



A UNIFIED COMPLIANCE PUBLICATION



DORIAN J. COUGIAS MARCELO HALPERN ERWIN RYDELL ERIK GRANLUND

Using the UCF Spreadsheets

Using the UCF
Within Your
Compliance
Framework
Processes

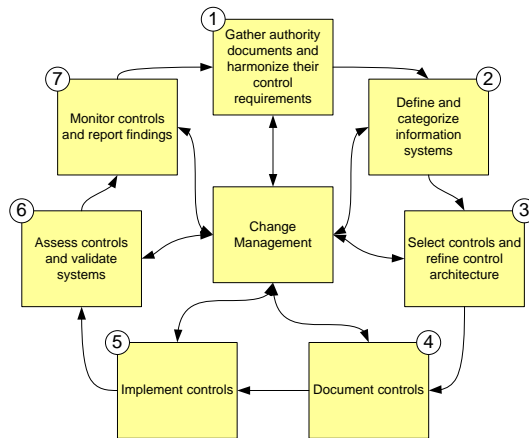
LATHAM & WATKINS LLP

Contents

Using the UCF Spreadsheets	1
Contents.....	3
The Compliance Lifecycle & the UCF Spreadsheets.....	4
The UCF Spreadsheet Release.....	7
Corporate vs. Single User Editions	8
The Controls Spreadsheets	9
What's What in the Controls Spreadsheets.....	10
Using the Controls Spreadsheets	11
Using the Controls Spreadsheets to Aid in Compliance.....	13
The Authority Documents Spreadsheet.....	15
Contacting the UCF Team	17

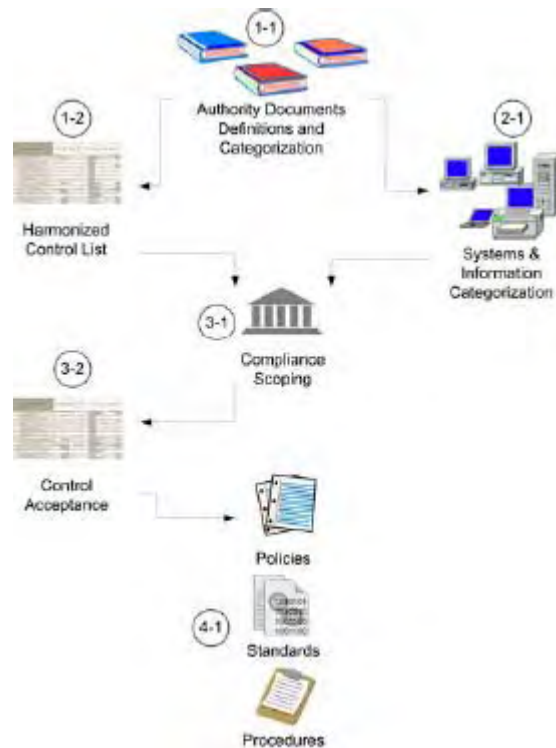
THE COMPLIANCE LIFECYCLE & THE UCF SPREADSHEETS

The compliance lifecycle has seven cyclical phases that interconnect with the change management process every phase of the way. The UCF spreadsheets are directly involved in phases one through three and again at phase six.



The seven phase compliance lifecycle

Within the seven phases of the compliance lifecycle, there several *key* documentation steps within the first four compliance phases, as shown in the following diagram. **The point is that you cannot accomplish the latter steps unless you accomplish the previous steps *first*.**



The key documentation steps within the first four phases of compliance

1-1 The first key step in documenting your compliance efforts is to define **what** authority documents *are* and **which** authority documents affect *your* organization. You'll then need to gather them and categorize them in order for them to be useful to your compliance effort.

The UCF spreadsheets already have a great number of authority documents listed in various categories that you can add to.

1-2 The second step is to then harmonize each of the controls listed in the various authority documents into a unified list of controls. The purpose of this unified list of controls is to de-duplicate the various controls listed in the various authority documents as many of them will overlap each other.

The UCF spreadsheets already have a great number of hierarchically listed controls that you can use for harmonization purposes, or you can add to them if necessary.

- 2-1 The third step will be to define and categorize your organizational systems and the information contained within those systems. **It is the information contained within the systems that defines your necessary levels of applying information assurance (confidentiality, integrity, availability, accountability) controls.** Information assurance controls are defined as falling into one of three categories of risk; low, medium, or high.

This step *does not include* the use of the UCF spreadsheets.

- 3-1 Compliance control scoping involves marrying the complete list of controls as defined by applicable authority documents together with the information risk levels of organizational systems in order to define a control winnowing methodology. In other words, the list of what you need to do can be reduced by analyzing which controls aren't necessary based upon the risk levels of the information you are working with.

This step *does not include* the use of the UCF spreadsheets.

- 3-2 Documenting your compliance control scoping process into your control framework is very important, as you'll need to provide proof that you examined each control and made a conscious decision to ignore or modify the controls you've defined as such.

The UCF spreadsheets can be used to document your various levels of control acceptance.

- 4-1 With a list of controls and a method for measuring your various levels of capability both completed, you can begin to link your control/capability matrix to the existing policies, standards, and procedures that you do have and list those which you need to create.

The UCF spreadsheets can be used to link your controls list to your policy, standards, and procedure documents.

THE UCF SPREADSHEET RELEASE

Every quarter Unified Compliance releases fifteen spreadsheets. Fourteen of the spreadsheets show all of the controls in the UCF, their mappings to various Authority Documents and Parent Categories, and the citations within the Authority Document for the control. The fifteenth spreadsheet contains all of the background information about the Authority Documents in the UCF and where to find them.

The purpose of these spreadsheets is to allow you to sift through the vast amounts of data about compliance in the UCF. By placing the data in spreadsheet form, it can easily be sorted, rearranged, and filtered to suit your needs.

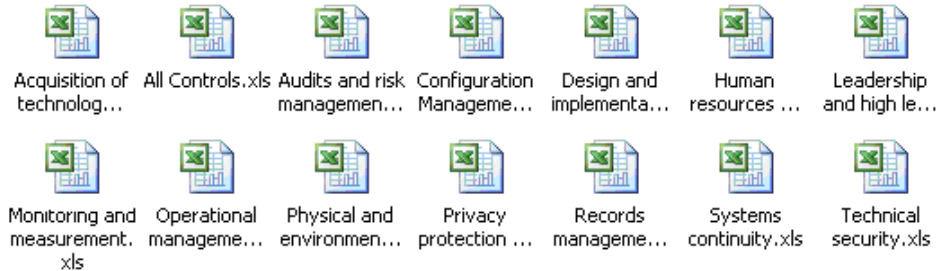
Corporate vs. Single User Editions

The Single User edition of our spreadsheets may only be used by one person and may not be copied or shared (e.g., via shared drive, posted on Sharepoint or other website, distributed through e-mail, etc.). You are granted the right to copy it to a backup device, but this backup device (e.g., CD-ROM, Flash drive, backup tape, etc.) may not be used by others to read or utilize the spreadsheets. The intellectual property (IP) remains with Network Frontiers LLC and Latham & Watkins LLP.

The Corporate edition grants you the right to copy and distribute the spreadsheet within your corporation. The intellectual property (IP) remains with Network Frontiers LLC and Latham & Watkins LLP.

The content is the same in both editions of our spreadsheets; only the usage rights are different.

The Controls Spreadsheets



All Fourteen Controls Spreadsheets

The Controls Spreadsheets are the fourteen spreadsheets that contain all of the controls known to the UCF and their respective citations. Thirteen of the fourteen spreadsheets are named with their Impact Zone in the title and contain controls relevant only to that Impact Zone with the fourteenth spreadsheet called "All Controls.xls" containing all of the Impact Zones.

To help improve readability, and due to a limitation on the number of columns allowed in Excel, all fourteen of the Controls Spreadsheets are split up into three sections: "US", "International", and "Systems Configuration".

What's What in the Controls Spreadsheets

Harmonized Control Title	Control ID	Banking and Finance Guidance	Energy Guidance	DOE OS 11	NERC	Healthcare and Life Sciences Guidance	NASD NYSE Guidance	NIST Guidance	Payment Card Guidance	Records Management Guidance	Securities Overlay Guidance	US Federal Privacy Guidance	US Federal Security Guidance	US Internal Remedies Guidance	US State Laws and Protection	Internal Guidance	Start ID
9 Configuration management plan is provided	01446																000 012 00
10 Developer security testing plan is provided	01447																000 012 00
11 Consider alternative courses of action	01129																000 012 00
12 Conduct an acquisition feasibility study	01129	1															000 012 00
13 Technological feasibility test environment	01130																000 012 00
14 Conduct an economic feasibility study	01131																000 012 00
15 Information architecture	01132																000 012 00
16 Formulation of acquisition strategy	01133	2															000 012 00
17 Third-party service requirements	01134	2															000 012 00
18 Risk Analysis report and decision approval.	01135	3															000 012 00
19 Procurement Control	01136	1															000 012 00
The use of personal devices will be approved only in extreme cases and only if the owner signs a forfeiture statement in case of a security incident	04599																000 012 00
20 Document the software product acquisition methodology	01138	1															000 012 00
21 Contract for and manage escrowed documentation	01139	1															000 012 00
22 Software licensing	01140	1															000 012 00
23 Software licensing	01140							2									000 012 00
24 Establish third-party software maintenance agreements	01143	1															000 012 00
25 Acceptance of facilities, technology, and technology services	01144																000 012 00
26 Examine received software for vulnerabilities	01898	1															000 012 01
27 Examine received hardware for vulnerabilities	01899																000 012 01

An example of a Controls Spreadsheet

1. Harmonized Control Title – The name of the Control that the row references.
2. Control ID – The assigned Control ID for the Control in the current column. The Control ID is a hyperlink that links to the UCF website to provide more detailed information about the Control.
3. Parent Category Columns – The name of a Parent Category. Each of the Parent Category Columns contains Authority Documents within it. If one or more Authority Documents within a Parent Category Column make a reference to a Control, a count will be placed in its Parent Category's column.

4. Authority Document Columns – The names of the Authority Documents that are in the expanded Parent Category. Each time an Authority Document makes a reference to a Control, a citation will be placed in its column.
5. Internal Guidance – A column used to store your notes or mappings while reviewing the UCF. For an example of how to use the Internal Guidance column, see *Using the Controls Spreadsheets to Aid in Compliance*.
6. Sort ID – A hidden column (unhidden in the above screenshot) that is used to restore the original document sort. See *Using the Controls Spreadsheets* for instructions on how to reveal this column.

Using the Controls Spreadsheets

Row	Control Title	Control ID	Banking and Finance Guidance	Energy Guidance	DIME CS 11	NERC	Healthcare and Life Sciences Guidance	NASD NYSE Guidance	NIST Guidance	Payment Card Guidance	Records Management Guidance	Sarbanes Oxley Guidance	US Federal Privacy Guidance	US Federal Security Guidance	US Internal Revenue Guidance	US State Laws and Proclamations Guidance	Internal Guidance	Sort ID
9	Configuration management plan is provided	01446																000 012 00
10	Developer security testing plan is provided	01447																000 012 00
11	Consider alternative courses of action	01120																000 012 00
12	Conduct an acquisition feasibility study	01129	1															000 012 00
13	Technological feasibility test environment	01130																000 012 00
14	Conduct an economic feasibility study	01131																000 012 00
15	Information architecture	01132																000 012 00
16	Formulation of acquisition strategy	01133	2															000 012 00
17	Third-party service requirements	01134	2						3	2	1			2	1			000 012 00
18	Risk Analysis report and decision approval	01135	3													4		000 012 00
19	Procurement Control	01136	1													2		000 012 00
20	The use of personal devices will be approved only in extreme cases and only if the owner signs a forfeiture statement in case of a security incident	04599																000 012 00
21	Document the software product acquisition methodology	01138	1															000 012 00
22	Contract for and manage escrowed documentation	01139	1															000 012 00
23	Software licensing	01140	1							2								000 012 00
24	Establish third-party software maintenance agreements	01143	1															000 012 00
25	Acceptance of facilities, technology, and technology services	01144																000 012 01
26	Examine received for vulnerabilities	01988	1															000 012 01
27	Examine received for vulnerabilities	01990	1															000 012 01

An example of a Controls Spreadsheet

1. The "1" and "2" buttons expand and retract all of the Parent Category Columns, showing and hiding all of the Authority Documents in the spreadsheet.
2. The "+" button above and to the right of each Parent Category Column is used to expand the Parent Category, exposing the Authority Documents within it. Once the Parent Category is expanded, press the "-" button to retract it.
3. The Parent Category and Authority Document columns allow the citations and controls to be sorted and filtered as desired. Clicking on the arrows in the bottom right of the cell allows the sort order to be changed, or the contents of the column to be filtered. The sort order and filter set affect the rest of the spreadsheet so be sure to unset the sort or filter by resetting it to "(All)".
4. These tabs switch between the different sections of guidance, "US", "International", and "Systems Configuration". If you wish to compare data between the tabs, full columns can be copied and pasted among the sections – or even into the other spreadsheets.
5. This column is initially hidden. To unhide it, select the entire "Internal Guidance" column and the column immediately to the right of it. Right click on either column and select "Unhide" from the menu that appears. To reset the sort for the entire spreadsheet, change the sort in this newly revealed column to "Sort Ascending".

Using the Controls Spreadsheets to Aid in Compliance

Control ID	Standardized Control Title	Banking and Finance Guidance	Energy Guidance	Healthcare and Life Science Guidance	IASO/NIJSE Guidance	MST Guidance	Payment Card Guidance	Records Management Guidance	Subacute Direct Guidance	US Federal Privacy Guidance	US Federal Security Guidance	US Internal Revenue Guidance	US State Laws and Provisions Guidance	Internal Guidance
270	Establish and maintain a reporting methodology program	02072	1						1	1	1			X
275	Employee sanctions	03442	2						2	1	4	1		X
314	Documenting all policies and procedures	0324	2	1			1		4	1	5			X
1775	Manage records as an integral part of each system	02663	3	1	1	1		1	1	1	5	1		X
	Determine each system's records preservation and disposition obligations	03804	1	1	1	1		2		1	7	1	1	X
1776	Determining how long to retain records and create a data retention policy	03836	6						5	1	5	2	6	X
1784	Manage the logical and physical handling of records	03831	2		1	2	2	1		3	1		1	X
1785	Maintain appropriate access controls for all records	03871	1		2					1	3			X
1833	Accounting of disclosures (audit trails)	03772	1		2					1	1			X
1849	Privacy protection for information and data	03328	6		1	2	4		2	8	2		7	X
	Establish personal information collection limitation boundaries	0507											1	X
1973	Data should be collected lawfully, fairly and honestly	00010							1	2				X
	Personal info must be collected directly from the individual													X

The Internal Guidance column with a filter showing only controls that have a Parent Category of "Payment Card Guidance" or "US Federal Security Guidance"

One way the UCF Spreadsheets make compliance easier is through the use of the Internal Guidance column. This column can be used to isolate the controls that apply to your specific compliance scenario.

Using the Internal Guidance Column

1. Go to the Parent Category or Authority Document that you must comply with and set the filter to "(NonBlanks)". Place an "X" in the "Internal Guidance" column for every row that is returned. You may use copy/paste or Excel's fill down functionality to speed this process.
2. Change the filter on the Parent Category or Authority Document column you were just using back to "(All)". Repeat Steps 1 and 2 for all Parent Categories or Authority Documents that you must comply with.
3. Once all of the controls for Parent Categories or Authority Documents have had X's placed in their Internal Guidance column, set the filter of the Internal

Guidance column to “(Nonblanks)”. This leaves only Controls that apply to your specific scenario displayed.

The Authority Documents Spreadsheet

UCF AD Official Name	UCF AD Parent Category	UCF AD Type	UCF AD Availability	UCF AD Originator	UCF AD Issuer	UCF AD Description	UCF AD URL
1. Korea Act on the Protection of Personal Information Maintained by Public Agencies (PIPA)	Asia and Pacific Rim Guidance	Statute	Free	South Korean Government	Global Legal Information Network	This Authority Document has 18 citations mapped to 16 UCF Common Control IDs. The document as a whole was last reviewed and released on 2003-01-01.	http://www.gln.gov/secure/action/799/EUC0007
2. Korea Act on Protection of Network Information	Asia and Pacific Rim Guidance	Statute	Free	South Korean Government	Global Legal Information Network	This Authority Document has 19 citations mapped to 19 UCF Common Control IDs. The document as a whole was last reviewed and released on 2003-01-01.	http://www.gln.gov/secure/action/799/EUC0008
3. Taiwan Computer Personal Data Protection Law (1996)	Asia and Pacific Rim Guidance	International or National Standard	Free	Taiwan Government	University Of California, Irvine	This Authority Document has 46 citations mapped to 46 UCF Common Control IDs. The document as a whole was last reviewed and released on 2009-03-01.	http://www.cc.ucl.edu/~isa/ibn/ibn/cp/2.html
4. Mac OS X Security Configuration for version 10.4 or later, second edition, Second Edition	System Configuration Guidance	Vendor Documentation	Free	Apple Computer	Apple	This Authority Document has 144 citations mapped to 88 UCF Common Control IDs. The document as a whole was last reviewed and released on 2009-03-01.	http://images.apple.com/secure/macosx/docs/79_507.pdf
5. Microsoft Windows Vista Security Guide Appendix A, Security Group Policy Settings	System Configuration Guidance	Vendor Documentation	Free	Microsoft	Microsoft Corporation	This Authority Document has 204 citations mapped to 201 UCF Common Control IDs. The document as a whole was last reviewed and released on 2008-03-01.	http://technet.microsoft.com/en-us/aa679420.aspx
6. Microsoft Windows XP Security Guide, 2006	System Configuration Guidance	Vendor Documentation	Free	Microsoft	Microsoft Corporation	This Authority Document has citations mapped to UCF Common Control IDs. The document as a whole was last reviewed and released on 30/10/01-01.	http://www.microsoft.com/downloads/details.aspx?guid=646302a-46c4557-3a164d4a4e1e&lang=en
7. Microsoft Office 2007 Security Guide, Version 2.0	System Configuration Guidance	Vendor Documentation	Free	Microsoft	Microsoft Corporation	This Authority Document has citations mapped to UCF Common Control IDs. The document as a whole was last reviewed and released on 30/10/01-01.	http://www.microsoft.com/downloads/details.aspx?guid=646302a-46c4557-3a164d4a4e1e&lang=en
8. Windows Server 2003 Security Guide, Version 2.0	System Configuration Guidance	Vendor Documentation	Free	Microsoft	Microsoft Corporation	This Authority Document has citations mapped to UCF Common Control IDs. The document as a whole was last reviewed and released on 2006-04-26.	http://www.microsoft.com/downloads/details.aspx?guid=646302a-46c4557-3a164d4a4e1e&lang=en

The Authority Documents Spreadsheet

1. UCF AD Official Name – The official, published name of the Authority Document.
2. UCF AD Parent Category – The Parent Category of the Authority Document; these categories show how the Authority Document is grouped in the UCF and in the Controls Spreadsheets.
3. UCF AD Type – The type of document that the Authority Document is, such as “Statute” or “Safe Harbor”.
4. UCF AD Availability – The availability of the Authority Document, such as “Free”, “For Purchase”, or “With Membership”.
5. UCF AD Originator – The organization where the Authority Document originated. Not to be confused with “UCF AD Issuer”, which is the actual author of the document.
6. UCF AD Issuer – The author, publisher, or promulgator of the Authority Document.

7. UCF AD Description – General information about the Authority Document including the number of Citations and Controls mapped to it, and last review/release date.
8. UCF AD URL – The URL to retrieve the Authority Document.

CONTACTING THE UCF TEAM

We welcome questions and comments about our release, and have vast amounts of documentation online including an FAQ.

If you have any questions about the spreadsheets, first take a look at our online FAQ at <http://www.unifiedcompliance.com/it-impact-zones/faqs-1/>.

If answers to your questions or comments cannot be found at the UCF website, technical questions should be sent to ProductSupport@UnifiedCompliance.com and non-technical ones to Info@UnifiedCompliance.com.