
UCF
The Science of Compliance


G
C
R
State of Compliance :: 2017
Ever-Increasing Compliance Requirements & Enforcement
Audit Overload
Complex Solutions, Difficult to Automate
Need to Connect Existing Policies to Actual Laws
Need to Follow Multiple Standards
Compliance by Spreadsheets
2

Solution:

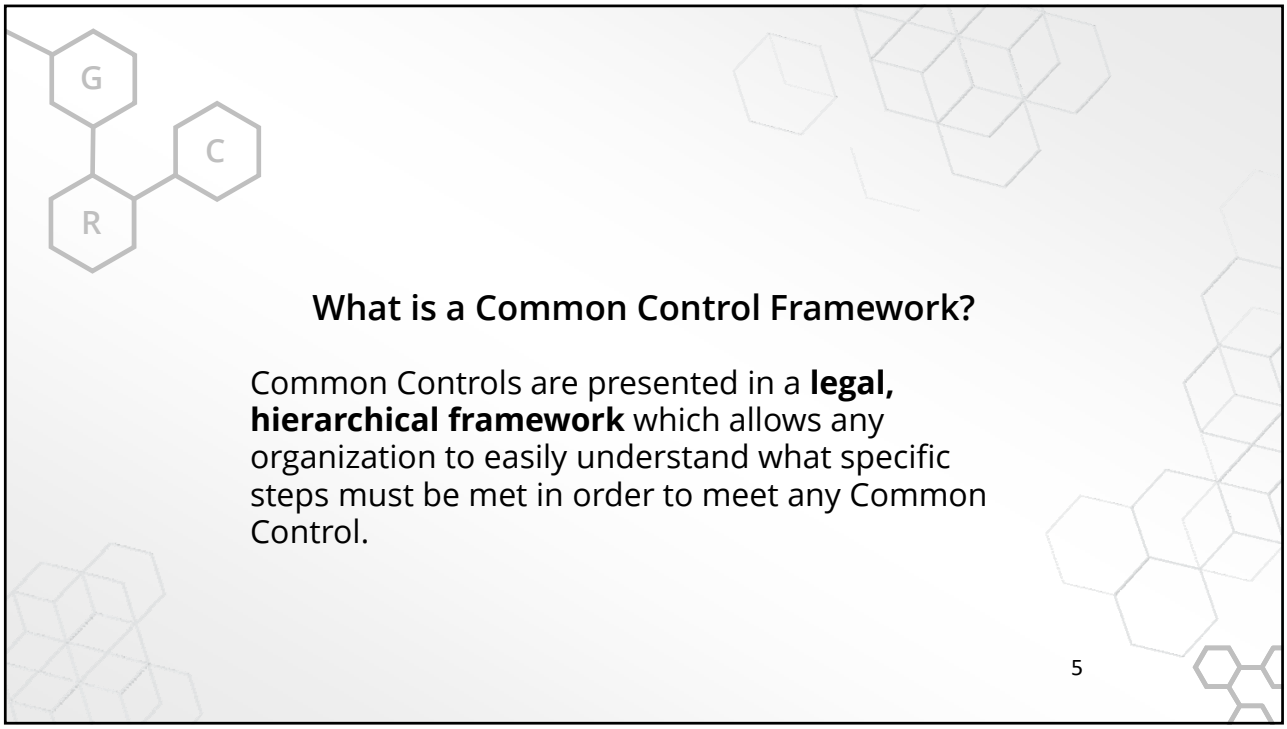
Leverage a Common Control Framework

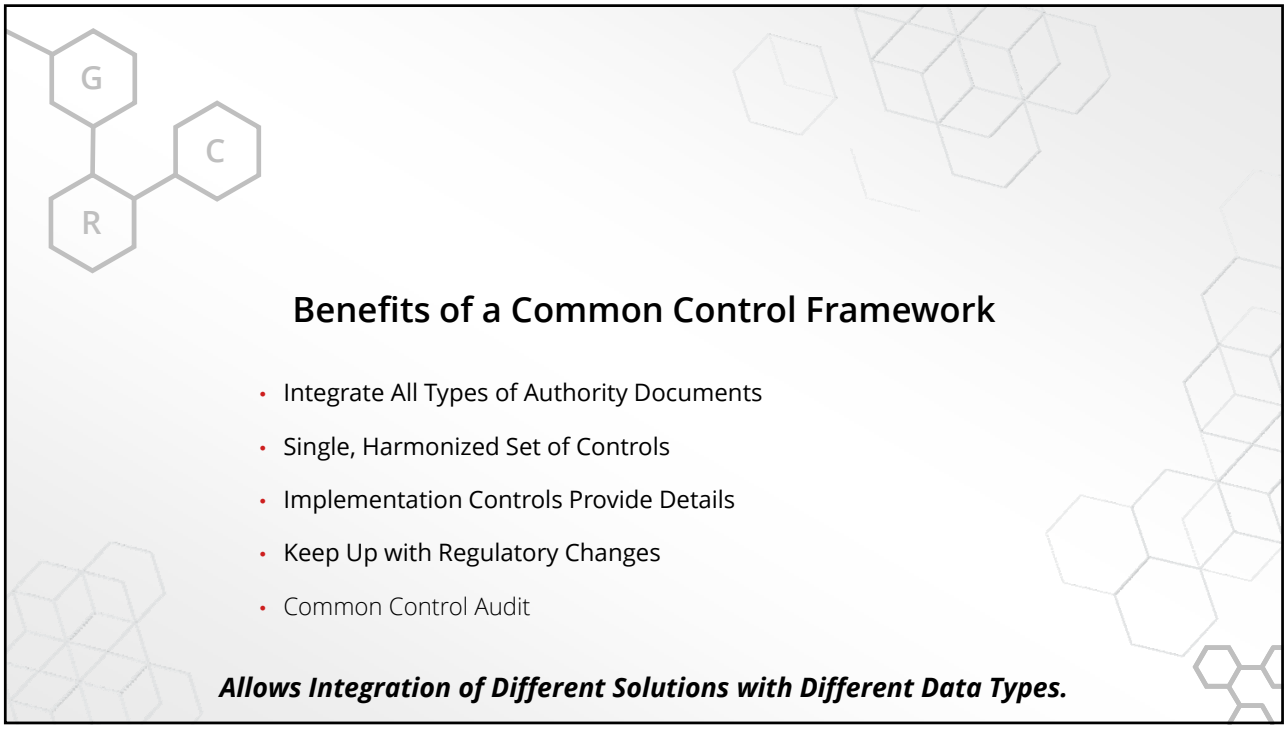
3

What is a Common Control?

A Common Control is a shared compliance requirement written in plain language and connected to the **original mandates** an organization must follow.

4


G
C
R
What is a Common Control Framework?
Common Controls are presented in a **legal, hierarchical framework** which allows any organization to easily understand what specific steps must be met in order to meet any Common Control.
5


G
C
R
Benefits of a Common Control Framework
Integrate All Types of Authority Documents
Single, Harmonized Set of Controls
Implementation Controls Provide Details
Keep Up with Regulatory Changes
Common Control Audit
Allows Integration of Different Solutions with Different Data Types.

Three Key Components

UCF

UCF Mapper

UCF Common Controls Hub

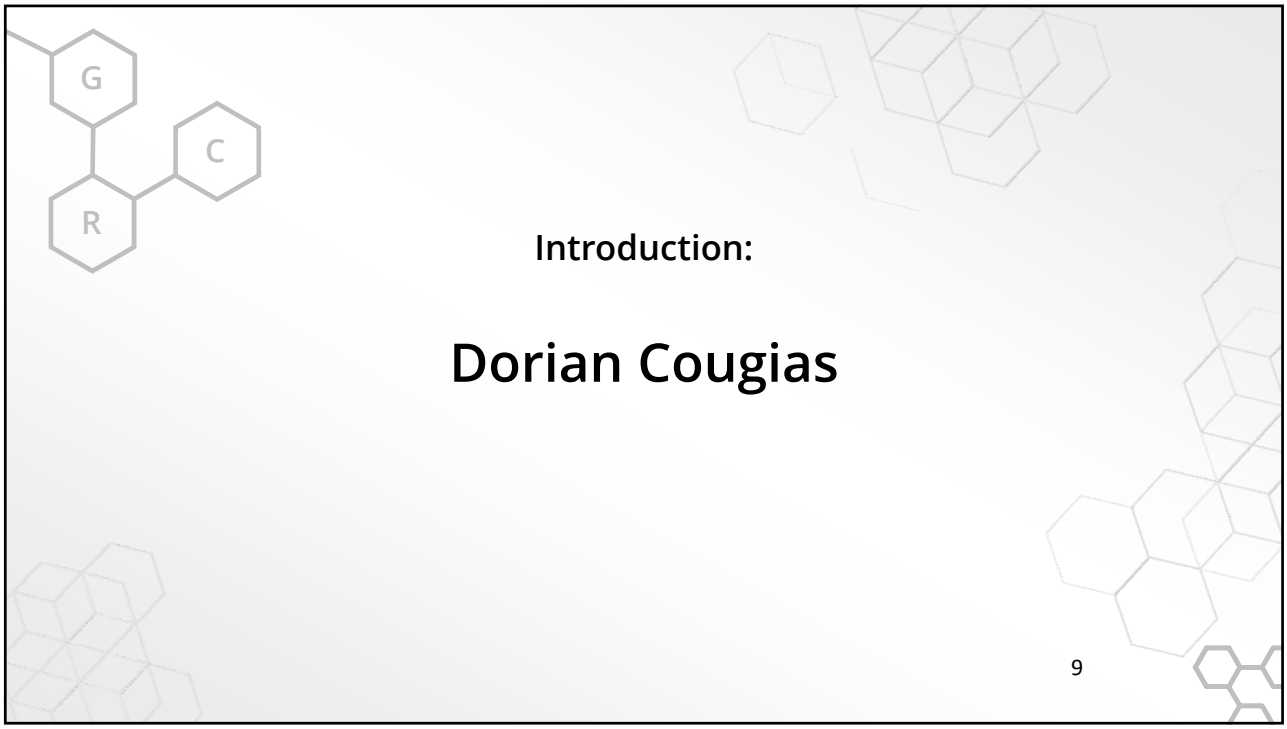
7

UCF Mapper

UCF

Patented Processes for Creating the UCF

8


G
C
R
Introduction:
Dorian Cougias
9


Most Compliance Mapping is wrong
But you already know that…

How do we know? They can't show their proof

- A proof is a series of *statements* or *outputs*, each of which follows *logically* from what has gone before.
- It *starts* with things we are assuming to be true and *ends* with the thing we are trying to prove. All proofs have a beginning, middle, and end.

- **Beginning** – things we can assume to be true.
- **Middle** – statements and outputs, each following logically from prior statements. These are the arguments.
- **End** – the thing we have proven.

A Compliance Mapping Proof

- **Beginning**
  - Is the **source** (the Authority Document) properly catalogued?
  - Are the correct **Citations** extracted properly and fully?
- **Middle**
  - Are the individual **Mandates** within each Citation tagged for the verbs and nouns?
  - Are each tagged term's in-context **definition** selected?
- **End**
  - Does the mapping of the Citation follow a well-defined rule, and is that mapping documented?

What you normally *get* in "mapping tables"

This is what you normally see

NIST ID.AM-1 Physical devices and systems within the organization are inventoried and an inventory of these assets shall be drawn up and maintained.

ISO/IEC 27001:2013 A.8.1.1

ISO/IEC 27001:2013 A.8.1.2

NIST SP 800-53 Rev. 4 CM-8

Here is the missing text

NIST ID.AM-1 Physical devices and systems within the organization are inventoried and an inventory of these assets shall be drawn up and maintained.

ISO/IEC 27001:2013 A.8.1.1 *Assets associated with information and information processing facilities shall be identified.*

ISO/IEC 27001:2013 A.8.1.2 *Assets maintained in the inventory shall be owned.*

NIST SP 800-53 Rev. 4 CM-8 *The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.*

Proof – Mandate Tagging and Definitions

REFERENCE	TAGGED MANDATES	NOUN AND VERB PAIRING
NIST ID.AM-1	[Physical devices] and [systems] within the organization are {inventoried} and	N: Physical Device or system (e.g., assets held by the organization) V: inventory (e.g., the activity of making a comprehensive complete list of things.)
	an [inventory of these assets] shall be {drawn up and maintained}.	N: inventory of the assets (e.g., the record produced after tallying) V: drawn up and maintained (e.g., the activity of creating and maintaining something)

Proof – Mandate Tagging and Definitions

REFERENCE	TAGGED MANDATES	NOUN AND VERB PAIRING
ISO/IEC 27001:2013 A.8.1.1	[Assets] associated with information and information processing facilities shall be *{identified}*.	N: Assets (e.g., assets held by the organization) V: identified (Establish and verifying what something is)
ISO/IEC 27001:2013 A.8.1.2	[Assets] maintained in the [inventory] shall be *{owned}*.	N: Assets (as above), inventory (as record) V: own (taking responsibility for)
NIST SP 800-53 Rev. 4 CM-8	The organization *{verifies}* that all [components within the authorization boundary of the information system] are [not duplicated] in other information system component [inventories].	N: system components (parts of assets), duplicate entries (record entries), inventory (as a record) V: verify (declare as true)

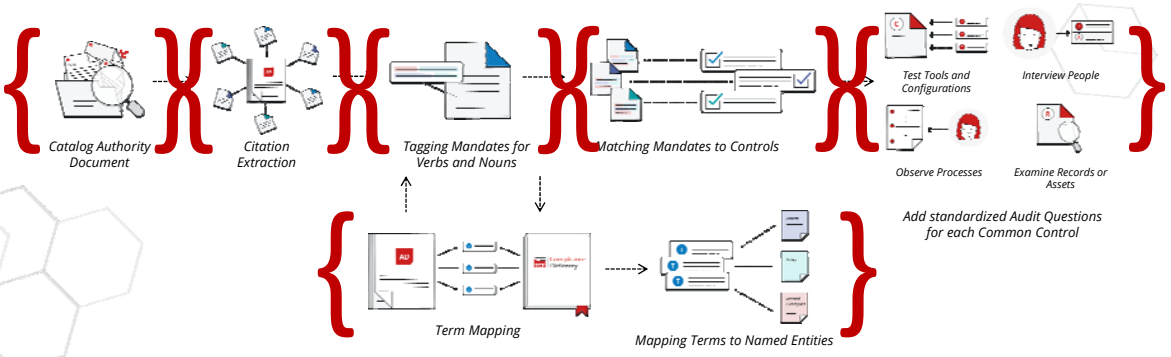
One (maybe two) out of three? Really?

NIST	NOUN AND VERB PAIRING	MATCHES?	Reference	NOUN AND VERB PAIRING
ID.AM-1	N: Physical Device or system (e.g., assets held by the organization) V: inventory (e.g., the activity of making a comprehensive complete list of things.)	**Yes**	**A.8.1.1**	N: Assets (e.g., assets held by the organization) V: identified (Establish and verifying what something is)
		No	**A.8.1.2**	N: Assets (as above), inventory (as record) V: own (taking responsibility for)
	N: inventory of the assets (e.g., the record produced after tallying) V: drawn up and maintained (e.g., the activity of creating and maintaining something)	**Maybe**	**CM-8**	N: system components (parts of assets), duplicate entries (record entries), inventory (as a record) V: verify (declare as true)

How do *we* map Citations?

(and provide your proof along the way)

The Compliance Mapping Process

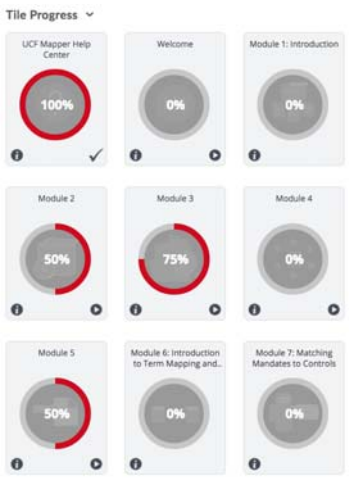


How do we (you too) do this?

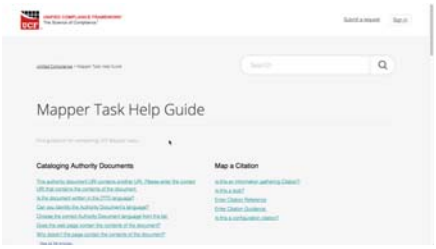
UCF | Mapper

Along with passing the Certificate in Compliance Mapping from (ISC)2

The coursework

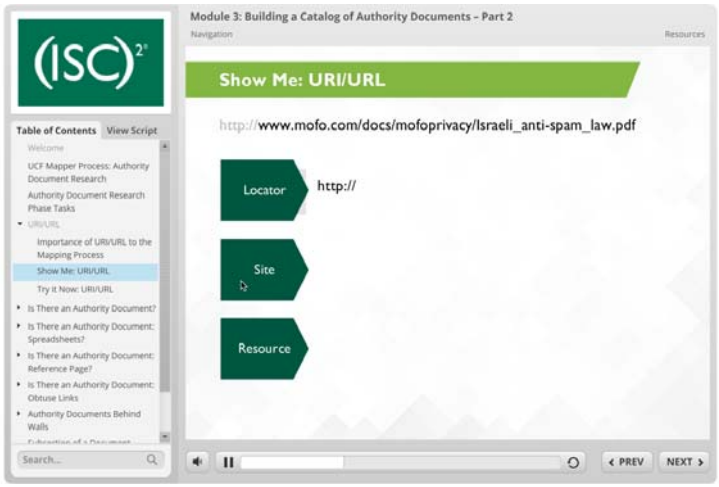


- The coursework is laid out in module format and delivered online.
- As a student, you are also connected to the UCF FAQs, Community, and individual how-tos for each step of the way!

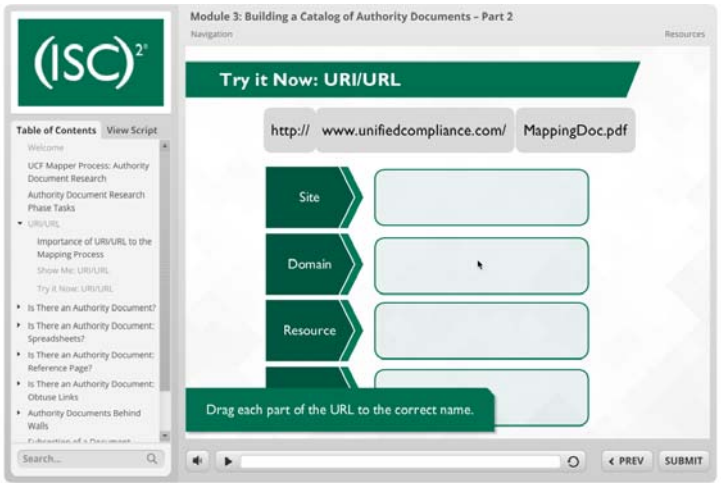


Presentation Materials

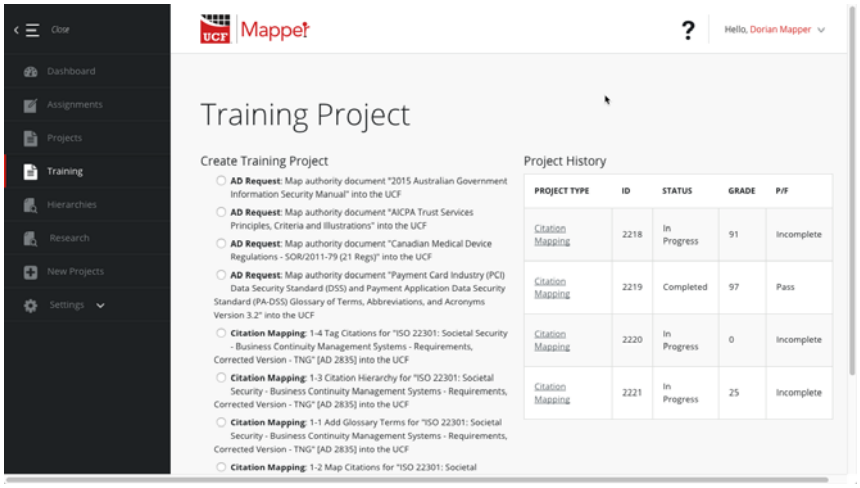
Show Me tutorials

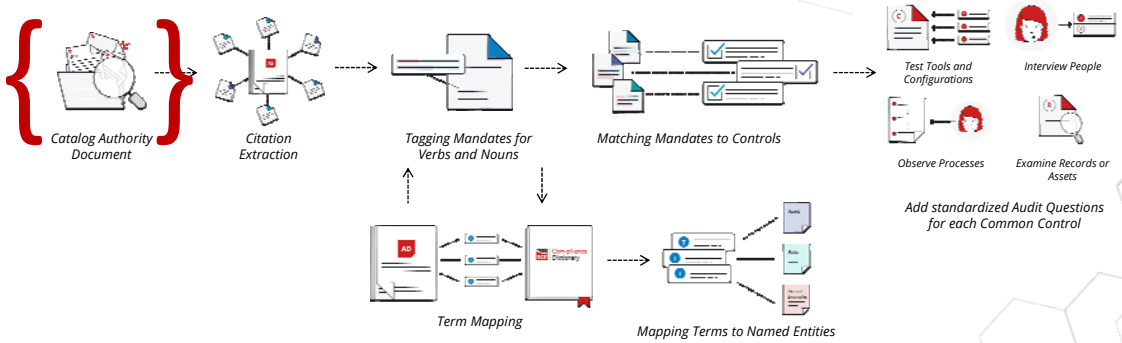


Try it Now quizzes



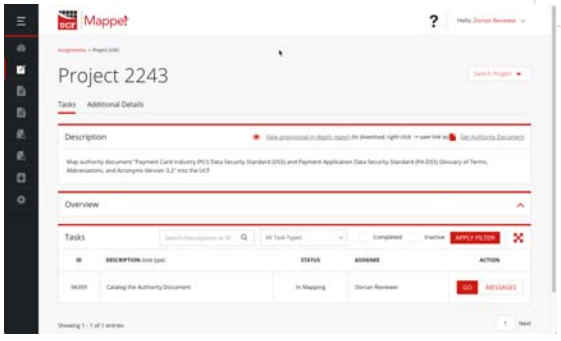
UCF Mapper Practice Activities

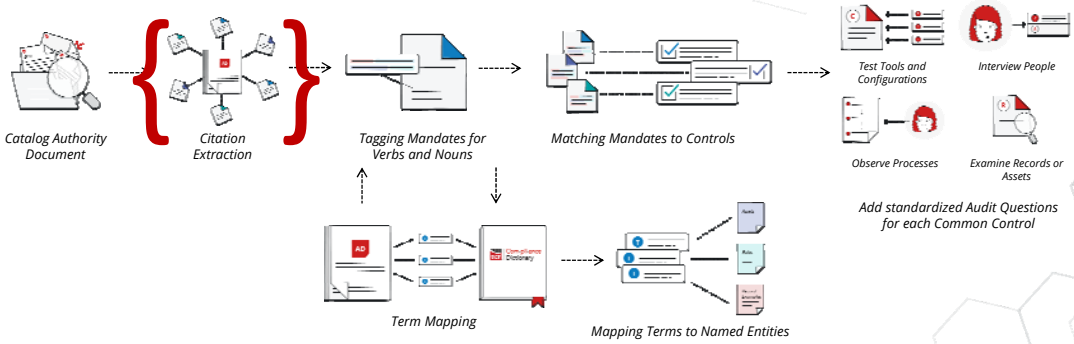




Cataloging Authority Documents

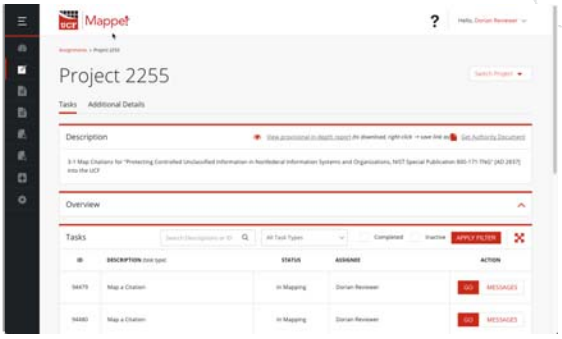
Cataloging Authority Documents

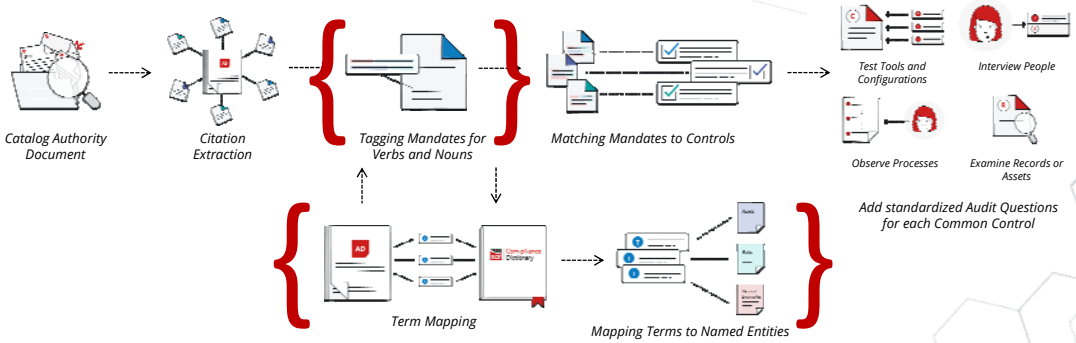




Citation Extraction

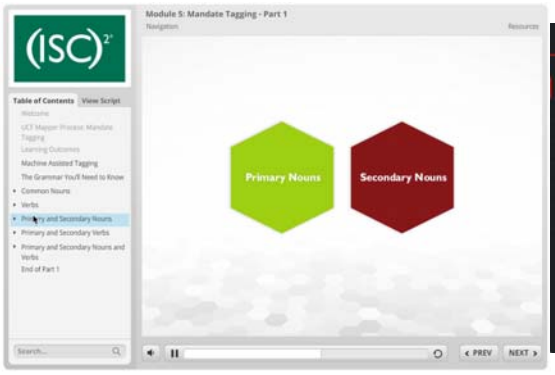
Citation Extraction

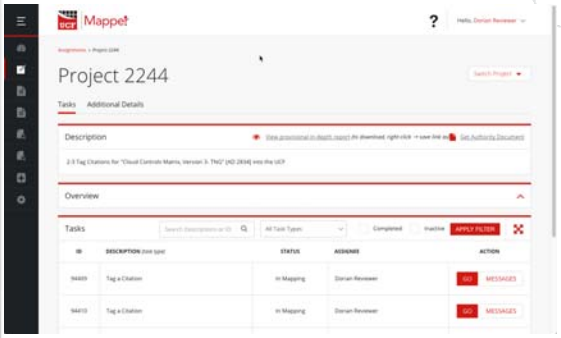




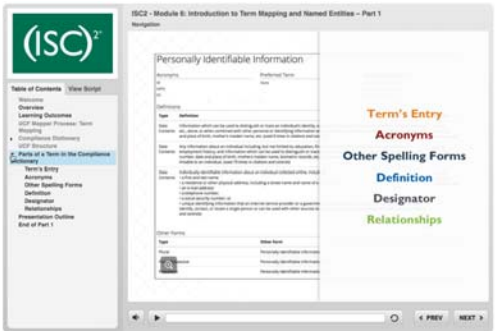
Tagging Mandates and Adding Terms

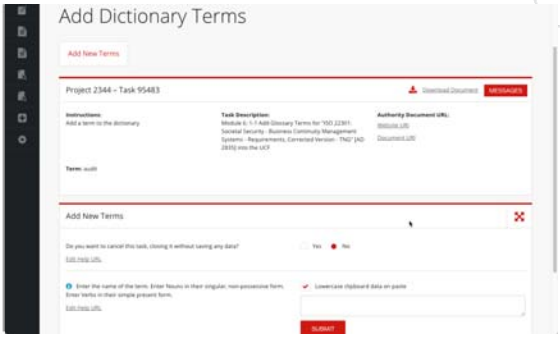
Citation Tagging



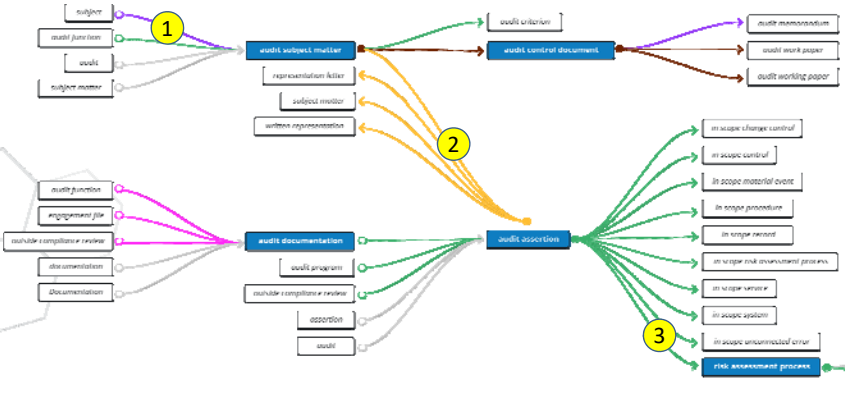


Adding new Terms





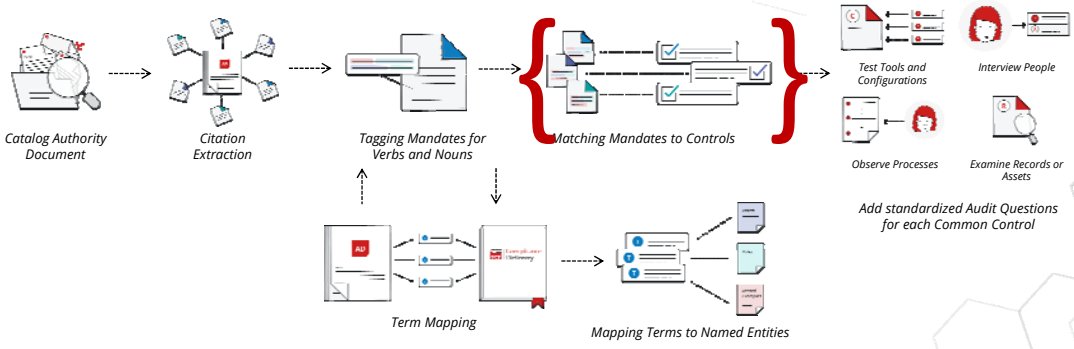
UCF Mapper Uses Semantic Crosswalking to Accurately Map Citations to Controls



Semantic Crosswalking Rules

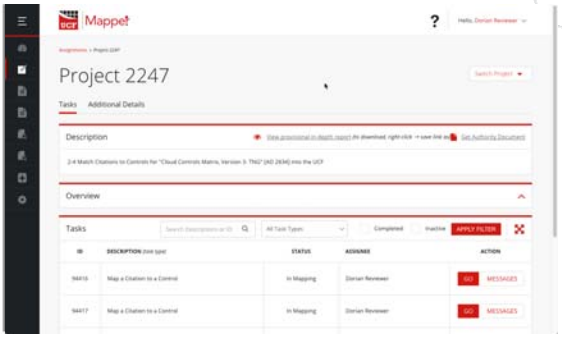
Verb Hops	Noun Hops	Accuracy	Grade
0	0	100.00%	A
0	1	95.00%	A
1	0	92.50%	A-
0	2	90.00%	A-
1	1	87.50%	B+
2	0	85.00%	B
0	3	85.00%	B
1	2	82.50%	B-
0	4	80.00%	B-
2	1	80.00%	B-
3	0	77.50%	C+
1	3	77.50%	C+
0	5	75.00%	C
2	2	75.00%	C

- The measurement of accuracy must be the equivalent of a letter grade between A and F on a standard percentage scale.

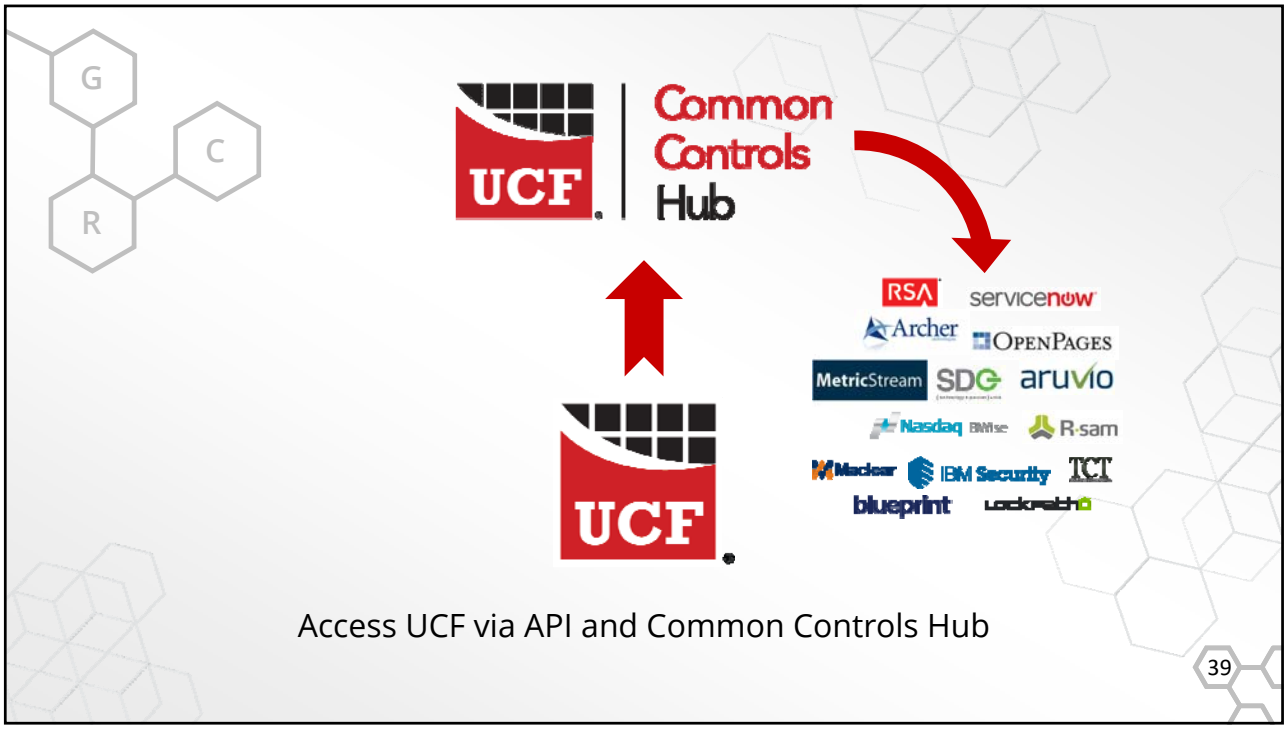


Matching Mandates to Controls

Matching Mandates to Common Controls



Three Key Components



Questions and Answers

UCF®

The Science of Compliance®