Authority Document types the UCF tracks

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)
2. Regulations
3. Regulatory Directive or Guidance
4. Contractual Obligation
5. International or National Standard
6. Self-regulatory Body Requirements
7. Audit Guideline
8. Safe Harbor
9. Best Practice Guideline
10. Vendor Documentation
11. Organizational Governance Documents

Statutes (aka Bills or Acts)

A statute is an act of federal, state, Parliament, or provincial legislation that declares the law pertaining to a certain subject (e.g., the Income Tax Act, The Canada Corporations Act, the Sarbanes-Oxley Act of 2002). Statutory law is legislatively created law. Administrative agencies adopt statutes as regulations, and lesser bodies adopt them as ordinances.

Failure to follow laws will get you put in jail or result in penalties.

Regulations

To regulate is to bring under *the force of law* or a *governing authority*. People and businesses are subject to national, regional, and local laws. Traditional regulators are those agencies within the aforementioned levels of government. When governmental agencies create their acts, they are codifying legal documents that resulted from deliberations of their legislative bodies. Often, however, the acts passed by those legislative bodies establish broad principles rather than detailed prescriptions for the behavior of people and companies and delegate to the regulators responsibility for filling in the details and gaps. The regulators are empowered to interpret how the laws are to be implemented and to establish rules for following those laws. Those rules are then documented as **regulations**, such as the "Code of Federal Regulations" that we have in the United States. *Regulations are enforceable by law*.

Failure to follow regulations will result in penalties.

Regulatory Directives or Regulatory Guidance

Directives can be legislative acts, such as those of the European Union, or organizational directives, such as those issued by the U.S. White House's Office of Management and Budget (OMB), which requires those organizations under the issuer's purview to achieve a particular result without dictating the means of achieving the result. Directives normally leave those entities that follow them with a certain amount of leeway as to the exact rules to be adopted. Some regulators like FDa are empowered to make regulations that impose criminal penalties for non-compliance.

Directives are only enforceable against and binding for the group they address.

Contractual Obligations

There is much confusion between "regulations" promulgated by government regulators as discussed above and the rules, standards, and, yes, "regulations" promulgated by other so-called regulatory bodies and other organizations that can and do emerge to reign in our actions. Variously known as "self-regulatory bodies", "standards bodies", or by similar names, these organizations are not part of the government and do not have the force of law behind their requirements, but failure to comply with those requirements may well disqualify an entity from participating in certain businesses. The promulgators of these rules may be industry-based organizations that band together to address a concern that is common to industry members. For example, the credit card companies (Visa, MasterCard, American Express, etc.) have banded together to create the Payment Card Industry Security Standard. The promulgators may be self-appointed watchdog organizations that have gained sufficient acceptance, prominence, and/or moral authority over time and to which people turn to as authorities in the field. For example, the ability to display the BBBOnline and TRUSTe seals in online commerce has achieved this type of prominence, so it makes it worthwhile for businesses to comply with their standards. Certain membership-based organizations promote similar types of rules as a condition of membership. The unifying principle is that they all have something you want and you're willing to contractually commit to playing by their rules to get it.

We'll get to the definition of a standard in a moment, but just because something is called a **standard** (it can't be called a law, act, or regulation, because it does not come from the government), it doesn't mean that it can be ignored without consequences. Yes, compliance with these types of contractual standards are, legally speaking, optional. If a company is not interested in accepting credit cards as a form of payment, it is not obligated to comply with the PCI standards. However, anyone

wanting to accept credit cards is required to contractually agree to comply with the PCI standards. Similarly, anyone wanting to display the BBBOnline seal must contractually agree to follow certain guidelines and processes. Failure to comply with these obligations creates a breach of contract and, depending on the contract terms, may result in a variety of fines and, potentially, the loss of valuable contractual rights — losing the ability to accept credit cards in the case of the PCI standards could have grave consequences for just about any merchant. Losing the right to use the BBBOnline or TRUSTe seals may not have as severe an effect on a merchant as being unable to accept credit cards, but it could drive customers away to competitor sites — particularly if the contractual breach is widely publicized. The payment card industry has already fined a great many organizations and affected the closure of at least one organization that we know of for not properly following its standard. Because the payment card industry can exercise authority over its user body, and that user body is so large, in this instance, they can be compared to regulators, even though they haven't been given the statutory mandate of a regulator. However, there is one (1) big difference between the payment card industry and true regulators — while the payment card industry may be able to put you out of business, they can't put you in jail.

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.

International and national standards

We love the origination of the term "standard". Originally, a standard was a conspicuous object (a tall pole with a banner, flag, or symbol on top) that was used to mark a rallying point in battle. Today, a standard is a criterion or criteria established by an authority (government or industry) that apply to a given situation in order to reach a certain level of quality or attainment. Control models are much the same thing but tend to focus more specifically on certain aspects of implementation. In contrast to the original definition, a standard today comes into existence *because* people rally around it, rather than the other way around. International standards and control models are consensus models that are generally accepted by the user community (or at least by the community creating the standard), such as the "Control Objectives for Information Technology" created by Information Systems Audit and Control Association (a control model) or the International Organization for Standardization's (ISO) various standards, such as its "ISO 27001-2005 Information Security Management Standard".

Formal international standards begin as draft documents, which are then published as a Request for Comments (RFC) document. As these RFCs mature through the editing process, they become proposed standards, draft standards, and, ultimately, the final published standard.

Is your organization *required* to follow any given standard? Not if the standard's author isn't a regulator or a body with contractual authority over it — meaning that the standard's authors can't *force* your organization to use their standard under threat of legal action or penalty. Some might think de facto standards must be followed, but that isn't true.

Standards are not enforceable by law. *However, failure to follow standards may result in actions contrary to regulations, which* ***are*** *enforceable by law*.

Self-regulatory Body Requirements

A set of compulsory conditions set forth by an organization that exercises some degree of regulatory authority over an industry or profession. These organizations are not part of the government and do not have the force of law behind their requirements, but failure to comply with those requirements may disqualify an entity from participating in certain businesses.

Audit Guidelines

In the world of regulatory compliance for information services, the CobiT audit standard comes pretty close to being *the* de facto standard. We've seen presentations in which the speaker mistakenly told the audience that this or that regulation *called for* the use of CobiT as the measuring stick against which they must judge whether they were following the regulation. That just isn't so. There isn't a single regulation that mandates the use of CobiT. However, the Sarbanes-Oxley Act did create the Public Company Accounting Oversight Board, which created and mandates the use of its own auditing standards. The Payment Card Industry Association also mandates the use of its PCI-DSS standard as the audit standard that must be followed when proving that you've met their guidelines.

Other Audit Guidelines, like those published by the Payment Card Industry Data Security Standards Council derive their authority from the Contractual Obligations that call for the organization to follow not only the guidelines set forth by the council, but their audit guides as well.

Finally, there are other audit guidelines that are inherent and are also safe harbors (more on that below), such as the Secure Technical Implementation Guides that define configuration standards for systems *and* can be used as Audit Guidelines.

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.

Safe Harbors

Nothing muddies the waters more than a good "safe harbor". While a safe harbor is intended to make laws and regulations easier to follow, oftentimes the safe harbor is used by consultants, speakers, and other well-meaning (or not so well-meaning) folks to support their position that a particular standard, guideline, procedure, or control is required under the law and that failure to adopt that particular standard, guideline, procedure, or control will subject the organization to legal action. Nothing could be further from the truth.

Now, what's its real purpose? A safe harbor in a law or regulation is a shortcut used by the regulators to ensure that the majority of people are in compliance with the law without requiring an in-depth analysis of each particular case. Thus, the safe harbor provides that *if* you take the steps required to be within the safe harbor, *then* you will (more or less) automatically be in compliance with that particular aspect of the law or regulation. However, the converse is not true – if you do *not* fall within the safe harbor, that does not necessarily mean that you are not in compliance with the law. What it does mean is that you will have to show that the steps you chose to take are also in compliance with the law.

Let's use our previously mentioned CobiT standard as an illustration. Suppose that some regulator enacted a regulation requiring that certain types of organizations conduct annual audits of their information services systems that adhere to auditing standards that are reasonable and customary in the industry. Suppose further that our helpful regulators add a statement along the lines of "The CobiT

audit standards are reasonable and customary standards in the industry." This safe harbor offers organizations the opportunity to reduce compliance risk by adopting the CobiT audit standards. However, there are many reasons why the CobiT standards are inappropriate for the particular organization — cost, complexity, etc., so its use may simply not be warranted. Is the organization bound to use CobiT anyway? (If you've read this far, you probably already know the answer.) The answer, of course, is no — the organization is free to use whatever auditing standard it chooses, provided that it meets the two-prong test of "reasonable" and "customary in the industry". However, if the organization chooses to use a standard other than CobiT, and the regulator doesn't like it, the organization will have an uphill battle to convince the regulator (and, perhaps ultimately, the court) that the chosen standard is reasonable and customary. Safe harbors tend to be very conservative and avoid gray areas.

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.

Best practice guidelines

Best practices are leading edge models of methods or actions for others to follow. These are combinations of activities, processes, policies, or procedures that document the *best possible* way of doing something.

Are they enforceable? Nope. As a matter of fact, many times they aren't even *desirable* — in their fullest sense, the "best" way to do something is often also the costliest. Too many times we've seen people spending $1,000 to fix a $100 problem by using an industry "best practice". Best practices must always be viewed in context and adapted to the particular situation.

Vendor Documentation

More and more, vendors are being called on to "bake in" security measures when building out their systems. For example, it is the foundation of the US' FDA's Postmarket Management of Cybersecurity in Medical Devices regulatory guidance. Because of that, vendors following the FDA's guidance and posting vendor documentation on how to secure their systems can elevate the standing of their security documentation to one level higher as a safe harbor. Vendors have a great deal to say about configuration guidance in the form of Secure Technical Implementation Guides, and the UCF team tracks these for you at STIGViewer.com.

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.

Organizational Governance Documents

A document that contains policies, standards, procedures, and practices designed to provide reasonable assurance that certain business objectives will be achieved and undesired events will be prevented or detected. These documents provide a description of what physical-, software-, procedural-, or people-related conditions must be met or be in existence in order to satisfy a core requirement. Following properly structured and validated organizational controls is the essential prerequisite to compliance, and failure to follow controls will directly lead to whatever fines or penalties the regulatory body can impose

Visit our website so see the documents we've mapped according to their types

www.CommonControlsHub.com

Contact sales@unifiedcompliance.com for more information about signing up for a CommonControlsHub Basic Subscription.