Active IT Audit Manual

Tutorial

Applicable to versions:

- Web
- Desktop v2.x

"IT Audit is an examination of implementation of IT systems to ensure that they meet the organization's business needs without compromising security, privacy, cost, and other critical business elements."

(WGITA – IDI HANDBOOK ON IT AUDIT FOR SUPREME AUDIT INSTITUTIONS)

"Audit of Information Systems may be defined as the examination of controls related to IT-driven information systems, in order to identify instances of deviation from criteria, which have in turn been identified based on the type of audit engagement - i.e. Financial Audit, Compliance Audit or Performance Audit."

(GUID 5100 PARAGRAPH 3.2)

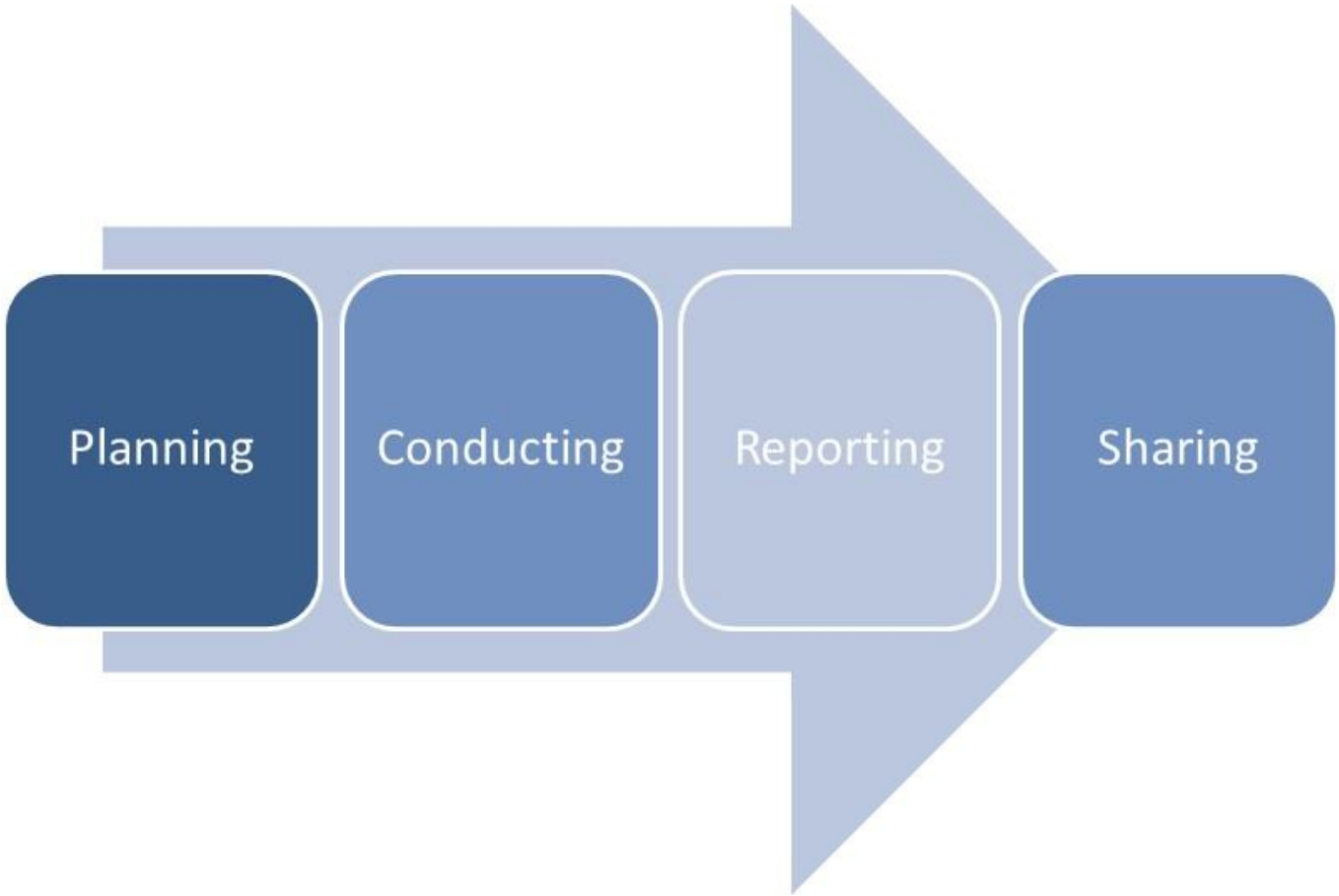
Objective

The ***Active IT Audit Manual*** tool is based on the *IT Audit Handbook* and have the essential objective of helping the auditor to plan and conduct IT audits

It provides the users with:

- practical guidance
- essential technical information, and
- key audit questions

The full process diagram can be see next:



It’s important to ensure that the audit process is preserved to enable subsequent verification, monitoring and share of the audit analysis procedures (ISSAI 100 PARAGRAPH 42). This involves documenting:

- The plan, scope and objectives,
- Audit program,
- Evidences collected.

Template activity plans, which includes the subject, criteria and scope are produced, as well audit matrices to help recording the findings during the IT audit conduct and executive summaries.

The matrices are actually taken from the annexes of the WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions and can be used by the auditors as working papers.

The obtained findings can be latter collected in a central point to help the auditor interpreting and judging against the audit questions previously raised at the planning stage. They also form the core of the information to share with the community, along with references for the published audit report, in the project" Control Space of e-Government" (the CUBE), an EUROSAI Initiative.

Desktop versions and coverage

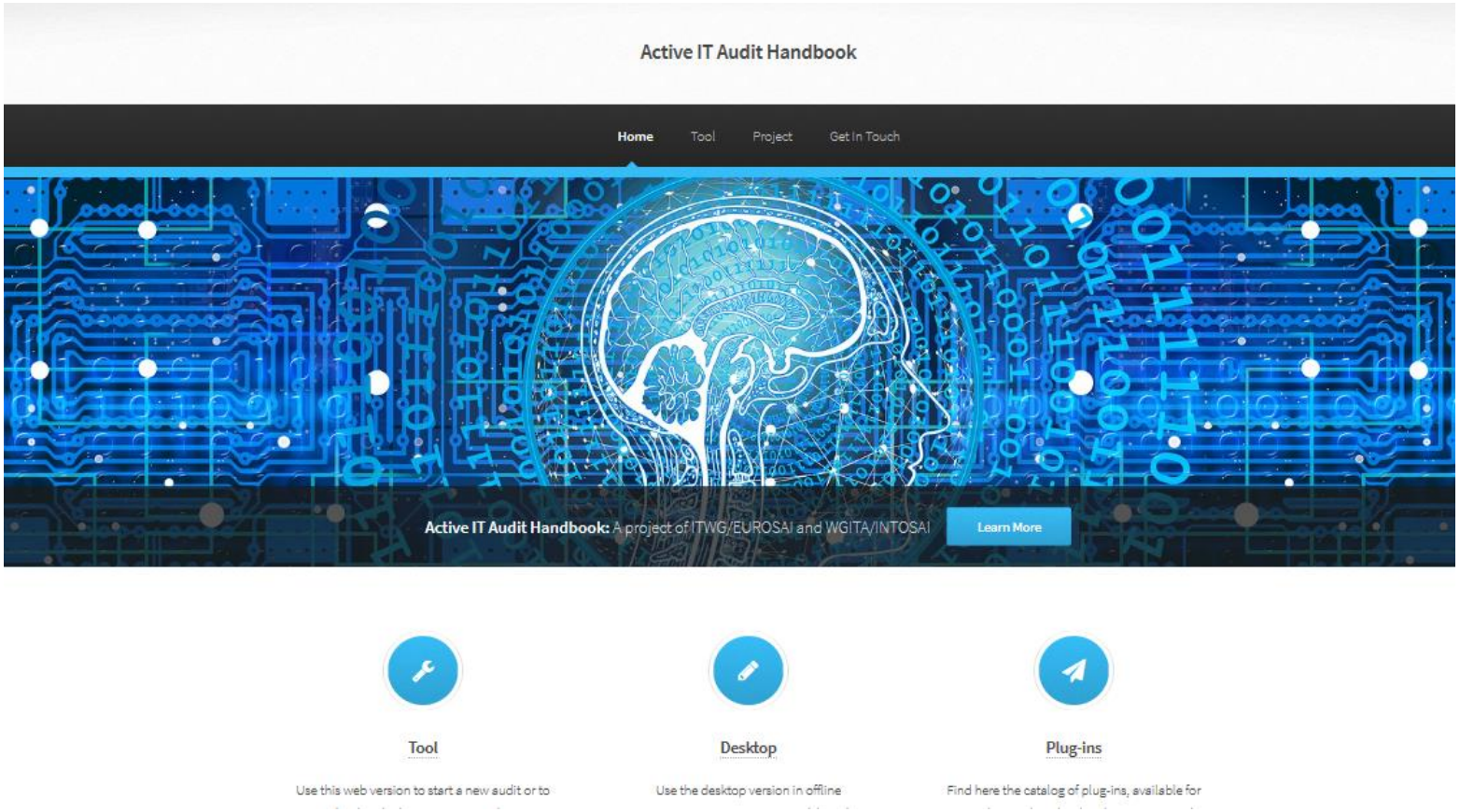
Developed and maintained:

- Under stable, wide accepted and (even) open productivity software;

- To support the major desktop ecosystems;

Web version

http://aitam.tcontas.pt



Configure the working environment

The **desktop version** is provided as a zip folder. It contains a spreadsheet in **MS Office** (StartHereMSOffice.xlsm) and in **Libre Office** (StartHereLibreOffice.ods) as a control dashboard for the audit development and several matrixes templates.

Once extracted, all files must be kept in the same folder and subfolders.

Configure the working environment

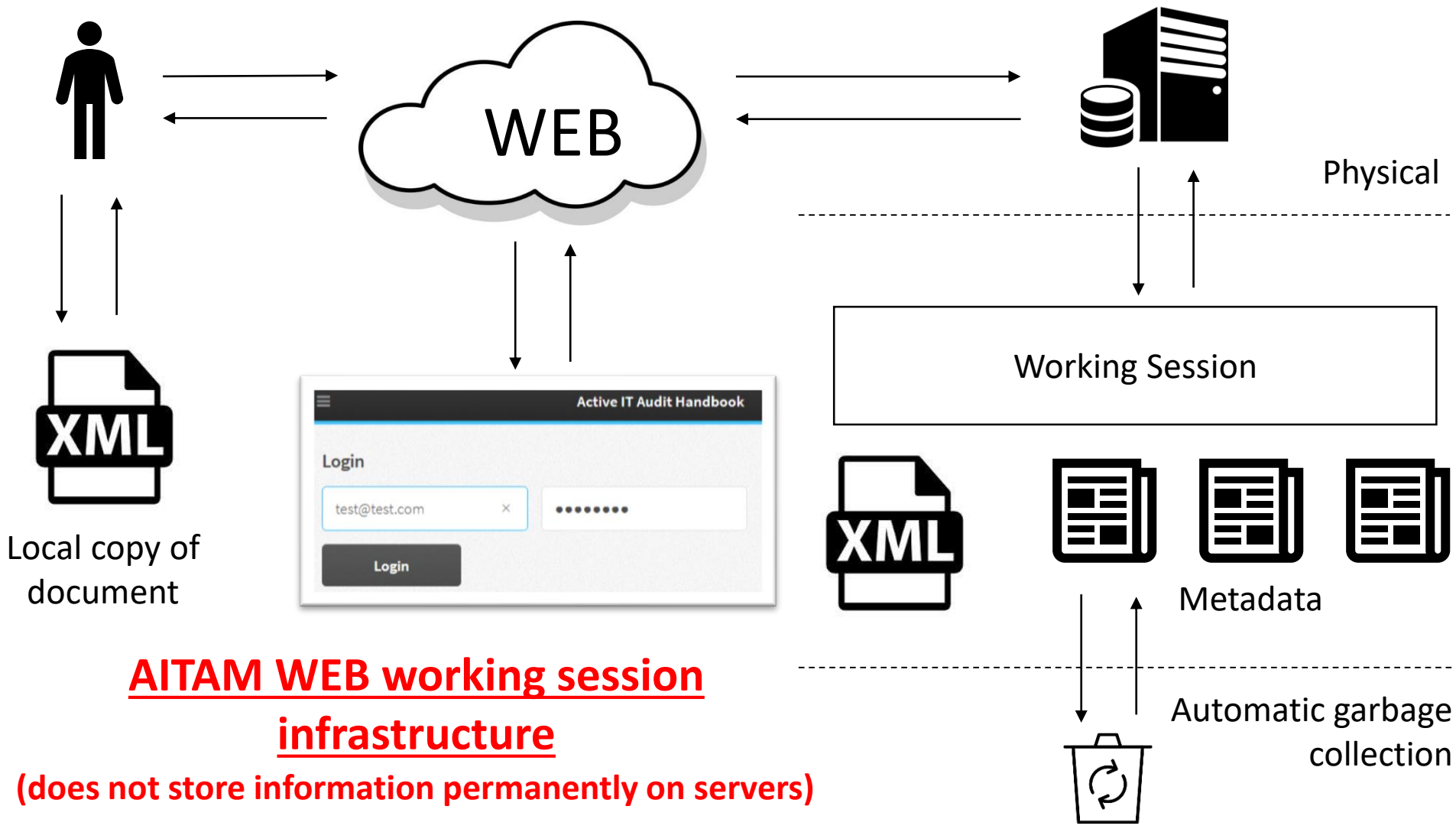
The internal behavior of the spreadsheets in desktop versions, as well of some text templates, was customized through macros, in VBA/BASIC. To help the code inspection is full commented in English. It only references functions and objects (late binding) pre-installed in OS (no need to reference additional libraries).

So, you only have to enable macros!

Web version

Single prerequisite to work in:

- Username / password.

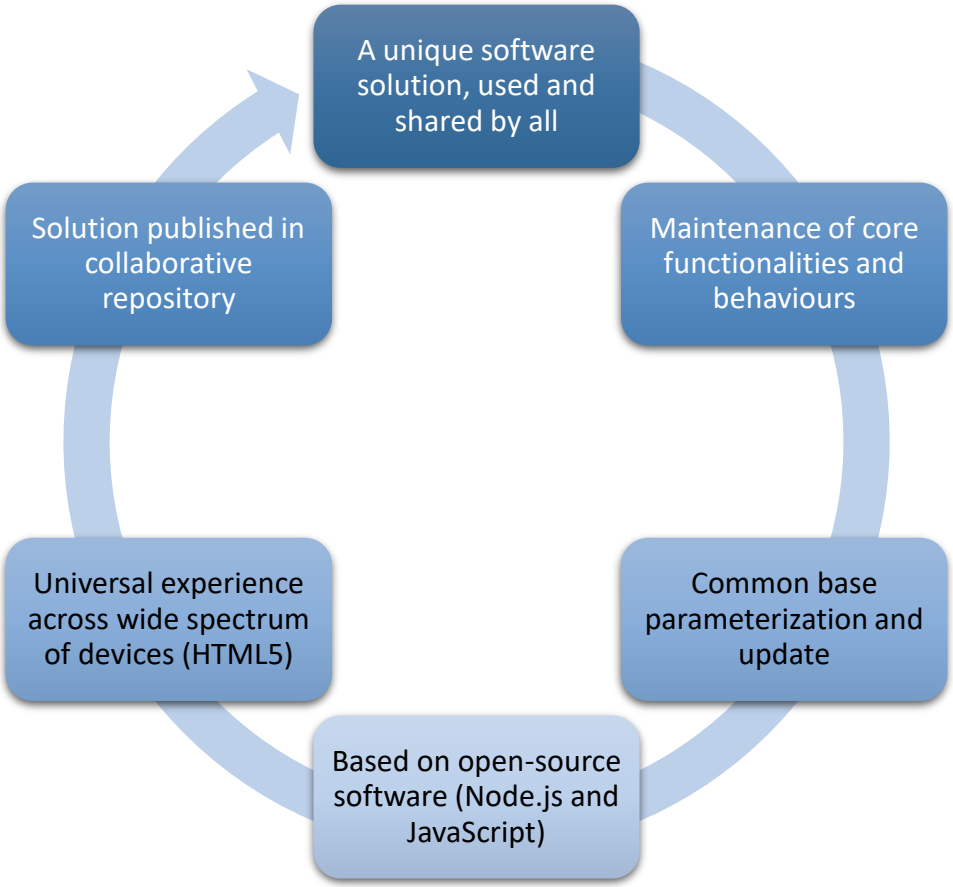


AITAM WEB working session infrastructure

(does not store information permanently on servers)

Web version

(Main) key ideas and challenges



Web and desktop versions

(Main) key ideas and challenges

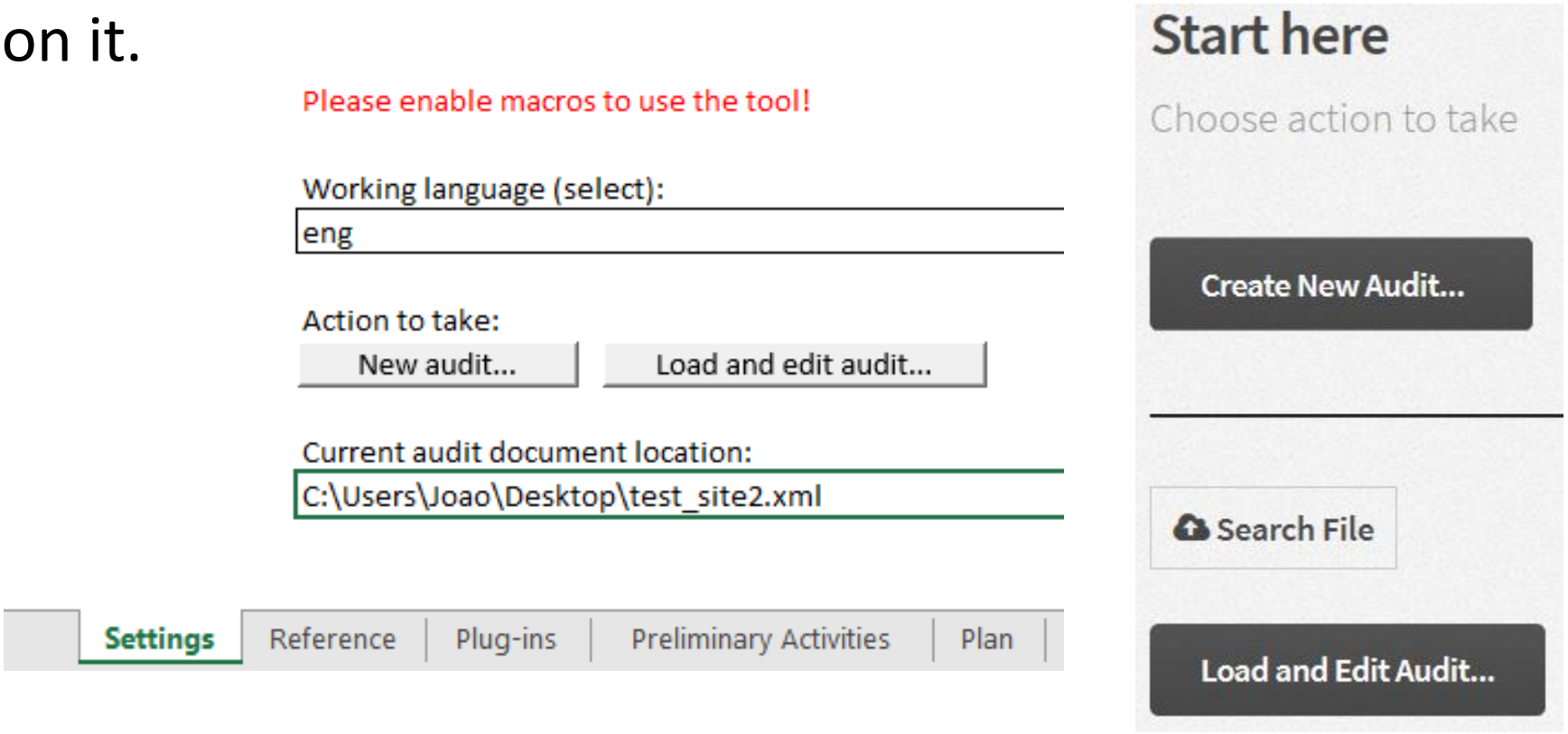
Core functionalities are maintained (but with slightly different mechanisms).

Same internal structure to store and distribute data (XML) as desktop version, preserving the formal description of the elements and the attributes.

Means: electronic data interchange across desktop and web current versions.

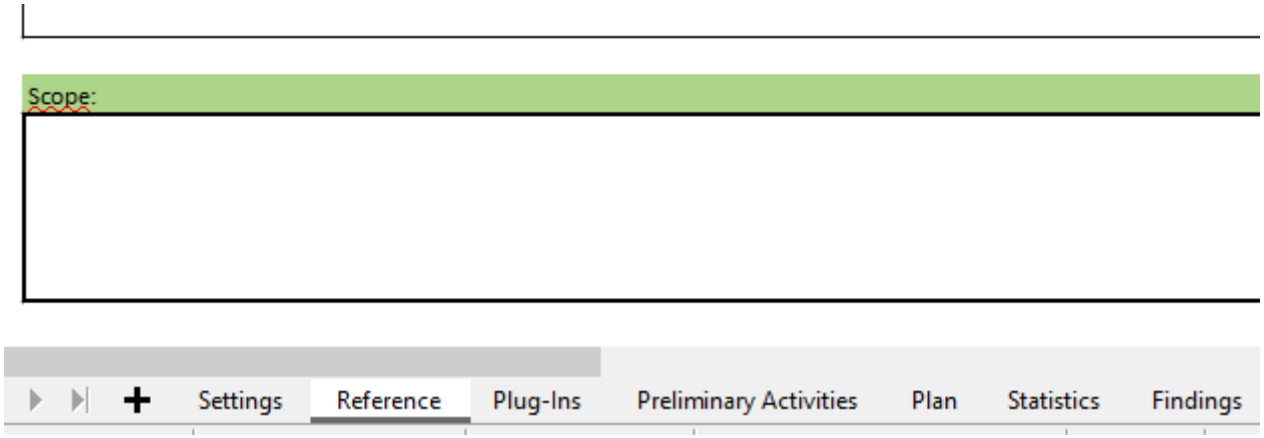
Working environment (initial set.)

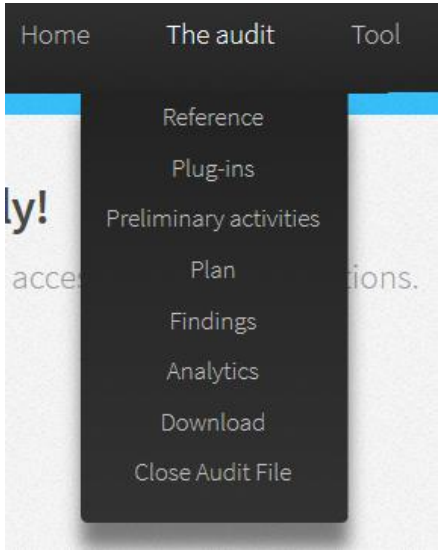
Start creating an audit or loading an existent one to work on it.



Working environment (structure)

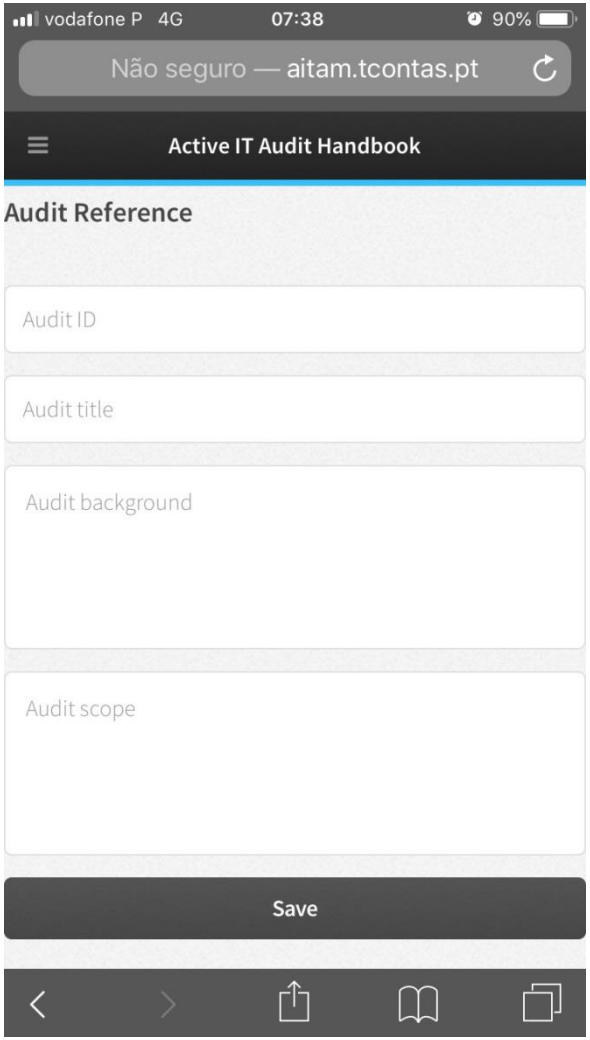
The core working areas are structured in worksheets (desktop version) or submenus/commands under the "Audit Menu".





(Audit) Reference

In the first worksheet/command (named “Reference”) auditors can describe the audit in more detail, starting customizing it.



Preliminary activities

"auditors should obtain an understanding of the nature of the entity/programme to be audited." (ISSAI 100 PARAGRAPH 49)

The worksheet/command "Preliminary activities" provides the user with additional guidance (as pointed out on ISSAI 5300):

- The role and timing of planning;
- Preliminary engagement activities;
- Planning activities;
- Knowledge of the auditee and of the environment;
- Scope of the assessment: Which information systems, which logical, physical or geographical boundaries?
- Resources available: Qualified staff or consultants, budgets, timeframes;
- Availability of reliable threat statistics and cost figures, appropriate for the local conditions; adaptation of the default values, as necessary;
- Additional considerations in initial audit engagements.

Preliminary activities

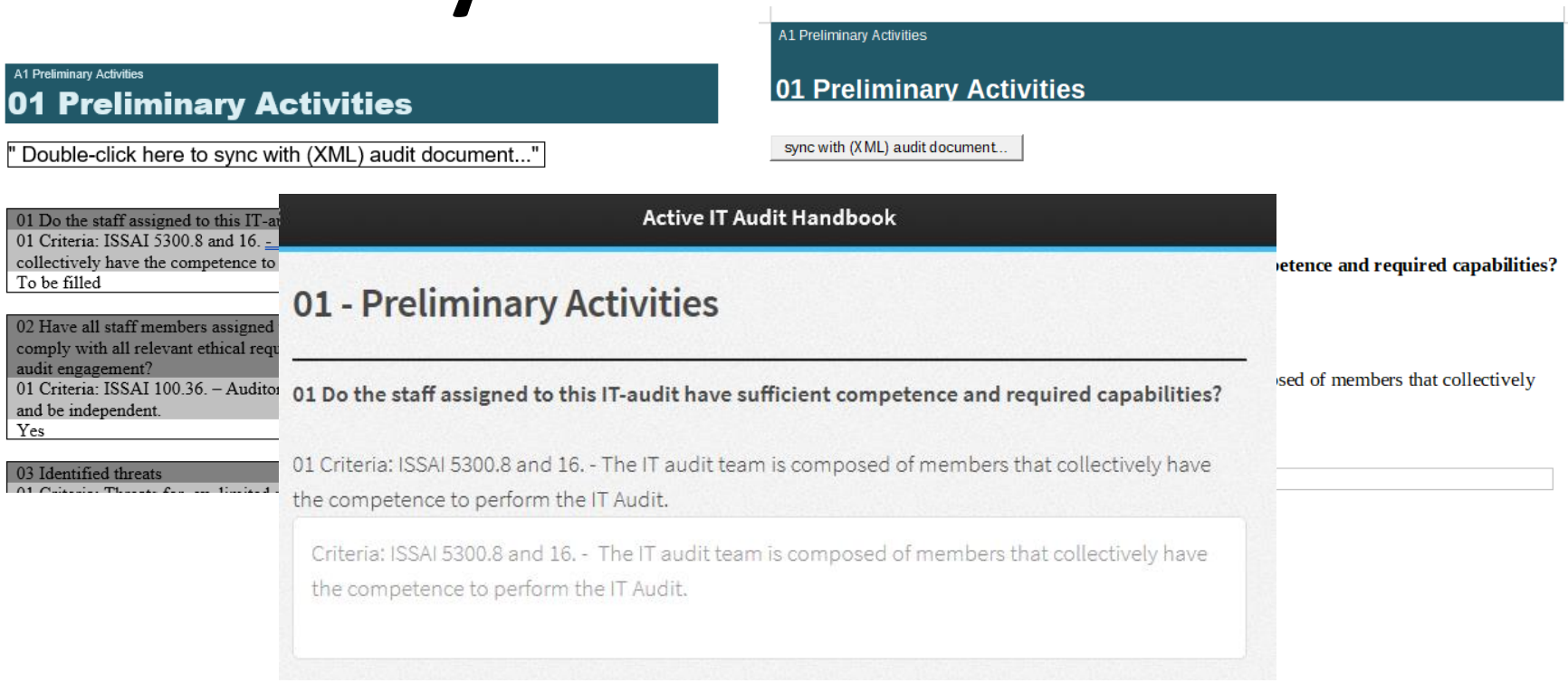
Reload list

Preliminary Activities and planning (start) the audit:

Area	Support Matrixes
A1 Preliminary Activities	01 Preliminary Activities
A1 Preliminary Activities	02 Planning meeting of the IT audit team
A1 Preliminary Activities	03 Opening meeting with the management of the audited entity
A2 Planning the Audit	01 Understanding the entity
A2 Planning the Audit	02 Understanding the IT-systems
A2 Planning the Audit	03 Input into audit strategy and audit plan

Those activities are aggregated in domains. They are a hyperlink for the corresponding matrix, which will assist the auditor.

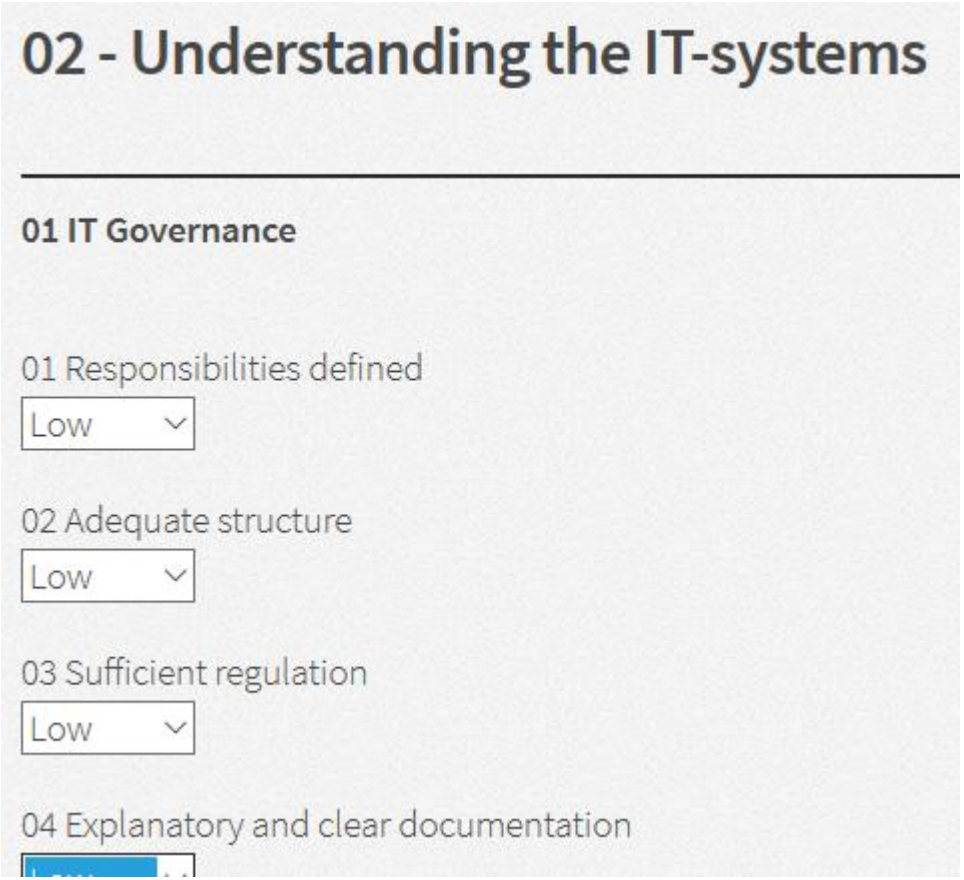
Preliminary activities



In the desktop versions the auditor will use the matrix to fill information and sync with dashboard. At web version, a form is provided, but the user can generate a print version.

Preliminary activities

In particular, the matrix named *02 Understanding the IT-systems*, under preliminary activities domain A2, is also automated. It maps the different IT domains and areas in order to help the auditor perform a preliminary assessment of IT Controls, as stated by ISSAI 5300 21.1. Once used and filled, it can be later synchronized with risk analysis as a suggestion and a guide to auditor judgment.



Pre-audit analysis

The pre-audit analysis goal is to provide data, which will support risk analysis, i.e. basis for the planning the audit and organising the initial audit folder. The process looks as follows:

Input:

- information obtained from auditee in the pre-audit phase;
- additional relevant data concerning the auditee and their IT systems;
- results of other audits at the auditee or covering similar types of problems.

Pre-audit analysis

The pre-audit analysis goal is to provide data, which will support risk analysis, i.e. basis for the planning the audit and organising the initial audit folder. The process looks as follows:

Steps:

1. Analyze available input data.
2. Generate the form *A2.02 Understanding IT systems* – it will depend of the type of IT audit you perform – standard *IT Audit Handbook* based or *Plug-in* based. The form will by generated automatically after clicking the *A2.02 Understanding IT systems*, and will take into account the basis of the IT audit.
3. Decide about qualifications of relevant fields in the form *A2.02 Understanding IT systems*.

Pre-audit analysis

The pre-audit analysis goal is to provide data, which will support risk analysis, i.e. basis for the planning the audit and organising the initial audit folder. The process looks as follows:

Steps (cont.):

4. Map the pre-audit analysis results to the risk analysis grid. For this particular step the user must, at first, access the “Plan” worksheet and press the action button “Get Areas and Issues” to obtain the information about different IT domains which will assist the IT auditors in identifying potential auditable areas. At the top an action button, named “Sync with pre-Assessment”, is available. Once pressed, triggers the synchronization process between the information previously collected and evaluated in the pre-assessment and the risk analysis.

Pre-audit analysis

The pre-audit analysis goal is to provide data, which will support risk analysis, i.e. basis for the planning the audit and organizing the initial audit folder. The process looks as follows:

Steps (cont.):

5. Complete the risk analysis by applying professional judgement

	Risks (Weight)	Include in Audit	Reasons, risks and remarks
	3 - High	Yes	Pre-Assessment: Domain - Medium; Area - Hig
	3 - High	Yes	Pre-Assessment: Domain - Medium; Area - Hig
	3 - High	Yes	Pre-Assessment: Domain - Medium; Area - Hig
	2 - Medium	Yes	Pre-Assessment: Domain - Medium; Area - Lov
	2 - Medium	No	Pre-Assessment: Domain - Medium; Area - Lov

The pre-audit analysis can be helpful in preparation of the audit and in more precise risk analysis. The tool will work, however, even if the analysis is not performed, which means the risk analysis is based on the professional judgment only.

Plan

Plan on a risk assessment based selection (map domains, areas and issues, design the audit)

Centered in detailed description of different IT domains which will assist the IT auditors in identifying potential auditable areas

- IT Governance
- IT Operations
- Development and Acquisition
- Outsourcing
- Information Security
- Business Continuity and Disaster Recovery
- Application Controls

Plan (scoping)

Start with planning on a risk assessment based selection

*We call it **scoping** through **IT domain cascade**:*

- *Identify a specific **domain** or a combination of domains*
- *Select the most critical **areas** and **issues***

Plan (scoping)

"The scoping of IT Audit would involve deciding the extent of audit scrutiny, the coverage of IT systems and their functionalities, IT processes to be audited, locations of IT systems to be covered and the time period to be covered."

(WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions)

The auditors should select the audit areas and issues through the planning process by analyzing potential areas and issues, as well identifying risks and problems.

As soon as you access the worksheet or the command named "**Plan**". It establishes the mapping table of different IT domains which will assist the IT auditors in identifying potential auditable areas.

Plan (scoping)

Domains, areas and issues

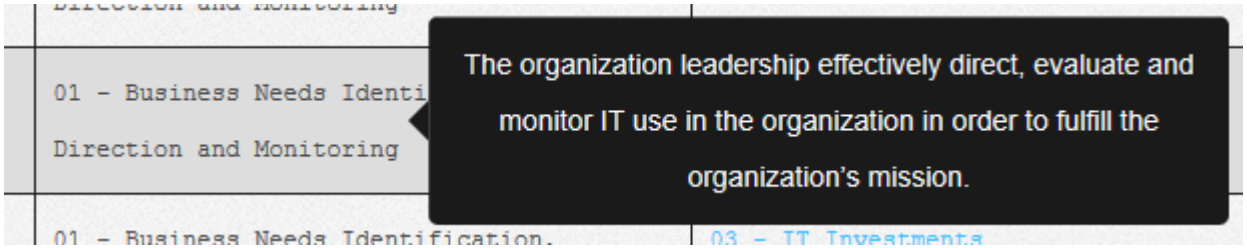
Filter by high risk, medium/high risk, include in audit, all issues

Domain	Area	Issue	Risks (weight)	Include in audit	Reasons, risks and remarks
01 - IT Governance	01 - Business Needs Identification, Direction and Monitoring	01 - Defining IT requirements	High	Yes	
01 - IT Governance	01 - Business Needs Identification, Direction and Monitoring	02 - Leadership	Low	Yes	
01 - IT Governance	01 - Business Needs Identification, Direction and Monitoring	03 - IT Investments	Medium	Yes	
01 - IT Governance	02 - IT Strategy and Planning	01 - Quality of IT strategy	Medium	Yes	

Plan (scoping)

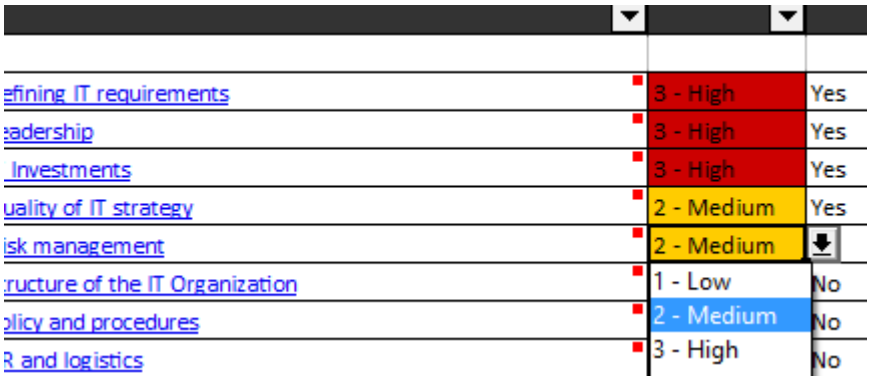
A dashboard with the different IT domains and respective areas and issues is obtained.

The domain and the area names have tooltips associated, which provides a short description. The guidance provided on each domain or area may help the auditor plan their audits.



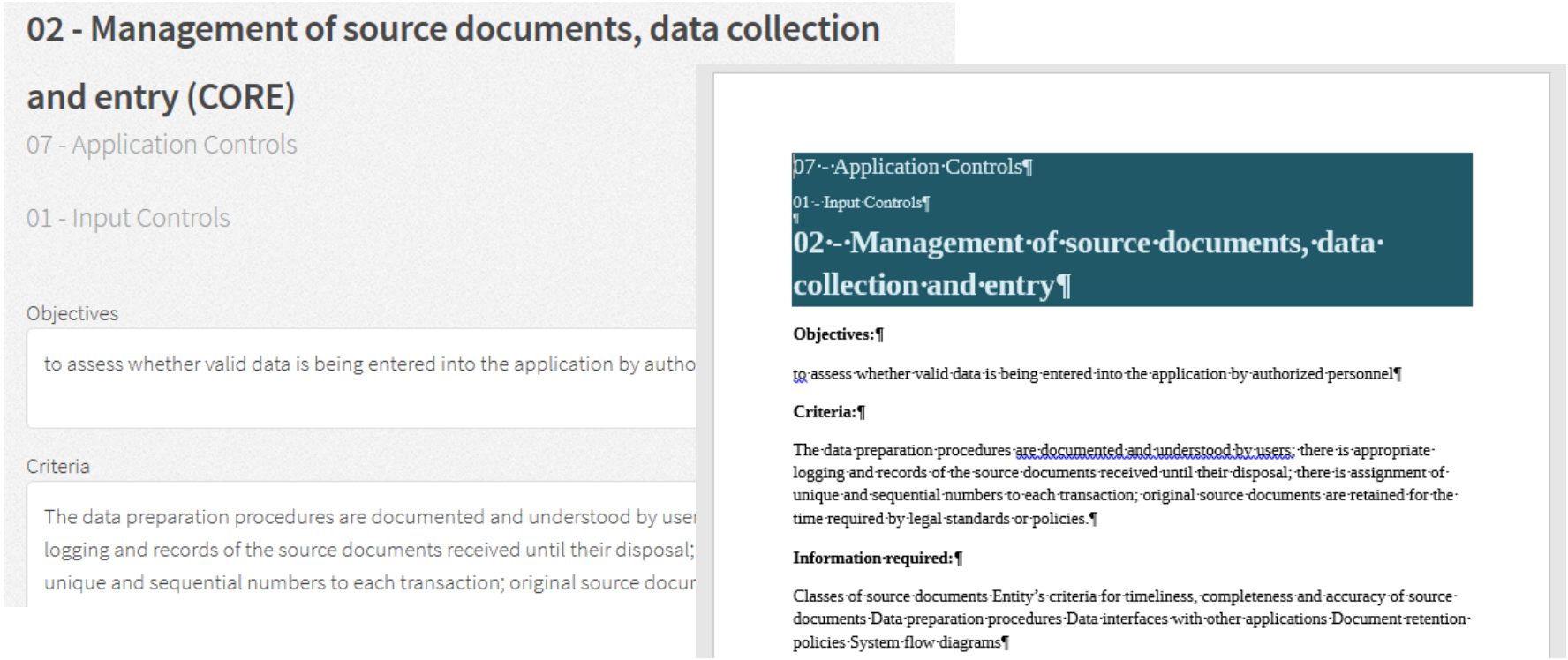
In this dashboard the user can **mark** (to include in audit) **and score the appropriate issues** (weight) for the selected audit focus.

Note: a high score (3) marks automatically the issue



Plan (scoping)

IT issues are now a hyperlink for the corresponding matrix, which will assist the auditor as a starting point to assess the controls that the organization has put in place to manage at an acceptable level and mitigate the risks they face in the domain/area.



Plan (scoping)

The audit matrices cover the IT auditing process. Their internal structure outline important audit issues, criteria, analysis methods under the different IT Audit domains/areas.

AUDITABLE AREA	
Audit objective:	
AUDIT Issue:	
Criteria:	
Information Required	**Analysis Method(s)**
Audit Conclusion To be filled in by auditor:	

Plan (scoping)

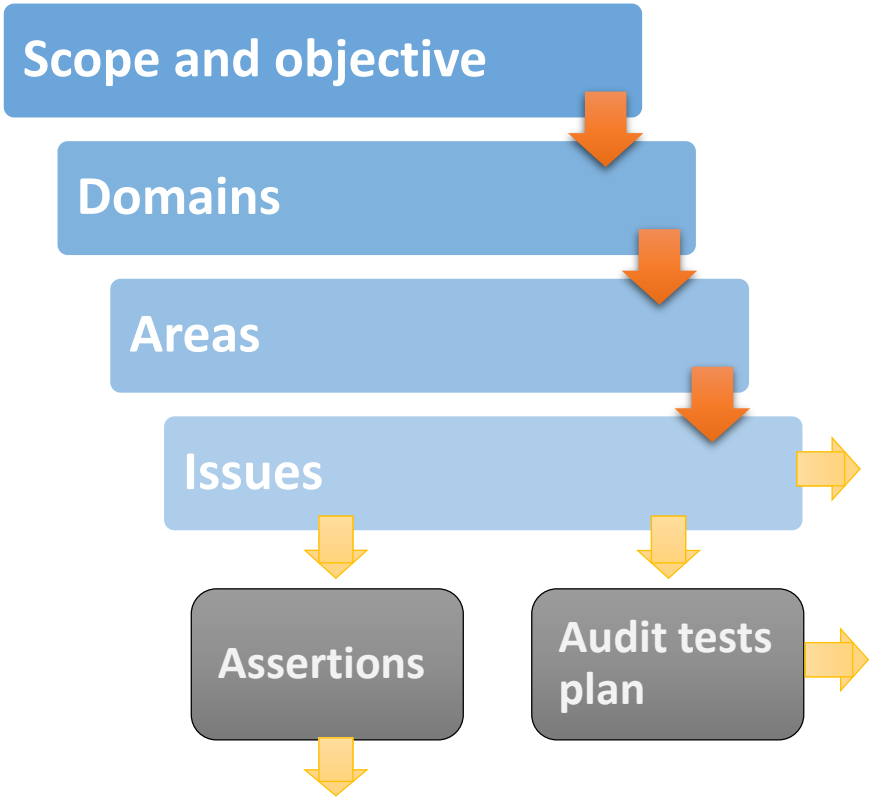
The matrices should be prepared at the planning stage, however the contents can be updated during IT audit process, if necessary.

Tips, examples and best practices are included in grey to guide the auditor. They can and should be replaced/extended with the appropriate information for the particular audit.

Note on matrices behavior:

In the desktop versions the auditor will use the matrix to fill information and sync with dashboard. At web version, a form is provided, but the user can generate a print version.

Plan (Mechanics)



Extract based on the scope and objective, then

On each level:

- Analyze, validate and optimize each selection
- Score relative importance within the extracted list
- Develop a weighted list

Use the information in related **Audit Matrices** at Criteria, Information Required and Analysis Method levels as work base and extend as necessary

1. Extract the audit steps
2. Check and adapt so that all key audit questions are covered

1. Identify the accountable and responsible roles
2. Establish what management claims are in place and if they are working well

Plan (Mechanics)

Formal techniques, such as risk analysis or problem assessments, possible sources of evidence, auditability and significance of the issue considered, that can help the planning process can be recorded in the **remarks** column.

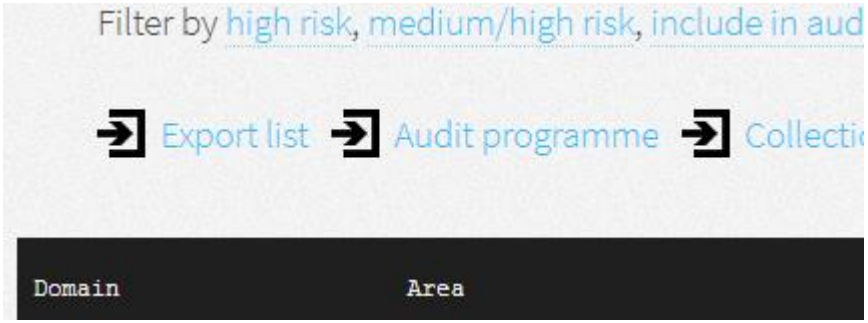
The key idea is to help the auditor to acquire sufficient knowledge about the audit objective and scope, discuss and mature it, ensuring therefore a proper plan.

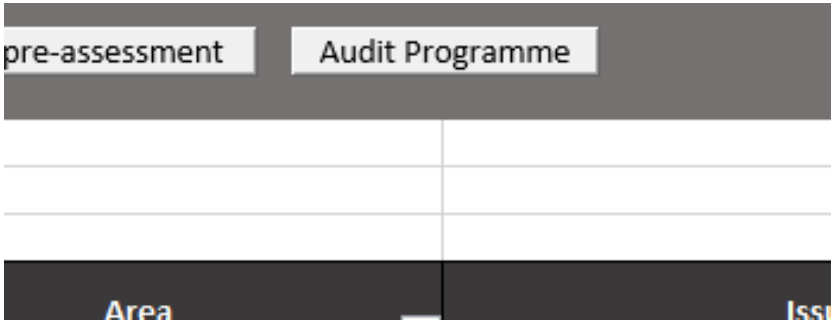
The user should analyze the result and adjust where necessary.

Plan (products)

Meeting with the ISSAI requirements related with the planning stage of audit process, the tool generates audit programmes, populated with the data previously recorded in the audit matrices, and ensures that they are preserved in standard containers to enable subsequent verification of the audit analysis procedures.

Only the issues marked to be included in audit will take part of the audit programme. Is generated by the auditor when pressing the matching action button.





Plan (products)

Despite the fact that the audit programme is produced at the audit planning stage, it includes the following features:

Audit programme coverage

Feature	Audit Programme
Audit objective	●
Audit Issue	●
Criteria	●
Information Required	●
Analysis Method(s)	●

The introduction and use of plug-ins

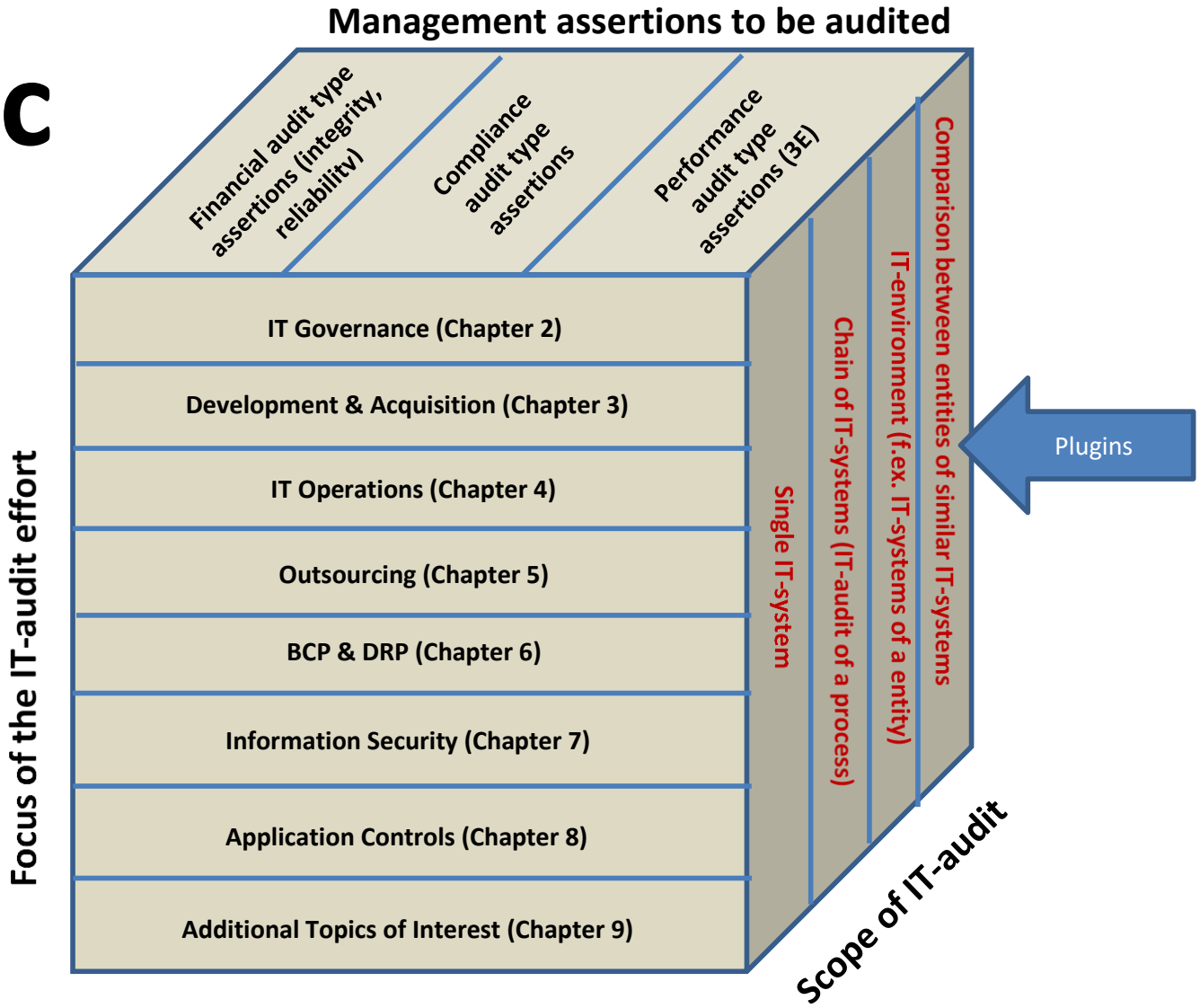
A plug-in (or plug-in, or extension) is a component that adds a specific feature to the “standard” Handbook on IT Audit for Supreme Audit Institutions

Purpose of plug-ins

- To enable SAI's creating abilities which extend or customize the tool
- To share and reuse knowledge among auditors in SAI or between SAI's
- To address new and emerging areas of interest for IT auditors, like cloud computing, Web Services or OPEN DATA initiatives

Cosoistic view

The plugins can be seen in the overall context of the tool as follows:



Future of plug-ins

The plug-in will be used to add new features and update the Handbook on IT Audit for SAI's, highlighting emerging areas of interest and providing the users with essential information and key questions needed for an effective planning of IT Audits.

Examples of plug-ins

#	Reference	Description
#1	E-GOV	E-Government & Other Web Services Roll Out
#2	LAND	Land Registry Automation
#3	OPENDATA	Open Data Strategy
#4	UPGRADEFINANCIAL	Upgrade of Financial Management IT System

Plug-ins (Mechanics)

The tool provides services that the plug-in can use, including a way for plug-in to register with the tool (desktop version) and a defined structure for the exchange of data with plug-ins.

A plug-in still depend on the service and the structures provided by the tool and do not usually work by himself. Conversely, the tool operates independently of the plug-in, using the “core” Handbook on IT Audit for Supreme Audit Institutions as operational and informational basis, making it possible for end-users to add and update plugins dynamically without needing to make changes to the host tool:

- **A plug-in extends (doesn’t replace)** the core IT Audit Handbook, adding new functionalities or characteristics.
- **A plug-in is instantiated and executed inside the application** and interacts with core through the same user interface.

Plug-ins (Mechanics)

The Active IT Audit Handbook supports a type of plug-in that reflects at least the general structure of the core Handbook (domain structure).

To include a new plug-in, some simple rules must be followed:

- At the web version, if present in catalogue, the plug-in is automatically available.
- At the desktop version:
  1. Download the desired plug-in from catalogue (is a xml file);
  2. Save it inside the folder “plugin”, under “ActiveManual”;
  3. If the spreadsheet (“StartHere.xlsm”) was already open, reload the list, pushing the corresponding action button.

Plug-ins (Mechanics)

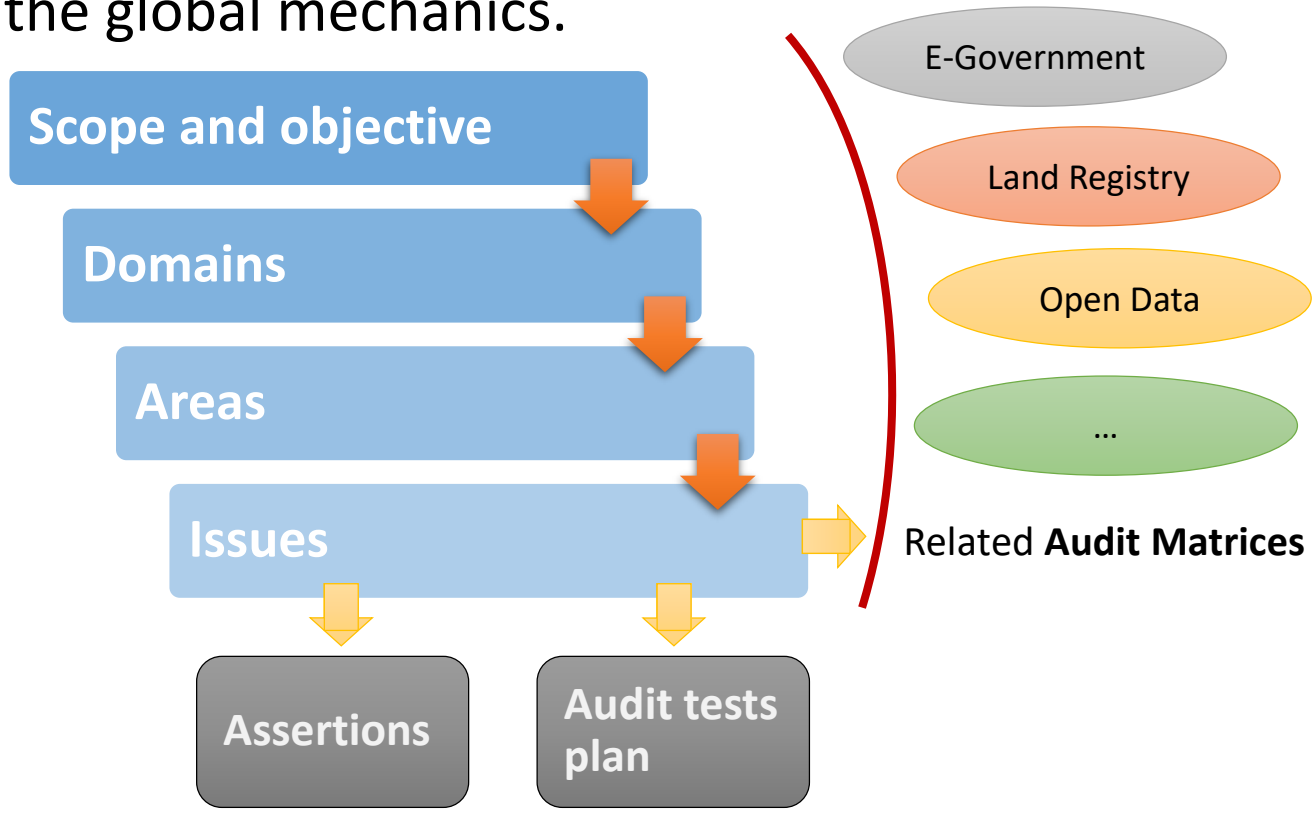
The application have a plug-in manager to guide the user

Plug-ins available to use in audit

Reference	Selected	Description	Version	File
E-GOV	No	E-Government & Other Web Services Roll Out	1.0	EGovernment.xml
LAND	No	Land Registry Automation	1.0	LandRegistry.xml
OPENDATA	Yes	Open Data Strategy	1.0	OpenDataStrategy.xml
UPGRADEFINANCIAL	Yes	Upgrade of Financial Management IT System	1.0	UpgradeFinancialITSystem.xml

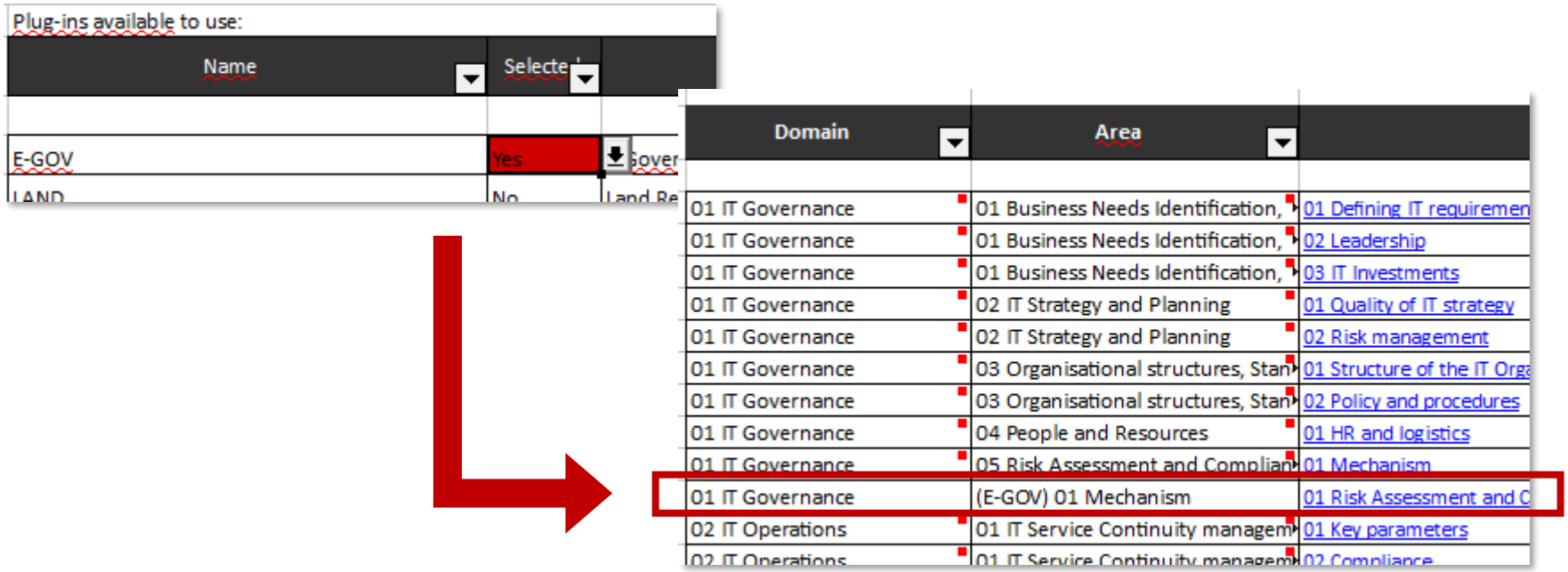
Plug-ins (Mechanics)

The plug-ins depend on the core IT Audit Handbook and preserve the global mechanics.



Plug-ins (Mechanics)

The plug-ins depend on the core IT Audit Handbook and preserve the global mechanics.



Conduct

(collect and consolidate obtained findings)

EVIDENCE, FINDINGS AND CONCLUSIONS

"Auditors should obtain sufficient appropriate audit evidence to establish findings, reach conclusions in response to the audit objectives and questions and issue recommendations."

(ISSAI 300 PARAGRAPH 38)

Collect findings

To assist the auditor collecting findings and suitable conclusions derived from the assessment the tool provides a dashboard inside the worksheet /command "Findings".

Support matrices are available.

Conduct

(collect and consolidate obtained findings)

Findings in audit

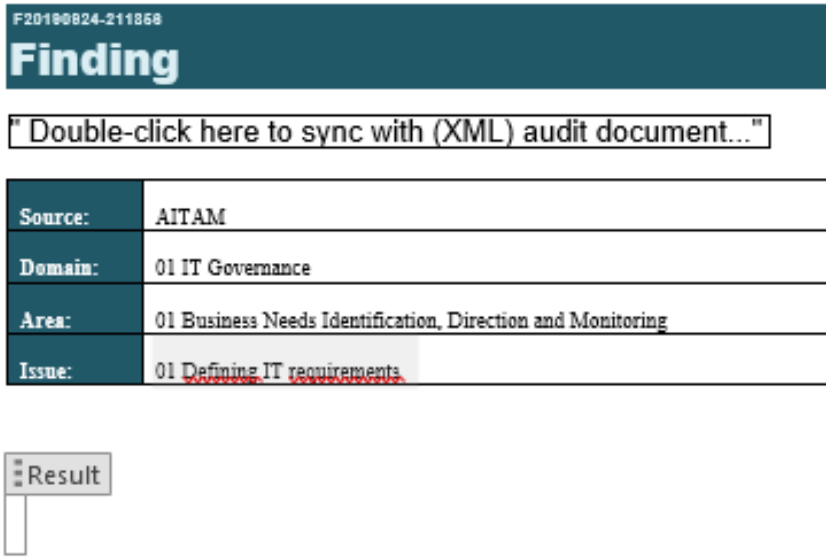
Use hyperlink on ID to visualize/edit the finding

Operation	ID	Source	Domain	Area	Issue	Cause	Result	Description	Legal Act	Reference in the report	Relevant
Delete...	F20181215-125507	AITAM	01 IT Governance	02 IT Strategy and Planning	02 Risk management	Cause	Result	I like Cherries.	Reference to Legal Act	Reference to the Report	Yes
Delete...	F20181215-125508	AITAM	01 IT Governance	02 IT Strategy and Planning	02 Risk management	Cause F20181215-125508	Result F20181215-125508	I like cats, but I'm allergic	Reference to Legal Act F20181215-	Reference to the Report F20181215-	No

Conduct

(collect and consolidate obtained findings)

Support matrices are available.

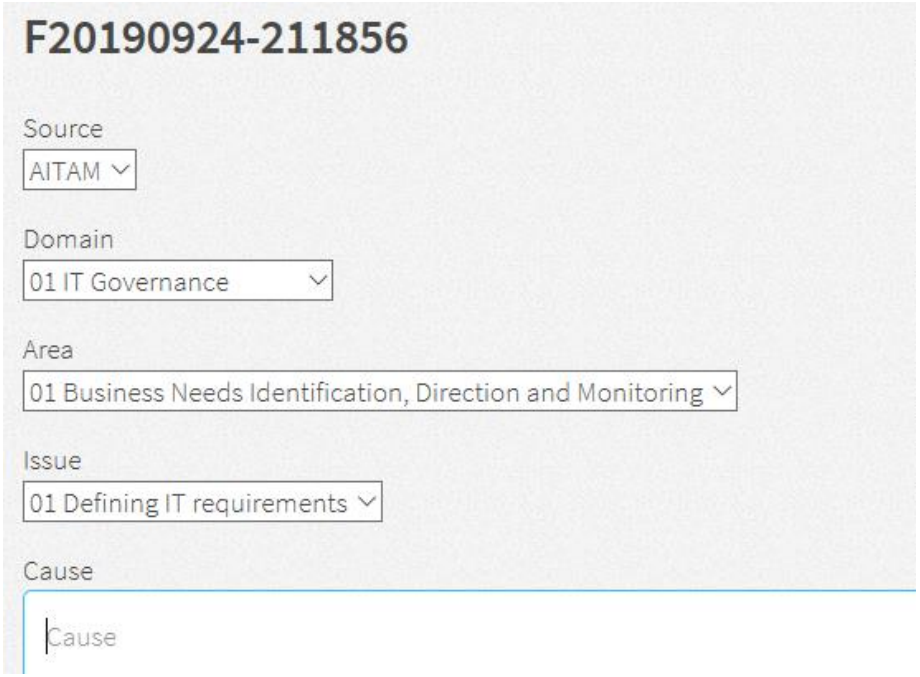

F20190824-211858

Finding

" Double-click here to sync with (XML) audit document..."

Source:	AITAM
Domain:	01 IT Governance
Area:	01 Business Needs Identification, Direction and Monitoring
Issue:	01 Defining IT requirements

Result


F20190924-211856

Source
AITAM

Domain
01 IT Governance

Area
01 Business Needs Identification, Direction and Monitoring

Issue
01 Defining IT requirements

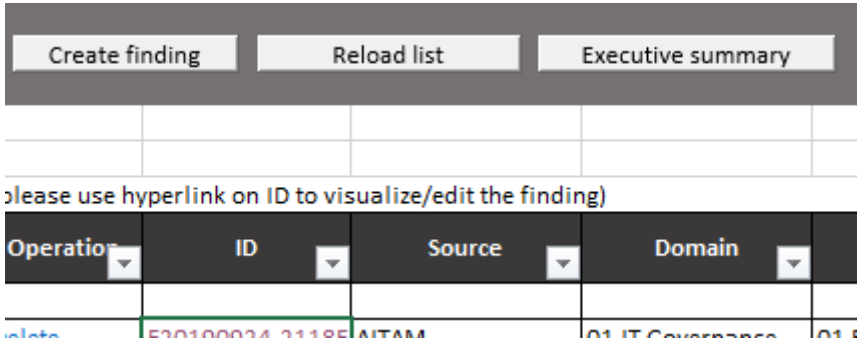
Cause
Cause

In the desktop versions the auditor will use the matrix to fill information and sync with dashboard. At web version, a form is provided, but the user can generate a print version.

Conduct (products)

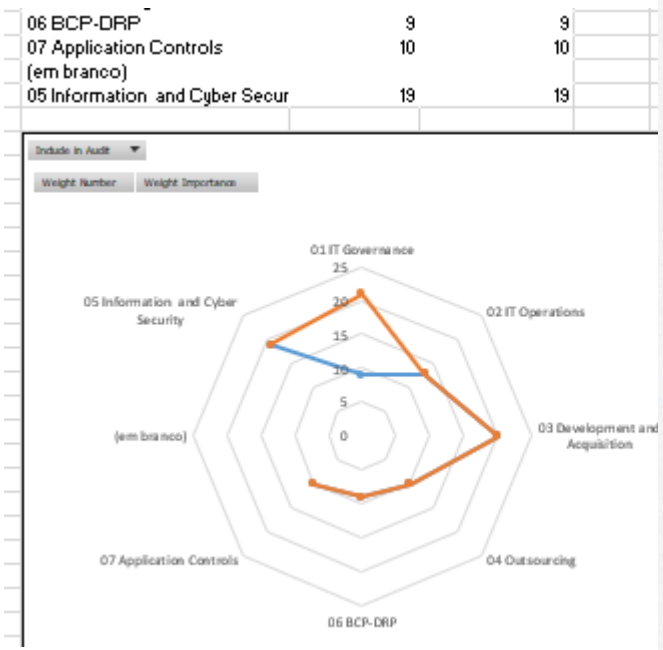
The tool generates executive summaries, populated with the information of the audit findings.

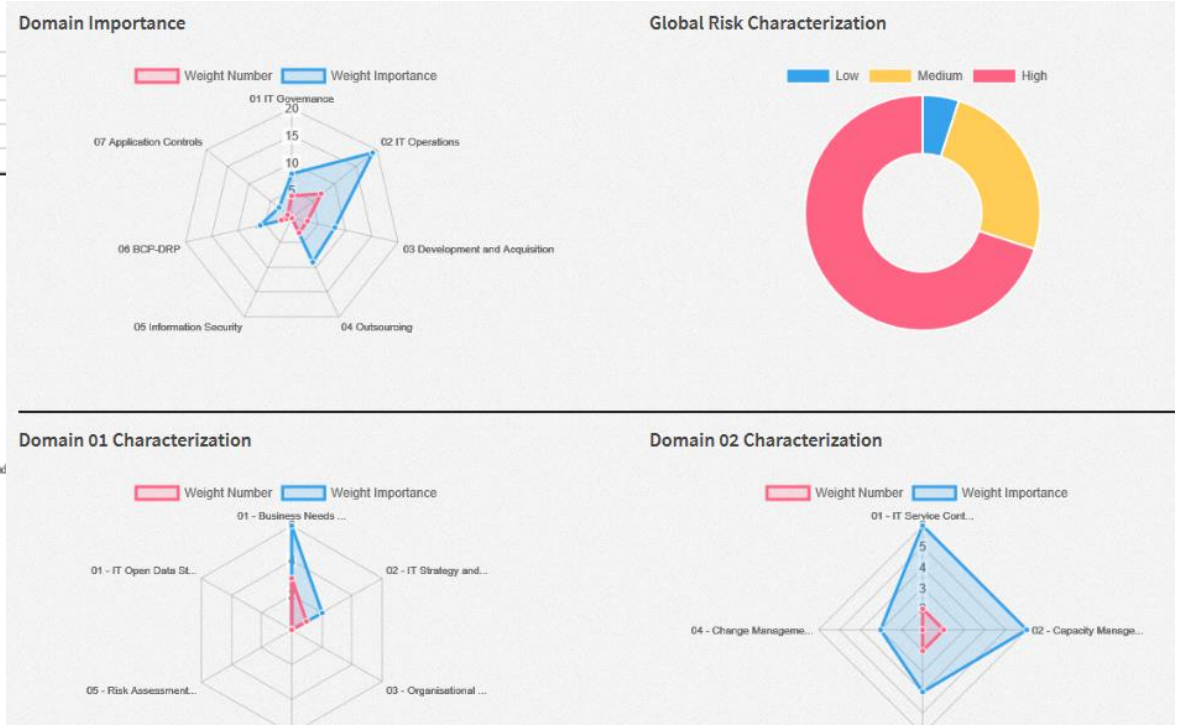
Only the findings marked as relevant will take part of the executive summary. This document is produced by the auditor when pressing the matching action button.



Analytics

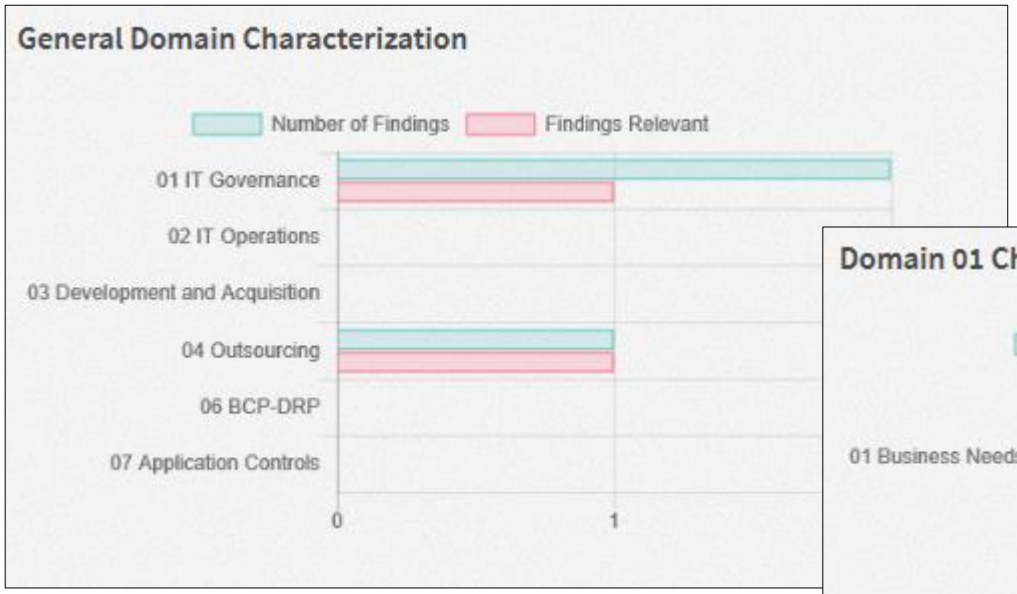
By making use of spreadsheet analytical and web graphical features, the tool provides the auditor with a simple range of data ("Metrics" worksheet / Analytics menu), to evaluate the domain importance and characterization (global and specific).





Analytics (web version only)

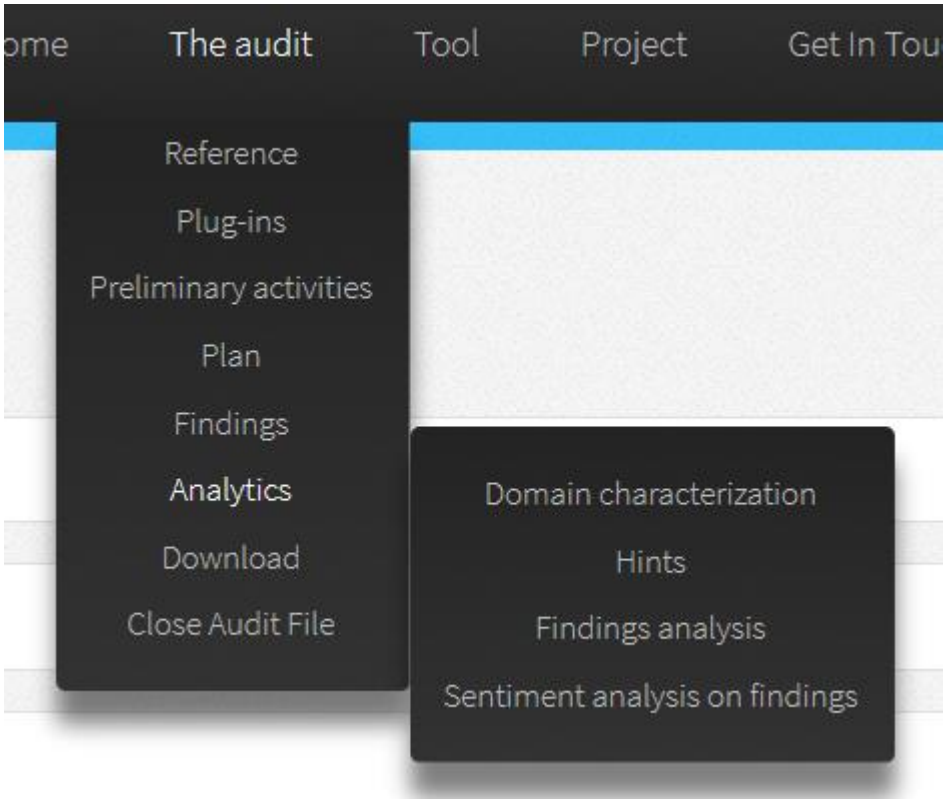
Includes an evaluation of findings to look for gaps among related relevant areas for audit



Analytics (web version only)

Opportunity to experiment and improve:

- New integration paths with CUBE;
- Apply Natural Language Processing (NLP), Graph Analytics and Machine Learning (ML).



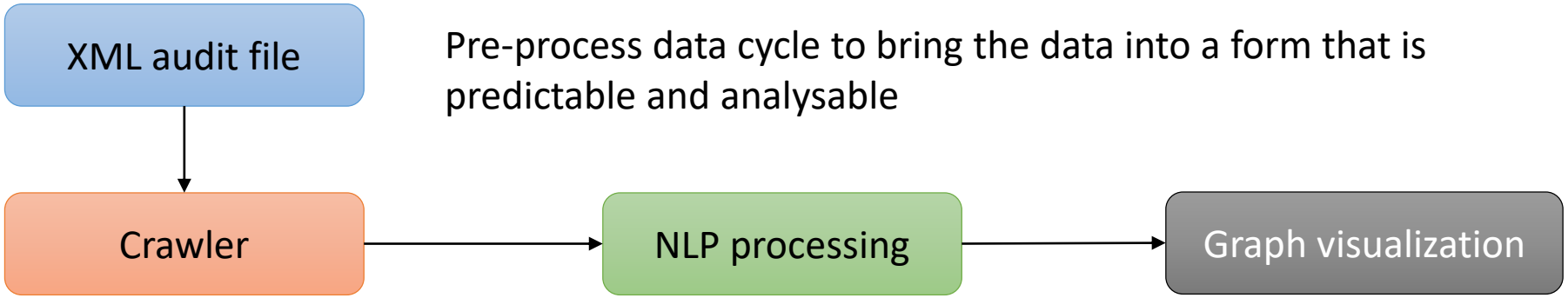
Hints for the audit (web version only)

An analysis based on NLP to consider and find out through the CUBE how other nearby audits can help to make better use of current resources, heading the user to know:

- Where are you?
- Opportunities, risks and threats to look for!
- How to get there? (and, potentially, obtain the desired outcome)

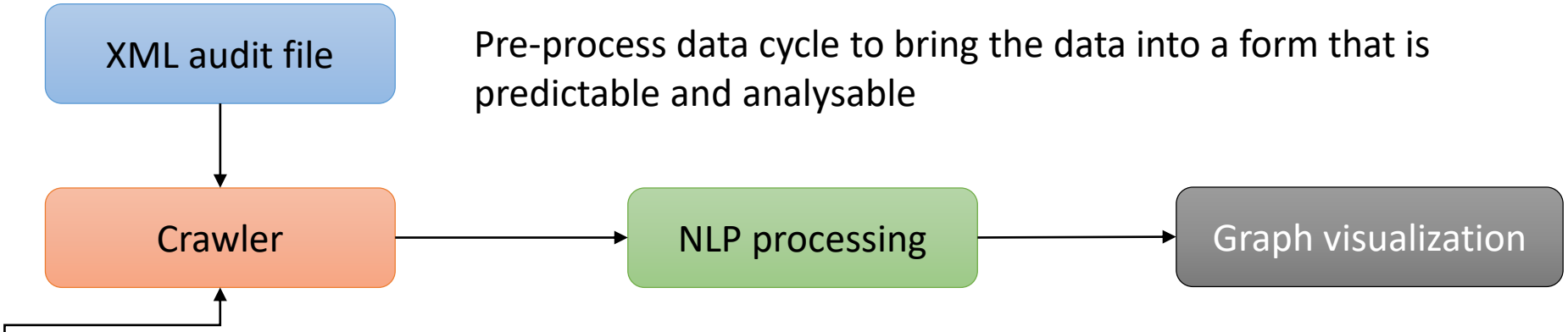
Such analysis can be performed at the planning or the execution phases of the audit.

Hints for the audit (web version only)



Pre-process data cycle to bring the data into a form that is predictable and analysable

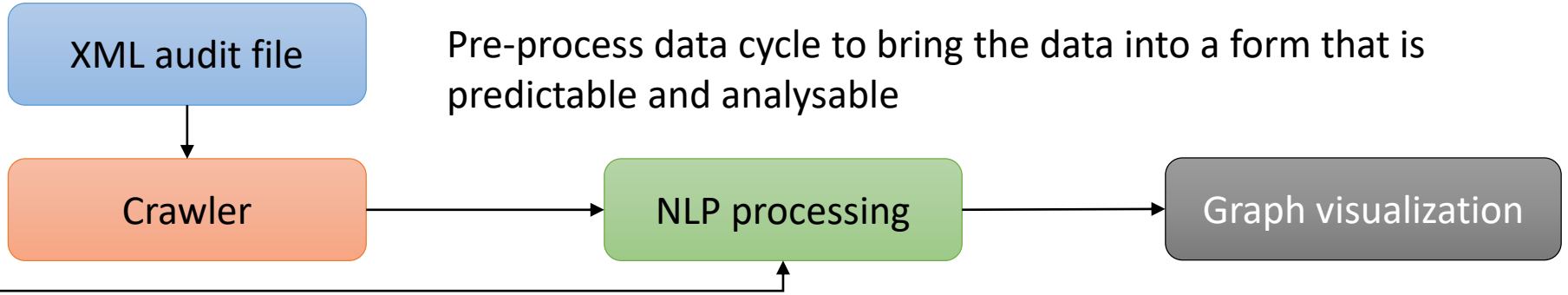
Hints for the audit (web version only)



(what is) Collected:

- Risks and notes selected to “Include in audit”
- Reference data form (attributes “title”, “background” and “ application notes”)
- Pre-assessment data form
- Findings (all)
- Issue Matrices selected for audit (attributes “objectives”, “criteria”, “Information Required”, “Analysis Method”, “Found Previously” and “Conclusion”)

Hints for the audit (web version only)



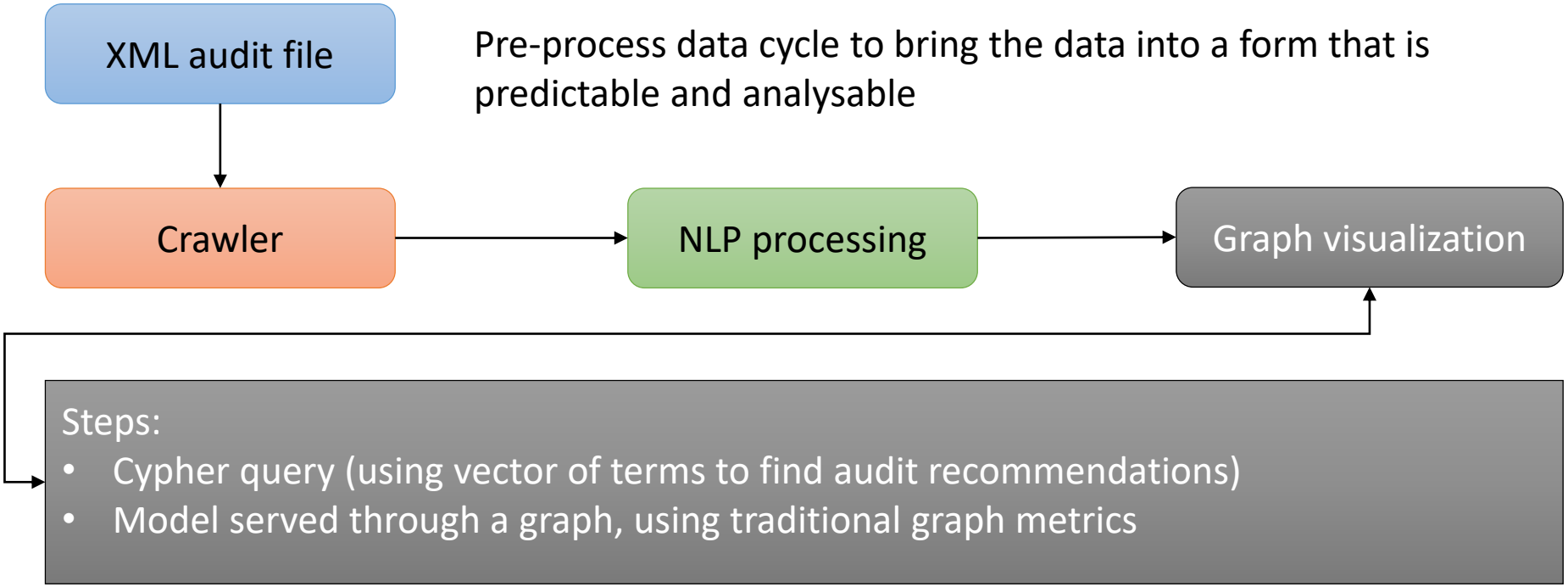
Pre-process data cycle to bring the data into a form that is predictable and analysable

Steps:

- Tokenizer
- Normalize (convert to lower case and inflector to singularize)
- Filter (tokens not alphabetic)
- Stop words filtering
- Entity extraction (identify potential tokens using gazetteers: token + annotation/context)
- Combine (list of unique terms/tokens)
- Term weighting (ID/IDF)
- Vector of terms

Lemmatization (Wordnet for mappings) and Stemming processes (like Porters Algorithm) not used: tests didn't show improvements in classification accuracy

Hints for the audit (web version only)



Connects with graph database

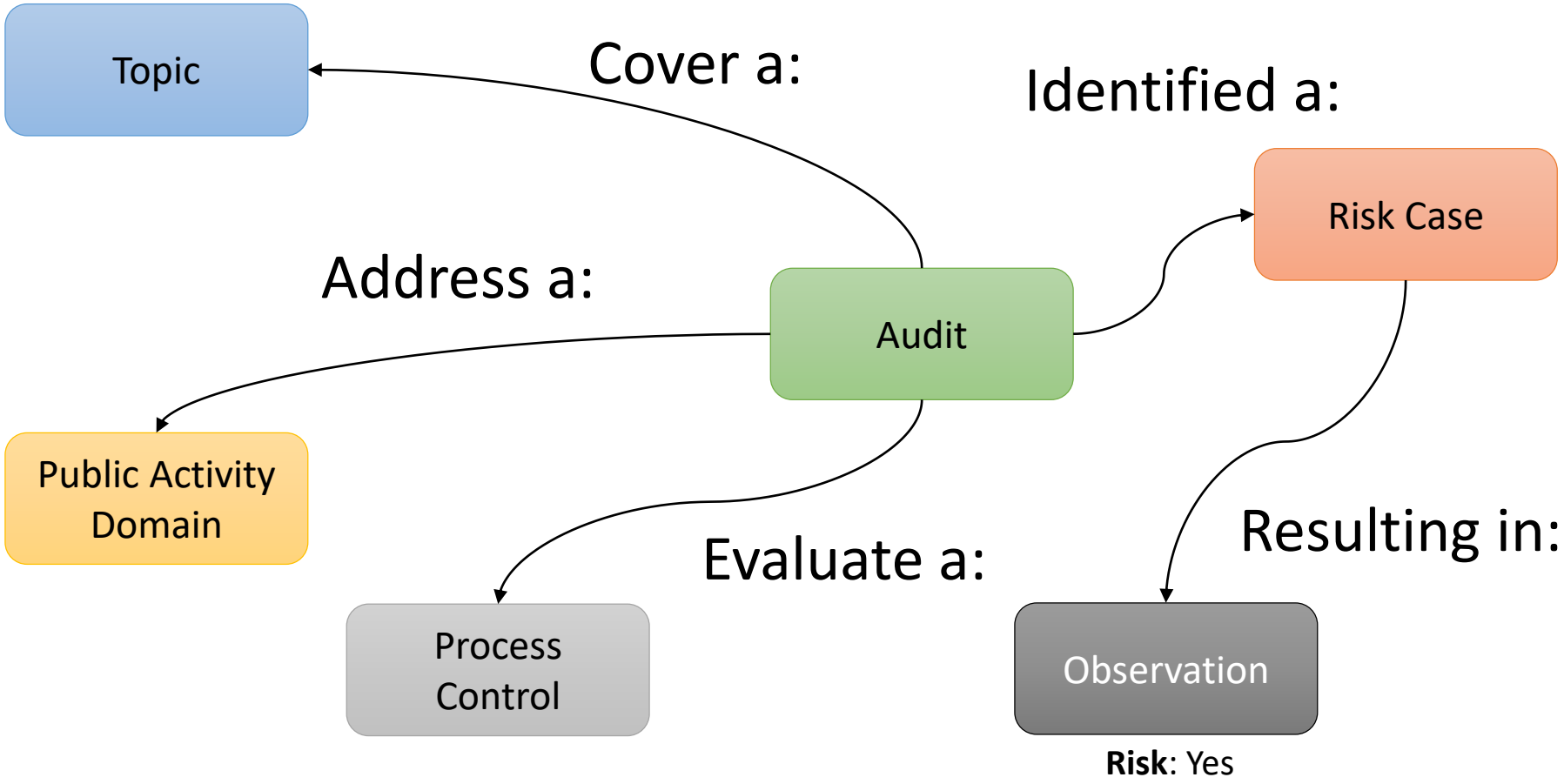
Hints for the audit (web version only)

Graph-like structures to support the find of similarities (an experiment to model audit):

- Graph-like structures to describe the audits and risk cases (use of a graph structure to find out useful paths between data);
- Store and present the information as nodes (data points) and relationships (connections) that the user can query and traverse;
- They can be represented as a "graph" and they can have one or more starting points in queries, or "anchors", in the graph from where the user can start traversing out and reach the audit report in the CUBE;

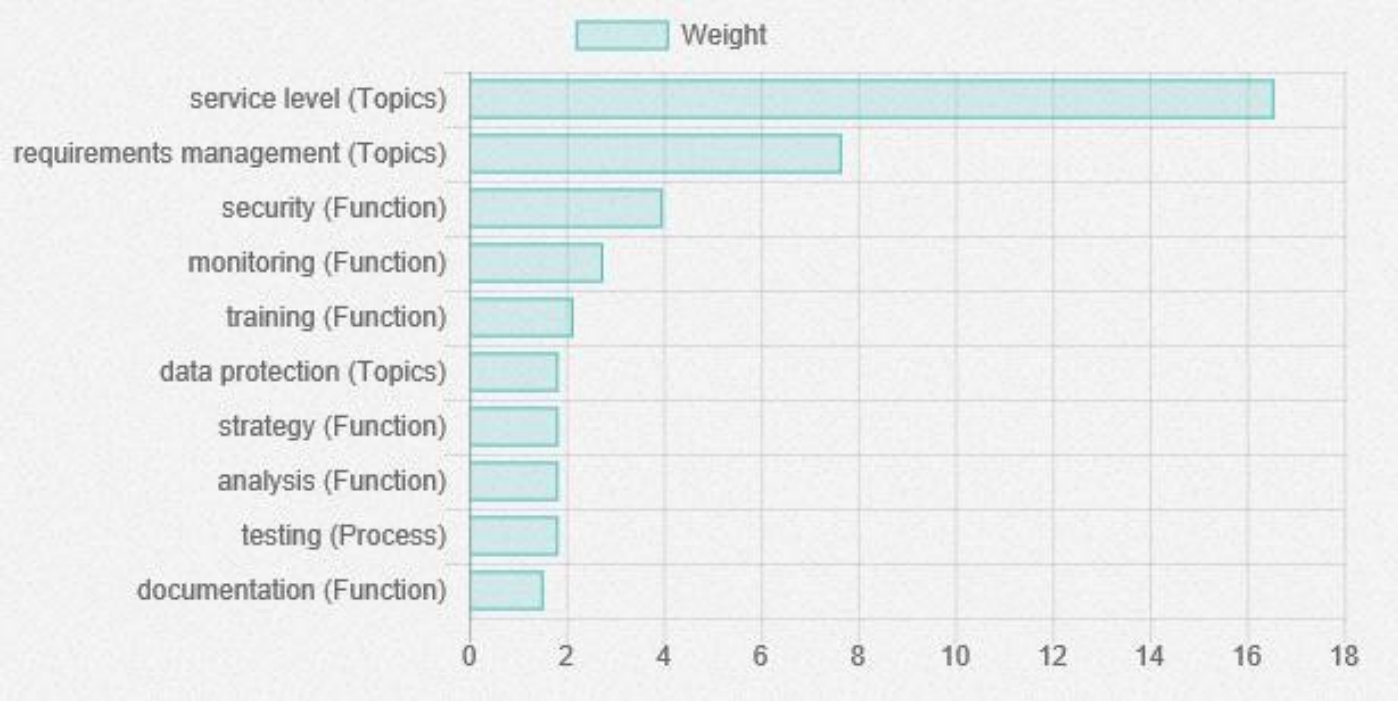
Hints for the audit (web version only)

Descriptive diagram (example)



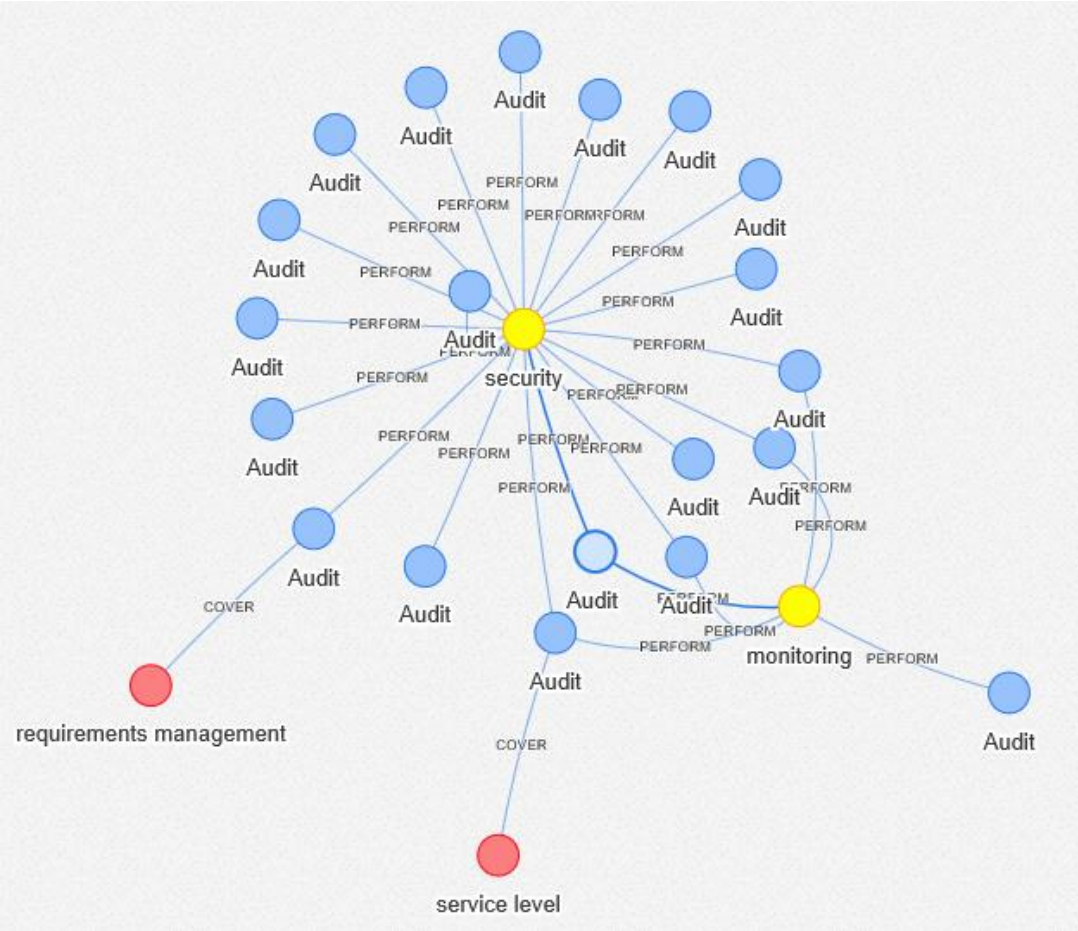
Hints for the audit (web version only)

Most relevant terms discovered and analyzed using Term Frequency-Inverse Document Frequency (TF-IDF) mechanism:



Hints for the audit (web version only)

Results as a graph



Hints for the audit (web version only)

Results as a table

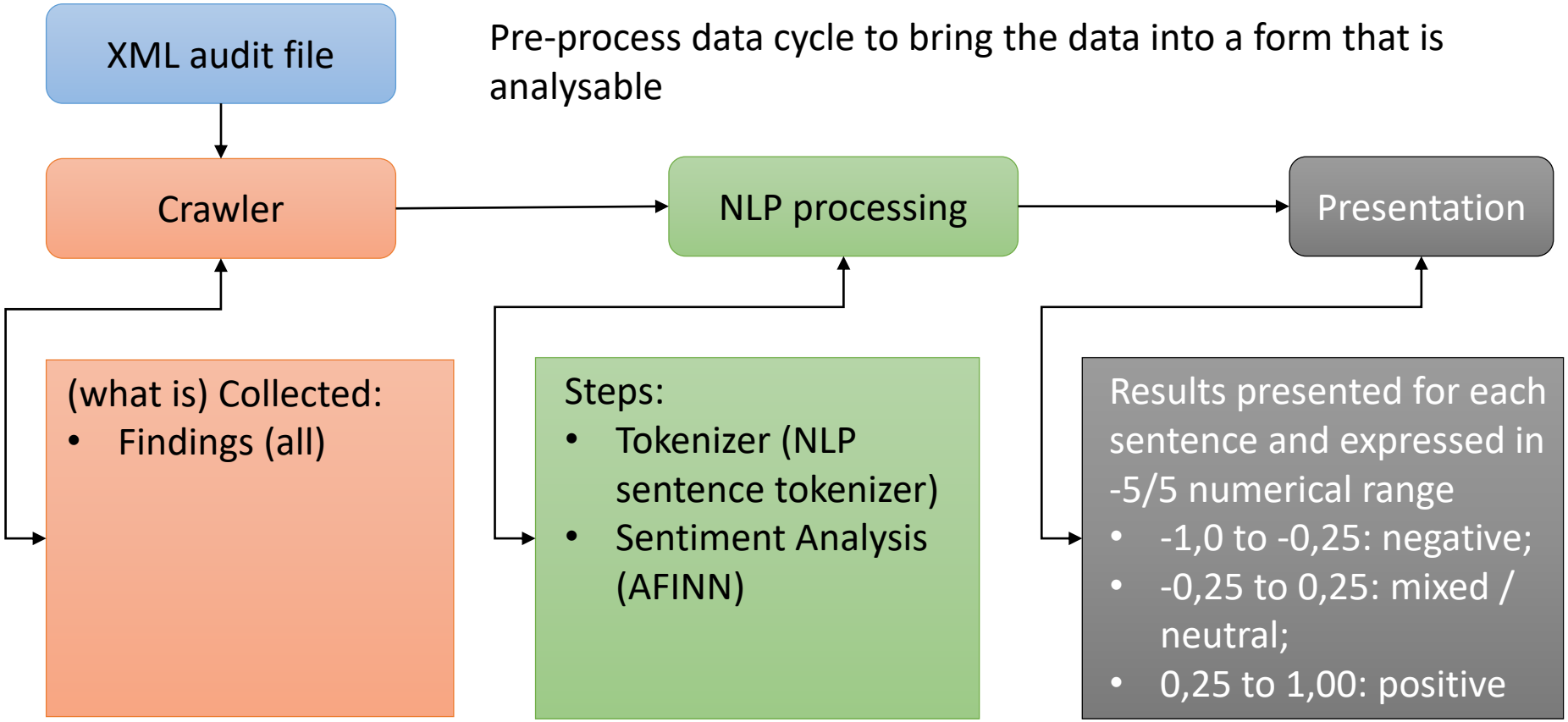
Audit Report	Author	Year	Present in
Management of Information Resources of the Ministry of Agriculture	National Audit Office of the Lithua	2013	security;
Audit of the Government, Government-guaranteed and Municipal Debt Management Information Systems in the Ministry of Finance of the Republic of Bulgaria	Bulgar Audit		

Sentiment analysis on findings
(web version only and experimental)

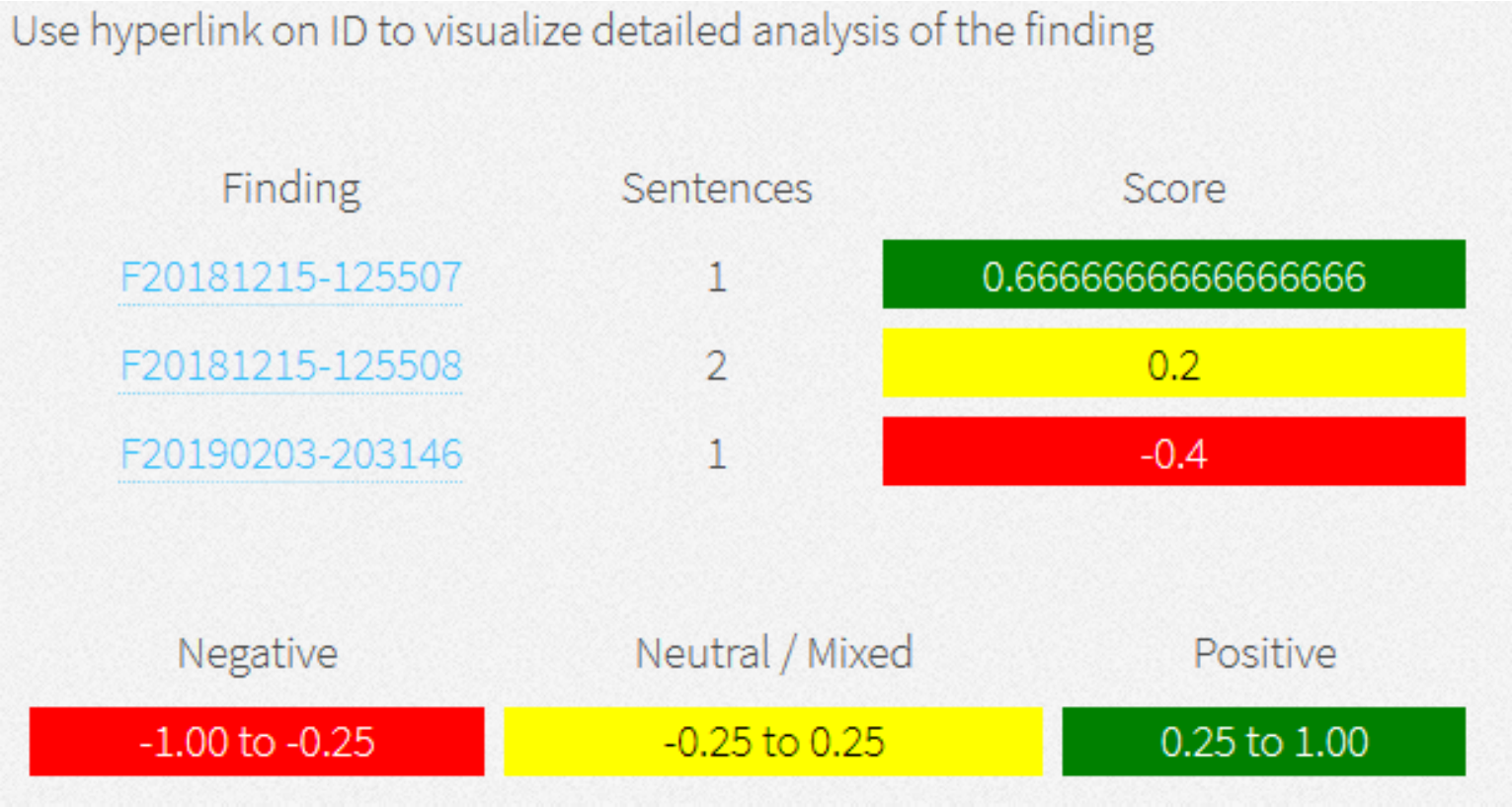
Analysis to measure attitude towards findings. Based on Natural language processing (AFINN algorithms) to consider and find out the polarity of a given text at the document:

- Addresses findings;
- Possibility: compare with pre-assessment and discover differences in emotional tones about same realities;
- Still in an early stage phase with comparative tests against Microsoft and Google API's.

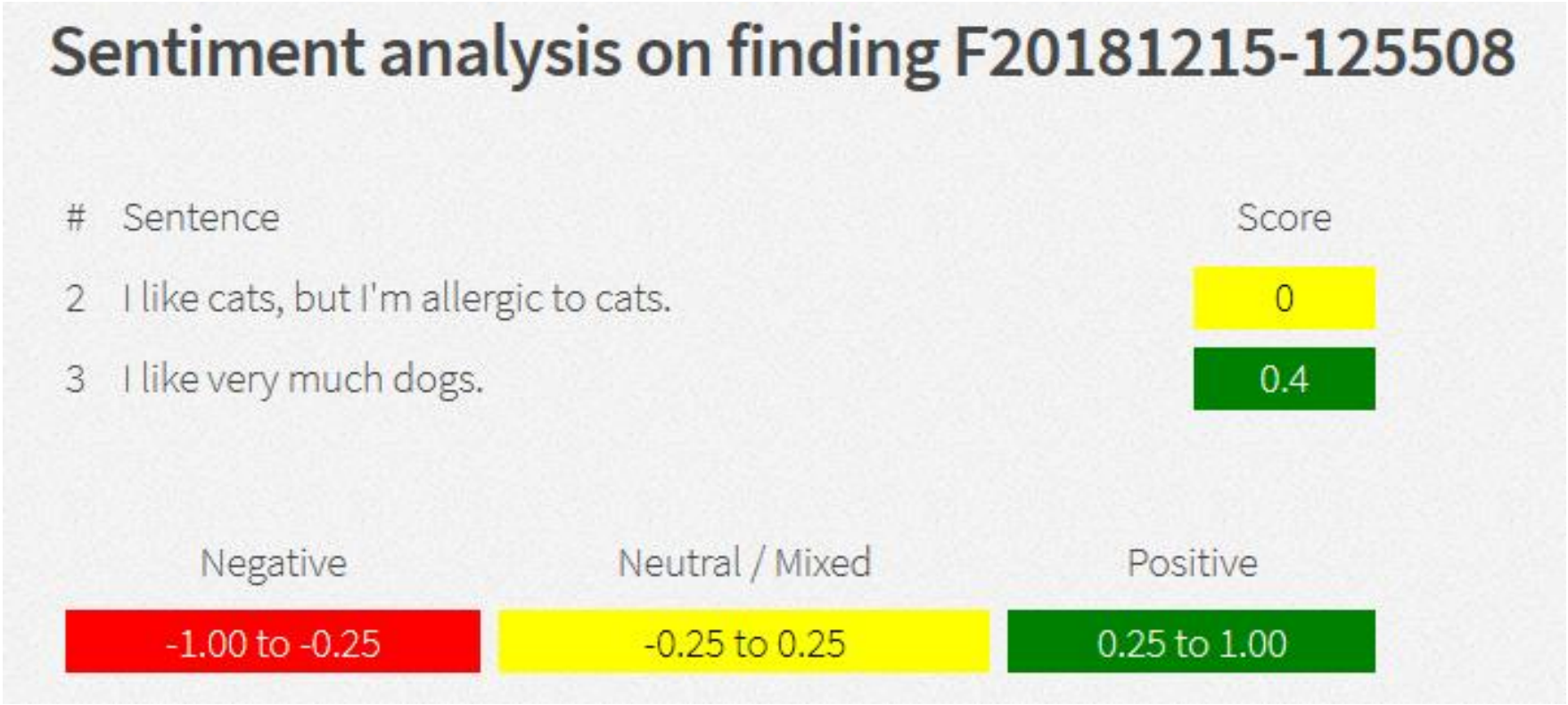
Sentiment analysis on findings
(web version only and experimental)



Sentiment analysis on findings
(web version only and experimental)



Sentiment analysis on findings
(web version only and experimental)



Active IT Audit Manual

Happy IT Audits!