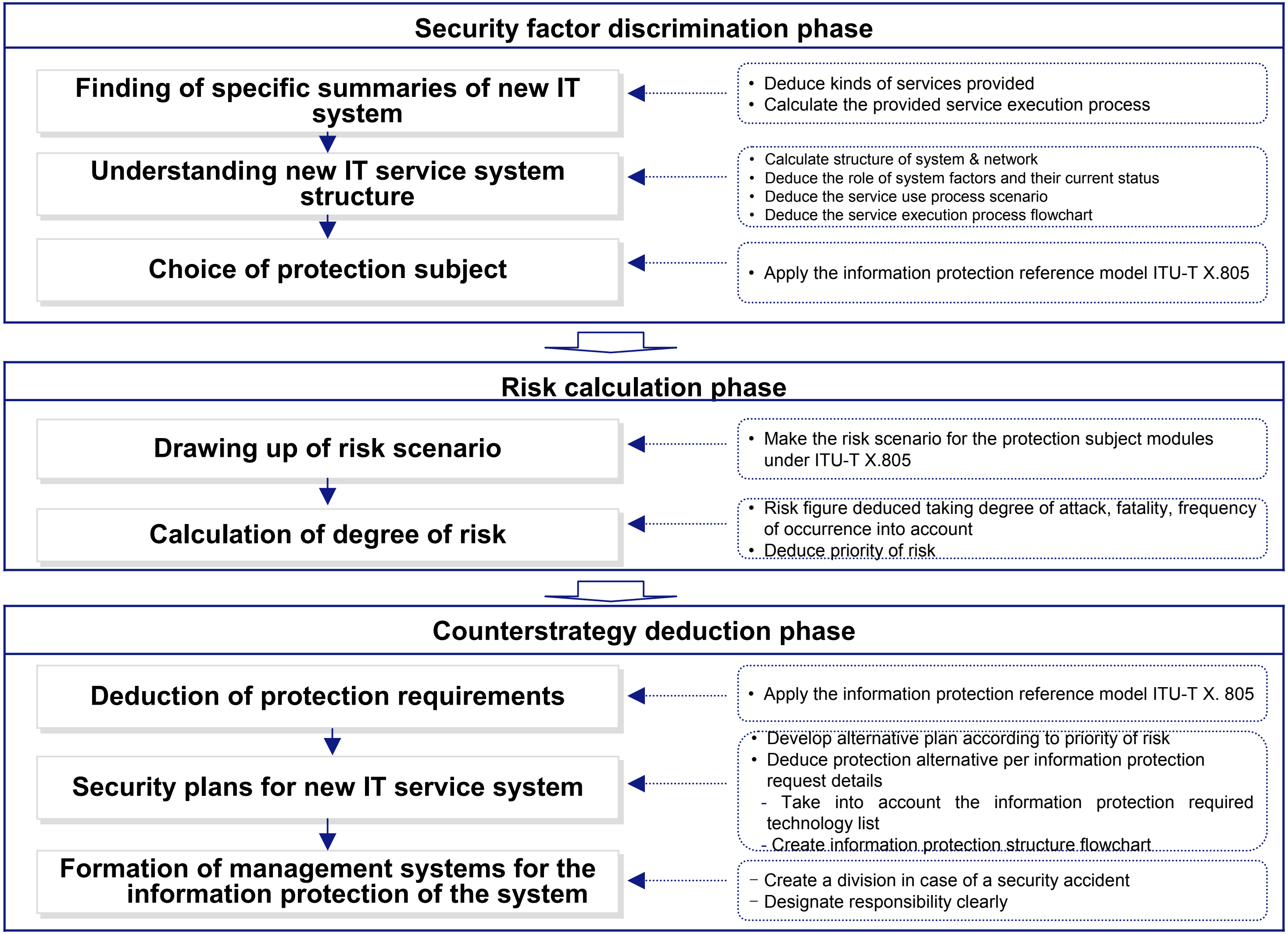
Management Security Plane:

- Concerned with OAM&P of Network Elements, Transmission Facilities, Operations/Business Systems
- Concerned with Management and Provisioning of Network Services and Applications
- Supports the FCAPS Functions
- May Be In-Band or Out-of-Band

Control/Signaling Security Plane:

- Enables the Efficient Delivery of Information, Services, and Applications Across the Network
- Machine-to-Machine Communications to Determine How to Best Route or Switch Traffic Across the Network
- May Be In-Band or Out-of-Band

Proposed frame of the methodology



Security factor discrimination phase

Finding of specific summaries of new IT system

- Deduce kinds of services provided
- Calculate the provided service execution process

Understanding new IT service system structure

- Calculate structure of system & network
- Deduce the role of system factors and their current status
- Deduce the service use process scenario
- Deduce the service execution process flowchart

Choice of protection subject

- Apply the information protection reference model ITU-T X.805

Risk calculation phase

Drawing up of risk scenario

- Make the risk scenario for the protection subject modules under ITU-T X.805

Calculation of degree of risk

- Risk figure deduced taking degree of attack, fatality, frequency of occurrence into account
- Deduce priority of risk

Counterstrategy deduction phase

Deduction of protection requirements

- Apply the information protection reference model ITU-T X. 805

Security plans for new IT service system

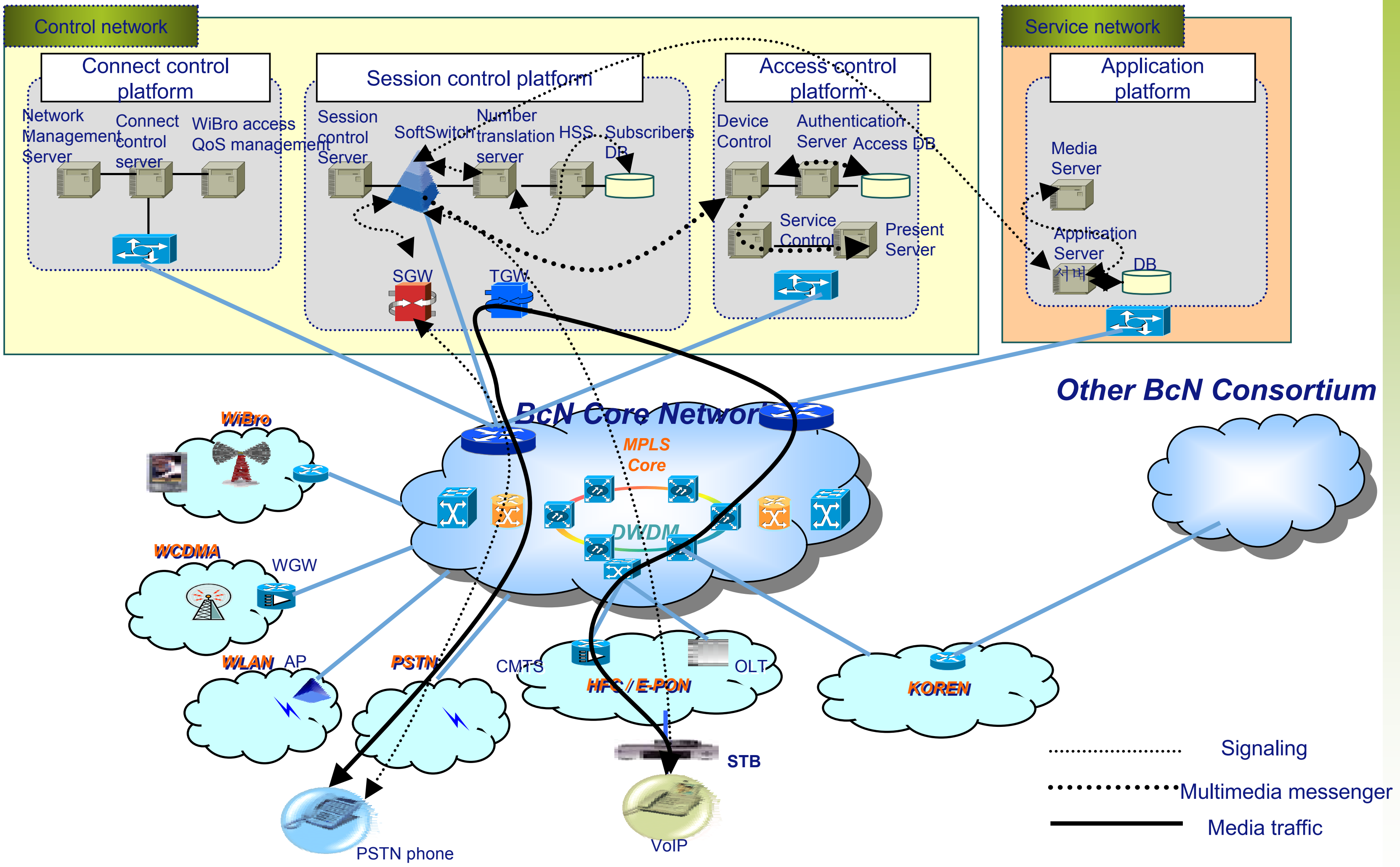
- Develop alternative plan according to priority of risk
- Deduce protection alternative per information protection request details
  - Take into account the information protection required technology list
  - Create information protection structure flowchart

Formation of management systems for the information protection of the system

- Create a division in case of a security accident
- Designate responsibility clearly

Examples

Finding of specific summaries of new IT system – BcN VoIP Service



Apply the information protection reference model ITU-T X.805

	Infra layer	Service layer	Application layer
Management plane	Network Management Server Connect control server WiBro access QoS management	VoIP server & G/W management info. (SNMP, HTTP, TFTP, Telnet, FTP, emote management etc.)	VoIP devices & Application management info. (SNMP, HTTP, TFTP, Telnet, FTP, emote management etc.)
Control plane	Session control Server Softswitch Number translation server Device Control Authentication Server SGW TGW	SIP, H.323, MGCP, MEGACO/H.248, SIP-T, SCTP etc	SIP, H.323, WLAN(802.11 a/b/g), Wibro, SMTP, HTTP
User plane	User information (User id/pw, IP etc) Subscribers DB HSS	RTP, RTCP, SIP, H.323	Voice info(RTP, RTCP, SIP, H.323 etc), Voice mail(SMTP, XML etc) Subscribers DB

Concept, characteristics & advantages of the methodology being presented

Clarity

- Processes defined in a clear and simple framework.
- Preparation of risk scenarios and protection measures for the 9 protection subject modules identified by applying the ITU-T X.805 information protection reference model.

Easy application

- The complex method of calculating the degree of risk is simplified by using just the level of difficulty, fatality and frequency.

Prior predictability of effects

- The methodology presents a way to identify the effects of the risk and seek countermeasures in advance, before the new IT service is actually introduced.

Thank you!

E-mail : herjune@kisa.or.kr