What you must do *before you comply* and why the UCF's mapping approach makes the job easier (and more scientific)

To understand the Unified Compliance Framework, you must first understand the enormous amount of work you must do *before* you can begin to comply, and why our scientific approach to this problem is a great solution.

The Main Thing

For those of you who don't like to read long-winded documents, here's the Main Thing you need to know:

- find your Authority Documents – the right ones with the right versions;
- then classify them according to a usable methodology;
- organize those Authority Documents into a searchable library;
- extract the Citations from the Authority Documents and then separate those Citations into individual mandates that you can map to Common Controls;
- categorize your Common Controls so that they are digestible to the different groups within your organization;
- and don't forget to create a glossary so that you know when one Authority Document says "turn off the spigot" and another says "shut the tap", you are dealing with the same thing.

Now, if you have a scientific way of doing this, and it is documented and repeatable from one group to another – without variance – then you don't need us.

However, if you are like most folks and don't really grasp the depth of what it takes to do everything we said above, then read on.

And then read the part about how we make it more scientific (repeatable without variance) and how we can help you. And you can help us.

Because that's what it's all about.

What does it mean to comply?

Compliance is ensuring that the requirements of laws, regulations, industry codes, and organizational doctrines are met. Period. This also applies to contractual arrangements to which the business process is subject, i.e., externally imposed business criteria. Compliance is a process, effected by management and other personnel as governance methods designed to provide reasonable assurance that transactions are executed in accordance with:

- laws governing the use of budget authority and other laws and regulations that could have a direct and material effect on the financial statements or required supplementary stewardship information;
- any other laws, regulations, and government wide policies identified in audit guidance;
- claims of adherence to industry codes or standards; or
- contractual obligations.

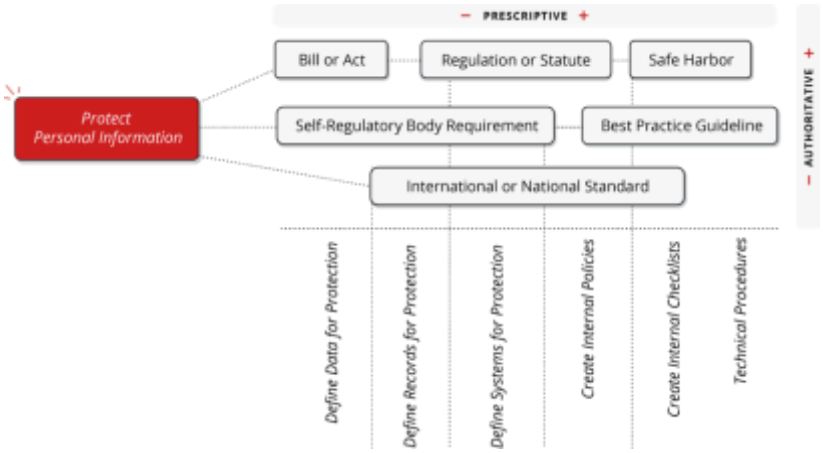
We call all of these types of documents "Authority Documents". In other words, compliance simply means following the rules that are set by people other than ourselves.

Compliance is following rules set by people other than ourselves

Compliance becomes complicated very quickly

To illustrate the point, let's start with the idea that something needs to be protected and follow the conversation from there. Once we know that we must put some type of constraints upon our actions, we know that we need to have rules to follow in order to enact those constraints. Let's take the case of protecting personal information. Lawmakers have seen fit to create bills and acts, which become laws that say we need to protect this type of information. However, laws aren't rules. Regulations must be derived from those laws in order to create the rules we need

to follow for protecting the information. Sometimes the rule makers turn to pre-existing documents, called safe harbors, in order to define very prescriptive rules and controls.



The types of Authority Documents that surround a protective idea

Lawmakers aren't the only group working on creating controls for compliance. Self-regulatory bodies (such as manufacturing groups, groups requiring contractual obligations to be members of, etc.) can, and do, jump into the fray, as well as international and national standards bodies. The difference between these groups is that while laws are prescriptively ambiguous, self-regulatory body requirements and standards organizations are very prescriptive.

As you can see in the previous illustration, what this leaves us with is both overlap and gaps between the various types of Authority Documents. Compliance, therefore, can often become a confusing mess.

Compliance can often be confusing when there are too many Authority Documents to follow

The task at hand for all organizations faced with complying with more than one Authority Document is to create a process by which these Authority Documents are identified, harmonized, consumed, and audited. This is a lengthy process if done

manually. And it all *has to be done before you can implement the mandates you've found!*

What you have to do *before* you can comply

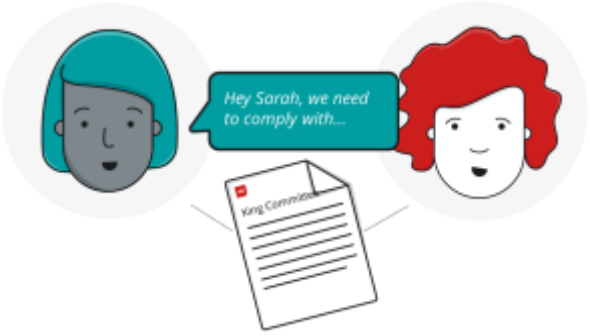
Before you can comply you have to follow a well-worn path for researching your Authority Documents, extracting their information, and making that information usable to your organization. The steps that you are going to follow, as illustrated in the diagram below.

Making Authority Documents usable to your organization

1. Identifying and organizing Authority Documents
2. Mapping mandates in the Authority Documents
3. Harmonizing mandates in Authority Documents
4. Creating a custom glossary

Identifying and organizing Authority Documents

The conversation normally starts like this; "Hey Sarah, we need to comply with…" followed by one or more Authority Document names. Sometimes these documents are familiar to you, sometimes they aren't.



Finding out you have to comply with some heretofore unknown document

There are three things you'll need to do in order to identify and organize Authority Documents:

1. find them,
2. classify them, and
3. organize them into some type of system.

Finding Authority Documents

The first thing people think of these days when finding *anything* on the Internet is to perform a Google search. That works great if you know what you are looking for. It even has search suggestions for you. However, if you are looking for something like the King Committee report, merely entering that information will bring up over 50,000 results.

*Google works **great** if you know what you are looking for*

Let's say you *did* spend the time to narrow down your search and find the PDF of the actual Authority Document you are looking for. Great! You've now spent about half an hour to an hour finding *one* Authority Document you need to address. You have about 20 more to go if you are a mid-sized organization. About two times more than that if you are a publicly traded organization. About twenty times more than that if you are a bank or a university or a healthcare organization.

Classifying Authority Documents

Once you've *found* the Authority Document, you are going to need to classify it so that you understand the level of importance you should ascribe the mandates you find in it. As an example, let's say that some law says "turn off the faucet" and you have to follow that law. And then someone in your organization tells you a best practice guideline says you need to "swing the tennis racket". But you only have enough money to implement *one* of the two mandates. It isn't a question of which one you are going to implement, is it – *once you know one of the Authority Documents carries more legal weight than the other*. It means that you've classified the two Authority Documents.

So what else should you know about each Authority Document before you dig in to them? What follows are a couple of points of interest that everyone agrees on.

The official title and version

We've heard conversations like this: "Okay Joe, I found the King Committee Report". "Great Fred. Which version, there are six." When classifying Authority Documents it is important to know not only the *name* of the document, but its *version* as well.

Any "nicknames"

As with the example we are using here, most Authority Documents have nicknames. Every couple of years the King Committee releases another report and they are then called King II, King III, and so on. People don't search for, or communicate, the official titles of many Authority Documents, instead choosing to use their various nicknames. And because of that, you'll need to track those, too.

Where it was found online

The UCF team was once mapping a document for the government, and as we were going over the edits with them, they kept telling us we had different content. We pointed out we got the document from *their* website that *they* pointed us to. About half an hour into the conversation we jointly discovered that in the *same* website (but in different sections) they had published *two* Authority Documents with the *exact same name*. So it's important to not only know the name and version of an Authority Document, but also *where and when* you found the Authority Document.

What geography it hails from

At one point there were two documents entitled "National CyberSecurity Standard". Knowing one was from the United States and that another was from Australia was a pretty important thing.

Its effective date (if it has one)

When PCI 3.1 was released, everyone was clamoring to immediately dig into it and start implementing it – except those with budget authority. *Those* folks realized that it had an effective date that was 18 months out from its published date, therefore they didn't have to spend a dime on it right now. Knowing *when* an Authority Document effects your bottom line is important.

And its legal precedent

When we say that we are "complying", we are saying that we are complying with authoritative rules that are not of our own creation. These authoritative rules can come in the form of regulations, principles, standards, guidelines, best practices, policies, and procedures. Which is which, and what makes one authoritative body a regulator and another a best practice author? Let's start with regulations and move on from there.

- Statutes, regulations, and directives are rules of law that, if not followed, can result in penalties. Regulations state *that* something must be done. Regulations are promulgated by governmental agencies to interpret or expand the reach of statutes.

- Contractual obligations are just that — contracts that, if not followed, can result in penalties.
- Standards are levels of quality or attainment created by organized groups or that are generally accepted within the industry. Standards determine *what* must be done.
- Guidelines are detailed outlines and plans for determining a course of action. Guidelines *prioritize and direct* the course of action.
- Best practices are programs, initiatives, or activities that are considered leading edge, or exceptional models for others to follow. Best practices *set the example* of *how to do* something the best way.

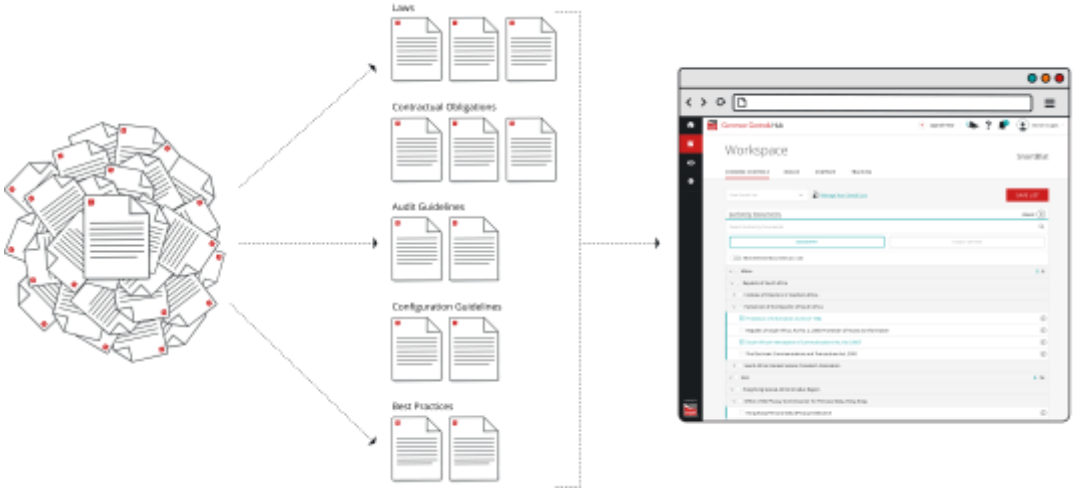
So yes, there is a legal hierarchy to the documents that the UCF tracks. We have identified 10 Authority Document types which are listed in their legal hierarchical status below.

1. Statutes (Bills or Acts) - *Failure to follow laws will get you put in jail or result in penalties.*
2. Regulations - *Failure to follow regulations will result in penalties*
3. Regulatory Directive or Guidance - *Directives are only enforceable against and binding for the group they address.*
4. Contractual Obligation - *Contractual structures promulgated by self-regulatory bodies are enforceable under contract. Failure to comply carries with it the remedies established by the contract, which may include fines and/or loss of valuable contract rights. Such consequences are enforceable under contract law.*
5. International or National Standard - *Standards are not enforceable by law*. *However, failure to follow standards may result in actions contrary to regulations, which **are** enforceable by law*.
6. Audit Guideline - *Failure to pass an audit brings with it "audit items" and other modes of enforcement that are only as strong as the standard, contractual obligation, regulatory guidance, or regulation that calls for the audit.*
7. Safe Harbor - *If a safe harbor is available, it's always good to know. However, the needs of the organization may dictate that it leave the safe harbor and enter riskier waters.*
8. Best Practice Guideline - *Are they enforceable? Nope*.
9. Vendor Documentation - *In and of themselves, vendor documentation is usually treated as a form of a best practice, or minimum standard of due care. Vendor documentation following regulatory guidance is treated with the same accord as a safe harbor.*
10. Organizational Governance Documents - Following properly structured and validated organizational controls that align with mandates that have to be followed is **the** essential prerequisite to compliance, and failure to follow

controls will directly lead to whatever fines or penalties the regulatory body can impose.

Organizing Authority Documents into a classification system

When you walk into a library, have you ever thought about the cataloging system that they had to put into place in order for you to find something? Without a way to bring order out of the chaos, what you'd have is more or less a jumble of books on a table, like the diagram of authority documents shown below on the left. However, once organized, the documents can be examined according to their category and version history.



Organizing classified Authority Documents

This categorization is formally called a taxonomic ontology. While the term might sound fancy, it actually isn't complicated at all. Many of the UCF's lists are in this taxonomic ontology format which we refer to simply as a hierarchical list. And if you are going to classify and organize Authority Documents on your own, you'll need to replicate what we at the UCF have done (or some close approximation of it).

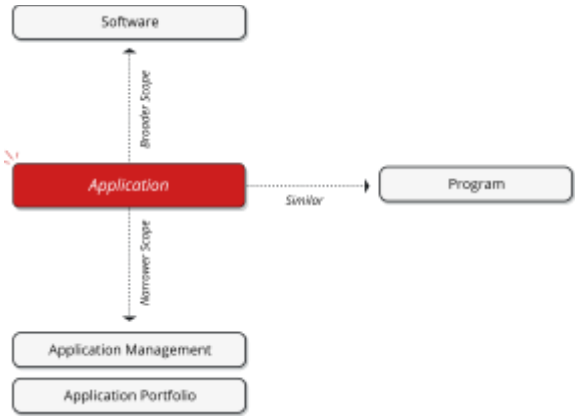
A quick background on taxonomies

In order to make sense of the world, as we process information bits, we have a natural tendency to categorize them. This means that, there must be *something* that underlies our categorization, some type of thinking and decision making process. To some, a category is a "class of objects that we believe belong together" Edward Smith (1990). Categorization. Thinking: An invitation to Cognitive Science. D. Osherson and E. Smith. Cambridge/London, The MIT Press. Vol. 3. This is a good definition because it leaves categorization an open-ended process to be developed as we develop our sense of that which is around us.

Most taxonomies follow one of two thought patterns. They either divide the world according to scope, or they divide the world according to dependency. Let's look at both methodologies, as both methodologies are used by the UCF team.

The taxonomy of scope

While many of the taxonomists use fancy terms like superordinate and hyponym, we aren't expecting anyone within the compliance space to do likewise. Again we are going to use different (simpler) words for the same thing: broader scope, similar, and narrower scope.



An example of a scope based taxonomy

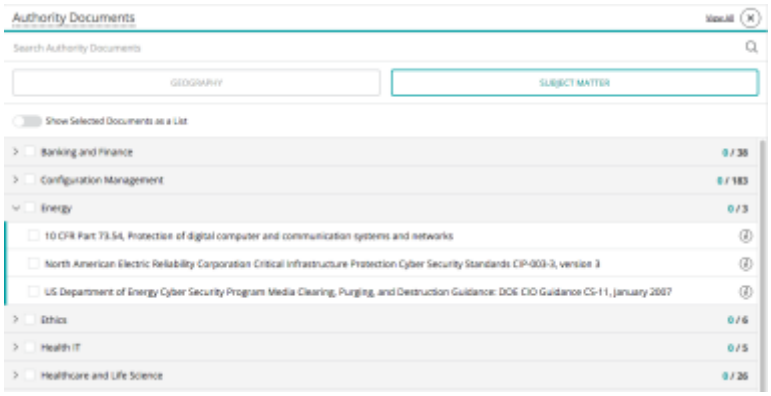
The rules for deciding where an item should be placed (in simple language) are as follows:

- A term is broader in scope when it has more attributes or features than another term it is being compared to. If you think in terms of software and application, software could be an operating system, utility program, major application, minor application, etc. because software is anything other than hardware or firmware or files. The scope could then be narrowed down to application, then application management, and even further to application portfolio.

- A term has similar terms (application and program are similar terms) when the terms can be used in place of each other. And in this example, we often hear people intermingling "program" and "application" in this context. Both terms are on the same basic level as each other.

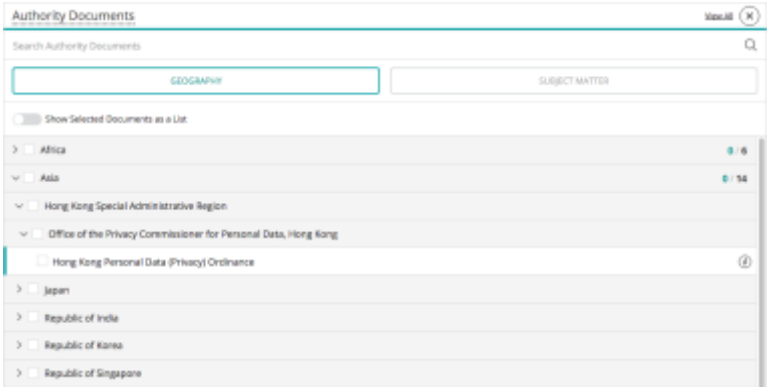
- To make things even simpler, a term that is more generic than the base term should be thought of as being of broader scope than the base term. A term that is more specific than the base term should be thought of as being narrower in scope than the base term.

In practical terms, you could easily create two scope-based taxonomies for tracking your Authority Documents; by subject matter and by geography. The subject matter scope would most likely present a single level list like the one shown below.



Authority Documents by subject matter scope

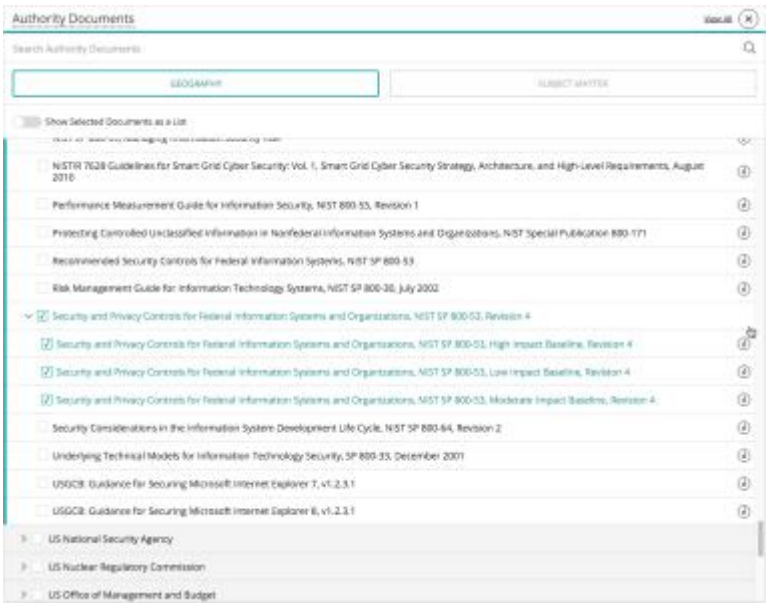
A geographically bound scope would produce a multi-tier list of Authority Documents with parentage being tracked through the geographic region, then legal regions within that, and then originating sources within that.



Authority Documents by geographic scope

The taxonomy of dependency

The taxonomy of scope moves from broader to narrower terms. The taxonomy of dependency creates an order out of items that cannot stand alone. Dependencies of taxonomy are used for creating a hierarchical order of tasks or controls that are contingent upon other tasks in the list. It is also used in library science to track guidelines that depend upon a core set of materials. Such is the case with the US' NIST 800-53. Not only is there a main document, but there are also versions of the document for low, moderate, and high impact baselines. Because the low, moderate, and high versions of the document are *dependent* upon the main document, they are placed in the list as subordinates to their parent document as shown below:



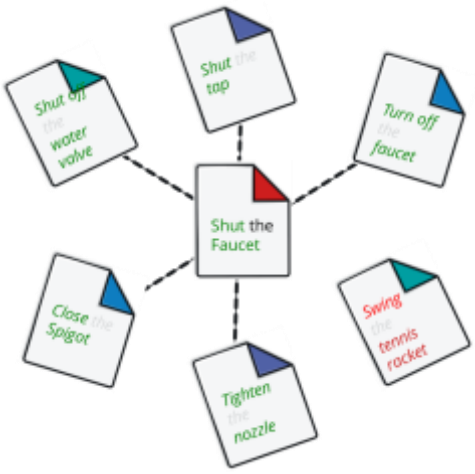
NIST 800-53 and its three children

Mapping and Harmonizing the mandates in Authority Documents

Once you have the Authority Documents organized, it's time to read them, interpret their Citations by digging out the mandates within them, and then harmonizing those mandates to Common Controls.

Most Authority Documents have both **mandates** and **explanatory text**. They will say "Go do this" (which is the mandate) and then sometimes explain what "*this*" is, or give references, or add additional information about how they want "*this*" done. The process you'll need to follow ignores everything but the mandates found within a Citation.

As you might expect, with all of the Authority Documents out there, there are a lot of those mandates that overlap each other. When one mandate says "close the tap" and another says "shut the spigot" and a third says "turn off the faucet", you can reasonably assume that those mandates, while in different documents and stated differently, can be treated as **Common Controls** between the documents. So a Common Control, in its essence, is a shared compliance requirement written in plain English that is the same across multiple Authority Documents. Well, how do we know when they are connected? A mandate can only be connected to a Common Control if the verbs are related and the nouns are related. The diagram that follows shows how five of the six mandates relate to the same Common Control because they all have verbs and nouns that are similar to each other. Just as important, the diagram shows that the mandate of "swing the tennis racket" does *not* match the same Common Control because its verb and noun *do not match*, nor is there any similarity between them.



Common Controls showing relationships between mandates

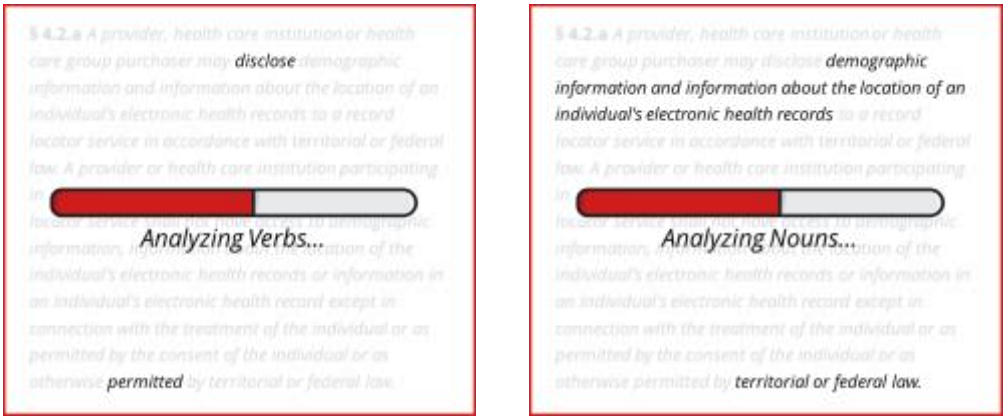
Extracting Citations and mapping Mandates to Common Controls

You will need to look at each and every section and each and every paragraph of the Authority Documents you must follow. And make sense of what they are writing. And many times, that isn't easy. Believe it or not (for those of you who haven't tried the daunting task of interpreting laws and regulations), the following diagram is a real citation from a real Authority Document.

§ 4.2.a *A provider, health care institution or health care group purchaser may disclose demographic information and information about the location of an individual's electronic health records to a record locator service in accordance with territorial or federal law. A provider or health care institution participating in a health information exchange using a record locator service shall not have access to demographic information, information about the location of the individual's electronic health records or information in an individual's electronic health record except in connection with the treatment of the individual or as permitted by the consent of the individual or as otherwise permitted by territorial or federal law.*

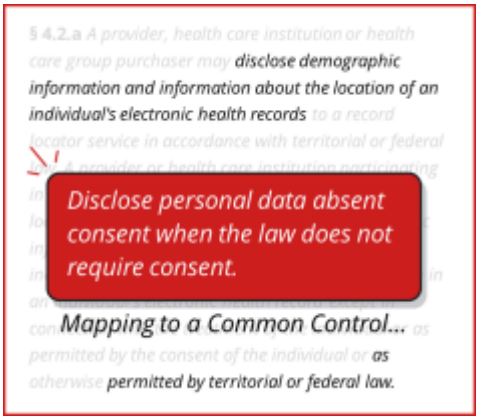
Somewhat typical Citation

After running the UCF for over a decade, it is our professional opinion that the purpose of this type of legalese wonk-speak is to inflate weak ideas, obscure poor reasoning, and inhibit clarity, making mandates an intimidating and impenetrable fog. However hard it may seem, your job is to read this poorly written material and extract both the primary and secondary verbs and the primary and secondary nouns. Believe it or not, that whole long passage in the diagram above has only two verbs you are going to care about, *disclose* and *permit*. Likewise, it has only two nouns you are going to care about, *demographic information and information about the location of an individual's electronic health records* and *territorial or federal law*.



Extracting the verbs (left) and nouns (right) from a Citation

Once extracted, the next step is to map the Citation's mandates to Common Controls that are well formed and easily understood, such as the one in the diagram below. Notice that the very long term *demographic information and information about the location of an individual's electronic health records* is really just another way of saying *personal data*.



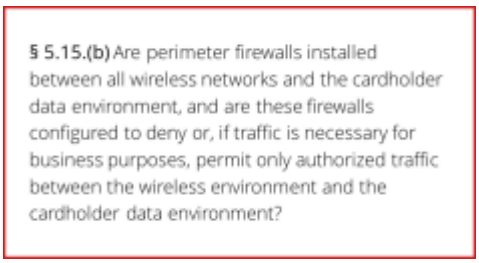
Mapping a mandate to a Common Control

Dealing with multiple mandates in a Citation

There are some Citations that are written with multiple mandates in them. The problem with multiple mandate Citations is that you can't really answer yes or no to the question of "did you perform this?" if you only performed one or the other. And, it's *impossible* to align a multiple mandate Citation to Common Controls because most documents' Citations have a single Control, so the alignment process is blocked if you try to align single mandate Citations with multiple mandate Citations.

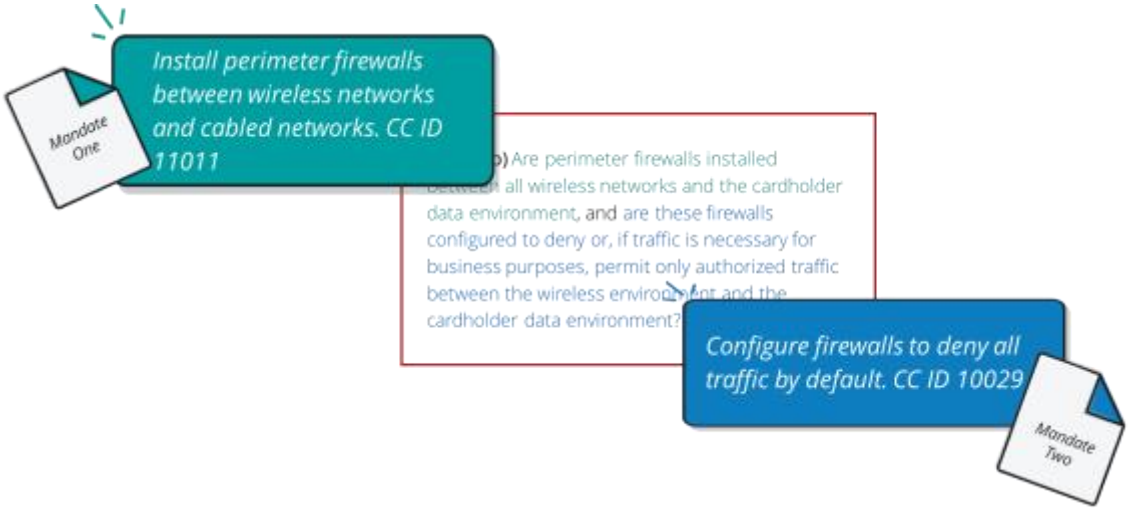
The following mandate is taken directly from the Payment Card Industry (PCI) Data Security Standard. You can easily tell when most Citations have multiple standards because they will say "close the door *and* milk the chickens" – they are tied together with a conjunction such as "and". Any time you see the most common

conjunctions (and, nor, but, or) you can usually bet that there will be multiple mandates in the Citation.



Citation with two mandates

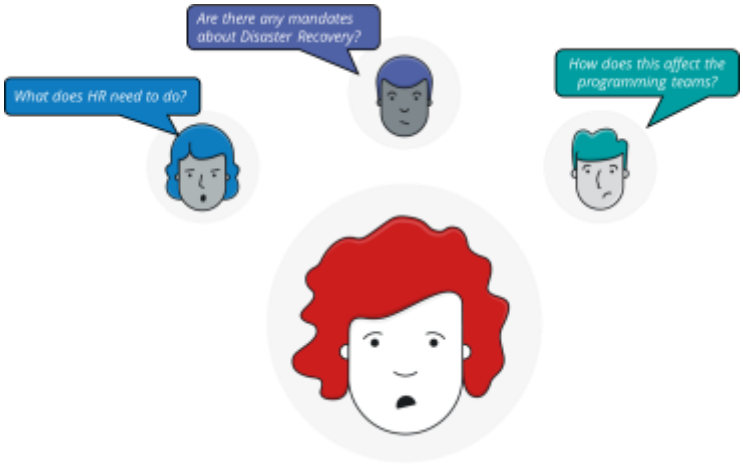
What you must do in these situations in break the Citations down into their individual mandates. With the result being that everything before an "and", if it has a pairing of a primary verb and a primary noun becomes the first mandate in the Citation. And then everything after the "and" in the Citation gets evaluated as well so that a pairing of a primary verb and a primary noun forms the second mandate. And then each mandate can be mapped individually to a Common Control as shown in the diagram below.



Mapping multiple mandates in a Citation to multiple Common Controls

Categorizing the Mandates in an Authority Document

Let's say that you've now examined an Authority Document, such as the US' CyberSecurity Standard with slightly over 100 mandates. Are you going to present *all* of the mandates to *all* of your team members? The first person you talk to is Erin in HR. She isn't going to care about anything other than the HR concerns. Then there's Tom the Disaster Recovery guy. He couldn't care less about any HR mandates. Then there's Sanjay in development who is going to be a bit apoplectic if he has to read and learn about anything outside of his technology domain.

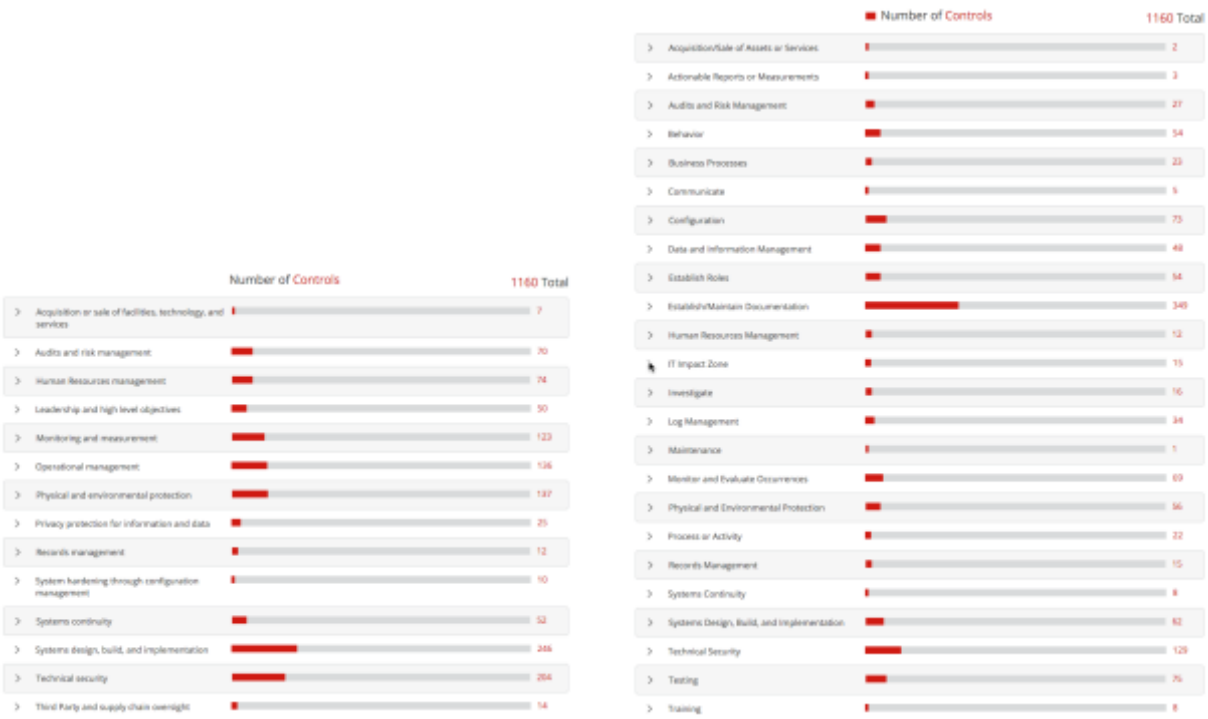


You shouldn't communicate everything to everyone

The only logical thing to do is break down the mandates into sections discernable by normal individuals. There are a couple of ways to do this. The first way is to break down mandates into large impact zones to those who must comply. An Impact Zone is a hierarchical way of organizing a suite of mandates, a taxonomy of dependency. Each Impact Zone deals with a separate area of policies, standards, and procedures: technology acquisition, physical security, continuity, records management, etc. You build this taxonomy by looking at the corpus of standards and regulations through the lens of unification and a view toward *how the mandates impact the organization overall*.

Or you could break down the mandates by Type. In this approach, each mandate is assigned a meta-data *type* to help you determine the **objective** of the mandate. These *types* include behavioral controls, process controls, records management, technical security, configuration management, etc. They are provided as another tool to dissect the Authority Document's mandates and assign them effectively within your organization.

The diagrams below show the breakdowns by Impact Zone on the left and by Type on the right. Notice how many more categories there are when you break them down by type.



US CyberSecurity Standard broken down by over-arching Impact Zones (left) and by type (right)

And for extra credit, you'll create a glossary

Authority Documents (laws, regulations, international standards, contractual obligations) are written and "bespoke terms" are created by their authors "as to make a point and discern our document's focus from others" said a regulatory drafter who'd rather not be named with the US's Office of the Comptroller of the Currency (OCC). She said this in a speech in which she introduced new audit guidelines for the banking community and was very proud of the fact that she created several brand new terms in her document. There are several problems with what she did. First, she didn't provide a definition in the document's glossary. In fact, the document didn't even contain a glossary. Second, she automatically assumed that people would understand her differentiation. In fact, they did not. Finally, she also assumed that auditors would be able to audit organizations according to her newly published guidelines. In fact, because she didn't define her terms, she can't expect anyone to audit against her document because of the lack of understanding it causes. And she's not the only one.

Over 75% of the Authority Documents mapped in the last decade by the Unified Compliance Framework team contain terms unique unto that document, that are not defined in the document, nor were they defined anywhere else at the time of the document's authoring. It seems that Authority Document authors are so caught up in wanting to make their specific point and wanting to create terms of art that they often forget they are writing documents to be shared by a world-wide

community. These Documents call organizations to action while at the same time also create maximum opportunities for misinterpretation.

Then there are those Authority Document authors, like the authors of the Shared Assessments auditing documents, that use more non-standard terms than standard ones. While we could cite over 100 non-standard uses of terms in just one of their audit guides, here are just a couple. Instead of the accepted use of calling an organization's staff and contractors "personnel" they routinely called them "constituents". Instead of using the widely accepted "Personally Identifiable Information", they used "private information", "personal information", and even "private personal information" in the same document.

Finally there's a UCF team favorite. While giving a speech to banking regulators in Washington DC, the UCF team challenged 23 regulatory drafters working on new banking CyberSecurity audit guidelines to a) spell CyberSecurity and b) write down their definition of CyberSecurity. I got all three spellings back (cyber security, CyberSecurity, cyber-security). Three guesses (and the first two don't count) on how wildly different definitions there were. Twenty four (one guy wasn't quite sure and gave us two very different definitions).

The problem you are going to face

The biggest problem you are going to face, other than poor writing as mentioned above, is that 90% of the terms being used in the various Authority Documents *aren't defined in the document*. They aren't in the document's glossary, or even published in a separate glossary. So you are going to have to hunt for the definitions online yourself. If you can't find those terms from a credible online source, you may also need to contact the author(s) to obtain an acceptable definition.

For example, here are three terms that many Authority Documents use, and yet almost none of them contain definitions for these terms in their glossary. In order for you to be able to communicate coherently about their mandates, you are going to need to maintain such a glossary.

authentication	The verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
authentication credential	Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process,
authentication data	Information used to verify the identity of a user.
authentication mechanism	Hardware or software-based mechanisms that forces users, devices, or processes to prove their identity before accessing data on an information system.

But *you* don't have to worry about doing *any of this on your own!*

Well, that's partially true. You don't have to worry about doing any of this on your own *if* you subscribe to the Unified Compliance Framework as an end user. That's because we do this all *for you*.

Not only do we do all of this for you; the researching of the Authority Documents, the mapping of Citations and Mandates, the categorizing of them, even creating glossaries for Authority Documents that don't have them – we also organize them into a library that can be accessed through the Common Controls Hub!

What we *can't do on our own* is all of the above *for every Authority Document you want in the library*. That requires a **massive** amount of effort. Our answer to this problem is that we've opened up the UCF's multi-patented, multi-award winning tools and processes so that any licensee of the UCF's Common Controls Library can map along with us.

Don't worry if you think all of the above is very complex. On its own, *it is*. But when using the UCF Mapper tool and our scientific processes, we've taken most of complexity out of the equation.

The scientific method of mapping Citation Mandates to Common Controls

What we presented above is a slightly simpler variant of what we do during the Unified Compliance Framework's Authority Document mapping process (we'll get to our flow a bit later). The big difference in what *we do* and *what everyone else does* is that we apply a scientific approach to the process.

Everybody talks about the "art" of mapping Citations

Compliance is ensuring that the requirements of laws, regulations, industry codes, and organizational doctrines are met. The task at hand for all organizations faced with complying with more than one Authority Document is to create a process by which these Authority Documents are identified, harmonized, consumed, and audited. Those are very distinct tasks that all require the organization to formalize an approach, a methodology to tackle the problem.

We often hear of individual contributors within an organization stating that their personal method of identifying and harmonizing an Authority Document is a preferred method for identifying, harmonizing, consuming, and auditing the implementation of mandates found within Authority Documents. "I've got this great method I use" is probably the scariest thing we hear on a regular basis. Why? Because normally the person employing that method is doing it as art and not science. They bring a nuanced, personal approach to each task – an approach usually not repeatable for any reason from it not being shared through not being documented and even just not being repeatable by anyone other than the originating individual.

Compliance shouldn't be an art – ever.

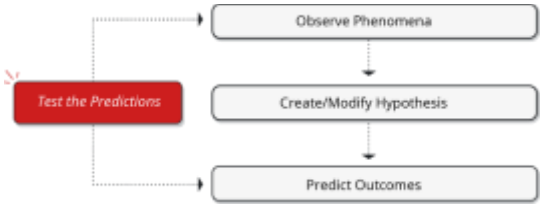
Compliance must be a repeatable and verifiable process. Undertaking the tasks of identifying, harmonizing, consuming, and auditing the implementation of mandates found within Authority Documents is something that every organization must do repeatedly and often. Therefore, the organization has to have a scientific method – a repeatable, demonstrable method – for tackling these problems. The UCF team applies a slight modification of the scientific method to everything that we do when we identify, harmonize, and create audit questions for the mandates in Authority Documents.

What is the scientific method?

In short, the scientific method is comprised of four stages, which are then slightly modified and repeated.

1. Observe some aspect of the universe, some phenomena happening.
2. Create a hypothesis to explain what you are seeing.

3. Use this hypothesis to predict the existing of other, related phenomena, or to predict the outcomes of additional observations.
4. Create tests to check the predictions and see if the hypothesis holds.



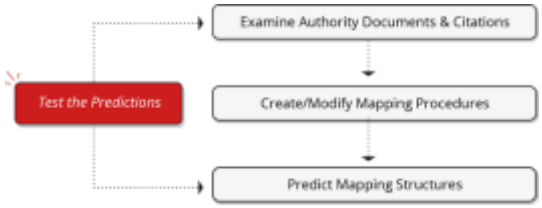
The scientific method

During the observation phase, if the hypothesis holds through multiple experiments, it is a good hypothesis. If it does not, it either needs to be modified or completely scuttled and the process begun anew.

The UCF's initial application of the scientific method

The UCF wasn't built in a day. Originally Dorian Cougias and Marcelo Halpern put their heads together and examined a slew of Authority Documents, putting together the mapping procedure hypothesis that if they could

- break down the documents into distinct mandates, and
- examine the linguistic structures of the mandates, then
- they could determine if overlaps exist between mandates in multiple Authority Documents.



The scientific method applied by the UCF

And that's exactly what happened. The team's hypothesis that each mandate's primary verb and primary noun could be examined using standard linguistic rules to determine if a mandate in Document A was the same, or different than a mandate in Document B — **when examined through the lens of a simplified Common Control**. The scientific mapping hypothesis laid out back in the very first months of the formation of the UCF still holds today:

> A match between an Authority Document Citation and a Common Control is created if;
>
> - the primary verb and primary noun are identical matches to the Common Control;

- either or both the primary verb and primary noun are synonyms of the Common Control;
- the "do not" version of the primary verb is an antonym of the Common Control and the primary noun matches that of the Common Control;
- the primary noun in the Citation is a linguistic child of the primary noun in the Common Control and the primary verb matches that of the Common Control.

An example of this hypothesis follows. There are two real examples for both Document A and Document B, both being mapped to a Common Control. The primary verb and noun are italicized for each document:

Document A	**Common Control**	**Document B**
The organization should *analyze* the *business activities* as part of the records management process.	Analyze organizational objectives, functions, and activities.	The organization should not consider individual business unit objectives alone, but should *analyze* the *objectives* and *activities* in terms of the entire organization.
The system must *monitor* and *control* all *communications* at *key internal boundaries* and at all *external boundaries*.	Identify and control all network access and control points.	The organization must *manage* and *control* all *Internet access points.*

In the first example, both Authority Documents used the exact same verb (analyze). Document B used the same primary nouns, while Document A used a subset of the term activities (business activities).

In the second example, again, both Authority Documents used the exact same verb (control). Document A used the terms "internal boundaries" and "external boundaries" while Document B used the term "Internet access points". We know from the UCF's dictionary that we maintain that "internal boundaries", "external boundaries", and "Internet access points" are all a type of "network access and control point".

Therefore, the hypothesis (with this as the example) holds: If two Citations point to the same Common Control, those Citations overlap each other. So far we have tested this hypothesis over 100,000 times and it has held true each time.

The scientific method is pervasive within the UCF

Everything the UCF team does in regards to developing the structures, developing the mapping methods, and the **doing** of the mapping follows the scientific method. We create, modify, and destroy structures and methods based upon examination and mapping of Authority Documents and their Citations.

Our initial theory that if we tracked an Authority Document by originator, name, and version (like a book) we could tell its uniqueness was killed when **one** Authority Document had the same originator, name, and version **but completely different contents**. Therefore, we had to change our hypothesis and begin tracking by the URI where the document was downloaded from, and the date it was downloaded, as well.

Our initial theory that Data Contents could be tracked as a simple list of data items was found to be incorrect as soon as the PCI document came out alternately lumping all cardholder data into Citations and then only calling out single Data Content types in other Citations. Therefore, we had to make the list a hierarchical list. And we had to change it again when the **same** Data Content types were being added to different categories of data. So now the list is a multi-hierarchy list instead of a simple non-hierarchical list.

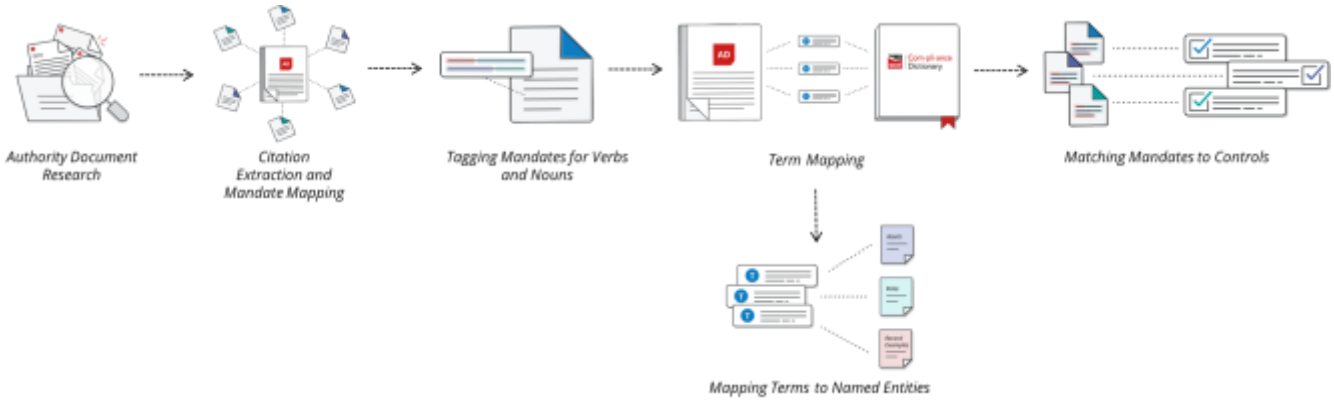
Our initial theory that the UCF could maintain a simple glossary of terms has been shattered. The UCF team had to completely reconstruct multiple structural hypotheses and have since converted the initial glossary to a full blown sense-based dictionary replete with alternate spellings and capitalization and multiple multi-hierarchy lists.

The point is this — nothing exists in the UCF's structures, mapping methodologies, or mapping practices that wasn't born from this method. Everything begins with examining the Authority Documents and their Citations and then turns into a hypothesis (at best) or multiple hypotheses (more usual) about what to **do** with what we are finding. And then we test. And we re-test. And we change our hypotheses until **one** hypothesis holds true. And then we continue to test and wait for the day when it no longer holds true and we once again have to change mapping methods, structures, practices, or all of the above.

And all the while, we map what we are doing into a control framework.

How we apply the scientific method to mapping Authority Documents

As stated earlier, the UCF team approaches mapping Authority Documents slightly different than everyone else. Instead of the more simplistic four step method for researching, mapping, harmonizing and then creating a glossary, the UCF team employs a cognitive learning, multi-patented approach with a few more steps. These steps give us the clearest picture of what is going on in Authority Documents, how they are structured, and what they really *mean* in the midst of what they are *saying*.



The UCF's approach to mapping an Authority Document

1. Authority Document Research
2. Citation Extraction and Mandate Mapping
3. Tagging Mandates for Verbs and Nouns
4. Term Mapping

4a. Mapping Terms to Named Entities

5. Matching Mandates to Controls

We aren't going to go into each of the steps listed above *here*. Each of these steps is broken down into its own document and training methodology. What we want you to know here is that we've got this figured it out. It's science. It's repeatable. And we will partner with you so that *you too* can do what we do.

How we partner with you to help you map

First, we've linked our UCF Mapper tool to the Common Controls Hub so that all of clients have access to the same tools we do. Second, we partner with the (ISC)2® organization so that they can provide the training and certification for organizations and people like yourself interested in performing mapping operations. Third, we've given you multiple options for making the documents you map available online.

Why would someone want to be a mapper?

There are several motivations behind becoming a mapper; monetary gain for the organization, monetary gain as an individual contributor, fulfilling a need for the organization, personal reasons.

Monetary gain for the organization

We are already working with multiple organizations that map content for their clients. We cover earning expectations below, so won't cover that here. They are providing mapping services to their clients. Therefore, the reasons are business-related and profit-related.

Monetary gain for the individual

Enough said.

Fulfilling a need for the organization

In the last year (we started officially tracking about a year ago) we have had over 150 organizations ask for the ability to map Authority Documents *only they care about*, as well as *internal documents*. This is a **huge** market.

Personal reasons

There are those folks (and I'm slightly making fun of them here) that like having an alphabet soup of certification letters behind their name. I have personally been asked at least twice a month if we are going to have a mapping certification program.

What other benefits can a mapper expect to get (organizational or individual)?

Certification

That's what the (ISC)2® team does very, very well. And that's why we partner with them.

The UCF team advertises mappers on our site and all other sites.

The UCF team advertises mappers to our GRC and other partners.

The UCF team advertises mappers to our VARs and Resellers.

The UCF team advertises mappers to the US and foreign governments we work with.

If you can think of any other ways of helping mappers, we are on board.

What can a mapper expect to earn and how much do mappers get paid?

The mapping process, and in more specific about how a Mapping Team is paid, is another document specific to that content. In general; they can be paid directly from a client if they are providing a service, they can be paid through the UCF's system if they are mapping the document for pay, and they can be paid by both if they negotiate a mapping service to allow them to also post the document as a for-pay document. How much can they expect to earn? We'll answer that for both as service and for-pay documents.

Working along with the UCF team as an individual contributor

When working with the UCF team as an individual contributor (i.e., a Mapper, Reviewer, or Approver), the contributor is paid *per task completed*. This rate is based upon the average number of tasks completed per day and is an ongoing, fluctuating calculation that is too complicated to delve into here.

For-Pay document earnings

For-Pay documents earn the Mapping Team 80% of the price of the document, with 20% going to the UCF for overhead costs.

The UCF Mapper application tracks all tasks that go into mapping the document, and using the same type of equations that book publishers use to determine book prices (think the longer and more complicated the book, the higher the price), the UCF Mapper application *suggests* the price the Mapping Team should set for the Authority Document. That price is always editable by the Mapping Team.

Much like other publishers, the UCF tracks all sales and then sends the Mapping Team a check at the end of the month. The UCF's system will have an online area for the Mapping Team to track sales live.

Each time the document is licensed to an organization, the Mapping Team is given credit. As long as the document is available and organizations are licensing the document, the Mapping Team receives payments at the end of the month for that month's sales.

Mapping as a Service

This is a *negotiated price between the Mapping Team and the Requesting Organization.* Much like the way the UCF Mapper application suggests a per-account access price for the for-pay Authority Documents, the UCF Mapper can also estimate the cost to map an Authority Document.