ETSI
The Standards People

Security Conference

Leverage AI in Cyber Security Audits

Presented by: Björn Fanta

Fabasoft®

19/10/2023

Björn Fanta

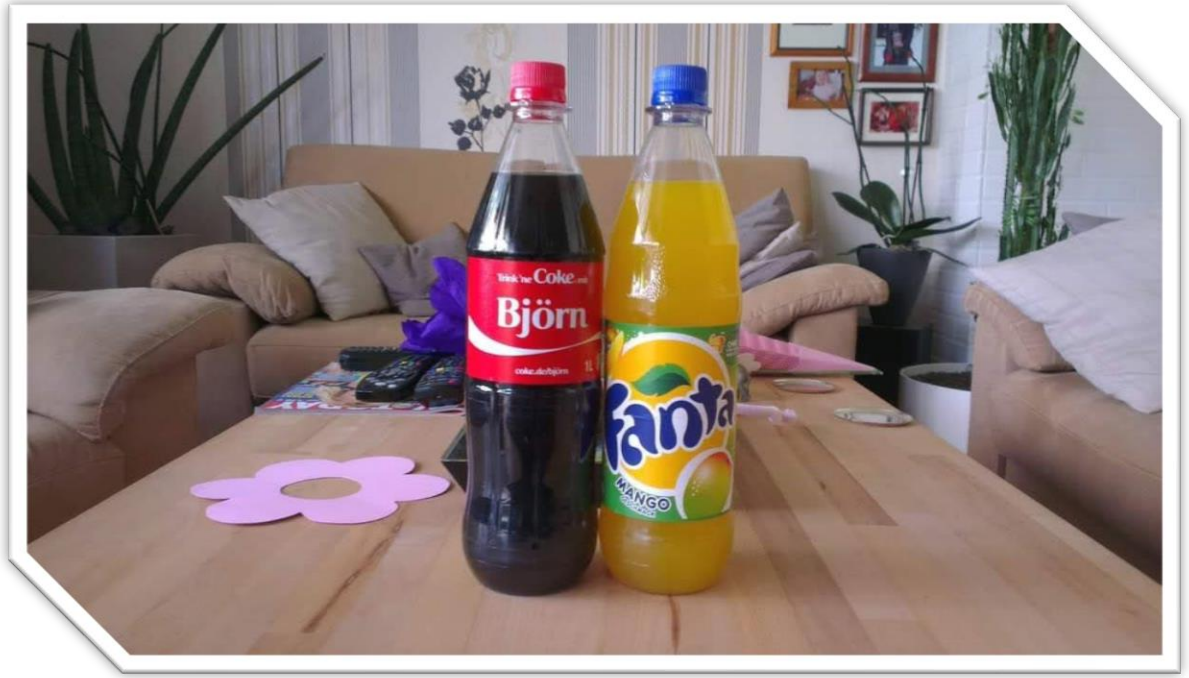
Head of Research

Fabasoft

Austria

Fabasoft

>whoAmI



Fabasoft

Where the following ideas come from

MEDINA

tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Fabasoft

Fraunhofer AISEC

BOSCH

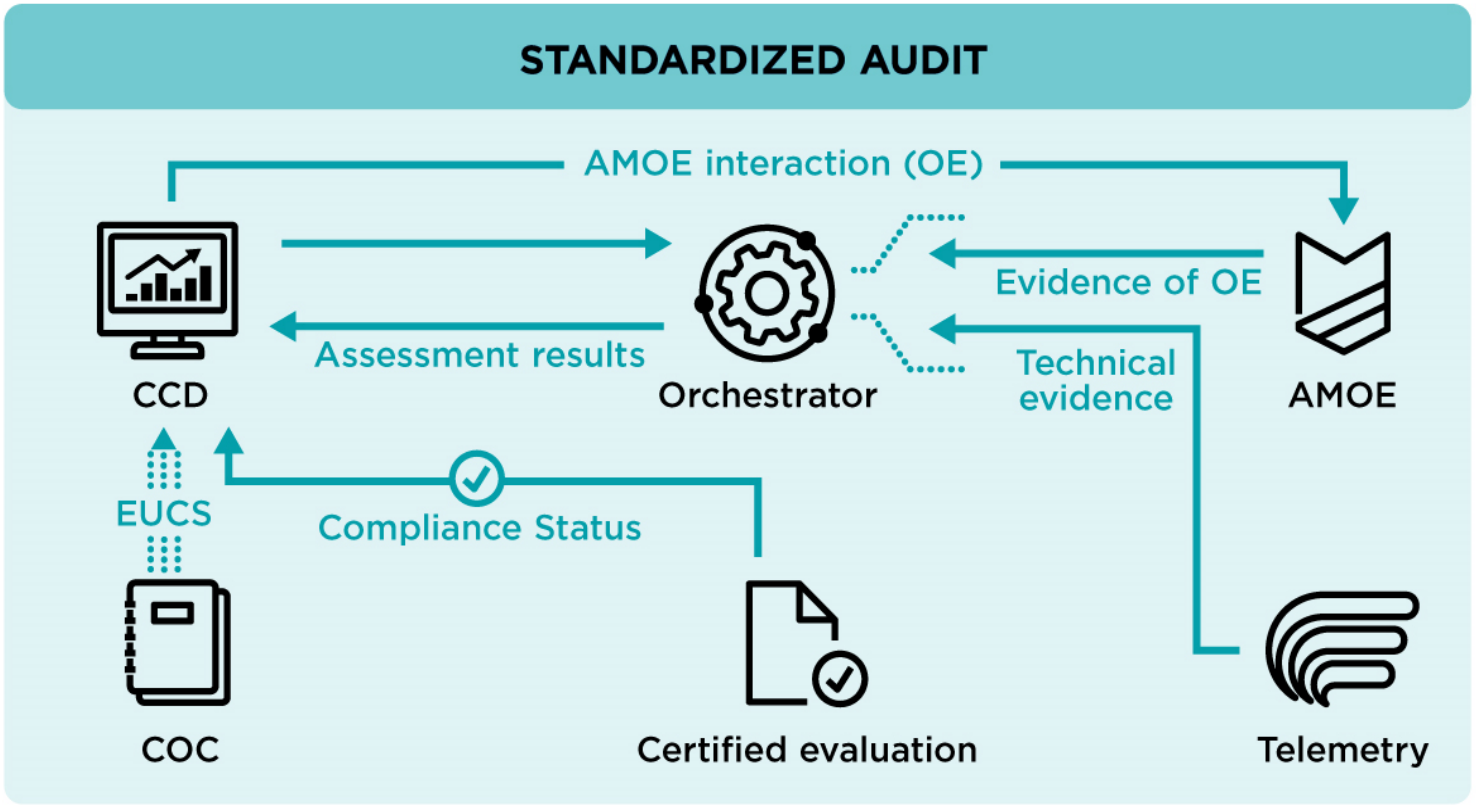
Hewlett Packard Enterprise

Consiglio Nazionale delle Ricerche

NIXU cybersecurity.

XLAB

Context



CCD Company Compliance Dashboard

OE Organizational Evidence

TE Technical Evidence

CoC Catalogue of Controls

ToE Target of Evaluation

AMOE Tool to Automatically Extract and Assess Organizational Evidence for Continuous Cloud Audit

One Pipeline for OE and TE

Fixed structure for each Catalogue

Compliance Information based on whole ToE context

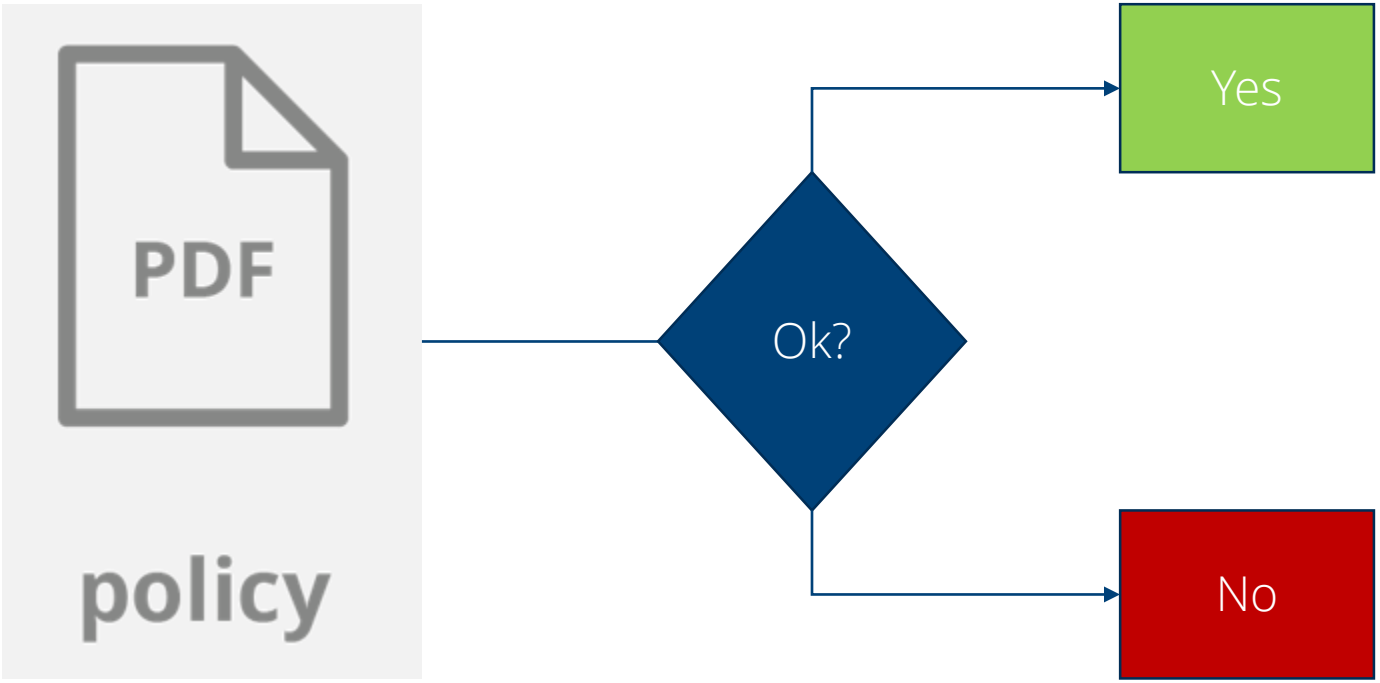
Fabasoft

So, what is this AMOE about?

- **A**utomated **M**anagement of **O**rganizational **E**vidence
- **Supports** assessment & management of org. evidence
- Evidence collection tool
  - **NOT** an assessment tool on its own

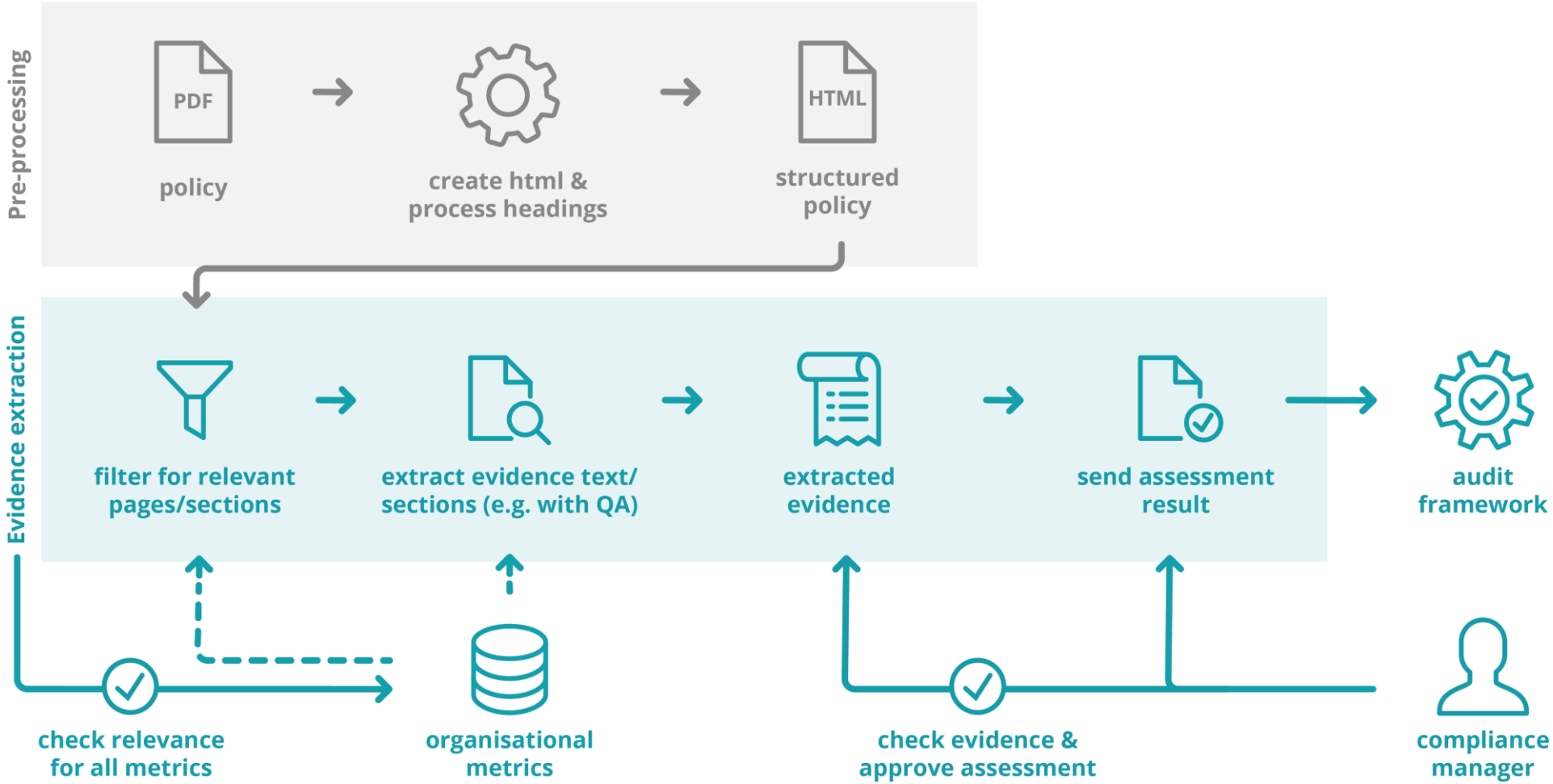
Fabasoft

Simplified: goal



Fabasoft

Complex: data flow



Fabasoft

AMOE’s approach for policy documents

- Pre-process (textual) evidence
- Extract relevant information as metadata
- Compare metadata to a target value
- Give compliance hints

Fabasoft

EUCS

IAM-08 - PROTECTION AND STRENGTH OF CREDENTIALS

Requirement id	IAM-08.1H
Requirement description	The CSP shall document, communicate and make available to all users under its responsibility rules and recommendations for the management of credentials, including at least: (1) Non-reuse of credentials; (2) Trade-offs between entropy and ability to memorize; (3) Recommendations for renewal of passwords; (4) Rules on storage of passwords. (5) Recommendations on password managers (6) Recommendation to specifically address classical attacks, including phishing, social attacks, and whaling
Requirement assurance level	High

Source: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

Fabasoft

Example: training data set

- Metric

Metric - PasswordPolicyQ2

Keywords	password, age, maximum
Target value	<= 90.0 (Integer)
Question	What is the passwords maximum age according to the password policy?

- Policy Document

2 Password Management

Passwords should have at least 10 upper -and lowercase characters and contain numbers as well as special characters. Do not reuse passwords for multiple services. Passwords should not be easy to guess and should not contain personal information such as your birthdate or the name of your child. Do not share the password with third parties and do not store it in plain text. It is best practice to use password managers to generate complex passwords and store the encrypted passwords. The password needs to be changed after a maximum time duration of 60 days.

Fabasoft

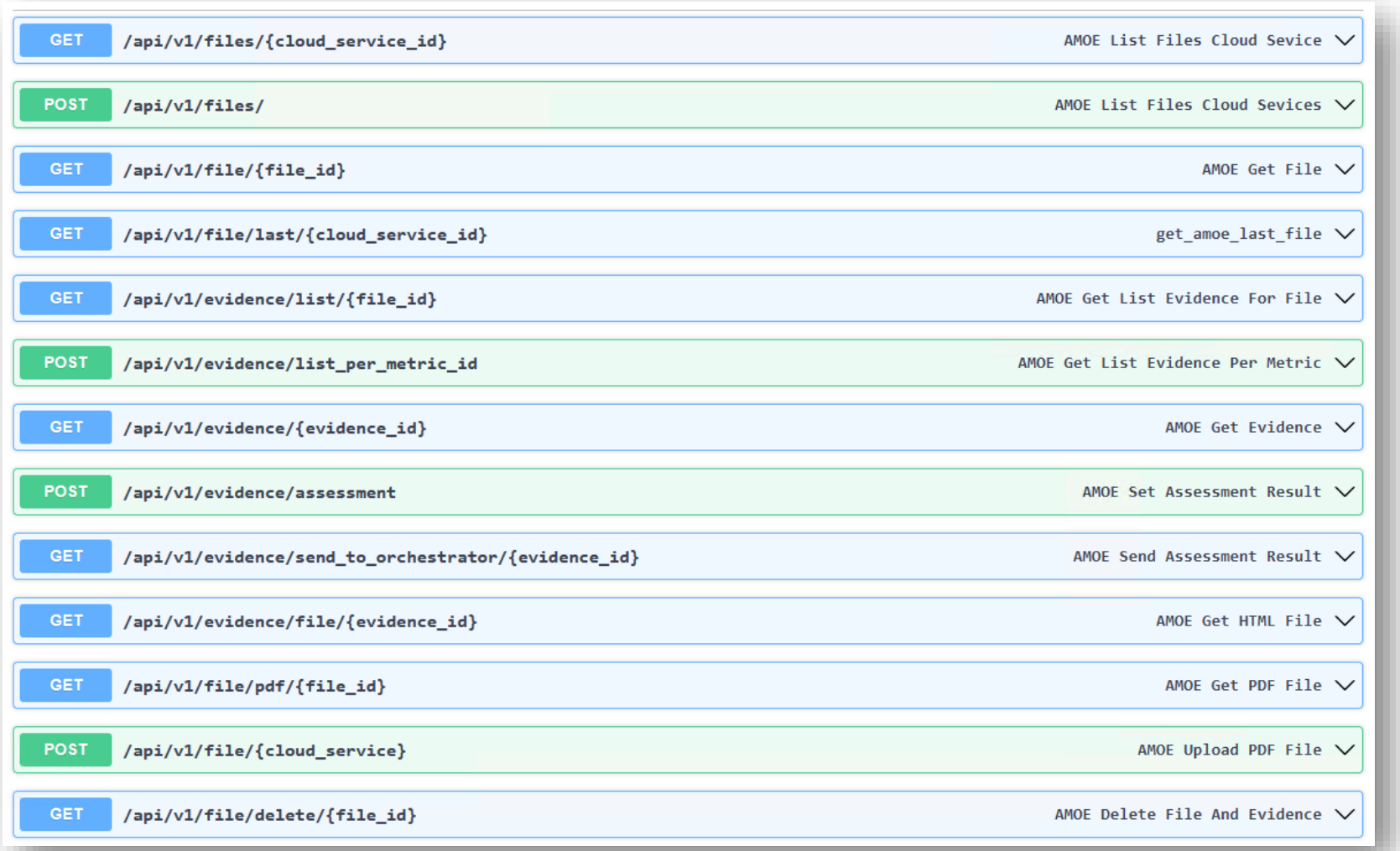
The “AI magic” or: necessary steps

- Pre-process
  - Document transformation, keyword definitions, lemmatization, …
- Customize a pre-trained NLP Q&A base-model
  - e.g., Roberta-base-squad2 (source: huggingface)
- Apply advanced methods
  - Keyword-Based Approach
  - Score-Based Approach
  - Similarity-Based Approach
  - Similarity + Score-Based Approach

Fabasoft

MEDINA PoC

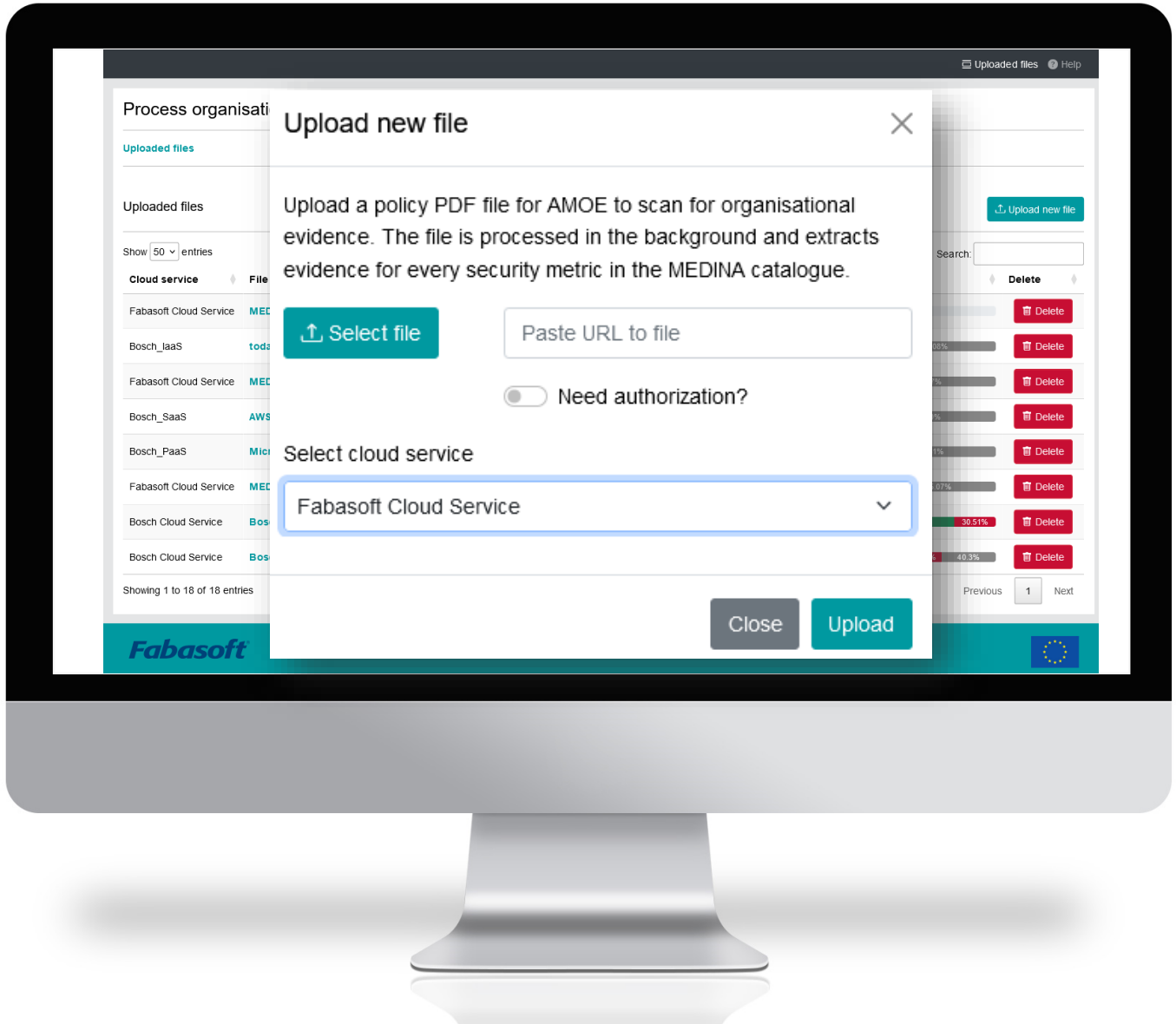
- API endpoints implemented by AMOE



Fabasoft

MEDINA PoC

- Let us look at the AMOE prototype



Process organisational evidence based on metrics

Uploaded files

Uploaded files

Upload new file

Show 50 entries

Search:

Cloud service	File name	Date	Progress	Delete
Fabasoft Cloud Service	MEDINA_dummy_policies_Fabasoft_M18v5.pdf	2023-05-31 10:30:37		Delete
Bosch_IaaS	today_Bosch_IoT_Cloud_Security_Concept.pdf	2023-04-20 12:43:35	5.4 90.08%	Delete
Fabasoft Cloud Service	MEDINA_dummy_policies_Fabasoft_M18v5.pdf	2023-04-13 07:40:45	99.17%	Delete
Bosch_SaaS	AWS_C5_-_DE_Final_Report_-_9_30_2018.pdf	2023-02-21 08:26:22	100.0%	Delete
Bosch_PaaS	Microsoft_Azure_Germany_SOC_2_Type_II_Report_10-1-2020_to_9-30-2021.pdf	2023-02-21 08:26:03	2 96.61%	Delete
Fabasoft Cloud Service	MEDINA_dummy_policies_Fabasoft_M18v4.pdf	2023-01-10 10:41:43	11.9 2 85.07%	Delete
Bosch Cloud Service	Bosch_IoT_Cloud_Security_Concept.pdf	2023-01-04 06:51:12	69.49% 30.51%	Delete
Bosch Cloud Service	Bosch_IoT_Cloud_Security_Concept.pdf	2022-12-09 09:49:31	32.84% 26.87% 40.3%	Delete

Showing 1 to 18 of 18 entries

Previous 1 Next

View evidence

Uploaded files / MEDINA_dummy_policies_Fabasoft_M18v5.pdf

Information about the file

Cloud service	FabasoftTestCCD
File id	63e5fd22e09529afe53309c0
File name	MEDINA_dummy_policies_Fabasoft_M18v5.pdf
Uploaded on	2023-02-10 08:15:30 by ccd_admin
Extracted evidence count	118 / 118

Filter CAB assessment

Compliant: 9 / 118 (
Not compliant: 3 /
Undefined: 106 / 118 (89.83%)

Reset filter

Extracted evidence

Show 50 entries

Search: passwordpo

MetricID	Question	Answer	AMOE assessment hint	CAB assessment	Submitted to Orchestrator
PasswordPolicyQ1	Which parameters define the password policy?	Passwords should have at least **10 upper -and lowercase characters and contain numbers as well as special characters** . Do not reuse passwords for multiple services. Passwords should not be	Undefined	✓ *True*	✓ *Submitted*
PasswordPolicyQ2	What is the passwords maximum age according to the password policy?	encrypted passwords. The password needs to be changed after a maximum time duration of **60 days** .	✓ *True*	✓ *True*	Submit
PasswordPolicyQ3	What is the passwords rotation frequency?	Passwords should have **at least 10** upper -and lowercase characters and contain numbers as well	× *False*	× *False*	Please add a comment to submit
PasswordPolicyQ4	Which requirements exist for password managers?	best practice to use password managers to **generate complex passwords and store the encrypted passwords** . The password needs to be changed after a maximum time duration of 60	Undefined	Undefined	Please set CAB assessment status

Showing 1 to 4 of 4 entries (filtered from 118 total entries)

Previous 1 Next

View compliance status

Uploaded files / MEDINA_dummy_policies_Fabasoft_M18v5.pdf / PasswordPolicyQ2

EUCS Requirement(s) linked to Metric

IAM-08 - PROTECTION AND STRENGTH OF CREDENTIALS

Metric - PasswordPolicyQ2		File	
Keywords	password, age, maximum	**File id**	63e5fd22e09529afe53309c0
Target value	<= 90.0 (Integer)	**File name**	MEDINA_dummy_policies_Fabasoft_M18v5.pdf
Question	What is the passwords maximum age according to the password policy?	**Extraction date**	2023-02-10 08:37:07
Answer	encrypted passwords. The password needs to be changed after a maximum time duration of **60 days** .		Show processed / Show original

Assessment

Assessment hint compliant (*60 days* <= 90.0 (Integer))

Assessment status compliant / not compliant

Last change on 2023-03-29 08:20:52 by admin

Compliance comment

Please enter a comment regarding the assessment status.

The comment has not been changed yet

Submit to orchestrator

No submission yet.

previous metric 84/118 next metric

2 Password Management

Passwords should have at least 10 upper -and lowercase characters and contain numbers as well as special characters. Do not reuse passwords for multiple services. Passwords should not be easy to guess and should not contain personal information such as your birthdate or the name of your child. Do not share the password with third parties and do not store it in plain text. It is best practice to use password managers to generate complex passwords and store the encrypted passwords. The password needs to be changed after a maximum time duration of 60 days.

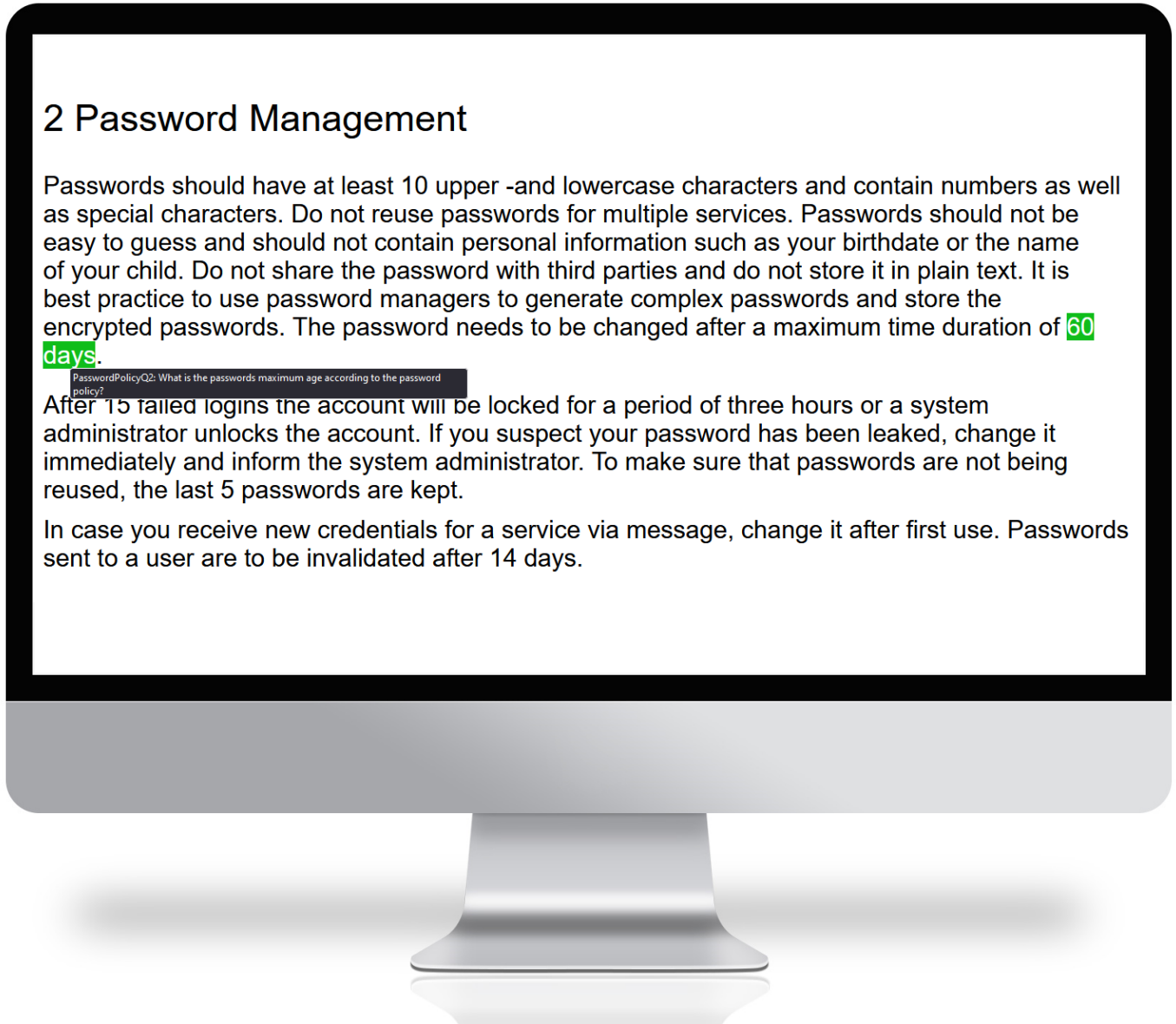
After 15 failed logins the account will be locked for a period of three hours or a system administrator unlocks the account. If you suspect your password has been leaked, change it immediately and inform the system administrator. To make sure that passwords are not being reused, the last 5 passwords are kept.

In case you receive new credentials for a service via message, change it after first use. Passwords sent to a user are to be invalidated after 14 days.

Fabasoft

Trust & Transparency

- The user can investigate, where the answer has been found
- Verification of results is possible through mouseover hints and explanations (for now)



Fabasoft

Summary

- AMOE acts as a tool to **assist** in continuous auditing
- Several evidence extraction approaches
- Addressing AI methods result in **time savings** for traditional audits
  - No manual searches for evidence
  - The increasing amounts of data in audits stay manageable for users
  - Pre-assessments become possible

Fabasoft

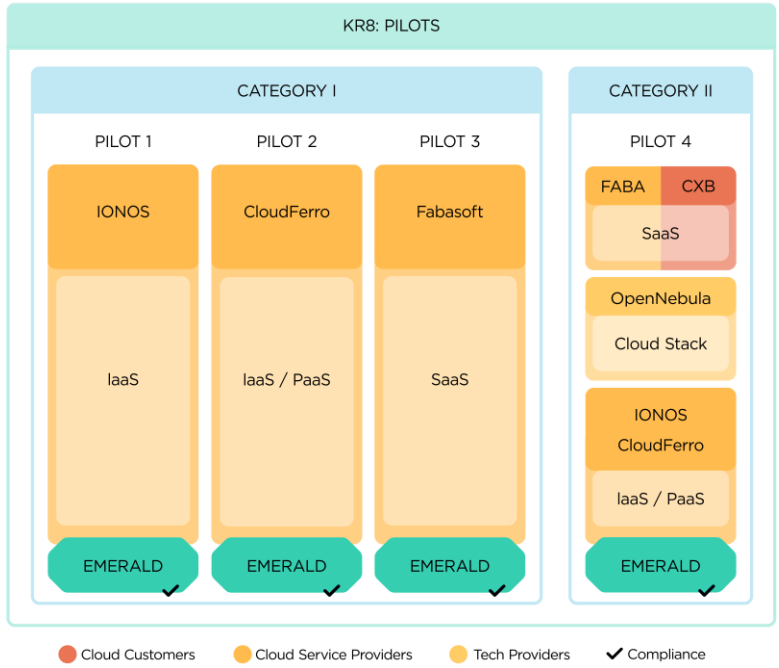
Future Work

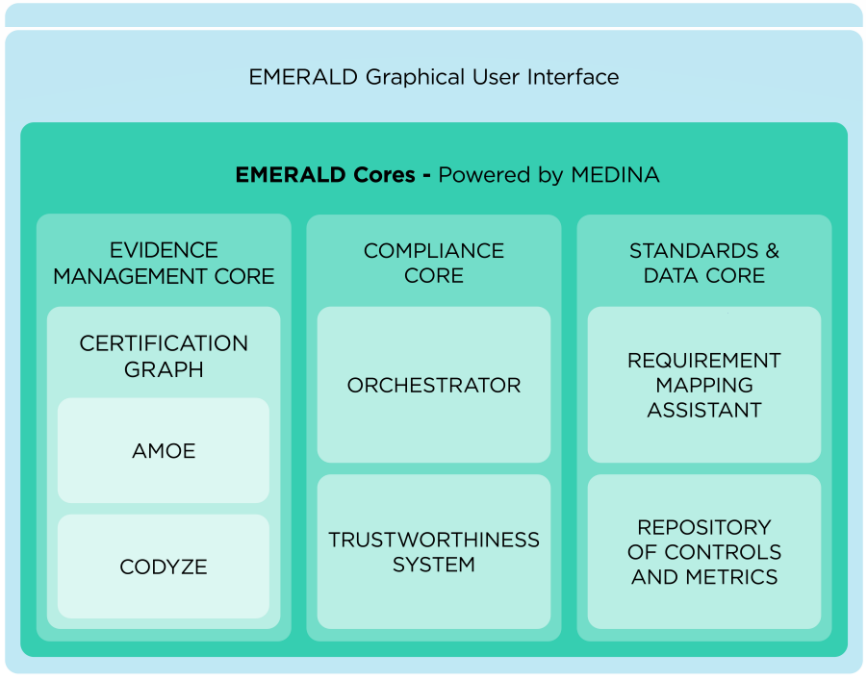
- Improve extraction approach
- Fine tune models/ try additional models
- Elaborate a transition from Q&A NLP models towards LLM
- Combinations of organizational and technical evidence

- Research on trustworthiness of AI support in audits; e.g., EMERALD

Fabasoft

Horizon Europe - EMERALD





tecnalia MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE
Fraunhofer AISEC
Fabasoft
Consiglio Nazionale delle Ricerche
scch software competence center hagenberg
KNOW Center
nixu cybersecurity.
1&1 IONOS
CloudFerro
OpenNebula
CaixaBank

DISCLAIMER

Fabasoft

Copyright © Fabasoft R&D GmbH, A-4020 Linz, 2023.

Fabasoft übernimmt in diesem Dokument weder implizite noch explizite Verpflichtungen, insbesondere nicht dafür, dass das Dokument vollständig und fehlerfrei ist. Fabasoft führt keinerlei Rechtsberatung durch. Die dargestellten Folien sollen nur einen groben Überblick über die Anforderungen der DSGVO aus Sicht von Fabasoft geben und einige Funktionen erklären, die Fabasoft zur Erfüllung der DSGVO bereitstellen kann.

Diese Präsentation enthält Angaben, die sich auf die erwartete zukünftige Entwicklung beziehen. Diese zukunftsbezogenen Aussagen werden üblicherweise – jedoch nicht ausschließlich – mit Begriffen wie „erwarten“, „schätzen“, „planen“, „rechnen mit“, usw. umschrieben. Sollten die den Aussagen zugrunde gelegten Annahmen nicht eintreffen oder Risiken – wie beispielsweise auch im Emissionsprospekt bzw. Risikobericht angesprochen – verwirklichen, oder sich die tatsächlichen Gegebenheiten in der Zukunft ändern, so können die tatsächlichen Ergebnisse von den zurzeit erwarteten Ergebnissen abweichen. Zukunftsbezogene Aussagen erheben keinen Anspruch auf Richtigkeit und Vollständigkeit, werden nicht aktualisiert und sind daher mit der gebotenen Vorsicht zur Kenntnis zu nehmen. Diese Präsentation wurde mit größtmöglicher Sorgfalt erstellt und die angegebenen Daten überprüft. Rundungs-, Satz- und Druckfehler können aber dennoch nicht ausgeschlossen werden. Bei der Summierung von gerundeten Beträgen und Prozentangaben können durch die Verwendung automatisierter Rechenhilfen rundungsbedingte Rechendifferenzen auftreten.

Fehler und Irrtümer vorbehalten.