Evaluation of application systems

by ISO/IEC TR 19791

JEITA IT Security Center

September 25, 2005

1. Outline and Goals
1.1. Outline

- ISO/IEC TR 19791 - Security techniques for system evaluation - being developed in order to evaluate suitably a "*system*".
- JEITA ITSC has carried out the pilot evaluation of an application system according to the ISO/IEC TR 19791.
- This presentation introduce a notion of how to evaluate the application system.

1.2. Goals

- Establishing trusted security standard for ”IT System evaluation”.
- Promoting effectively and efficiently evaluation method for “IT System”.

2. Background
2.1. Definition of "*System*"

- "*System* " is defined as ...

  A specific IT installation, with a particular purpose and operational environment which covered by personnel, procedures, processes, and physical measures.

2.2. Examples of "*System*"

- Ministry of *A*, Online application system
- *B* City, The Resident Register system
- Online Bunking System of *C* Bunk
- Inventory and logistics management system of *D* Factory
- :

2.3. Characteristics of "*System*"

- "*System*" consists of several products.
- The specific IT installation. (There is only one in the world.)
  - The location and facilities exist actually.
  - The peripheral equipments exist actually.
  - The operational procedures exist actually.
  - The operators are uniquely identified. (The users may be uniquely identified.)

2.3. Characteristics of "*System*"

- "*System*" configuration is changed frequently.
  → Programs are changed frequently.
  → Equipments are changed frequently.
  → Roles of personnel are changed frequently.
- "*System*" is across the four life cycle stages – i.e. Development/Integration, Installation, Operation and Maintenance stage.

2.4. Methodology of "*System evaluation*"

Evaluate

Characteristics of "*System*"

- Several products.
- Procedures and rules based on security objectives.
- Operational environment which changes frequently.

ISO/IEC TR 19791 is being developed and will be merged into ISO/IEC 15408.

2.5. Feature of the "System Security Target"

TR 19791

- **No "Assumption".**

→ STOE is operated in an actually existing environment. STOE is located in "Real site".

- **No "IT environment".**

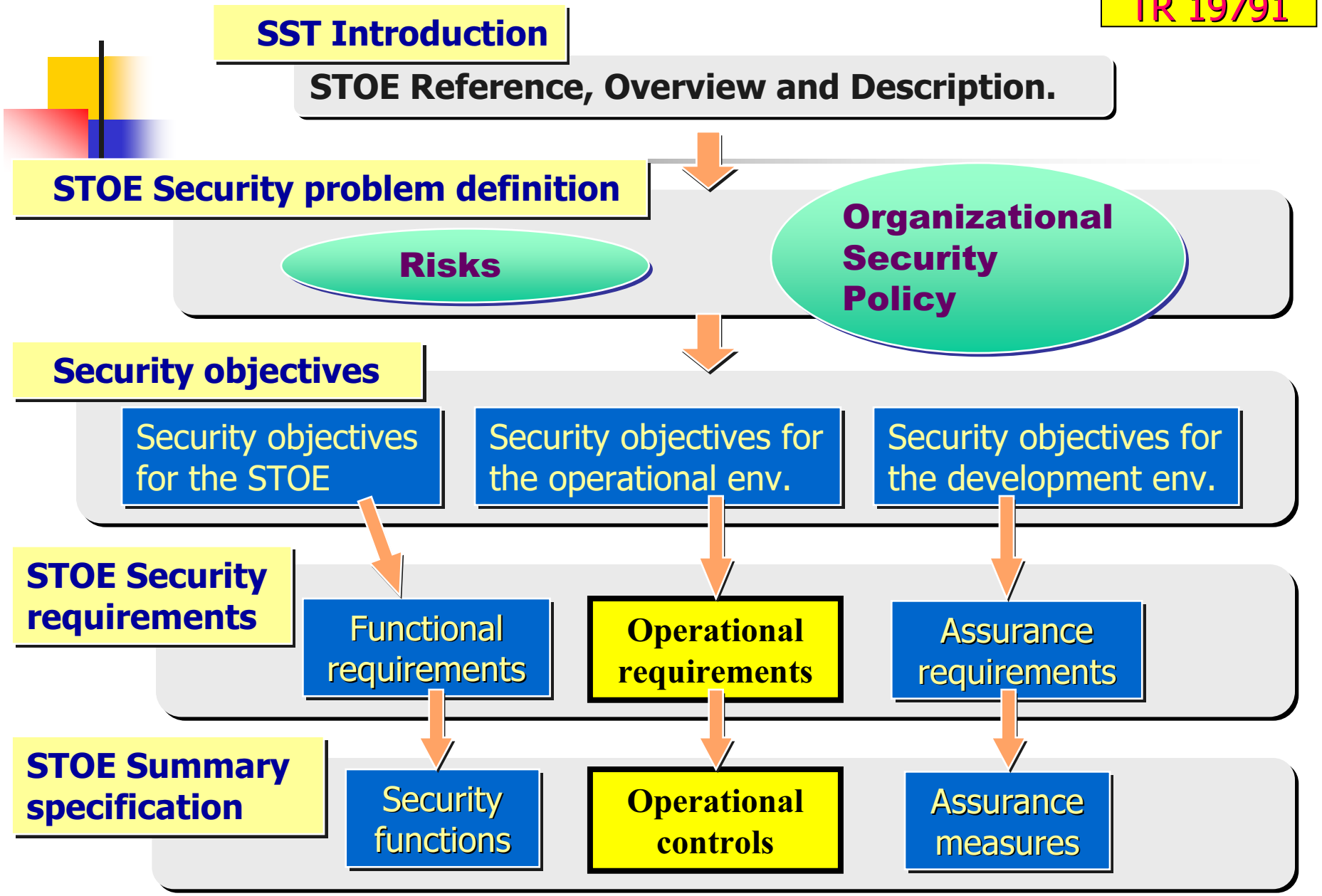
→ STOE shall be defined as a whole of "System ".

- **Identify "Risks" instead of "Threats".**

→ "Risk" is defined as "Threat" and "Vulnerability" in operational environment for STOE.

2.6. Structure of *"System ST"*

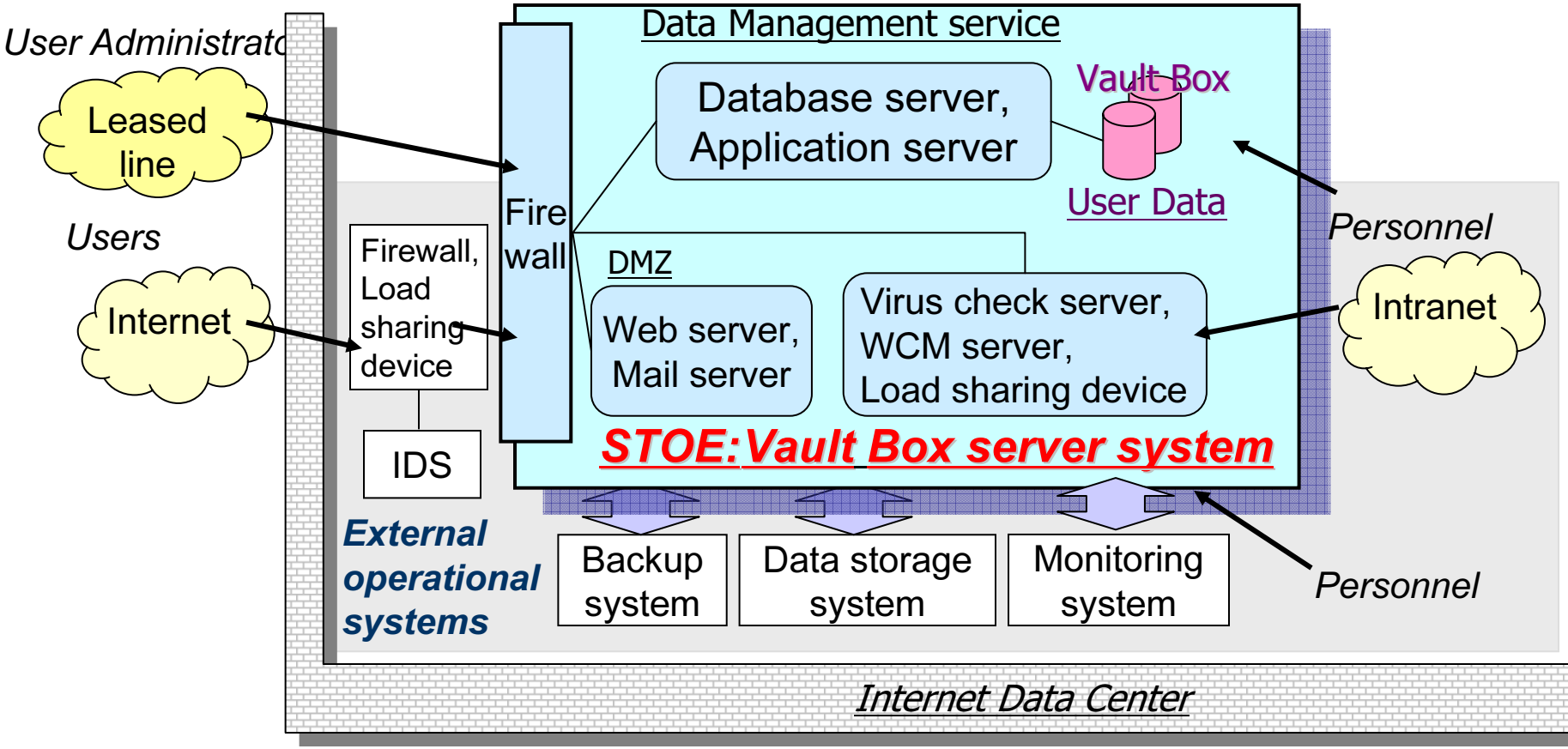
TR 19791



3. Present work

3.1. Feature of *system model*

- ITSC has been evaluated following model system in order to verify the ISO/IEC TR 19791.



3.2. Technical requirements and operational requirements

Logical scope of the model system

TR 19791

Security policy

Risk management with -in the organization

Access control

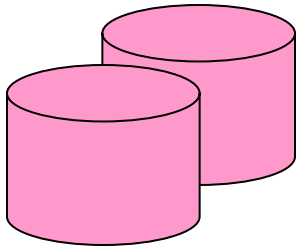
Information flow Control

Identification and Authentication

Session Locking

Trusted Path

Vault Box



Protected assets

Network Security

Audit Logs

Legal advice

Protection of assets

Impact analysis

Management of security attribute

Management of TSF data

4. Issues and Suggestions

4.1. What is Problem ?

① Unique identification of a "*System*".

- How can uniquely identify a system ?
  Configuration items are changing frequently.

② Identification of "*Risks*".

- Evaluator cannot determine what level of risks should be countered by STOE, since there are too many candidates of "*Risks*".

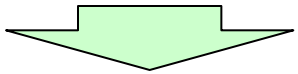
③ "*Documentation*" cannot be provided.

- As "*System*" may contain third party products, design documents of the third party products cannot be provided.

4.2. Unique identification of a "*System*"

Issue-1

- "*System*" configuration is changed frequently.
  - The programs are updated at any time.
  - The equipments are exchanged at any time.
  - The personnel changes occur at any time.



How can uniquely identify a system ?

4.2. Unique identification of a "*System*"

Suggestion-1

- Changes of STOE are able to be accepted, if the configuration management rules or baseline management rules are obeyed.
- STOE continues to have an "Identical version" easily identified from users within the acceptable changes.
  - The acceptable changes do not have an effect on "Risks".

4.2. Unique identification of a "*System*"

Acceptable changes (Cases when "Risks" are not influenced.)

- Updating of the programs for bug fix in accordance with baseline management rule.
- Exchange of the hard disk device with disk failure in accordance with assets maintenance rule.
- Personnel change according to office regulations.

Unacceptable changes (Cases when "Risks" are influenced.)

- Add new external interface.
- Add new security function, or remove security function.
- Add fundamental device which is not described in SST.
- Change owner in the organization which manages STOE.

4.2. Unique identification of a "*System*"

Example of "Configuration list" of the model system.

Vault Box Server System version 1.0

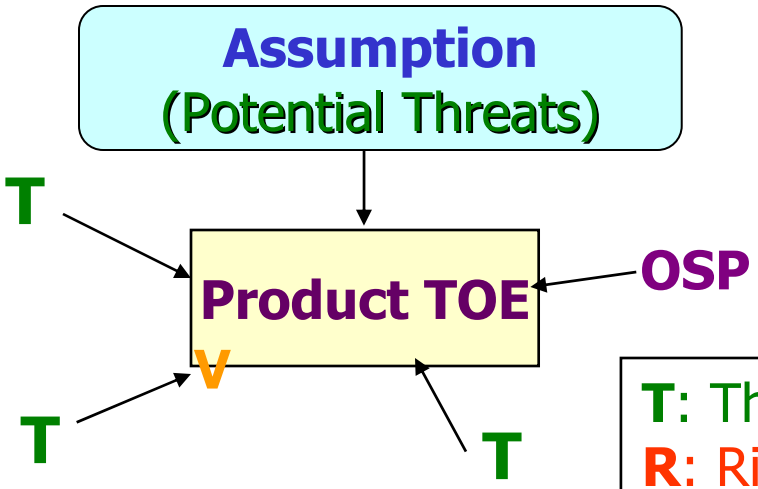
	Item name	install date (and version)	change date (and version)	change date (and version)	…
H/W	Firewall	2005/03/15	---	---	
H/W	switch	2005/03/15	2005/04/10	---	
:	:	:	:	:	
S/W	Linux ***	2005/03/25 Ver.**	---	---	
S/W	DBMS ***	2005/03/25			
S/W	Application program	2005/04/02 Ver.1.0	2005/04/28 Ver.1.1	2005/07/24 ver.1.2	
:	:	:			

It is "Identical version" within acceptable changes.

4.3. Identification of "*Risks*"

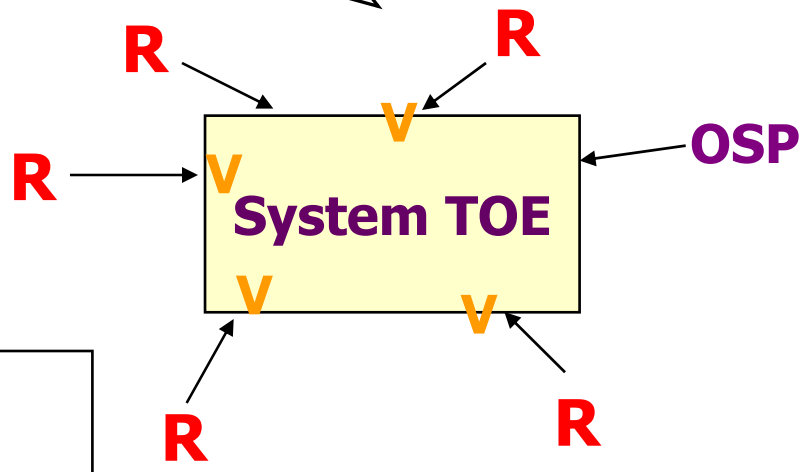
Product TOE

Some Threats can be excluded by identifying **"assumptions".**



System TOE

All Risks have to be identified.
(No assumption allied.**)**



T: Threat
R: Risk
V: Vulnerability

4.3. Identification of "*Risks*"

Issue-2

- Various countermeasures are implemented in the environment of STOE. -e.g.
  - The "*System*" is installed in facility which takes account of natural disaster.
  - The operators of the "*System*" possess proficient knowledge of a level.

Evaluator cannot determine what level of risks should be countered by STOE, since there are too many candidates of "Risks".

4.3. Identification of "*Risks*"

Suggestion-2

- Developer/integrator should describe the result of the risk assessment in the SST with reasons why the developer/integrator identified or did not identify candidates of risk as risks.

4.3. Identification of "*Risks*"

Example of "Security problem definition" in the SST.

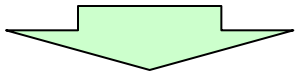
Result of risk assessment in the model system.

	Candidates of risk	Judge	Reason of the judge
1	The administrator may do injustice.	Yes	A possibility of malice should be considered.
2	STOE may be damaged by flood.	No	STOE is installed in the fifth floor.
3	An attacker may capture data being transferred across a network.	No	The capture is impossible, since the network is closed leased line.

4.4. "*Documentation*" cannot be provided

Issue-3

- No design documents of third party products are provided.
  - The design documents of multipurpose OS cannot be provided.
  - The design documents of general purpose package products cannot be provided.



How should evaluate third party products ?

4.4. "*Documentation*" cannot be provided

Suggestion-3

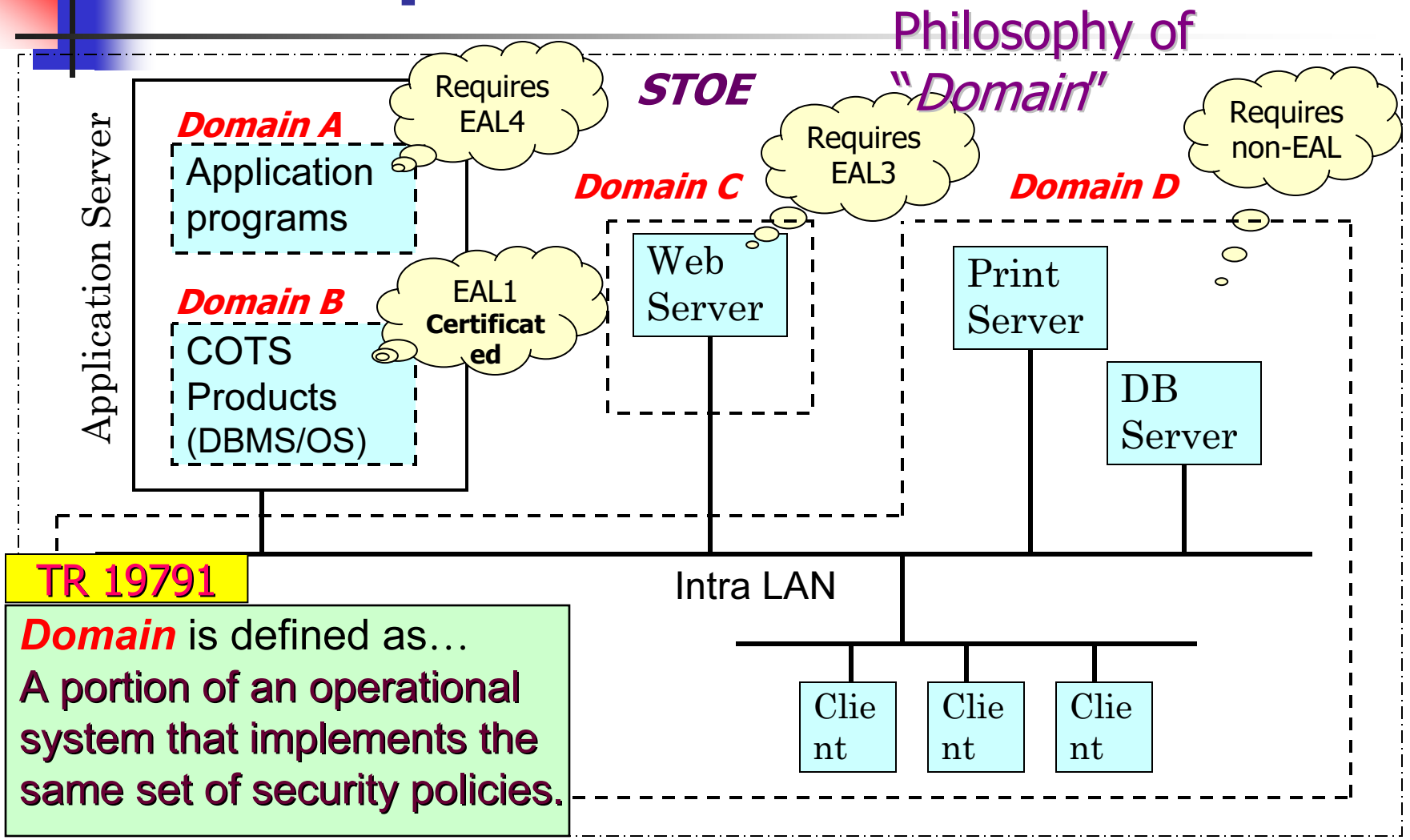
- The portion without evaluation evidence should be separated as a "*Domain*".
- This "*Domain*" can be evaluated by using the interfaces between individual products in the "*System*".

TR 19791

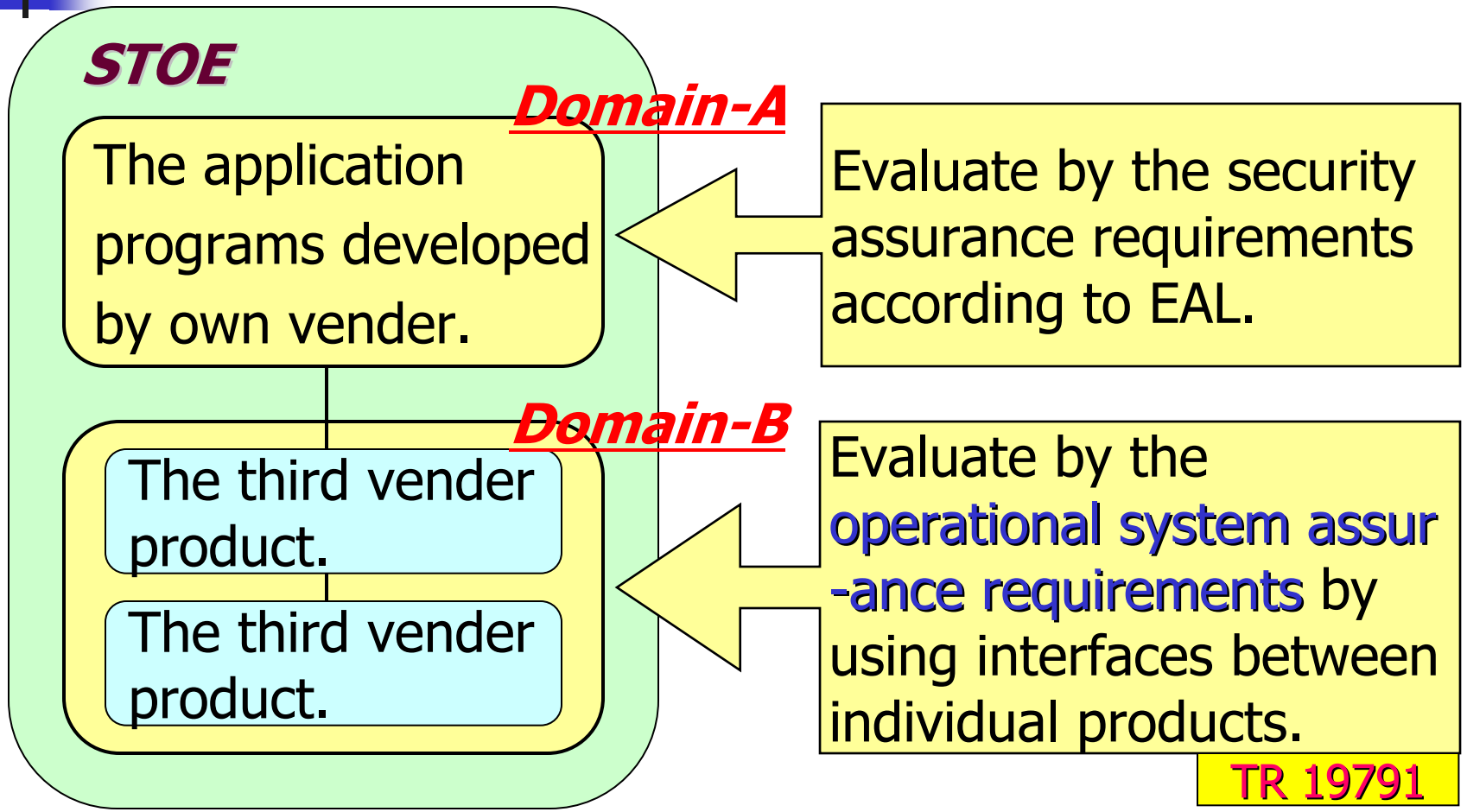
I.e. TR 19791 defines "System assurance requirements".

- ASD_SAD: System architecture design
- ASD_IFS: System interface functional specification etc..

4.4. "*Documentation*" cannot be provided

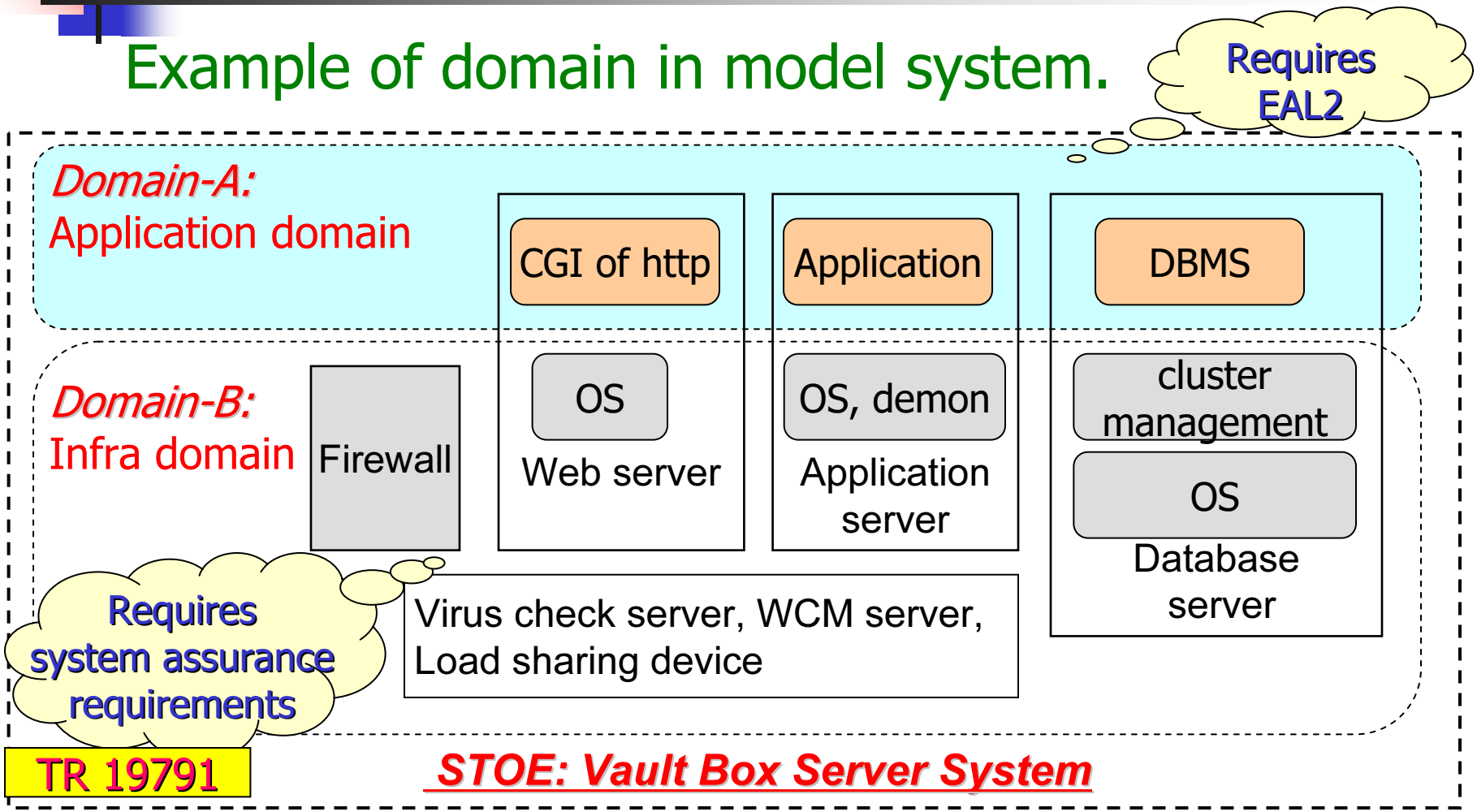


4.4. "*Documentation*" cannot be provided



4.4. "*Documentation*" cannot be provided

Example of domain in model system.



4.4. "*Documentation*" cannot be provided

X system security target

1. SST introduction
2. Conformance claims
3. Security problem definition
4. Security objectives
5. Security requirements
6. STOE summary specification

Construction of "System ST"

Domain part

Domain part

Domain part

TR 19791

7.1. Security domain introduction
7.2. Security domain Conformance claims
7.3. Security domain security problem definition
7.4. Security domain security objectives
7.5. Security domains security requirements
7.6. Security domain summary specification

4.5. Conclusion

① Unique identification of a "*System*".

- STOE can continue to have an "Identical version" as far as obeying the life cycle regulation.

② Identification of "*Risks*".

- For all candidate risks, developer/integrator should state "result of the risk assessment" in SST.

③ "*Documentation*" cannot be provided.

- The portion without documentation is able to be evaluated by using the "system assurance requirements".

5. Epilogue
5.1. Effort to the future

- ISO/IEC TR 19791 should be converted into an International Standard to support ISO/IEC 15408 specifically for evaluation of operational "*System*".

THANK YOU

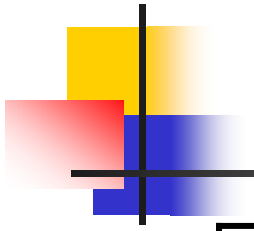
ARIGATOU GOZAIMASHITA

JEITA IT Security Center

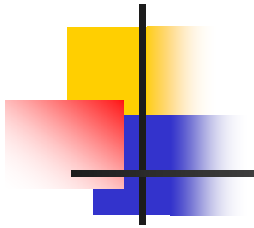
ITSC@jeita.or.jp

Annex-A
List of Operational System Functional Requirements

Class	Family
FOD: Administration	FOD_POL: Policy administration
	FOD_PSN: Personnel administration
	FOD_RSM: Risk management administration
	FOD_INC: Incident management administration
	FOD_ORG: Security organization administration
	FOD_SER: Service agreements administration
FOS: IT Systems	FOS_POL: Policy for IT systems
	FOS_CNF: Configuration of IT systems
	FOS_NET: Network security of IT systems
	FOS_MON: Monitoring of IT systems
	FOS_PSN: Personnel control of IT systems



FOS: IT Systems	FOS_OAS: Operational systems assets of IT systems
	FOS_RCD: Records for IT systems
FOA: User Assets	FOA_PRO: Privacy data protection
	FOA_INF: User assets information protection
FOB: Business	FOB_POL: Business policies
	FOB_BCN: Business continuity
FOP: Facility and Equipment	FOP_MOB: Mobile equipment
	FOP_RMM: Removable equipment
	FOP_RMT: Remote equipment
	FOP_SYS: System equipment
	FOP_MNG: Facility management



FOT: Third Parties	FOT_COM: Third party commitments
	FOT_MNG: Third party management
FOM: Management	FOM_PRM: Management of security parameters
	FOM_CLS: Management of asset classification
	FOM_PSN: Management of personnel security responsibilities
	FOM_ORG: Management of security organization
	FOM_INC: Management of security reporting

Annex-B
List of Operational System Assurance Requirements

Class	Family
ASP: System Protection Profile evaluation	
ASS: System Security Target evaluation	
AOD: Operational system guidance document	AOD_OCD: Operational system configuration specification
	AOD_ADM: Administrator guidance for an operational system
	AOD_USR: User guidance for an operational system
	AOD_GVR: Guidance document verification
ASD: Operational System Architecture, Design and Configuration Documentation	ASD_SAD: Operational system architecture design
	ASD_IFS: Operational system interface functional specification
	ASD_SSD: Operational system subsystem design

	ASD_CMP: Operational system primitive component design
	ASD_IMP: Implementation representation
	ASD_COM: Security concept of operations
	ASD_GVR: Design document verification
AOC: Operational System Configuration Management	AOC_OBM: Operational system baseline configuration
	AOC_ECP: Evaluated component products
	AOC_PPC: Conformance with PPs
	AOC_NCP: Non-evaluated component products
AOT: Operational System Test	AOT_FUN: Operational system functional tests
	AOT_COV: Operational system test coverage
	AOT_DPT: Operational system depth
	AOT_IND: Independent testing
	AOT_REG: Regression testing

AOV: Operational System Vulnerability Analysis	AOV_MSU: Operational system misuse
	AOV_SOF: Strength of operational STOE security functions
	AOV_VLA: Vulnerability analysis
AOL: Operational System Life Cycle Support	AOL_DVS: Identification of operational security measures
ASI: System Security Installation and Delivery	ASI_AWA: Awareness training
	ASI_CMM: Communication
	ASI_SIC: Site interoperability check
ASO: Records on Operational System	ASO_RCD: Operation records of operational controls
	ASO_VER: Verification of operational controls
	ASO_MON: Monitoring of operational controls