

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

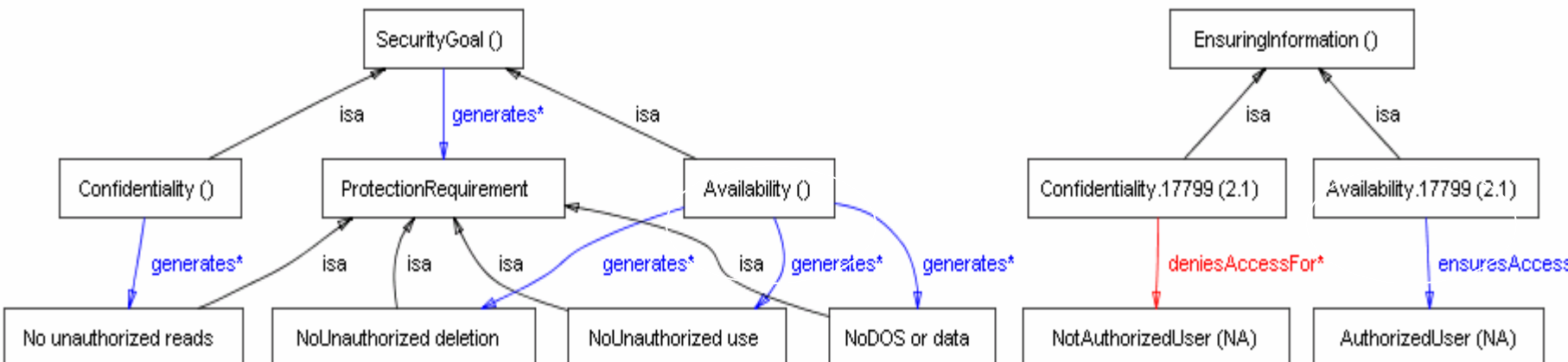
SP800-30 (Appendix A):

The security goal that generates the requirement for protection against intentional or accidental attempts to

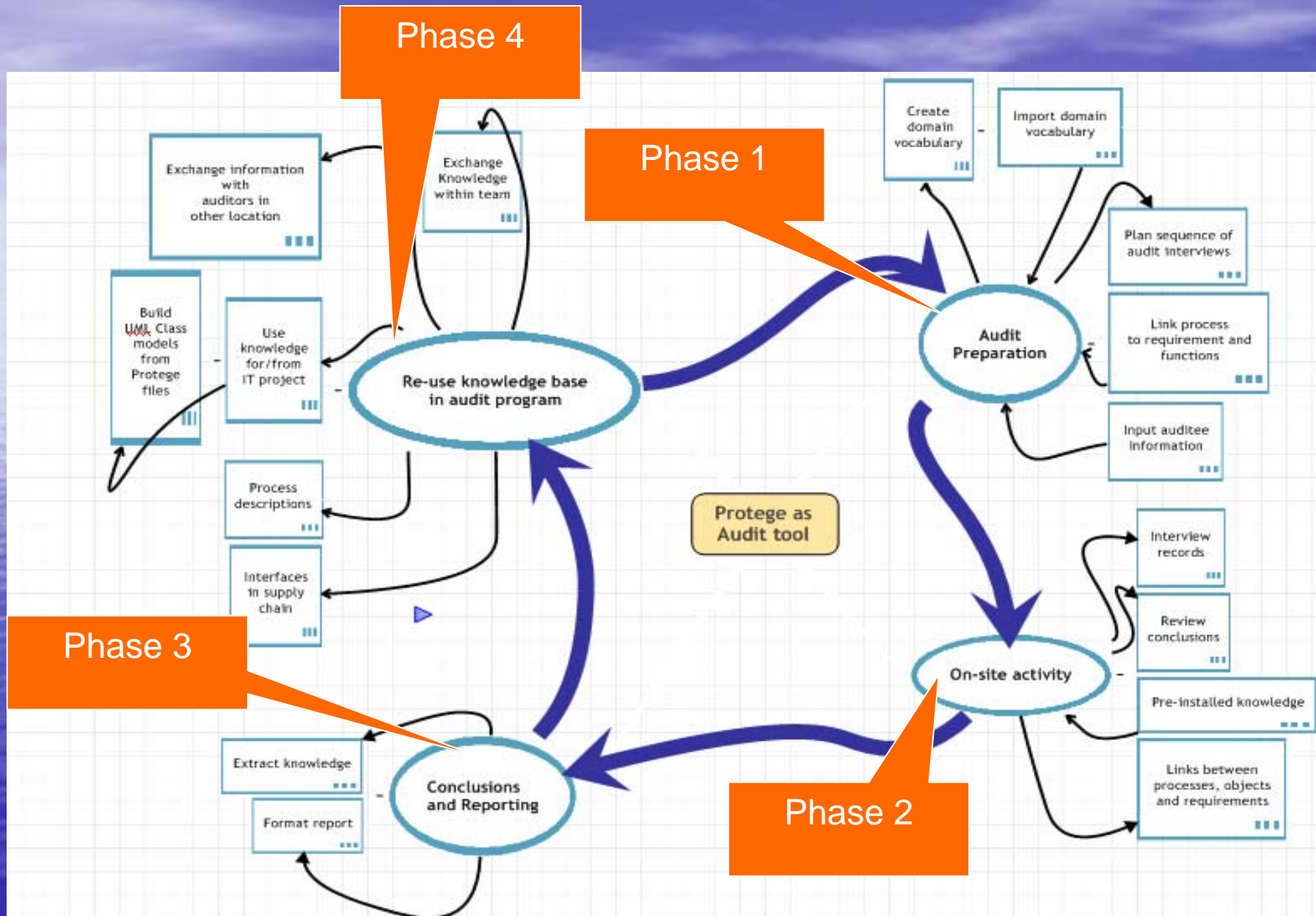
- Perform unauthorized deletion of data or
- Otherwise cause a denial of service or data
- Unauthorized use of system resources

• ISO/IEC 17799:2000 :

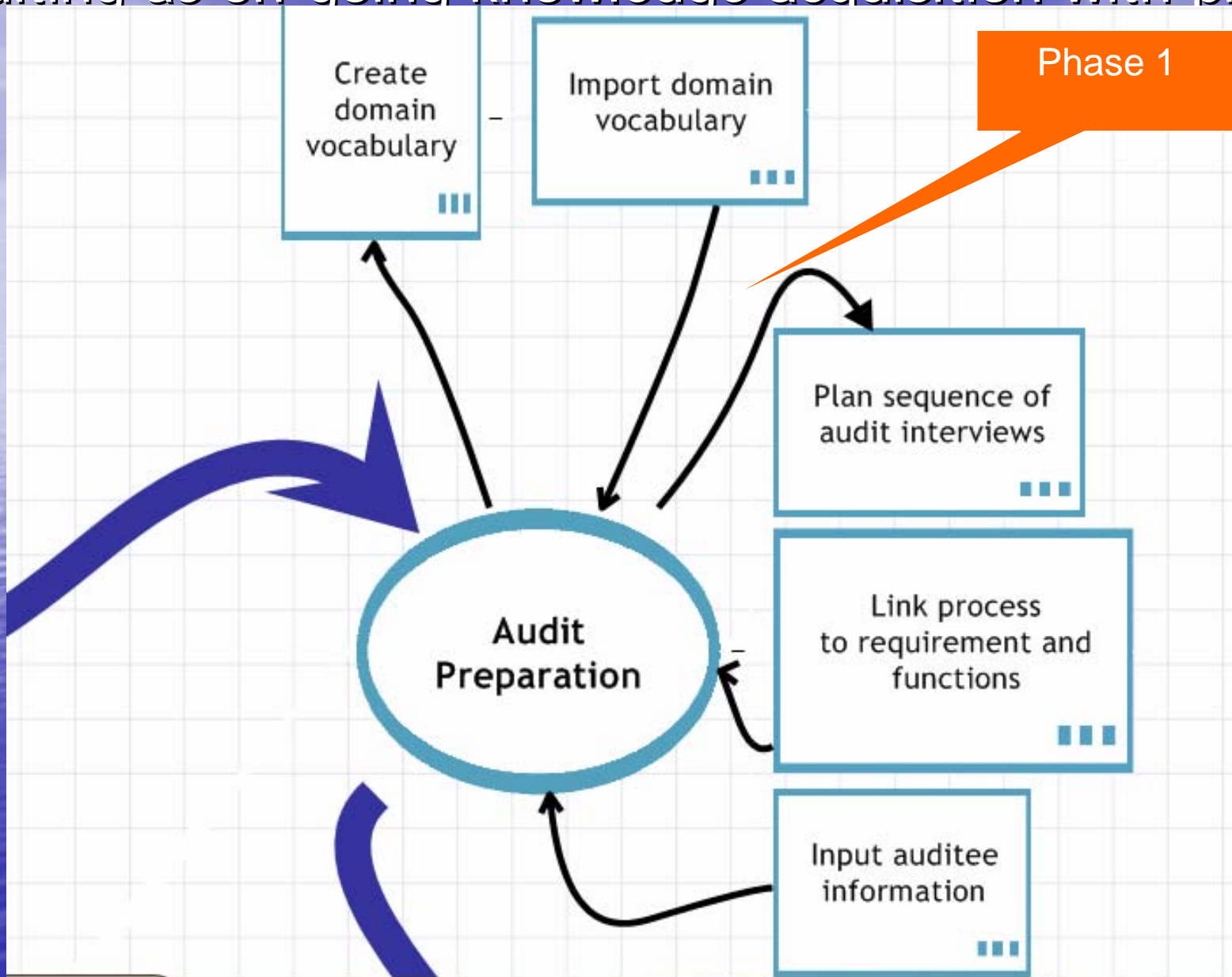
ensuring that authorized users have access to information and associated assets when required



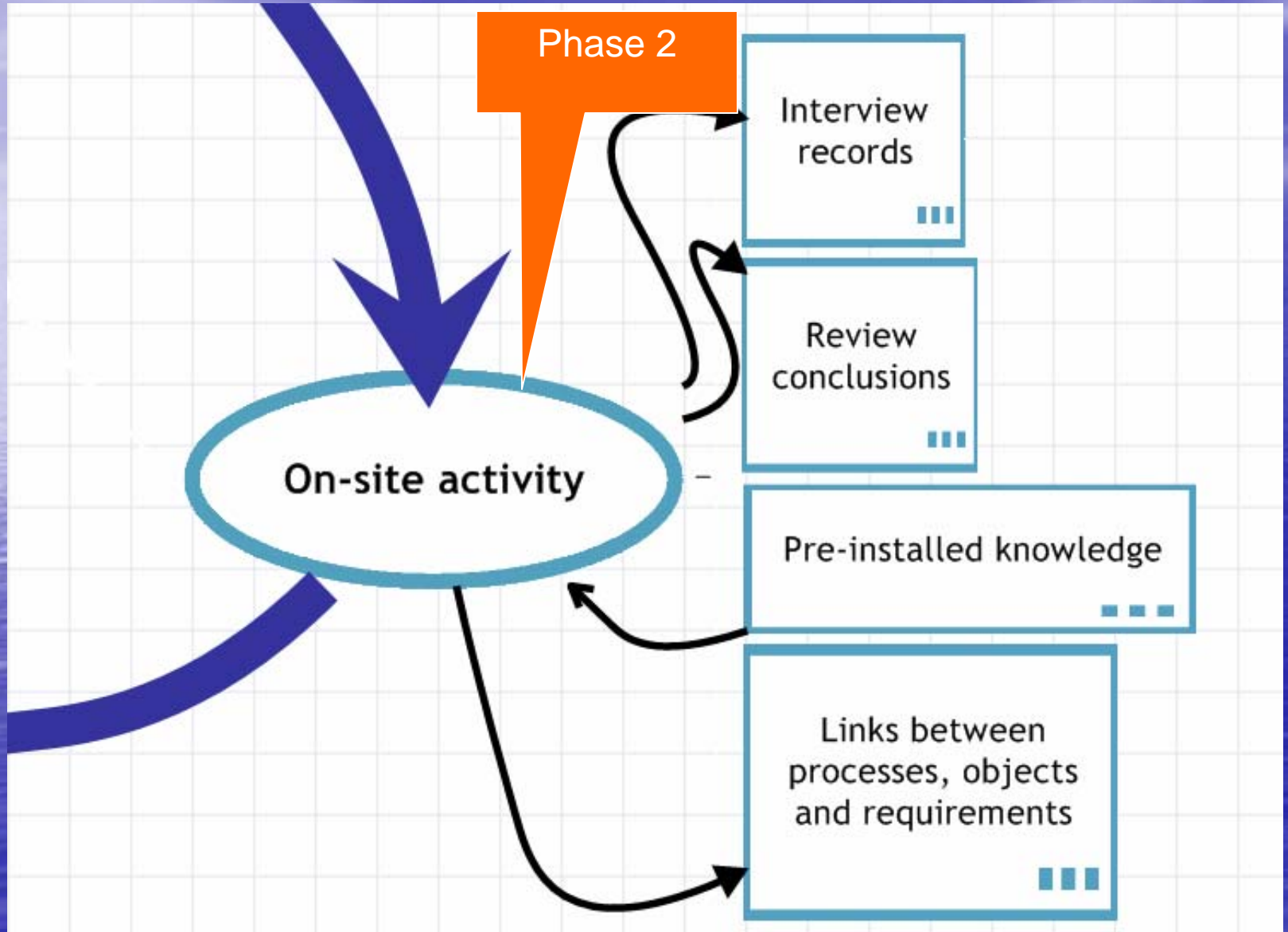
Auditing as on-going knowledge acquisition with Protege



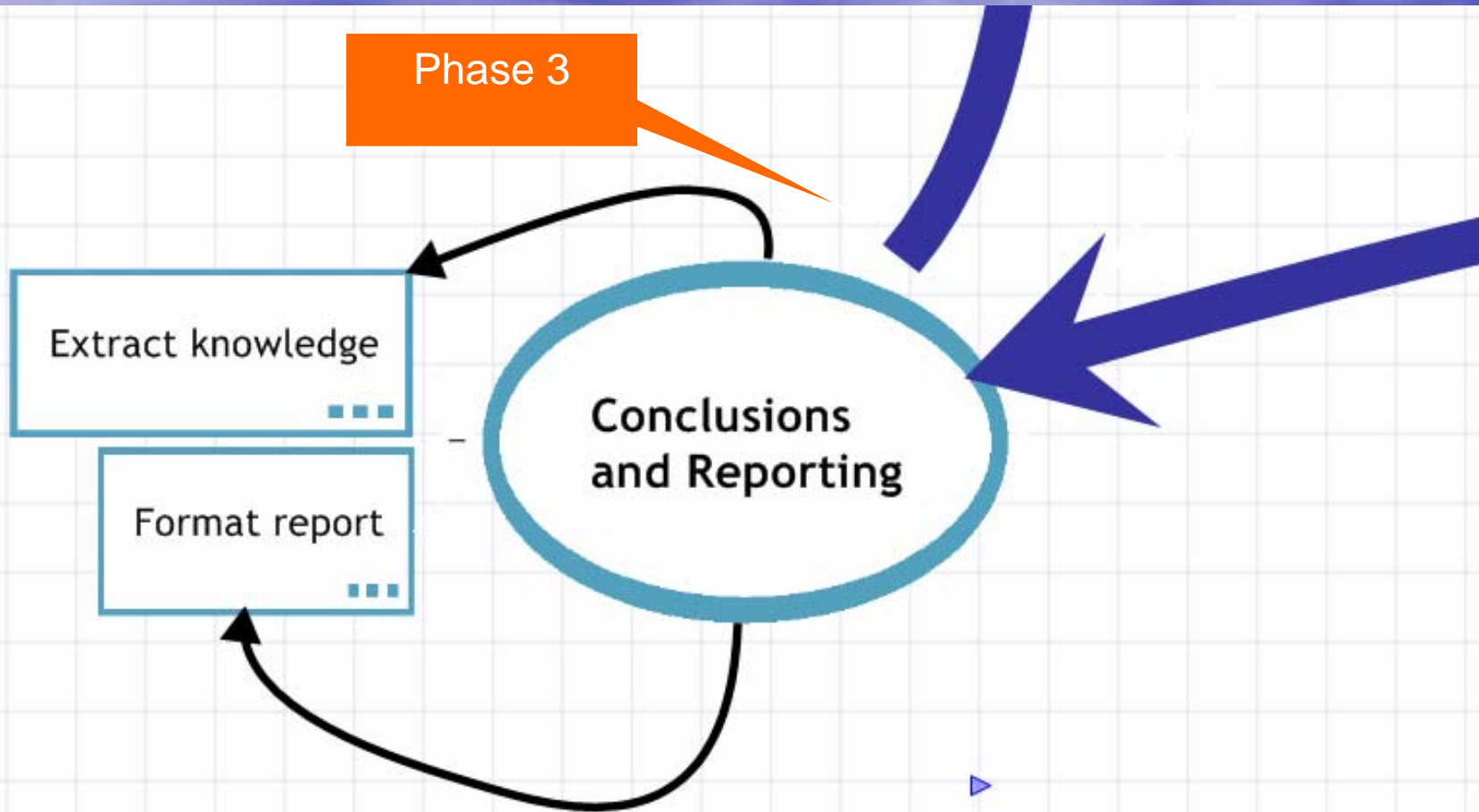
Auditing as on-going knowledge acquisition with protégé



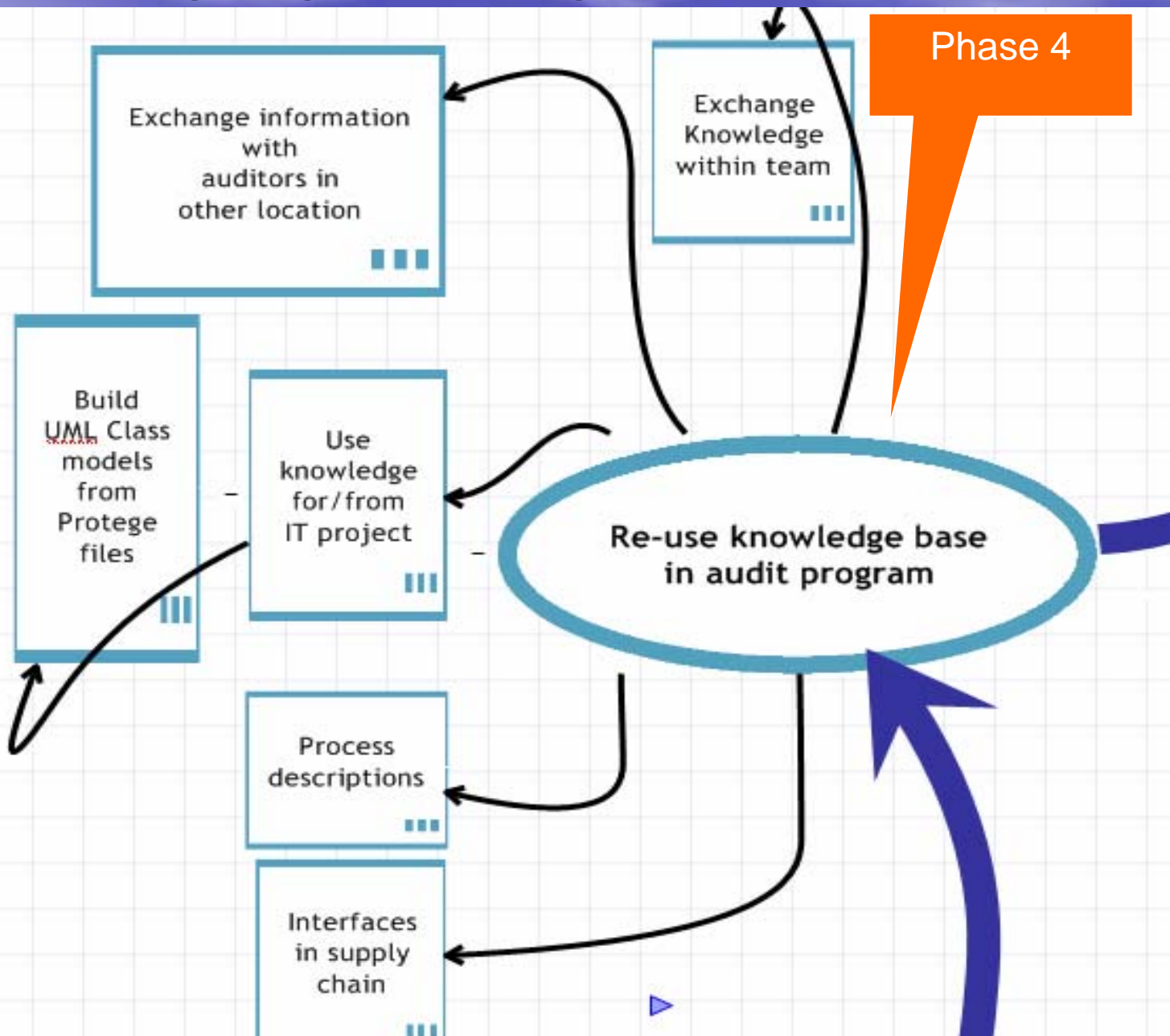
Auditing as on-going knowledge acquisition with protégés



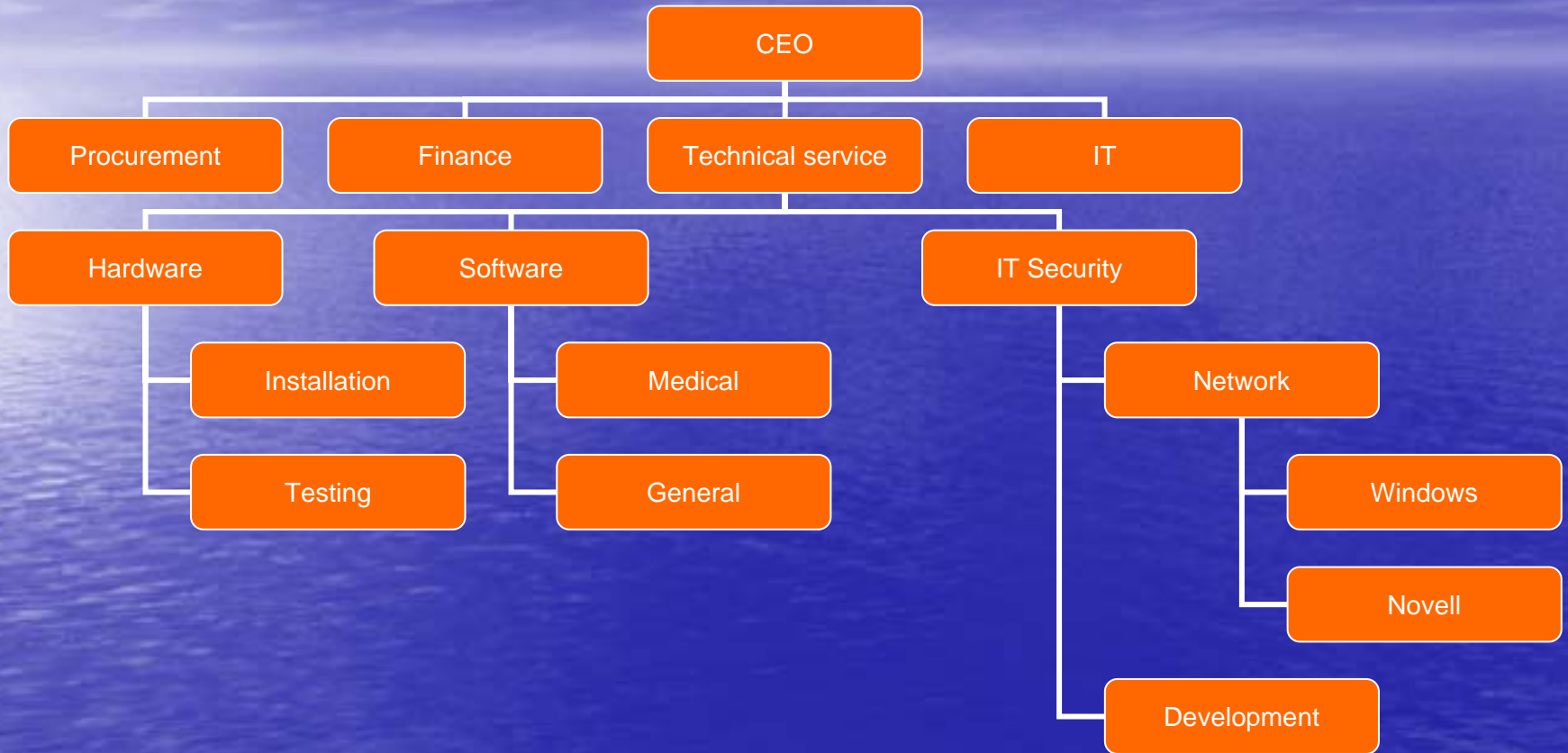
Auditing as on-going knowledge acquisition with protégés



Auditing as on-going knowledge acquisition with protégé



-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

```
graph LR; A[Understand Organizational Structure] --> B[Identify Applicable Requirement]; B --> C[Interpret Requirement In context]; C --> D[Select Right Level in organization]; D --> E[Select Right interviewee]; E --> F[Gather facts]; F --> G[Verify Common Understanding]; G --> H[Move in Organization]; H --> I[Link information]; I --> J[Confirm findings]; J --> K[Make conclusions];
```

Identify Applicable Requirement

Interpret Requirement In context

Select Right Level in organization

Select Right interviewee

Gather facts

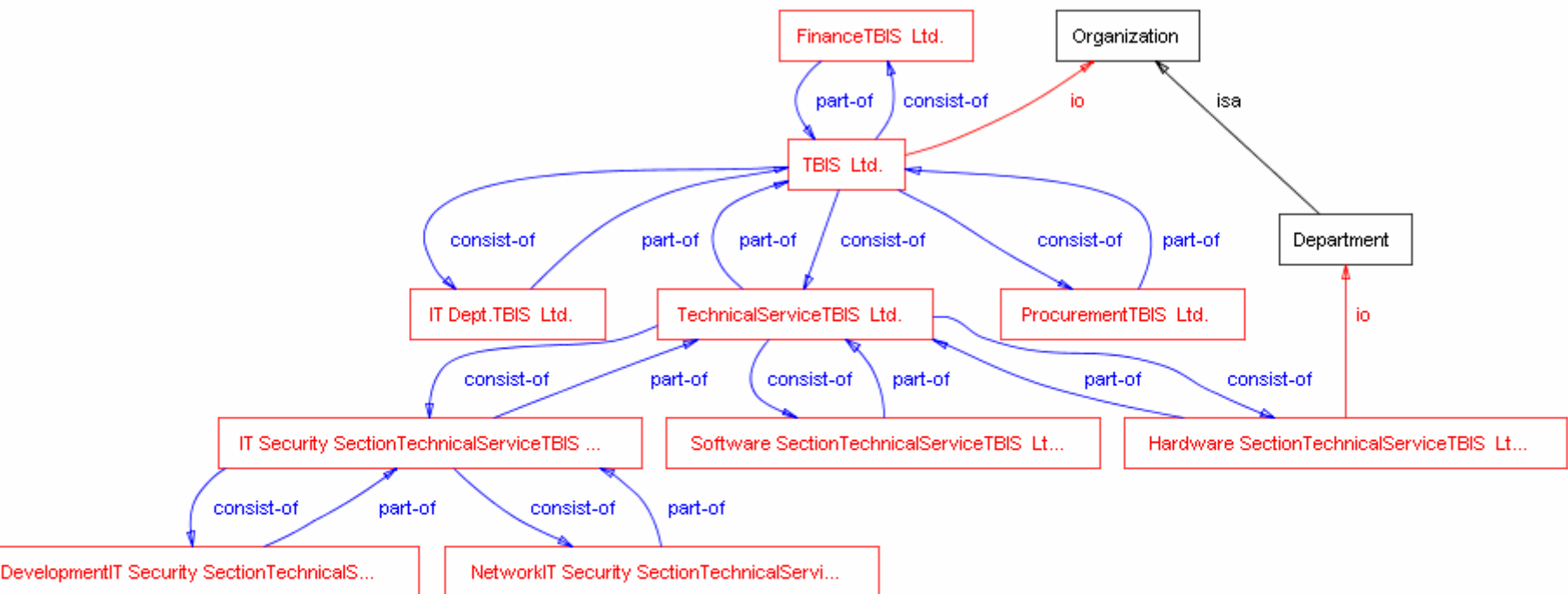
Verify Common Understanding

Move in Organization

Link information

Confirm findings

Make conclusions



TBIS structure

-organizational units-

Understand 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

Select Classes

- () QMSSpecification
- (4) QualityManagementSystem)
- (5) Management responsibility)
- (7) Product realization)
- (7.1) Planning of product realization)
 - (7.2) Customer-related processes)
 - (7.2.1) Determination of requirements related to the product.9k1)
 - () Post-delivery activities)
 - () Determine)
 - (7.2.2) Review of requirements related to the product.9k1)
 - (7.2.3) Customer communication.9k1)
 - (7.3) Design and development)
 - (7.4) Purchasing)
 - (7.5) Production and service provision)
 - (7.6) Control of monitoring and measuring devices)
- (8) Measurement, analysis and improvement)
- (6) Resource management)

OK Cancel

Understand Organizational Structure

Identify Applicable Requirement

Interpret 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

Next Audit Step/Document

(7.2.1) Determination of requirements related to the product.9k1 (type=RequirementMeta.gmpo, name...

Name of Requirement: Determination of requirements related to the product.9k1

Class: 7.2.1

RequirementType: QMS

Requirement: Concrete

System Name: Determination of requirements related to the product.9k1

Class Requirement Documentation

The organization shall determine

- a) requirements specified by the customer, including the requirements for delivery and post-delivery activities,
- b) requirements not stated by the customer but necessary for specified or intended use, where known,
- c) statutory and regulatory requirements related to the product, and
- d) any additional requirements determined by the organization.

RequiredActivity/Process

Select Concrete CIs

- MeasureProcess()
- AnalyseProcess()
- IdentifyControlOfOutsourcedProcesses.9k1()
- ReviewActivity()
- Determine and Define()
- DefineEvaluationRequirementsForAction()
- Define requirements for determining potential causes of nonconformities()
- DetermineNecessaryCompetence()
- DetermineInfrastructure()
- DetermineRequiredInspection()
- DetermineRequiredValidation()
- DetermineMethodsForObtainingCustomer Requirements()
- Determine records of evidence that result in nonconformities()
- Determine required monitoring activities()
- Determine need to establish processes()
- DetermineCommunicationArrangement()

Understand 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

Recording an interview

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

Understand Organizational Structure

Identify Applicable Requirement

Interpret Requirement In context

Select Right Level in organization

Select Right interviewee

Gather facts

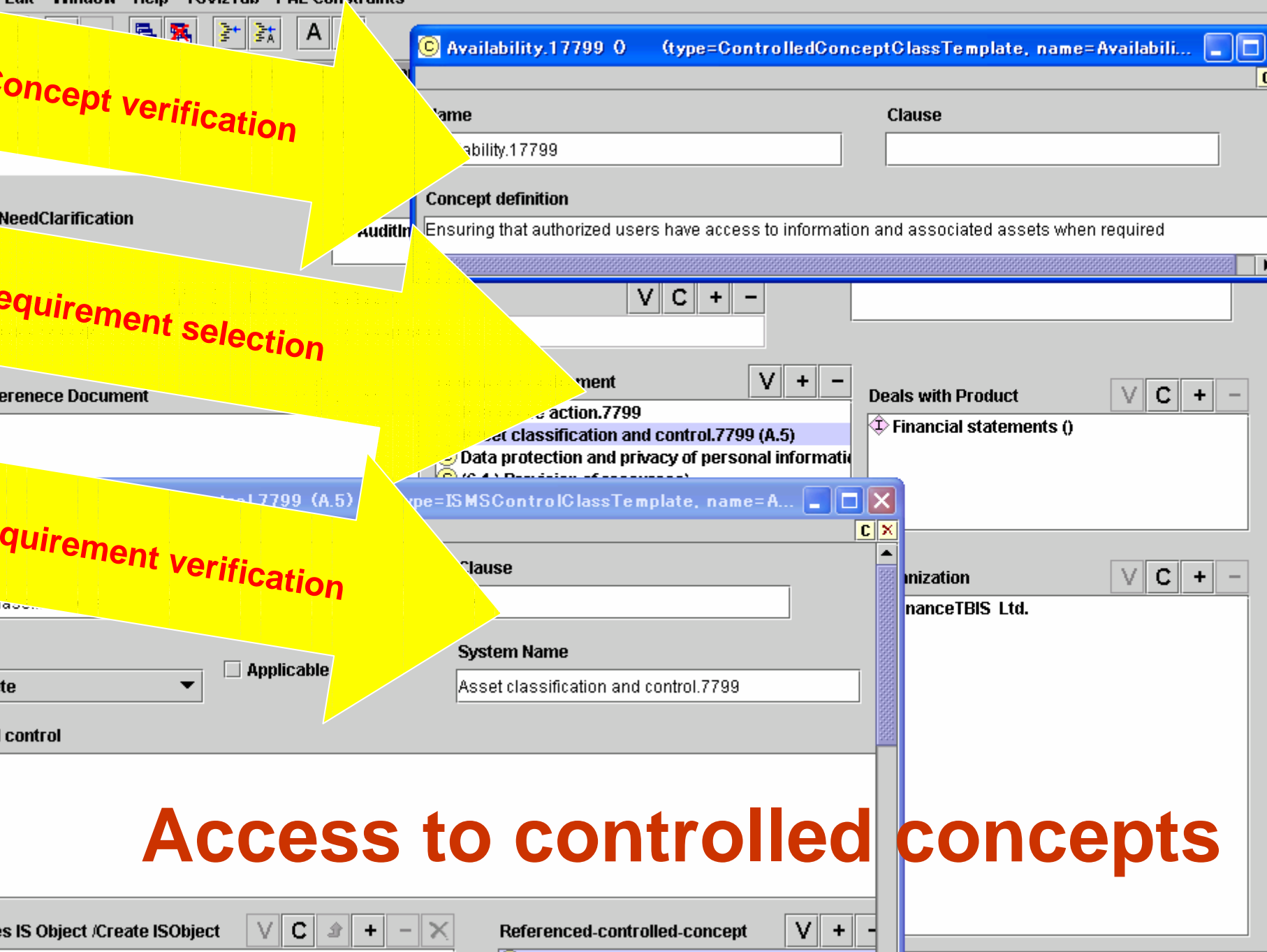
Refer to controlled concepts

Move in Organization

Link information

Confirm findings

Make conclusions



Concept verification

Requirement selection

Requirement verification

Access to controlled concepts

Understand Organizational Structure

Identify Applicable Requirement

Interpret Requirement In context

Select Right Level in organization

Select Right interviewee

Gather facts

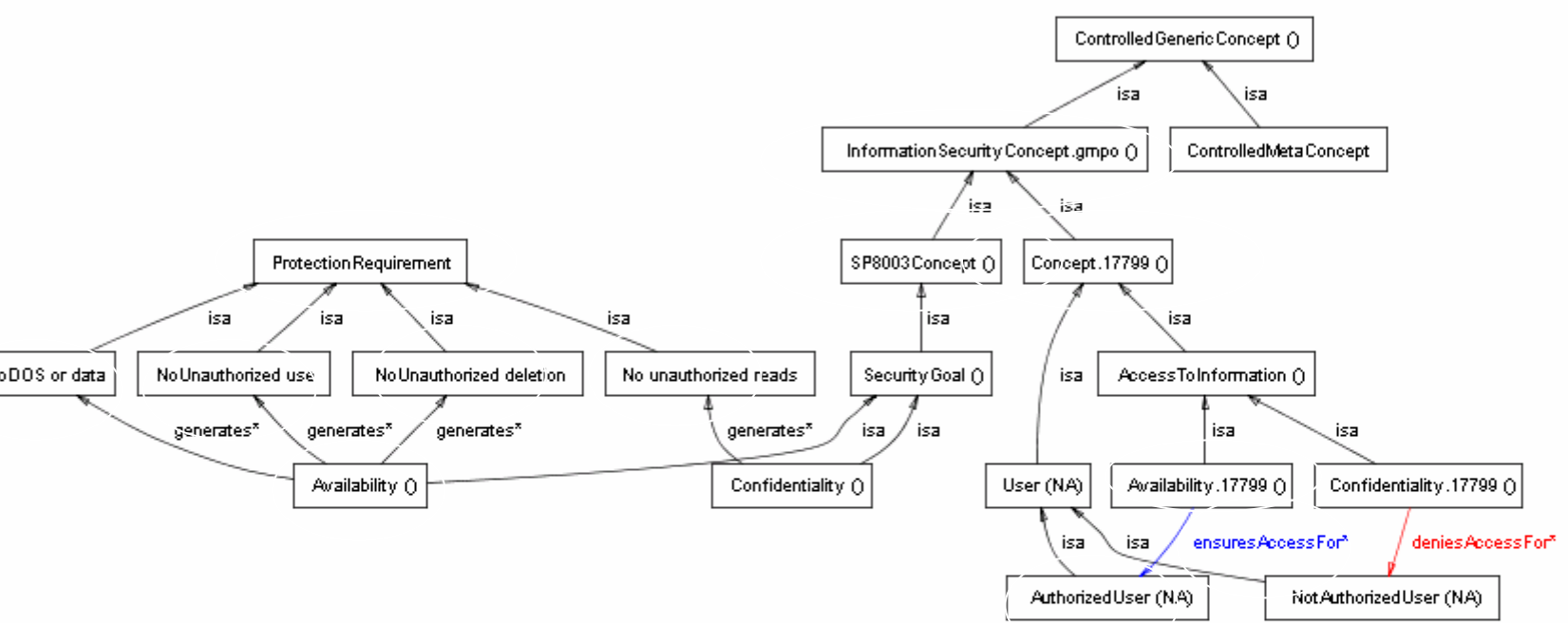
Verify Common Understanding

Move in Organization

Link information

Confirm findings

Make conclusions



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

The audit console in Protege

The screenshot displays the Protege software interface, specifically the audit console. The top navigation bar includes tabs for Classes & Instances, PAL Constraints, Jambalaya, Individuals, PAL Queries, Instances, and Ontology. The main workspace is divided into several sections:

- Classes & Instances:** Shows a tree view of classes. The 'Product' class is expanded, showing 'Network Design' and 'Consultancy for Process' as subclasses. A red box highlights this section.
- Instances:** Lists various instances such as 'Mr.I.T.Perfect', 'Procurement', 'Finance', 'TechnicalService', 'IT Dept.', 'Hardware SectionTechnicalService', 'Software SectionTechnicalService', 'IT Security SectionTechnicalService', 'NetworkIT Security SectionTechnicalService', and 'DevelopmentIT Security SectionTechnicalService'.
- Workflow Diagram:** A central diagram on a grid background showing a sequence of steps connected by 'nextStep' arrows:
 - 'Opening TBIS' (green circle) leads to 'Team Split' (grey triangle).
 - 'Team Split' branches into 'Finace Dept(false)' (blue circle) and 'Procument Dept. (false)' (blue circle).
 - 'Finace Dept(false)' leads to 'IT Security Section(false)' (blue circle).
 - 'Procument Dept. (false)' leads to 'Technical Service Dept. (false)' (blue circle).
 - 'IT Security Section(false)' leads to 'Technical Service Dept. (false)'.
 - 'Technical Service Dept. (false)' leads to 'Team Join' (grey triangle).
 - 'Team Join' leads to 'Audit Team Meeting' (grey circle).
- Conclusion:** A section at the bottom left with a 'Note' field, containing text like 'Process approach week', 'Annual statement 57/70 preventive action ()', and 'Handling of non-conformity'.

At the bottom of the screen, there are two system tray notifications: 'Administrator, 3 12 11:23' and 'Administrator, 3 09 17:34'.

Understand Organizational Structure

Identify Applicable Requirement

Interpret Requirement In context

Select Right Level in organization

Select Right interviewee

Gather facts

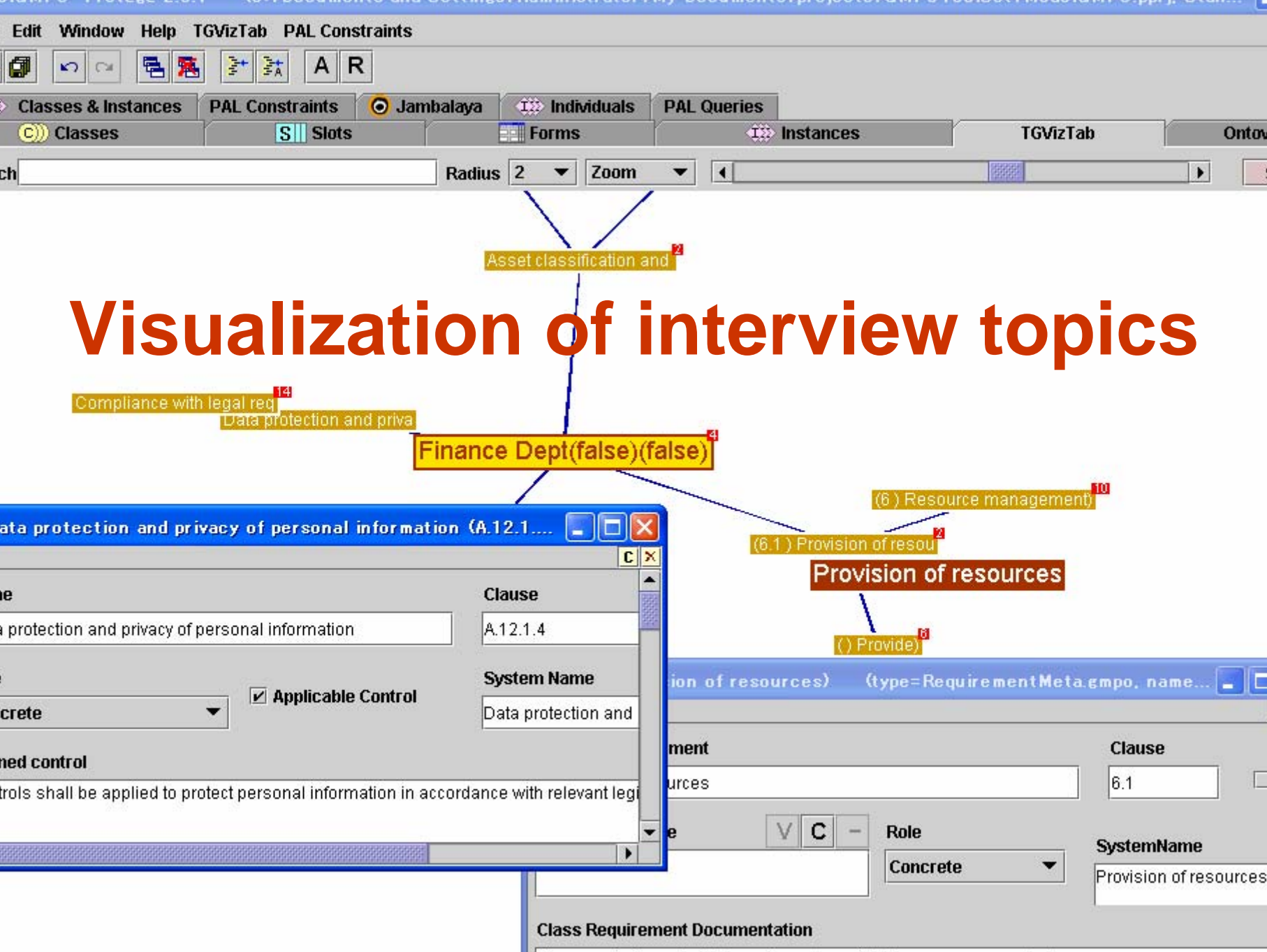
Verify Common Understanding

Move in Organization

Review situations, Link information

Confirm findings

Make conclusions



Visualization of interview topics

Finance Dept(false)(false)

Asset classification and

Compliance with legal req

Data protection and priva

(6) Resource management

(6.1) Provision of resou

Provision of resources

() Provide

Data protection and privacy of personal information (A.12.1....)

Clause	A.12.1.4
System Name	Data protection and
Applicable Control	<input checked="" type="checkbox"/>

Concrete

Controlled control

Controls shall be applied to protect personal information in accordance with relevant legi

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

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 protege

Use/Phase	Description	Benefits	Obstacles
Audit planning	Modeling of organization structure and organizational artifact	Fast understanding by visualization and taxonomies	Requires understanding of ontology concepts
On-site audit	Creation of instances of organization concepts Linking artifacts	Auditors have pre-defined concepts available	Requires a reasonable degree of skill to use protégé Speed problems.
Audit documentation	Is required but not a purpose in itself	Knowledge base stored in XML Audit findings and conclusions extracted	Need customization of user interface/print/representation
Communication within team	Necessary for auditing in a team	Instantaneous	High technical requirement Understandability of knowledge representation
Re-usability of knowledge	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 acquisition
- 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