Ontology support for Management System Audit Programs

Protégé Assisted Management System Auditing

A. Gehrmann, S. Ishizu
Aoyama Gakuin University, Japan

Auditing and audit programs

- Caution: The term audit is used in many domains: Management, Computer security, Finance etc.,
- We refer to Management System Audits as defined in ISO 19011:2002:
  - systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled;

    ISO 19011:2002 clause 3.1 audit
- A set of audits for a defined purpose constitutes an audit program; e.g. evaluation of effectiveness of management system

Problem and approach

- 3rd Party Management System Auditing is criticized for not delivering values; we see the difficulty to deal with organizational complexity as one main obstacle to value-adding auditing
- We understand the management of complexity of organizations as a main factor for improvement and propose the use of an audit ontology and protégé for enhancing the value of auditing

Origins of complexity in 3 rd party auditing

1. Third party auditors have to **deal with hundred of less familiar domain concepts** in a very short time, but as human beings can cope only with 7 (+ / - 2) concepts at a time
2. Management standards are **generic in nature and give raise to many interpretational issues**, therefore fundamental concepts such as Quality, Contract, Design Integrity and Availability of Information assets lacking often on clarity in the context of an organization and are not shared consistently between the auditee and the auditors; leads to conceptual inconsistencies / clashes
3. **Many requirements** might be applicable : Quality and Information Security, IT risk management based, Quality Manuals, Internal Procedures, Auditee's client's specification, Auditee's client's quality procedures
4. Demand on **documentation** is high
5. Organizational **complexity is high** (horizontal, vertical)
6. Auditing needs **team communication**

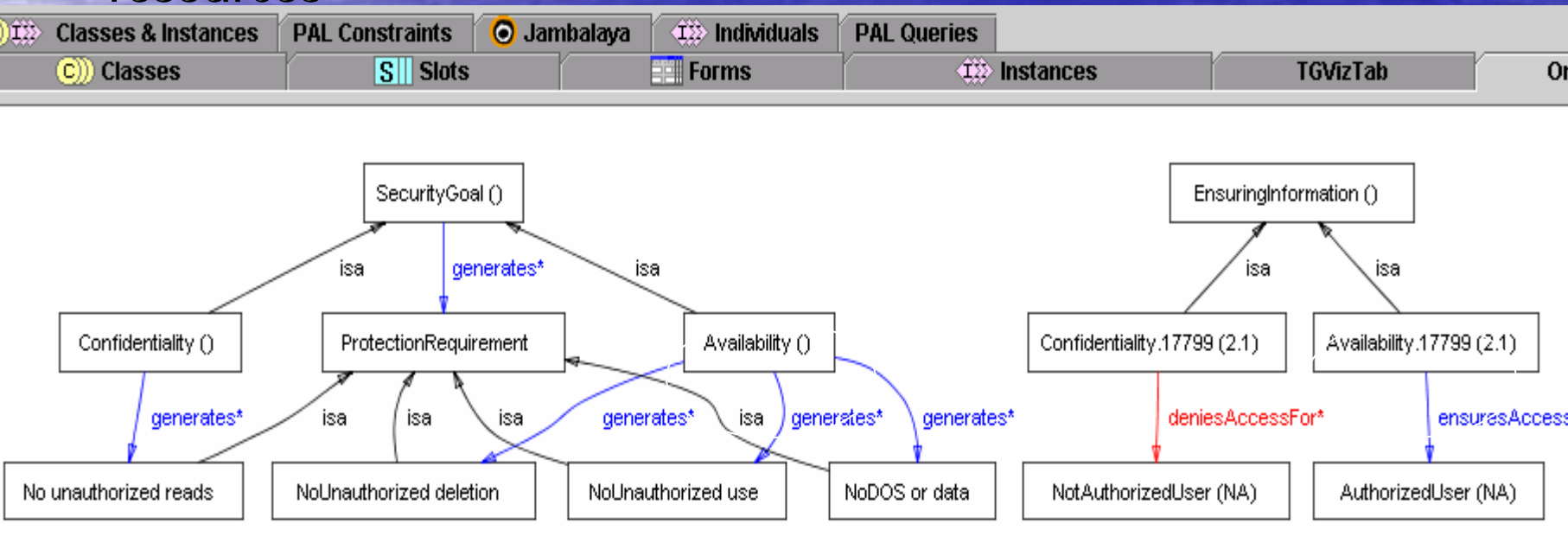
Conceptual clashes: Availability

SP800-30 (Appendix A):

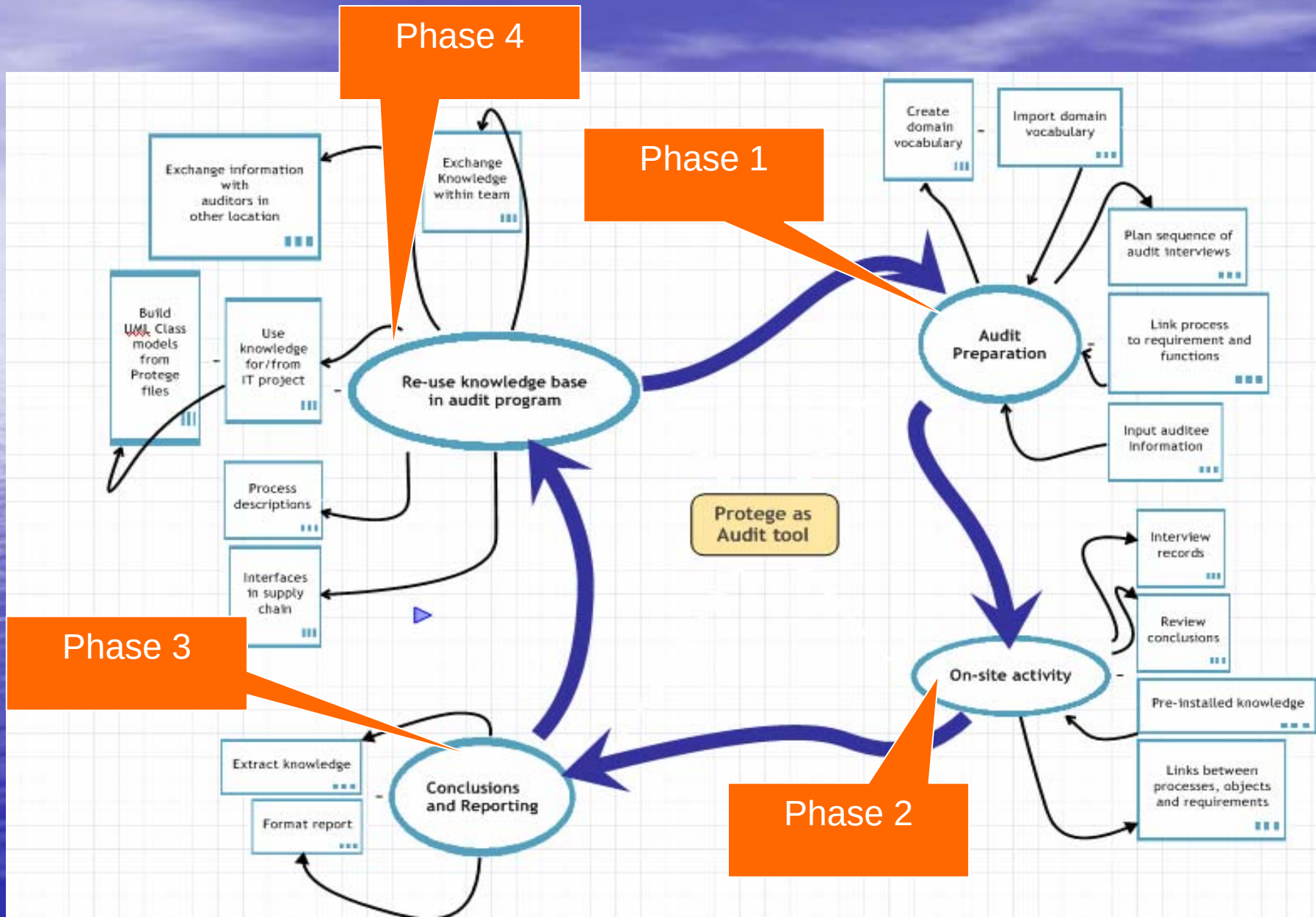
he security goal that generates the equirement for protection against ntentional or accidental attempts to

- Perform unauthorized deletion of data or
- Otherwise cause a denial of service or data
- Unauthorized use of system resources

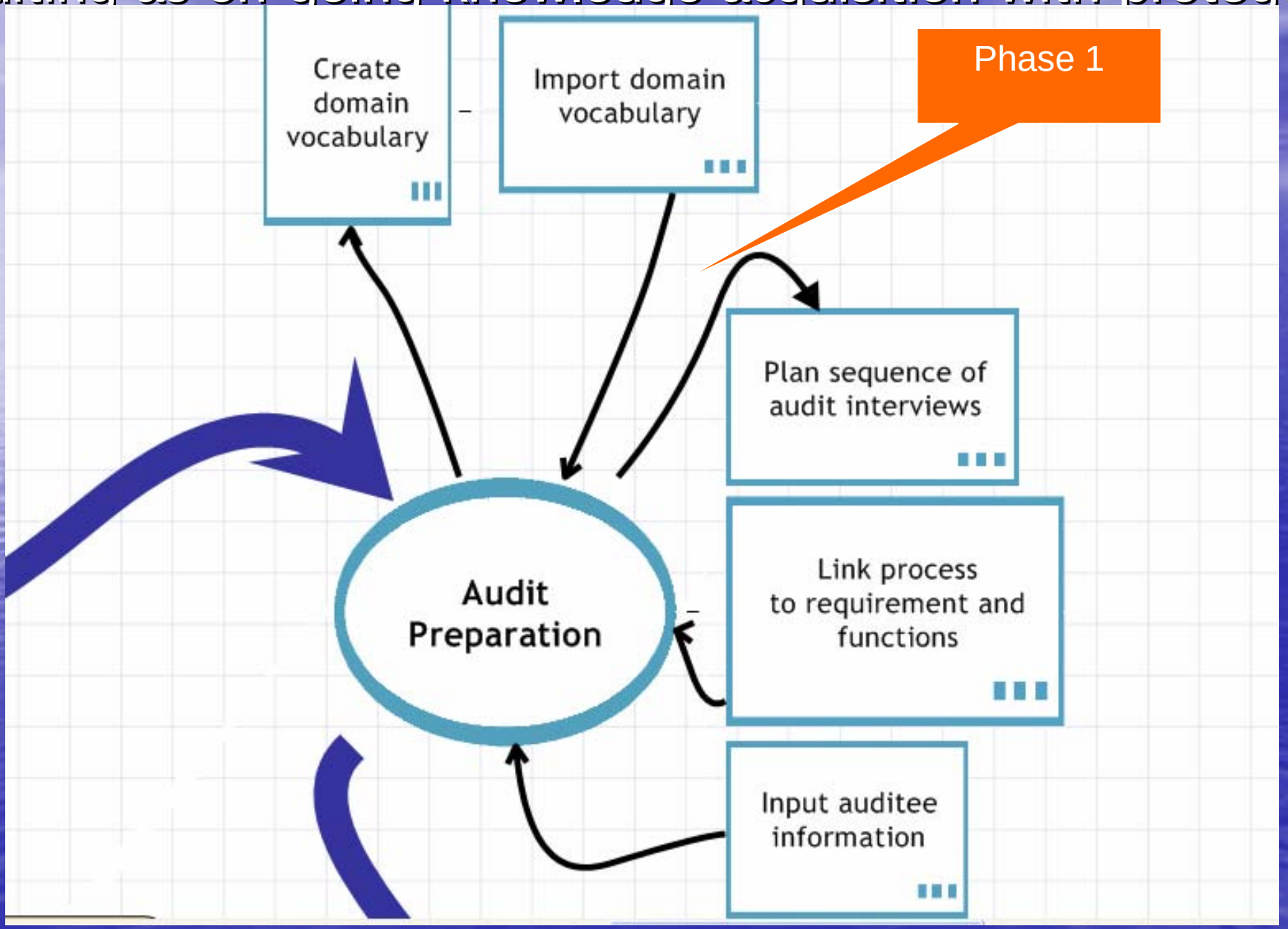
- **ISO/IEC 17799:2000** : ensuring that authorized users have access to information and associated assets when required



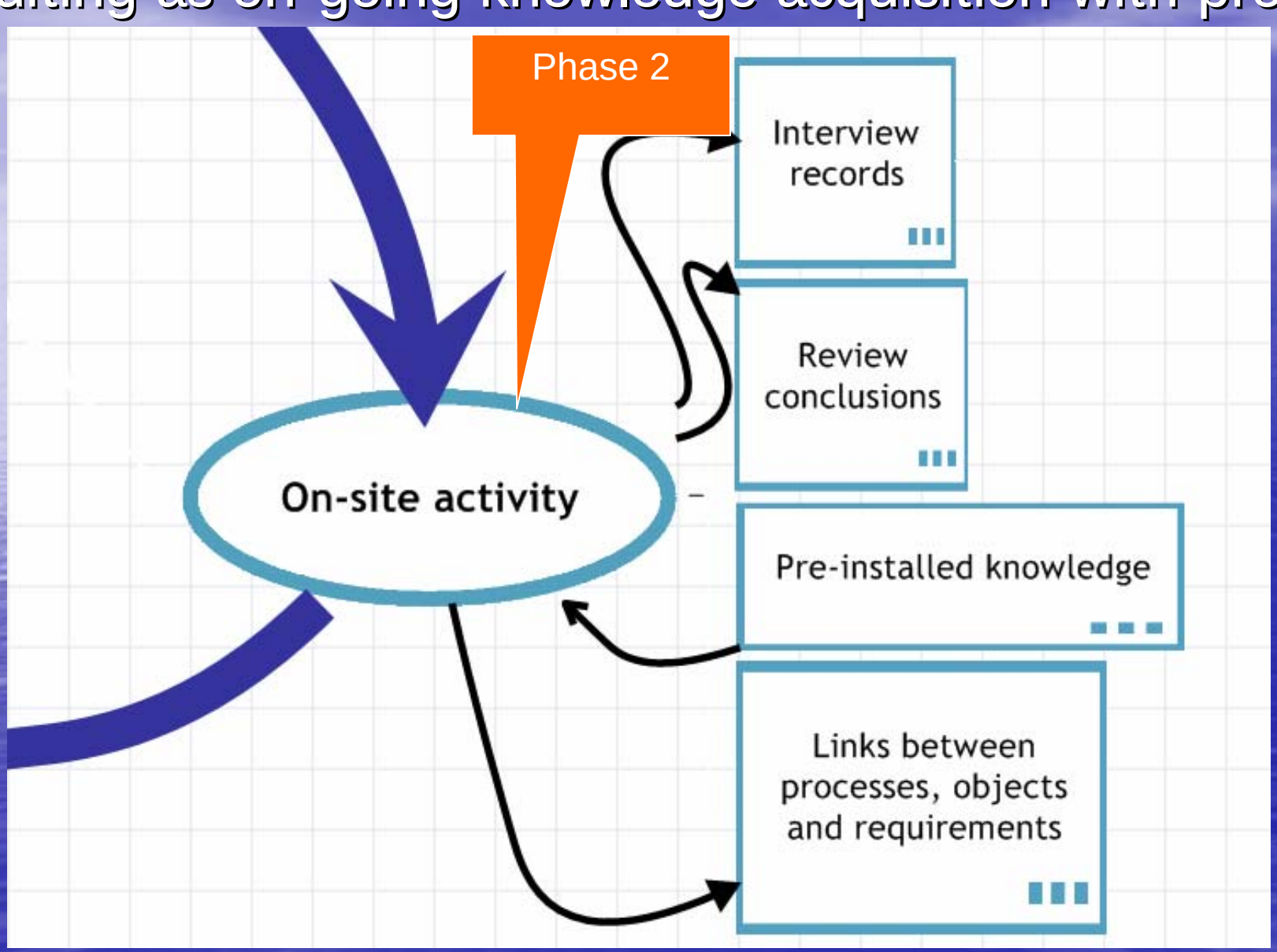
Auditing as on-going knowledge acquisition with Protege



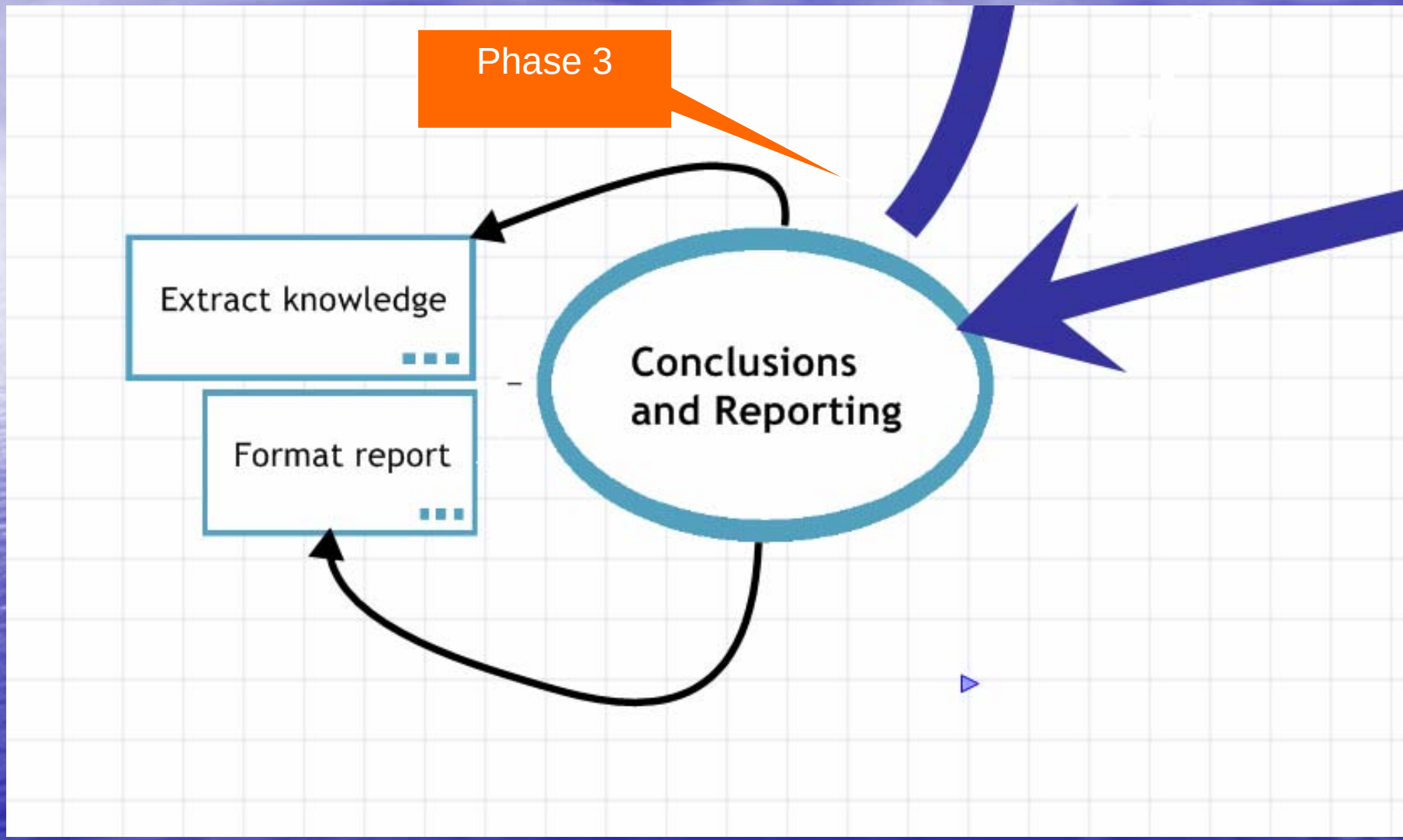
Auditing as on-going knowledge acquisition with protége



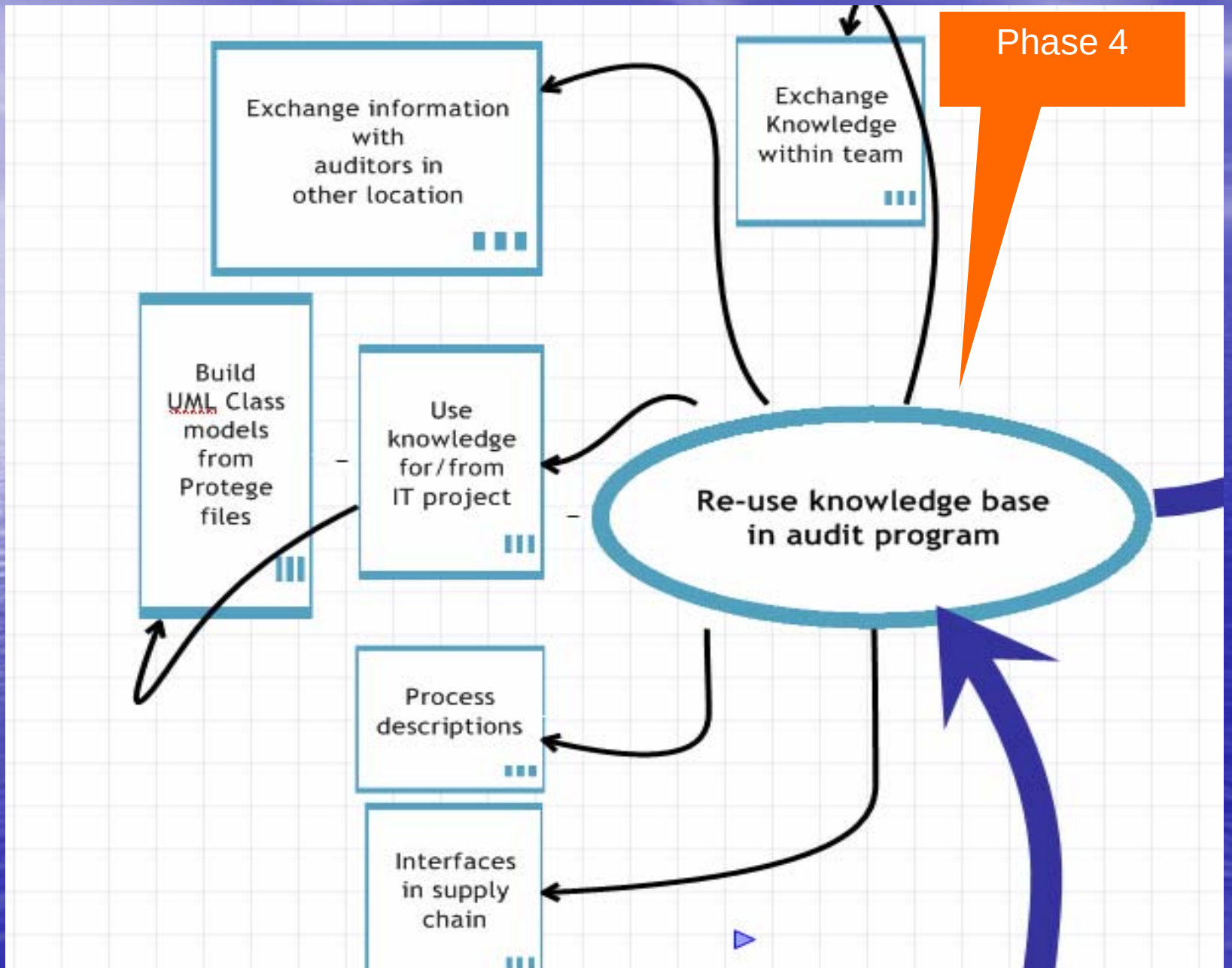
Auditing as on-going knowledge acquisition with protége



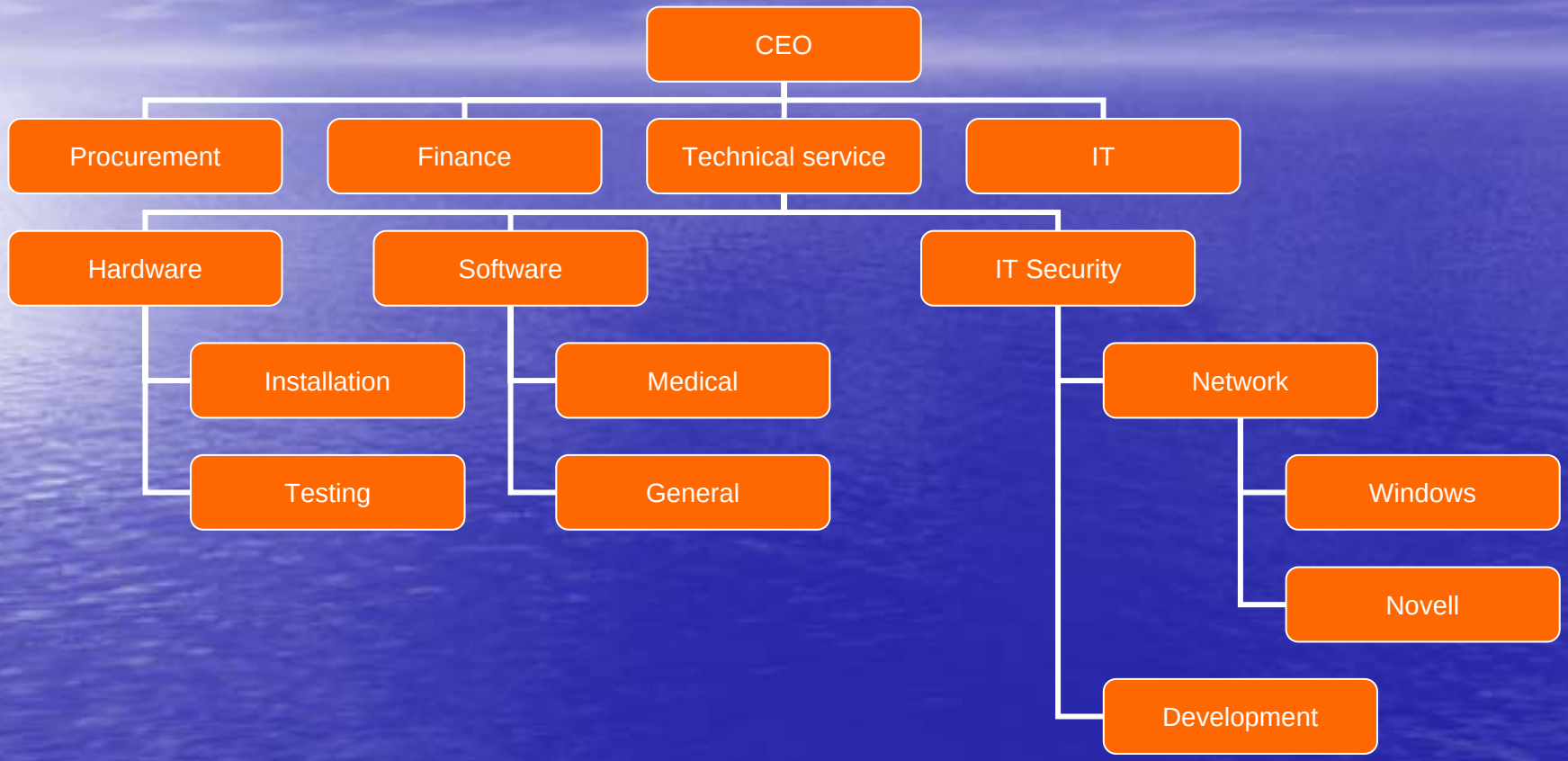
Auditing as on-going knowledge acquisition with protége



Auditing as on-going knowledge acquisition with protége



A case: The auditee
-Total Business Information Systems Ltd.-



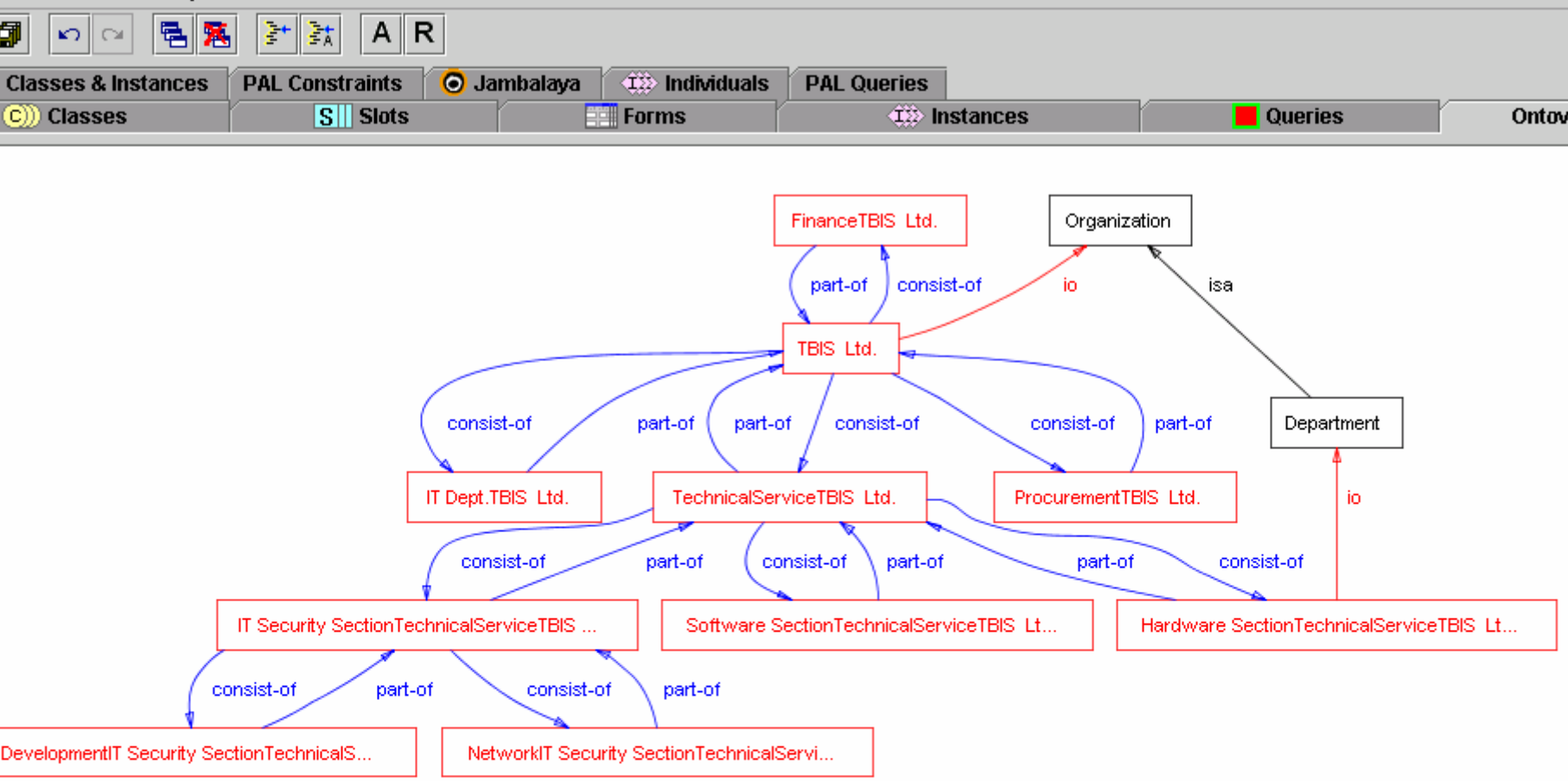
5 Levels, 50 Engineers, 10 technical assistants, 10 clerical staff

Service: Total network solutions including information security solution

The task ahead

- 12 Interviews at 5 levels covering variety of engineering fields
- Time available is limited to 3 working days
- 2 auditors
- CEO is non-technician, lawyer
- Managers: Former Hacker, MBA
- Students, Part-timer, non-technical clerics
- 300 pages internal procedures and Management standard


Understand Organizational Structure
Identify Applicable Requirement
Interpret Requirement In context
Select Right Level in organization
Select Right interviewee
Gather facts
Verify Common Understanding
Move in Organization
Link information
Confirm findings
Make conclusions

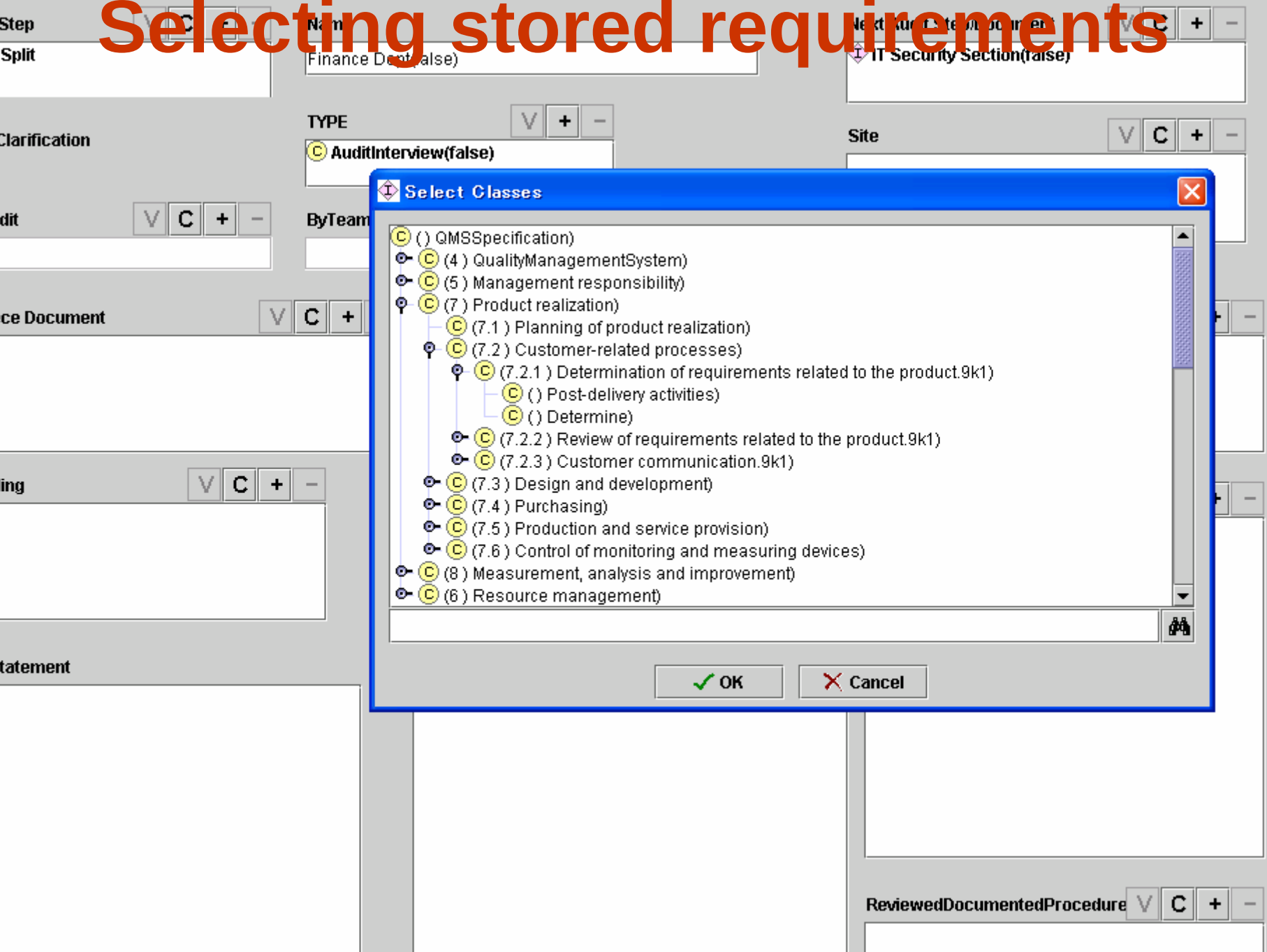


TBIS structure

-organizational units-

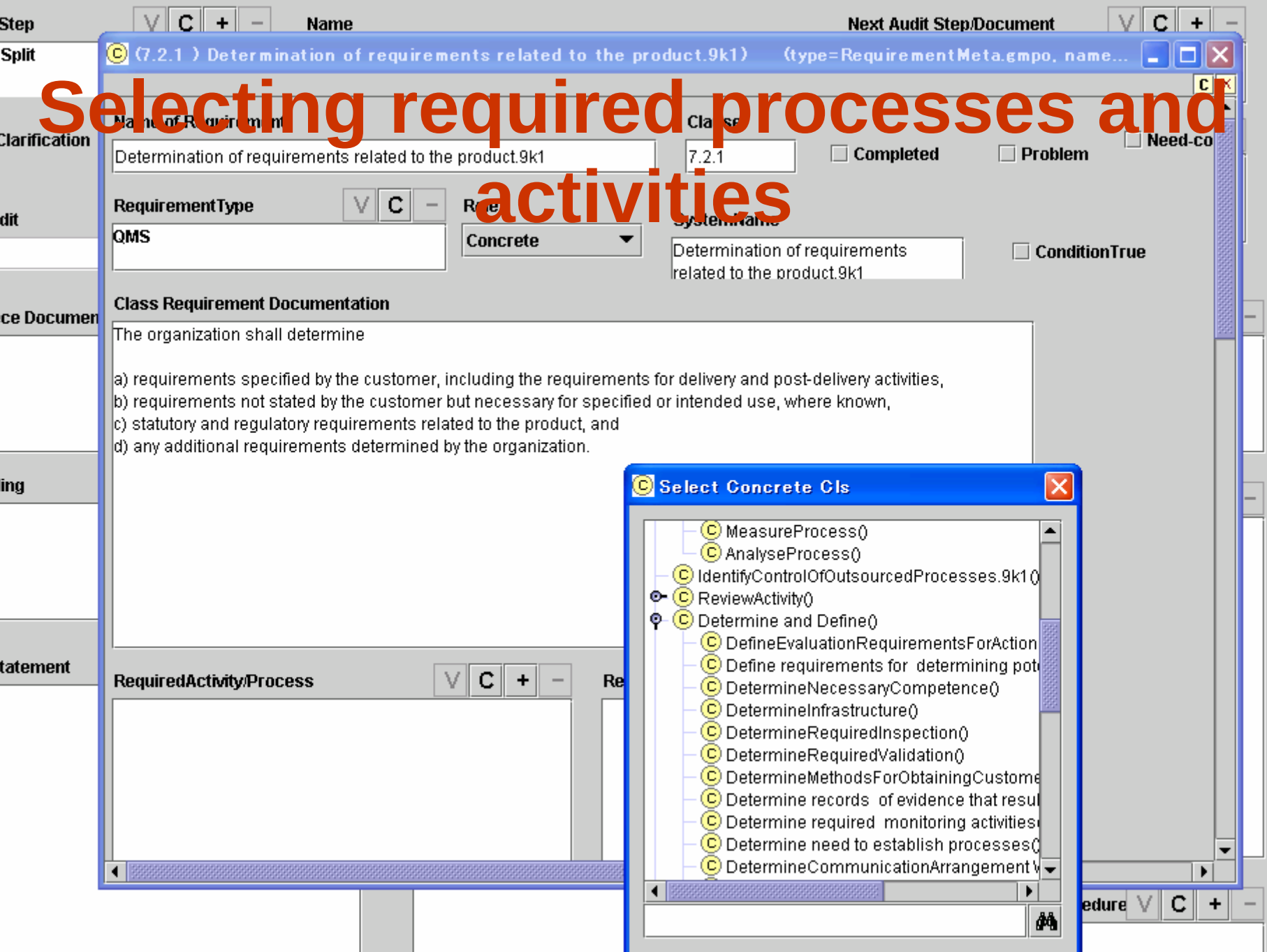

nderstand Organizational Structure
Identify Applicable Requirement
Interpret Requirement In context
Select Right Level in organization
Select Right interviewee
Conduct interview, Gather facts
Verify Common Understanding
Move in Organization
Link information
Confirm findings
Make conclusions

Selecting stored requirements

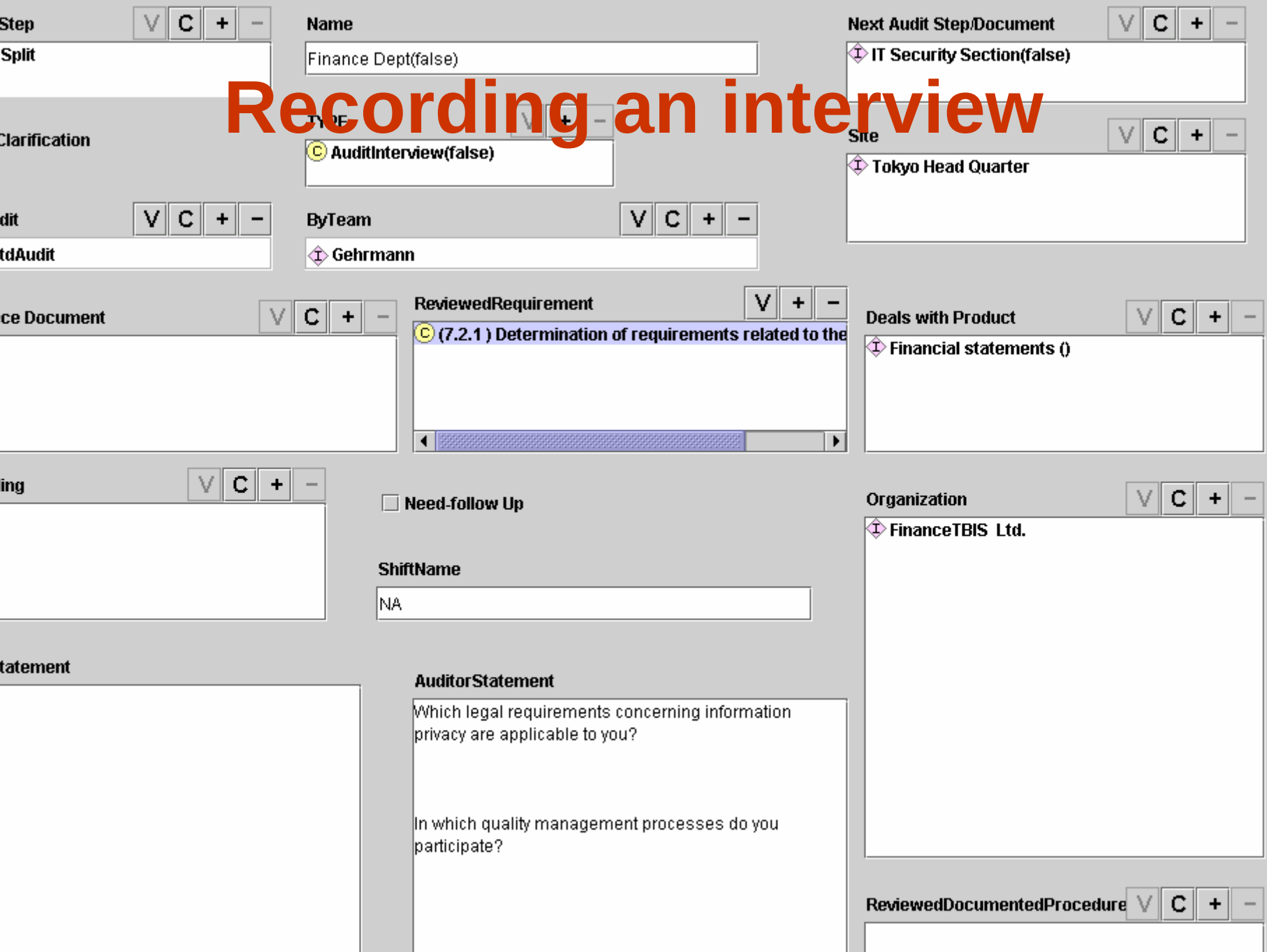



nderstand Organizational Structure
Identify Applicable Requirement
terpret Requirement In context of a process
Select Right Level in organization
Select Right interviewee
Gather facts
Verify Common Understanding
Move in Organization
Link information
Confirm findings
Make conclusions

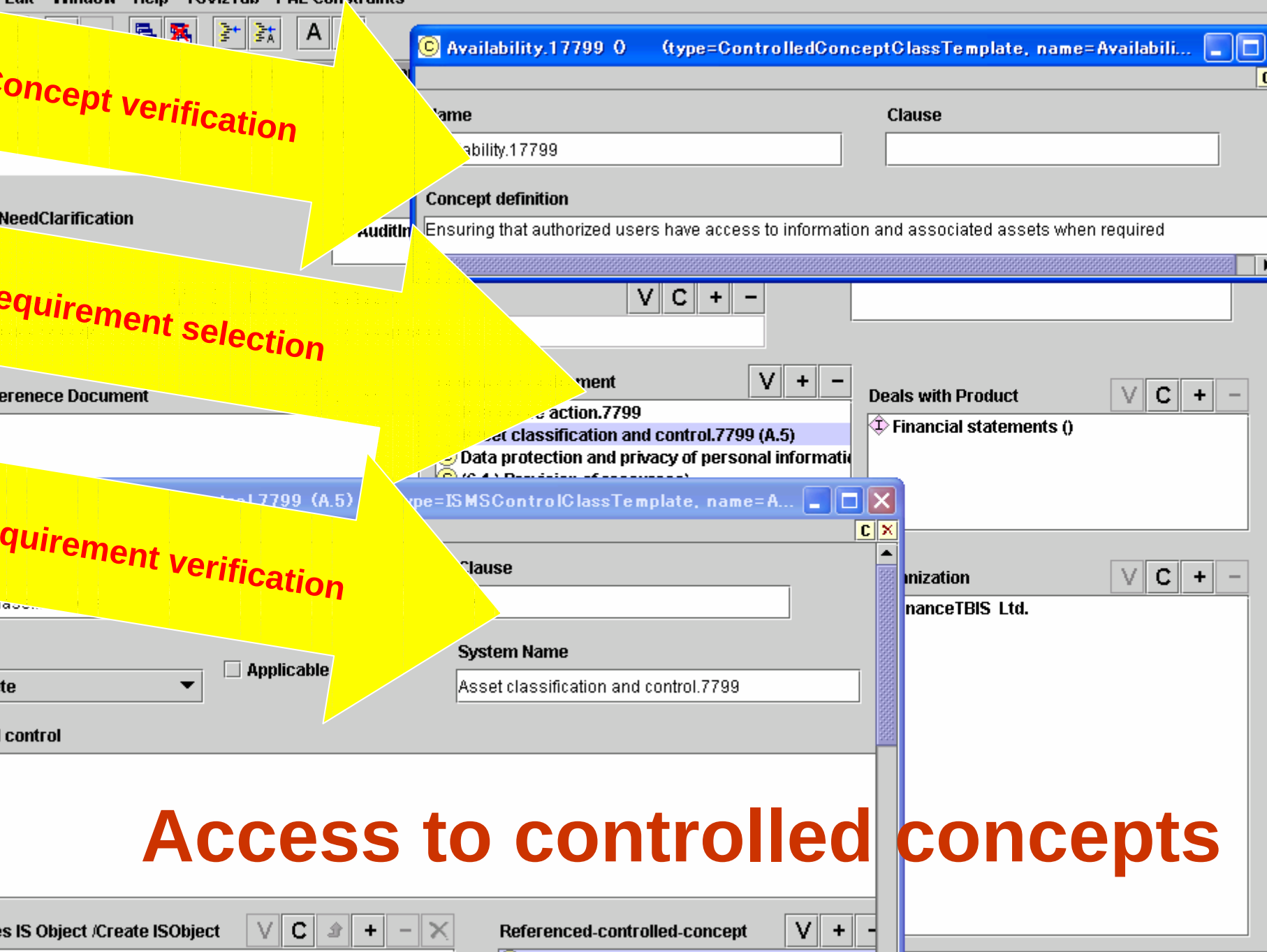
Selecting required processes and activities



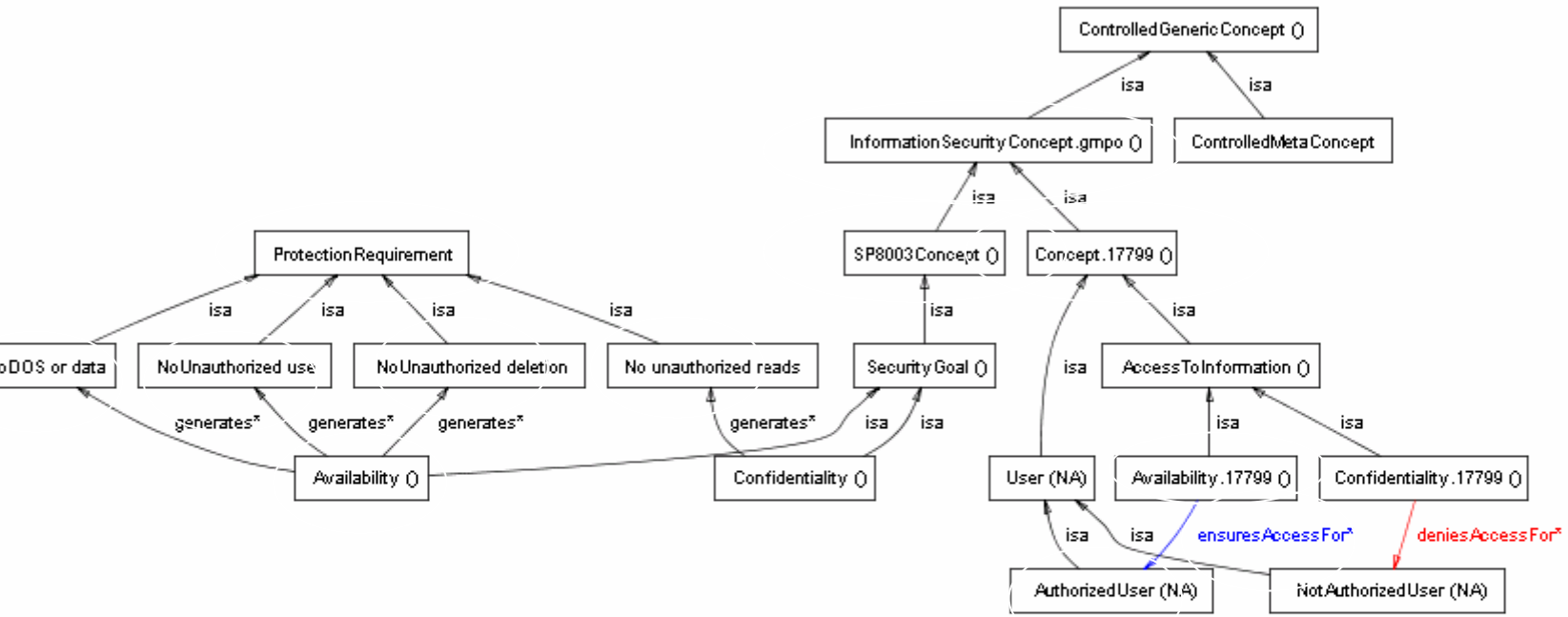

nderstand Organizational Structure
Identify Applicable Requirement
Interpret Requirement In context
Select Right Level in organization
Select Right interviewee
Conduct interview, Gather facts
Verify Common Understanding
Move in Organization
Link information
Confirm findings
Make conclusions

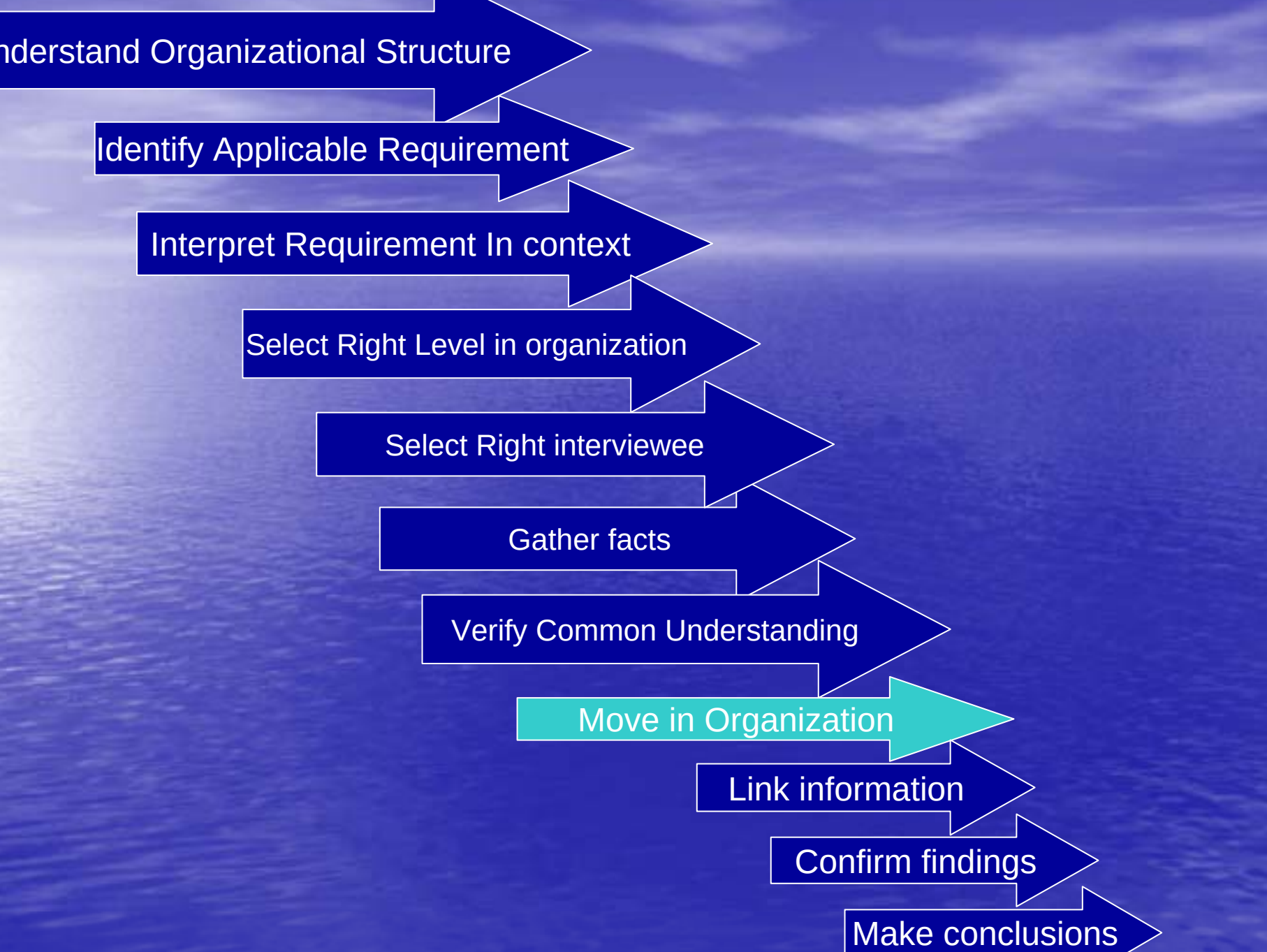

Step
Split
Name
Finance Dept(false)
Next Audit Step/Document
IT Security Section(false)
Recording an interview
Clarification
TYPE
AuditInterview(false)
Site
Tokyo Head Quarter
dit
tdAudit
ByTeam
Gehrmann
ce Document
ReviewedRequirement
(7.2.1) Determination of requirements related to the
Deals with Product
Financial statements ()
ing
Need-follow Up
Organization
FinanceTBIS Ltd.
ShiftName
NA
tatement
AuditorStatement
Which legal requirements concerning information privacy are applicable to you?
In which quality management processes do you participate?
ReviewedDocumentedProcedure


nderstand Organizational Structure
Identify Applicable Requirement
Interpret Requirement In context
Select Right Level in organization
Select Right interviewee
Gather facts
Refer to controlled concepts
Move in Organization
Link information
Confirm findings
Make conclusions

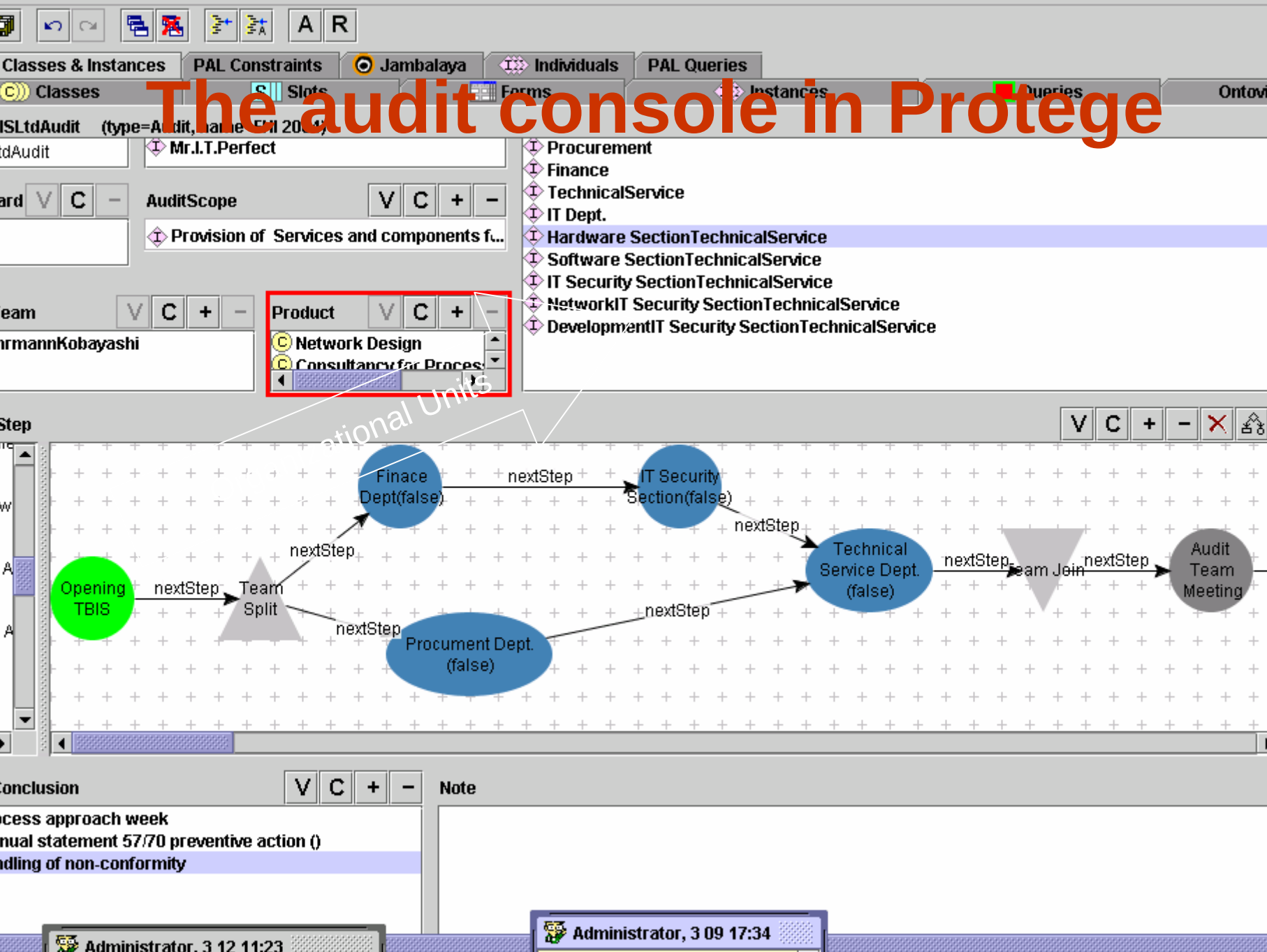

Concept verification
Availability.17799 0 (type=ControlledConceptClassTemplate, name=Availabili...
Name
Clause
Concept definition
Ensuring that authorized users have access to information and associated assets when required
NeedClarification
Requirement selection
Deals with Product
Financial statements ()
Data protection and privacy of personal informati
Requirement verification
(type=ISMSControlClassTemplate, name=A...
Applicable
System Name
Asset classification and control.7799
Access to controlled concepts
Referenced-controlled-concept


nderstand Organizational Structure
Identify Applicable Requirement
Interpret Requirement In context
Select Right Level in organization
Select Right interviewee
Gather facts
Verify Common Understanding
Move in Organization
Link information
Confirm findings
Make conclusions

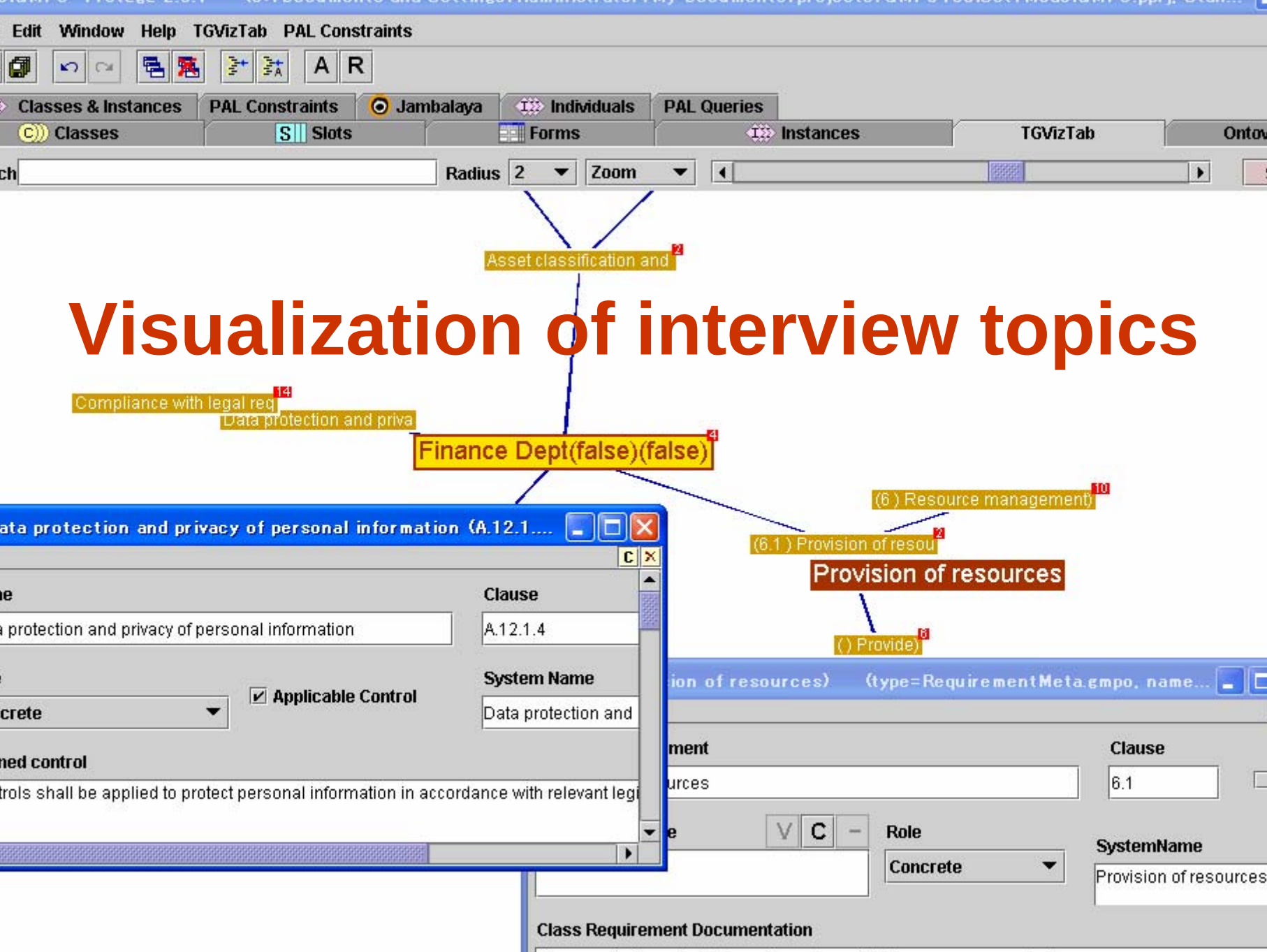

Controlled Generic Concept ()
isa
isa
Information Security Concept.gmpo ()
Controlled Meta Concept
isa
isa
Protection Requirement
SP8003 Concept ()
Concept.17799 ()
isa
isa
isa
isa
isa
isa
oDOS or data
No Unauthorized use
No Unauthorized deletion
No unauthorized reads
Security Goal ()
isa
Access To Information ()
generates*
generates*
generates*
generates*
isa
isa
isa
isa
Availability ()
Confidentiality ()
User (NA)
Availability.17799 ()
Confidentiality.17799 ()
isa
isa
ensures Access For*
denies Access For*
Authorized User (NA)
Not Authorized User (NA)


nderstand Organizational Structure
Identify Applicable Requirement
Interpret Requirement In context
Select Right Level in organization
Select Right interviewee
Gather facts
Verify Common Understanding
Move in Organization
Link information
Confirm findings
Make conclusions

The audit console in Protege




nderstand Organizational Structure
Identify Applicable Requirement
Interpret Requirement In context
Select Right Level in organization
Select Right interviewee
Gather facts
Verify Common Understanding
Move in Organization
Review situations, Link information
Confirm findings
Make conclusions


Edit Window Help TGVizTab PAL Constraints
Classes & Instances
PAL Constraints
Jambalaya
Individuals
PAL Queries
Classes
Slots
Forms
Instances
TGVizTab
Radius 2
Zoom
Asset classification and
Visualization of interview topics
Compliance with legal req
Data protection and priva
Finance Dept(false)(false)
(6) Resource management
(6.1) Provision of resou
Provision of resources
( ) Provide
ata protection and privacy of personal information (A.12.1....
Clause
a protection and privacy of personal information
A.12.1.4
System Name
Applicable Control
Data protection and
ned control
trols shall be applied to protect personal information in accordance with relevant legi
ion of resources)
(type=RequirementMeta.gmpo, name...
Clause
6.1
Role
Concrete
SystemName
Provision of resources
Class Requirement Documentation


nderstand Organizational Structure
Identify Applicable Requirement
Interpret Requirement In context
Select Right Level in organization
Select Right interviewee
Gather facts
Verify Common Understanding
Move in Organization
Review situations, Link information
Confirm findings
Make conclusions

Summary - Key functions of an audit ontology

Conduct systematically the audit

Document audit process for obtaining audit evidence

Evaluating evidence

Determine the extent to which the audit criteria are fulfilled

- Protégé for systematic conduct and planning; Protégé as organizer
- Protégé as documentation tool
- Protégé as evaluation support tool
- Protégé for keeping track audit findings

Solutions for coping with complexity with a Protégé audit ontology

1. Protégé helps to **organize** concepts and make it possible to **manage hundreds** of them at a time
2. An audit ontology helps to **identify conceptual clashes** and helps to understand generic concepts in the context
3. Audit **requirements are retrievable** and their relationship are linked to concepts and required activities
4. Audit **documentation can be prepared** on the fly by using transformation for XML documents
5. Teams can **exchange ontologies** for improved communication
6. Organizational **complexity can be managed** by using an **organizational model** in the audit ontology

Usability of an audit ontology in protégé

Use/Phase	Description	Benefits	Obstacles
udit planning	Modeling of organization structure and organizational artifact	Fast understanding by visualization and taxonomies	Requires understanding of ontology concepts
n-site audit	Creation of instances of organization concepts Linking artifacts	Auditors have pre-defined concepts available	Requires a reasonable degre of skill to use protégé Speed problems.
udit ocumentation	Is required but not a purpose in itself	Knowledge base stored in XML Audit findings and conclusions extracted	Need customization of user interface/print/representatio
ommunication ithin team	Necessary for auditing in a team	Instantaneous	High technical requirement Understandability of knowledge representation
e-usability of nowledge	Currently not the focus of auditing; missed chance	Domain vocabulary can be extended Usage in IT projects Part of system	none

Future applications / expectations

Expectation about features of protégé :

- Speed improvements (drawing, visualization)
- Possibility for customizing interface for knowledge acquisation
- Build-in documentation customizing

Implementation in OWL for reasoning and consistency

Remote login and sharing ontology over distributed clients

Import of industry ontologies SUO

Mobile devices: tablet computer

Protégé as server component for customized clients tool (files) for simplifying interface

Q/A