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 3rd 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 Protégé

Phase 1
- Exchange Knowledge within team
- Re-use knowledge base in audit program

Phase 2
- Plan sequence of audit interviews
- Audit Preparation

Phase 3
- Pre-installed knowledge
- Links between processes, objects and requirements

Phase 4
- Use knowledge in/on IT project
- Build UML Class models from Protege files

Conclusions and Reporting
- Format report
- Extract knowledge

On-site activity
- Interview records
- Review conclusions

Protege as Audit tool
- Link process to requirement and functions
- Input auditee information
Auditing as on-going knowledge acquisition with protégé

Phase 1

- Create domain vocabulary
- Import domain vocabulary
- Plan sequence of audit interviews
- Link process to requirement and functions
- Input auditee information

Audit Preparation
Auditing as on-going knowledge acquisition with protégé

Phase 2

- Interview records
- Review conclusions
- Pre-installed knowledge
- Links between processes, objects and requirements
Auditing as on-going knowledge acquisition with protégé

Phase 3

Extract knowledge

Format report

Conclusions and Reporting
Auditing as on-going knowledge acquisition with protégé

Phase 4

- Exchange information with auditors in other location
- Exchange Knowledge within team
- Build UML Class models from Protege files
- Use knowledge for/from IT project
- Re-use knowledge base in audit program
- Process descriptions
- Interfaces in supply chain
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
TBIS structure

-organizational units-
Selecting stored requirements
Selecting required processes and activities
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
Access to controlled concepts

- Requirement selection
- Concept verification
- 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
The audit console in Protege
Visualization of interview topics

- Asset classification and
- Compliance with legal reg...
- Data protection and priva
- Finance Dept(false)(false)
- (6) Resource management
- (6.1) Provision of resou
- Provi...
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 protégé

<table>
<thead>
<tr>
<th>Use/Phase</th>
<th>Description</th>
<th>Benefits</th>
<th>Obstacles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit planning</td>
<td>Modeling of organization structure and organizational artifact</td>
<td>Fast understanding by visualization and taxonomies</td>
<td>Requires understanding of ontology concepts</td>
</tr>
<tr>
<td>On-site audit</td>
<td>Creation of instances of organization concepts</td>
<td>Auditors have pre-defined concepts available</td>
<td>Requires a reasonable degree of skill to use protégé Speed problems.</td>
</tr>
<tr>
<td>Audit documentation</td>
<td>Is required but not a purpose in itself</td>
<td>Knowledge base stored in XML</td>
<td>Need customization of user interface/print/representation</td>
</tr>
<tr>
<td>Communication within team</td>
<td>Necessary for auditing in a team</td>
<td>Instantaneous</td>
<td>High technical requirement Understandability of knowledge representation</td>
</tr>
<tr>
<td>Re-usability of knowledge</td>
<td>Currently not the focus of auditing; missed chance</td>
<td>Domain vocabulary can be extended</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Usage in IT projects</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Part of system documentation</td>
<td></td>
</tr>
</tbody>
</table>
Future applications / expectations

- 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