


**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



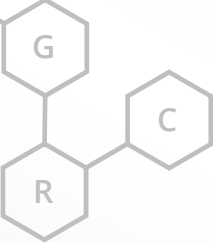
The slide features a light gray background with a molecular structure pattern of interconnected hexagons. On the left side, there is a logo consisting of three hexagons: one labeled 'G' at the top, one labeled 'R' at the bottom left, and one labeled 'C' at the bottom right, all connected by lines. In the bottom right corner, there is a small hexagon containing the number '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



## 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



## 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

The diagram features a light gray background with a faint molecular structure pattern. In the top left corner, there is a chemical structure consisting of three hexagons labeled G, R, and C. The central text reads "Three Key Components". Below this, three logos are displayed: the UCF logo (a red square with a white grid pattern and the letters "UCF" in white), the UCF Mapper logo (the UCF logo followed by the word "Mapper" in red), and the UCF Common Controls Hub logo (the UCF logo followed by the words "Common Controls Hub" in red). A small hexagon with the number "7" is located in the bottom right corner.

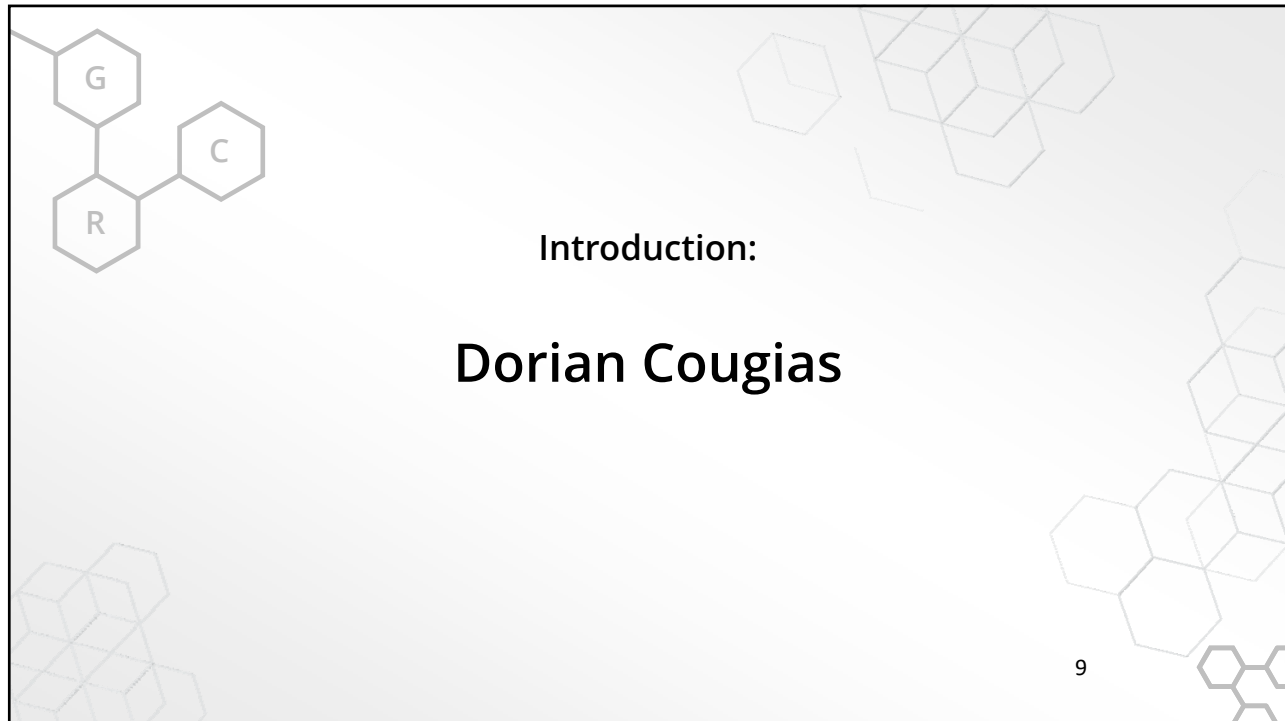
UCF Mapper

UCF

Patented Processes for Creating the UCF

8

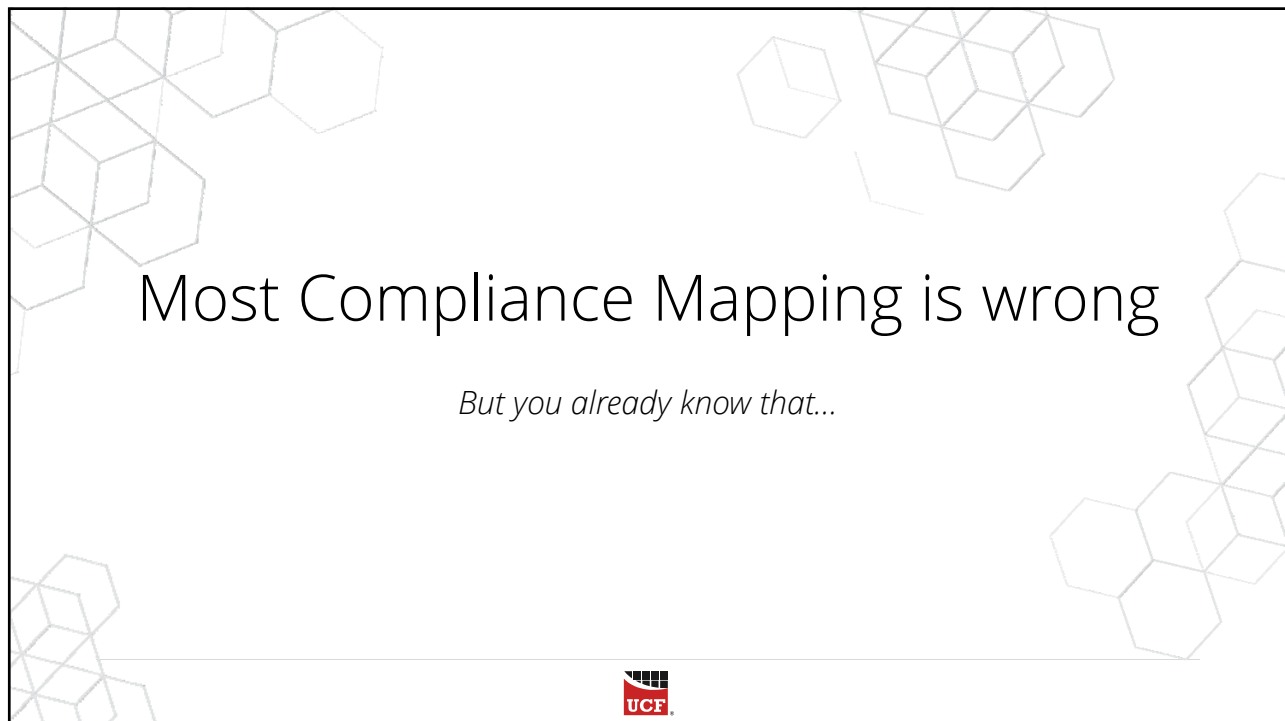
The diagram features a light gray background with a faint molecular structure pattern. In the top left corner, there is a chemical structure consisting of three hexagons labeled G, R, and C. The central text reads "Patented Processes for Creating the UCF". Above this text is the UCF Mapper logo (the UCF logo followed by the word "Mapper" in red). Below the text is a large red downward-pointing arrow, and below the arrow is the UCF logo (a red square with a white grid pattern and the letters "UCF" in white). A small hexagon with the number "8" is located in the bottom right corner.



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 { <i>identified</i> }.	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 { <i>owned</i> }.	N: Assets (as above), inventory (as record) V: own (taking responsibility for)
NIST SP 800-53 Rev. 4 CM-8	The organization { <i>verifies</i> } 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)

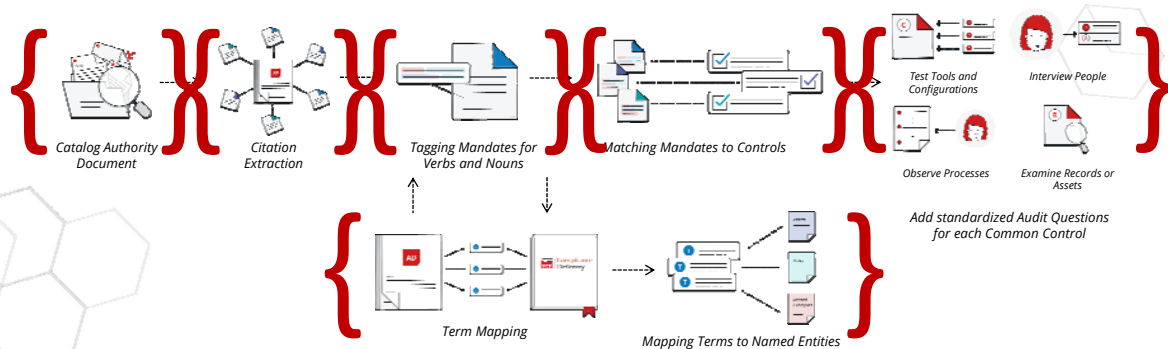


# How do we map Citations?

(and provide your proof along the way)



## The Compliance Mapping Process



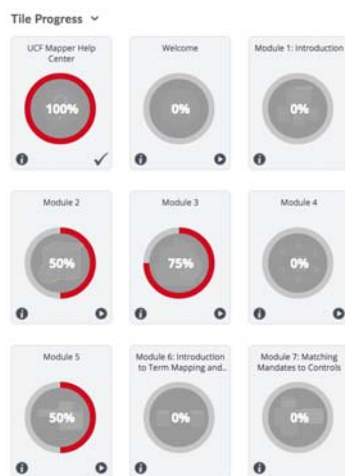
How do we (you too) do this?



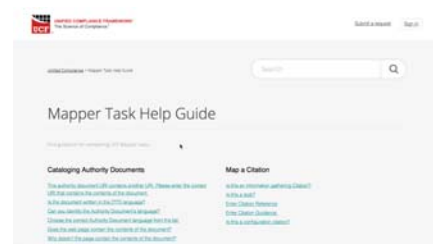
Along with passing the Certificate in Compliance Mapping from (ISC)2



## 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

The screenshot shows a presentation slide for 'Module 2: About the UCF Mapper Software'. The slide features the (ISC)<sup>2</sup> logo in the top left corner. Below the logo is a 'Table of Contents' menu with items such as 'Welcome', 'Learning Outcomes', 'Accessing the Software', 'UCF Mapper Layout', 'UCF Mapper Dashboard', 'Accepting or Declining Assignments', 'Assignments', 'The Structure of Projects', 'Projects', 'Task Pages', 'Task Workflows', 'Task Steps', 'Summary', and 'End of Module'. The main content area of the slide is titled 'ABOUT THE UCF MAPPER SOFTWARE' and contains a collage of images showing people working at computers. A large red banner with the 'UCF' logo is prominently displayed in the center. At the bottom right of the slide, there is a text box that says 'Click the next button to continue.' Below the slide content is a navigation bar with a search field, a play button, a progress bar, and a 'NEXT >' button.



## Show Me tutorials

The screenshot shows a presentation slide for 'Module 3: Building a Catalog of Authority Documents - Part 2'. The slide is titled 'Show Me: URI/URL' and features the (ISC)<sup>2</sup> logo in the top left corner. Below the logo is a 'Table of Contents' menu with items such as 'Welcome', 'UCF Mapper Process: Authority Document Research', 'Authority Document Research', 'Please Tasks', 'URI/URL', 'Importance of URI/URL to the Mapping Process', 'Show Me: URI/URL', 'Try it Now: URI/URL', 'Is There an Authority Document?', 'Is There an Authority Document: Spreadsheets?', 'Is There an Authority Document: Reference Page?', 'Is There an Authority Document: Obsolete Links', and 'Authority Documents Behind Walls'. The main content area of the slide displays the URL 'http://www.mofo.com/docs/mofoprivacy/Israeli\_anti-spam\_law.pdf'. Below the URL are three green arrow-shaped buttons labeled 'Locator', 'Site', and 'Resource'. The 'Locator' button is currently selected. At the bottom of the slide is a navigation bar with a search field, a play button, a progress bar, and 'PREV' and 'NEXT >' buttons.



## Try it Now quizzes

Module 3: Building a Catalog of Authority Documents - Part 2

Navigation Resources

### Try it Now: URI/URL

http:// www.unifiedcompliance.com/ MappingDoc.pdf

Site

Domain

Resource

Drag each part of the URL to the correct name.

Search...

PREV SUBMIT



## UCF Mapper Practice Activities

UCF Mapper

?, Hello, Dorian Mapper

### Training Project

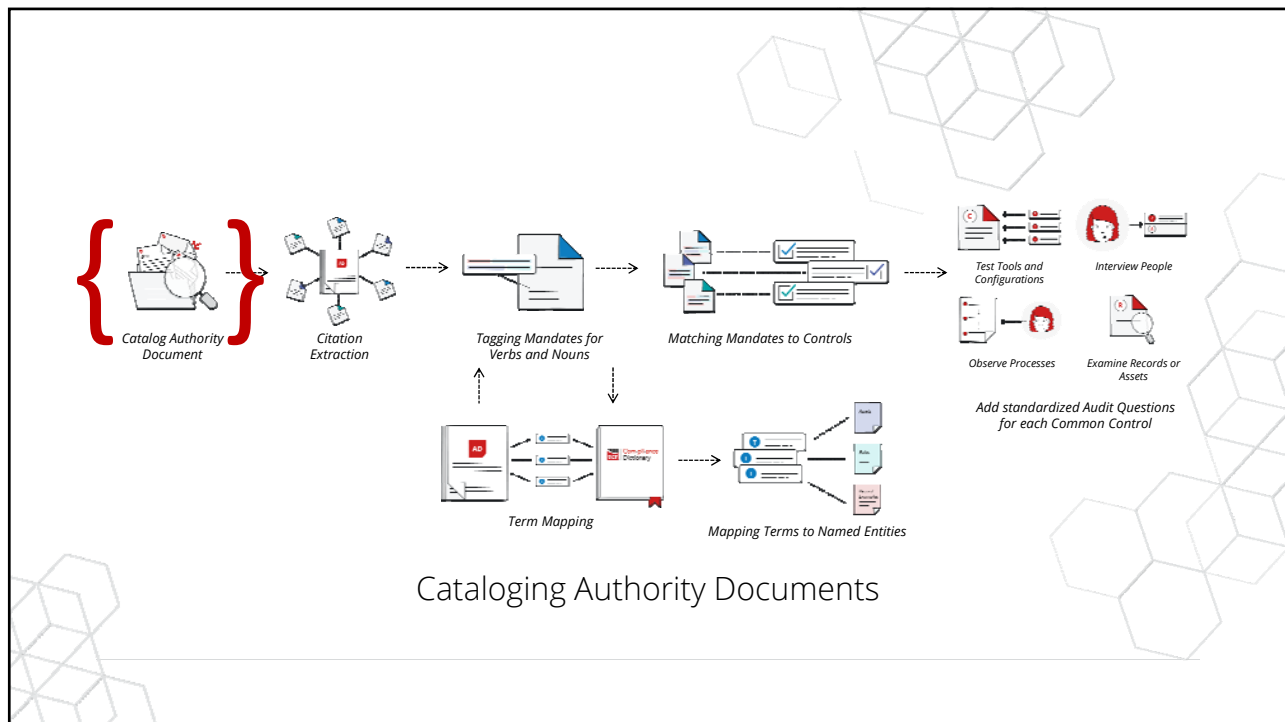
Create Training Project

- AD Request: Map authority document "2015 Australian Government Information Security Manual" into the UCF
- AD Request: Map authority document "AICPA Trust Services Principles, Criteria and Illustrations" into the UCF
- AD Request: Map authority document "Canadian Medical Device Regulations - SOR/2011-79 (21 Regs)" into the UCF
- AD Request: Map authority document "Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS) Glossary of Terms, Abbreviations, and Acronyms Version 3.2" into the UCF
- Citation Mapping: 1-4 Tag Citations for "ISO 22301: Societal Security - Business Continuity Management Systems - Requirements, Corrected Version - TNG" (AD 2835) into the UCF
- Citation Mapping: 1-3 Citation Hierarchy for "ISO 22301: Societal Security - Business Continuity Management Systems - Requirements, Corrected Version - TNG" (AD 2835) into the UCF
- Citation Mapping: 1-1 Add Glossary Terms for "ISO 22301: Societal Security - Business Continuity Management Systems - Requirements, Corrected Version - TNG" (AD 2835) into the UCF
- Citation Mapping: 1-2 Map Citations for "ISO 22301: Societal

Project History

PROJECT TYPE	ID	STATUS	GRADE	P/F
Citation Mapping	2218	In Progress	91	Incomplete
Citation Mapping	2219	Completed	97	Pass
Citation Mapping	2220	In Progress	0	Incomplete
Citation Mapping	2221	In Progress	25	Incomplete





## Cataloging Authority Documents

Module 2: Building a Catalog of Authority Documents - Part 2

**BUILDING A CATALOG OF AUTHORITY DOCUMENTS PART 2**

UCF

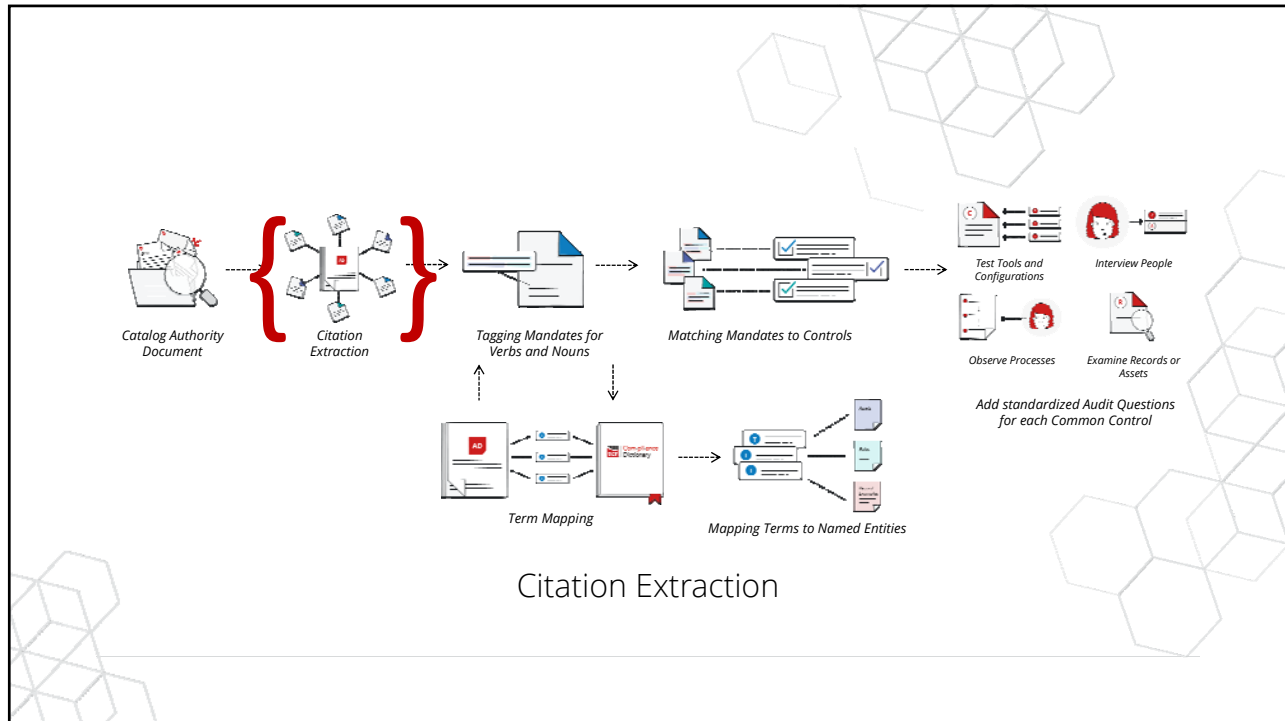
**Mappet**

Project 2243

Tasks: Additional Details

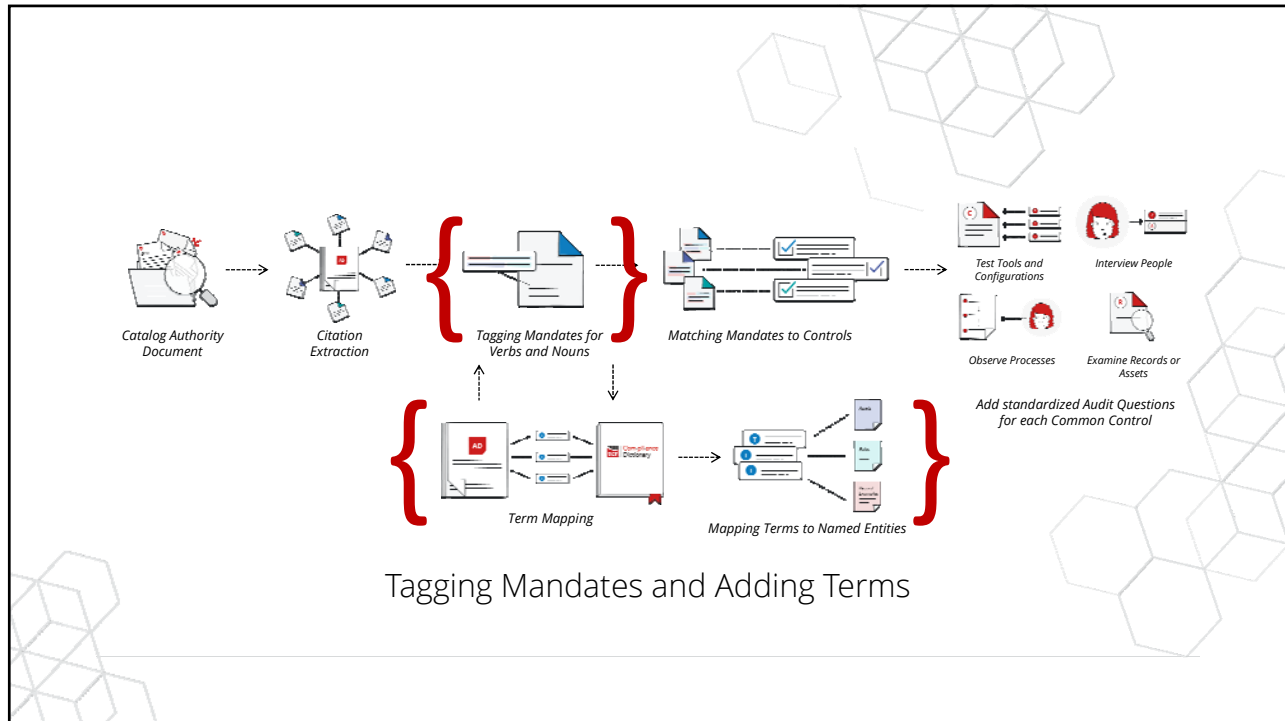
Description: Map authority document "Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS) Summary of Terms, Abbreviations, and Acronyms Version 3.2" into the UCF

DESCRIPTION (task type)	STATUS	ASSIGNEE	ACTION
2243 Catalog the Authority Document	In Mapping	Debrah Rowland	MESSAGES



## Citation Extraction

ID	DESCRIPTION (see type)	STATUS	ASSIGNED	ACTION
16475	Map a Citation	In Mapping	Dorian Reisman	MESSAGES
16480	Map a Citation	In Mapping	Dorian Reisman	MESSAGES



Tagging Mandates and Adding Terms

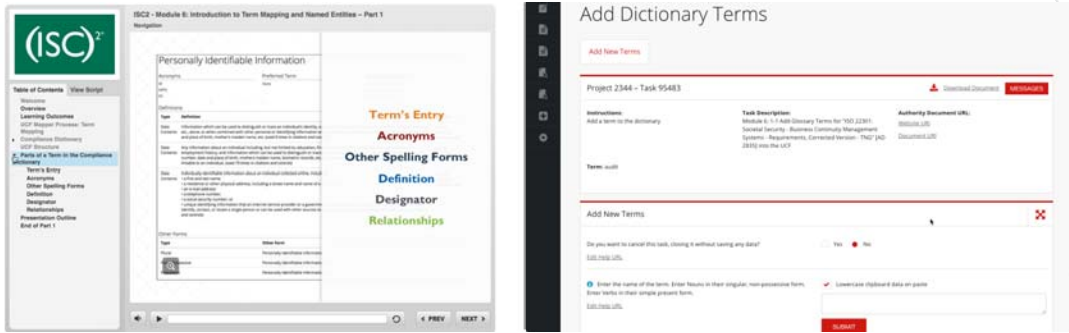
## Citation Tagging

The left screenshot shows the ISC2 Mappet interface for 'Module 5: Mandate Tagging - Part 1'. It features a 'Table of Contents' on the left and a central graphic with two hexagons labeled 'Primary Nouns' (green) and 'Secondary Nouns' (red). The right screenshot shows the 'Project 2244' page with a 'Tasks' table.

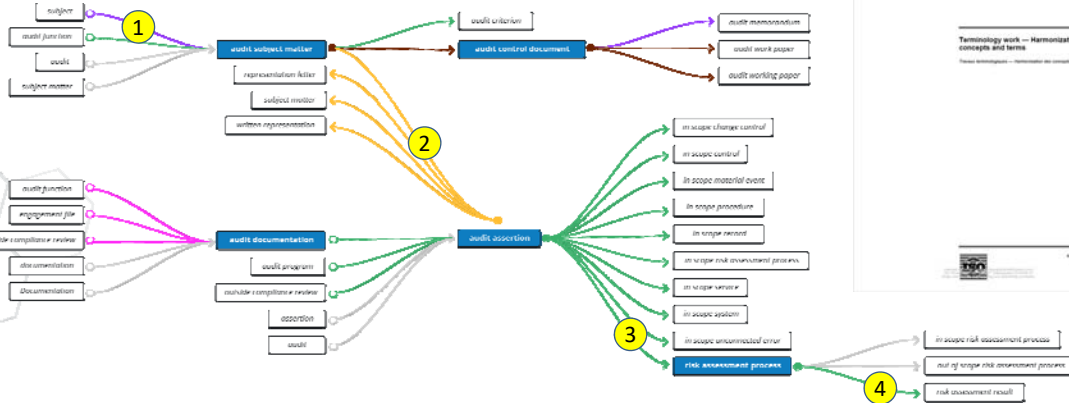
ID	DESCRIPTION (see spec)	STATUS	ASSIGNEE	ACTION
W400	Tag a Citation	In Mapping	Garret Peterson	REASSIGN
W401	Tag a Citation	In Mapping	Garret Peterson	REASSIGN



# Adding new Terms



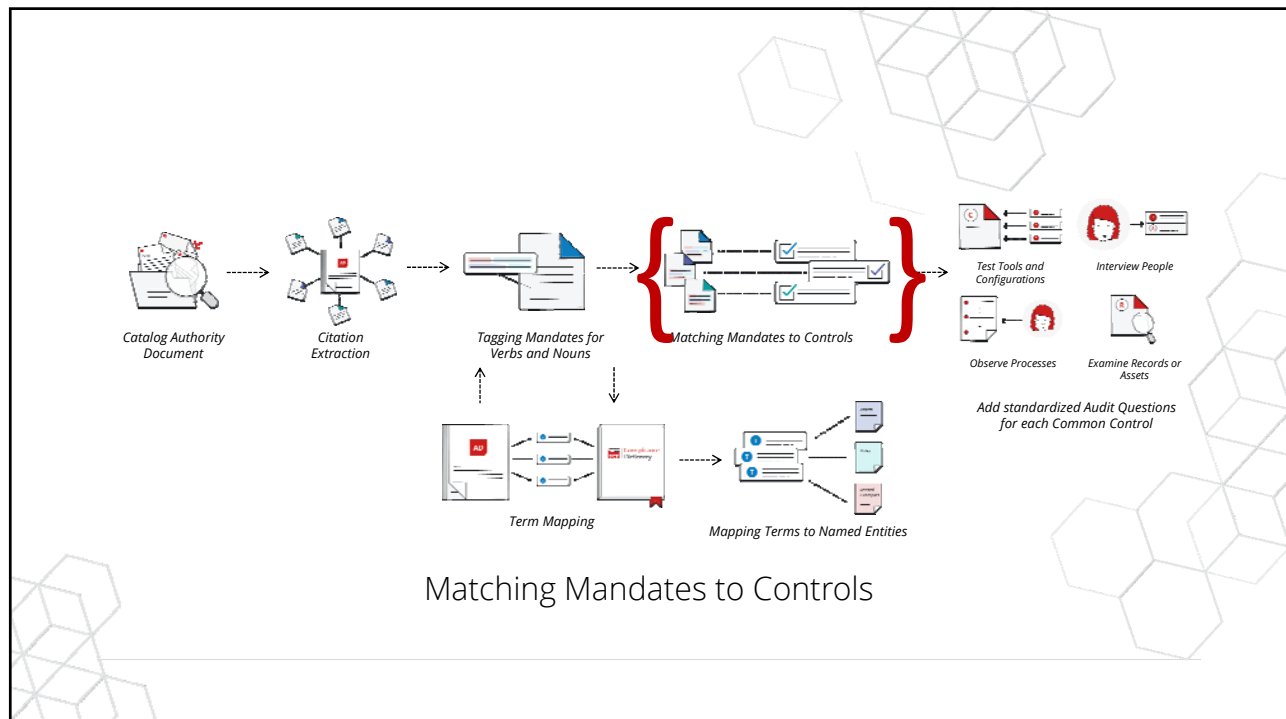
# UCF Mapper Uses Semantic Crosswalking to Accurately Map Citations to Controls



## 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

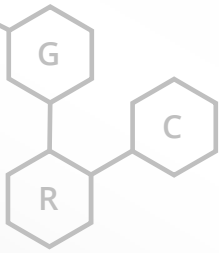
- The measurement of accuracy must be the equivalent of a letter grade between A and F on a standard percentage scale.



# Matching Mandates to Common Controls

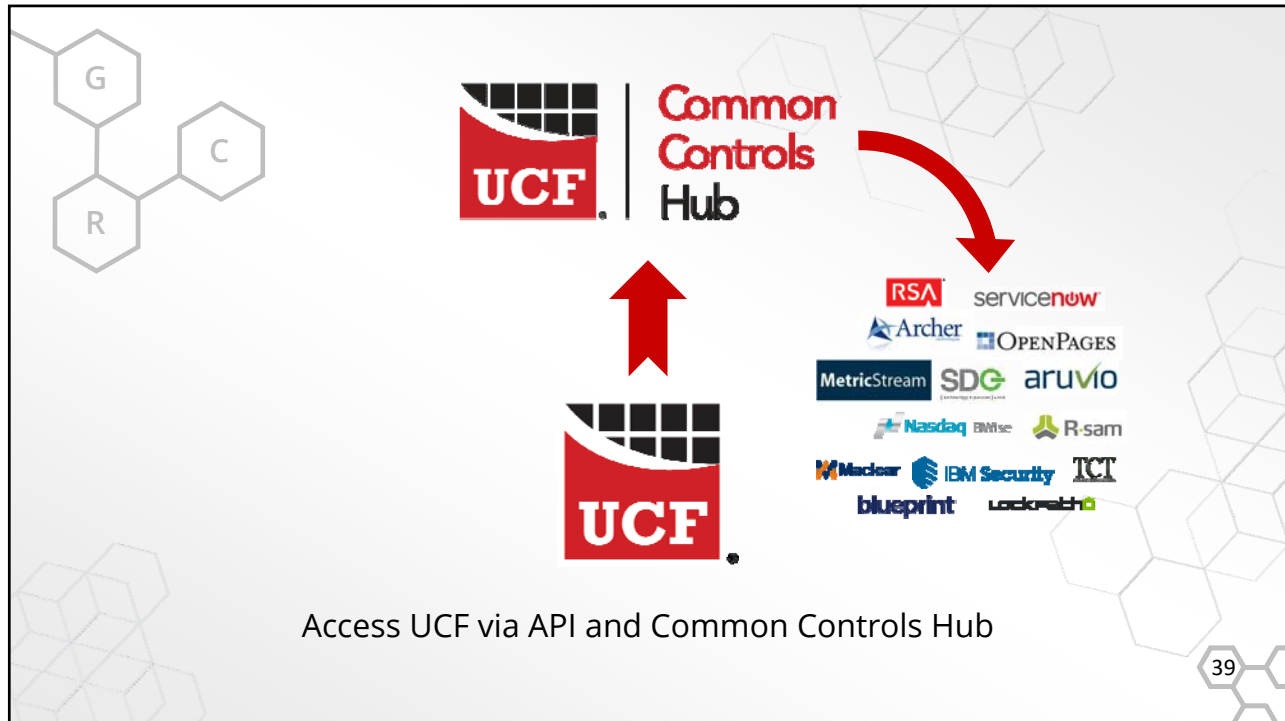
The image shows two screenshots of software interfaces. The left screenshot is from ISC2, titled 'Module 7: Matching Mandates to Controls'. It features a 'MATCHING MANDATES TO CONTROLS' section with a UCF logo and a 'Click the next button to continue' instruction. The right screenshot is from Mappet, showing 'Project 2247' with a table of tasks. The table has columns for ID, Description, Status, Assignee, and Action.

ID	DESCRIPTION	STATUS	ASSIGNEE	ACTION
22470	Map a Control to a Control	In Mapping	Dorian Reusser	MESSAGES
22471	Map a Control to a Control	In Mapping	Dorian Reusser	MESSAGES



## Three Key Components





## Questions and Answers



The Science of Compliance®