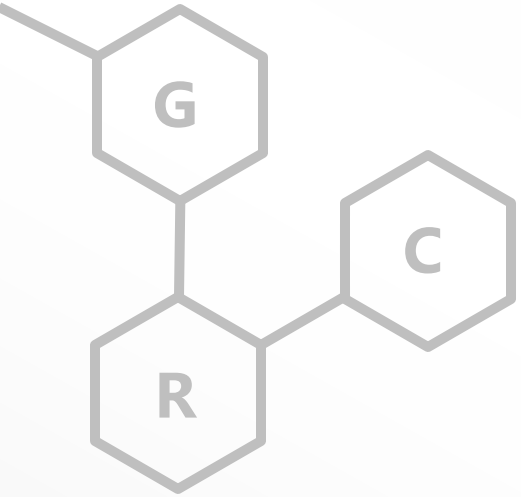
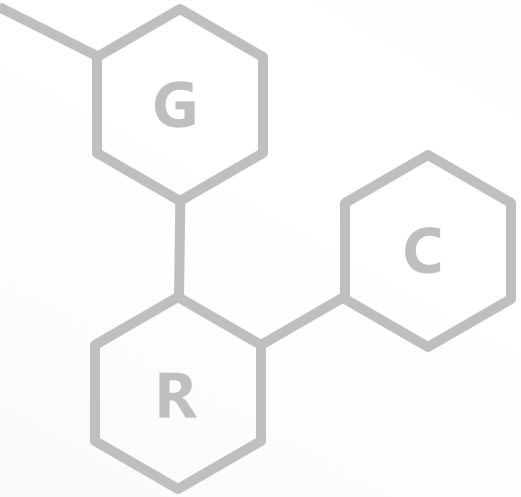


UCF®

The Science of Compliance®



State of Security & Compliance :: 2017

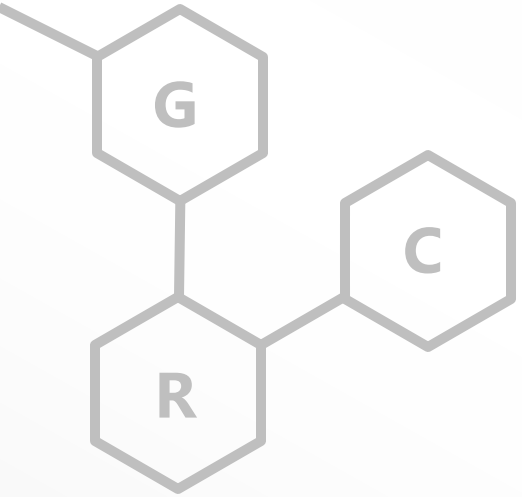
- Ever-Increasing Compliance Requirements & Enforcement
- Audit Overload
- Complex Solutions, Difficult to Automate
- Need to Connect Existing Policies to Actual Laws
- Need to Follow Multiple Standards
- Too Many Spreadsheets

Common Solution:

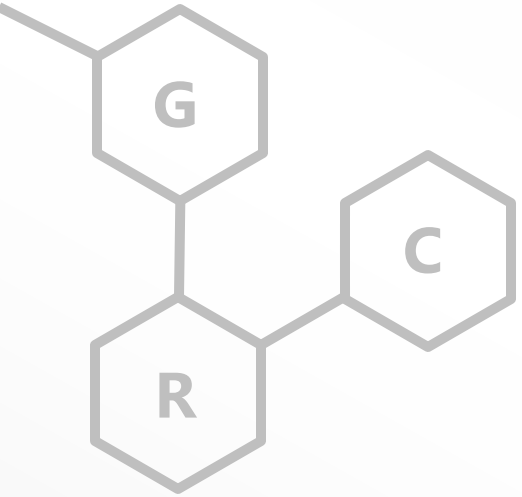
Leverage a Standard

Benefits of Leveraging a Standard

- Single Source
- Other Organizations Also Follow
- Thousands of Resources Specific to the Standard
- Events!



What Could Go Wrong?



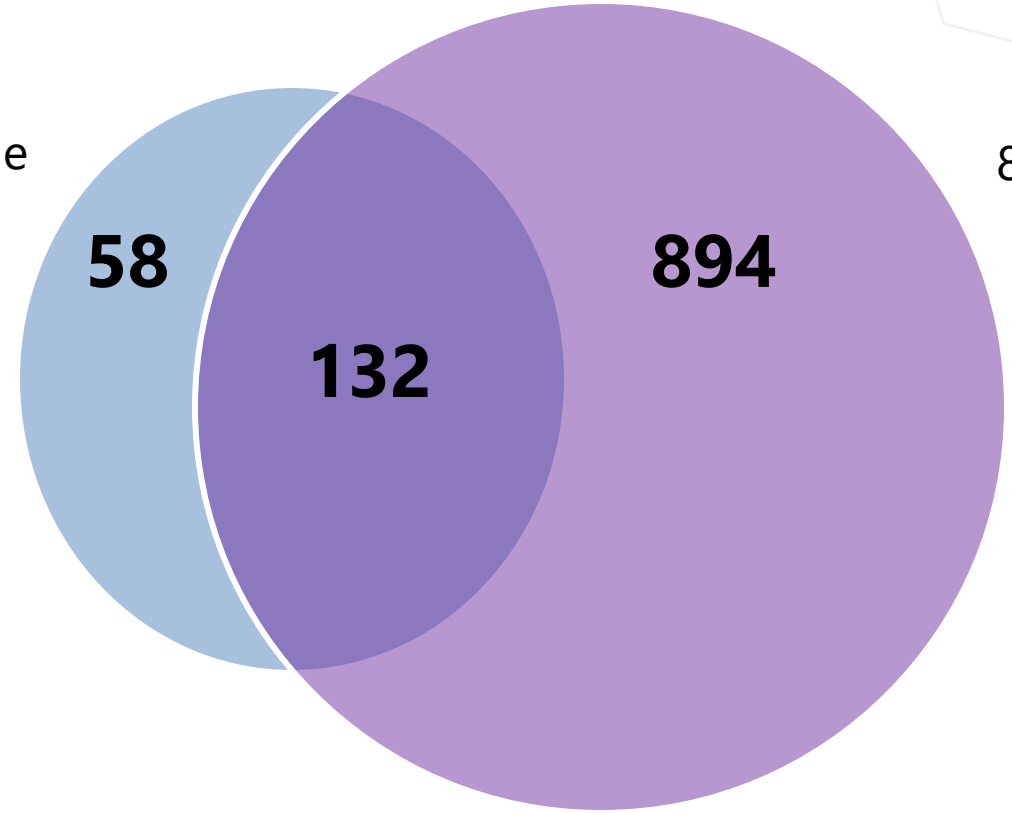
Standard Issues

- Blindly Following a Standard Can Cause Huge Misses
- Standards Are Not Designed to Cover Everything
- Might Influence Resources to be Misguided
- What about the Law?

How Does ISO 27001 Compare to Actual Legal Requirements?

ISO 27001 vs. Banking Requirements

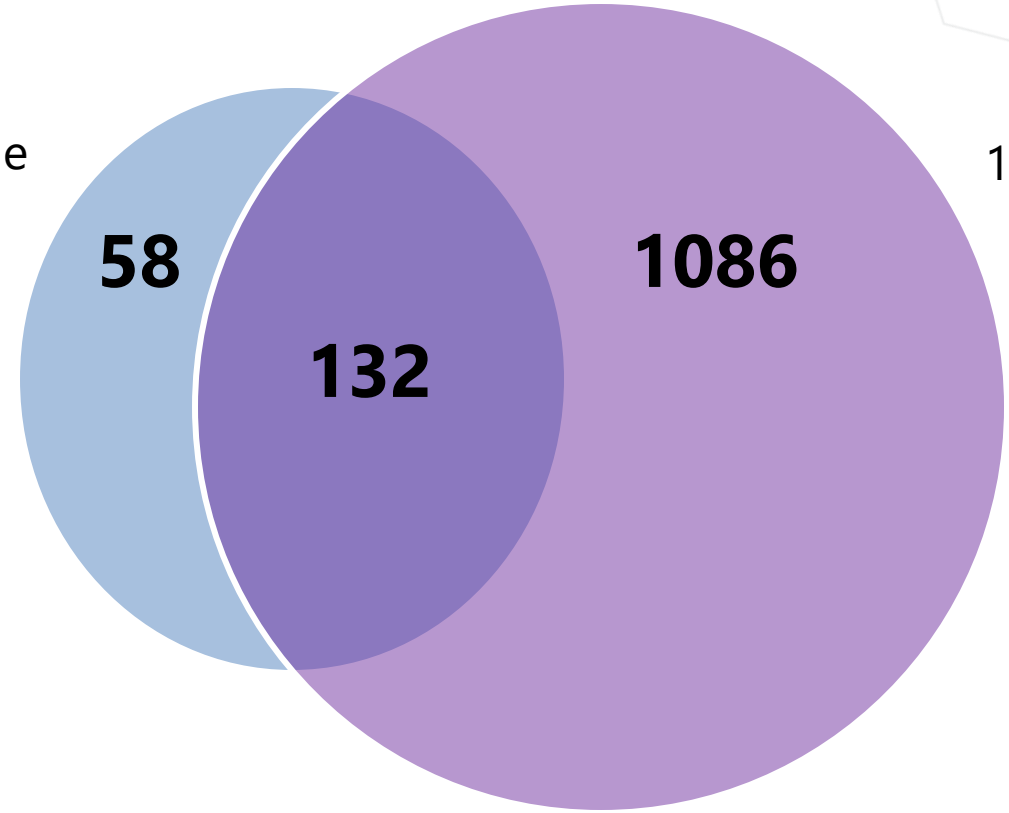
58 Controls unique to ISO 27001



894 Controls not covered by ISO 27001

ISO 27001 vs. Health Care Requirements

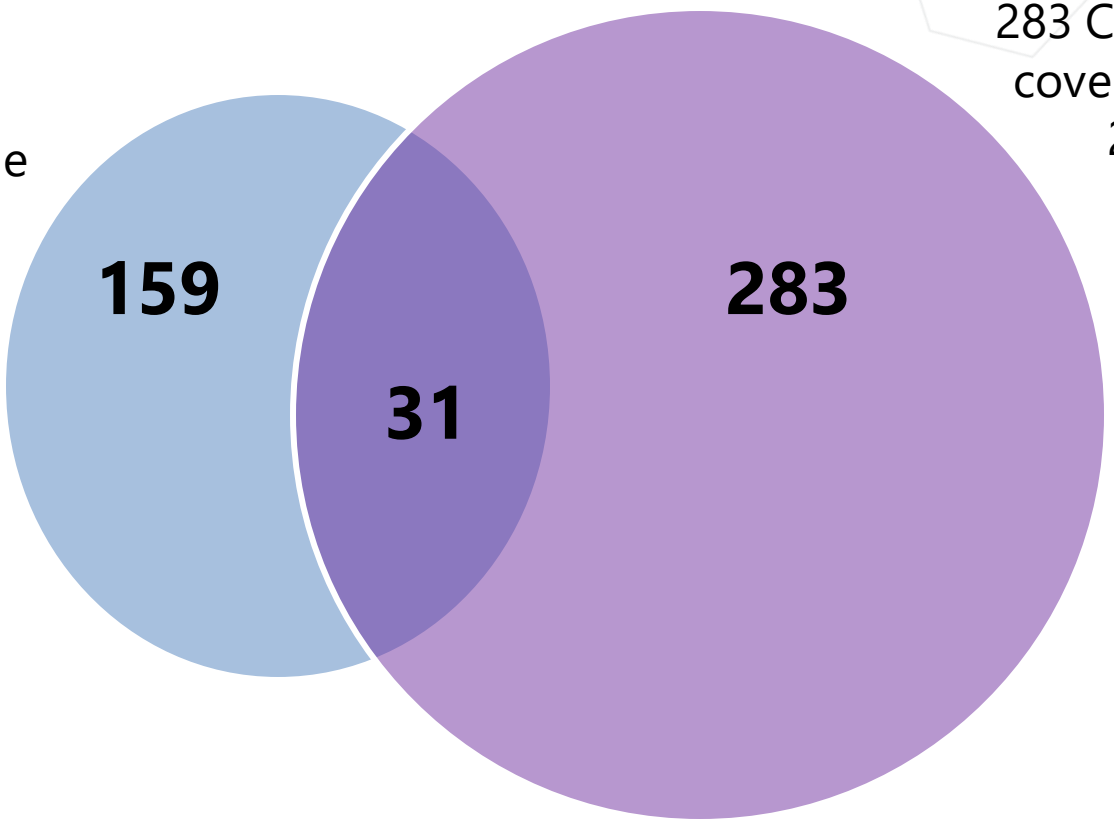
58 Controls unique to ISO 27001



1086 Controls not covered by ISO 27001

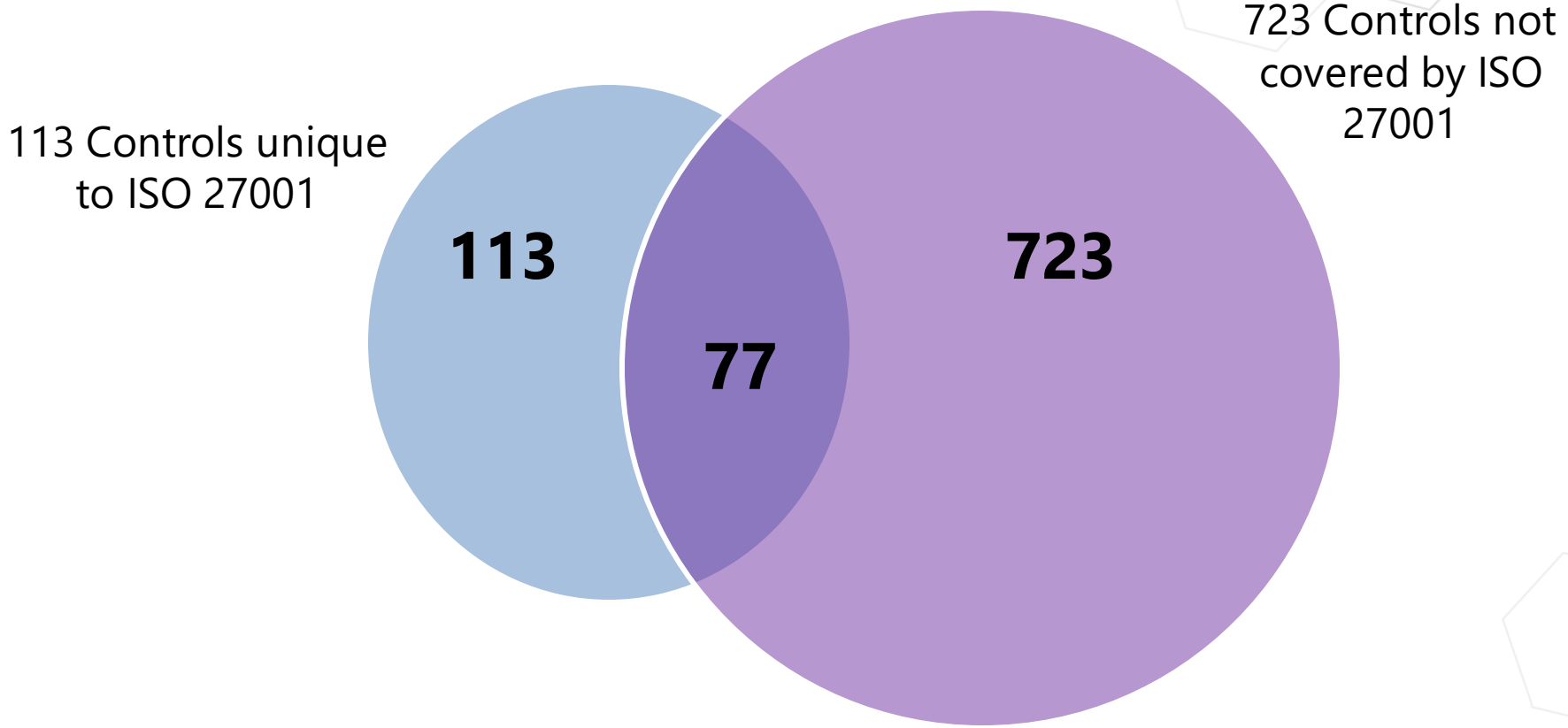
ISO 27001 vs. PCI

159 Controls unique to ISO 27001



283 Controls not covered by ISO 27001

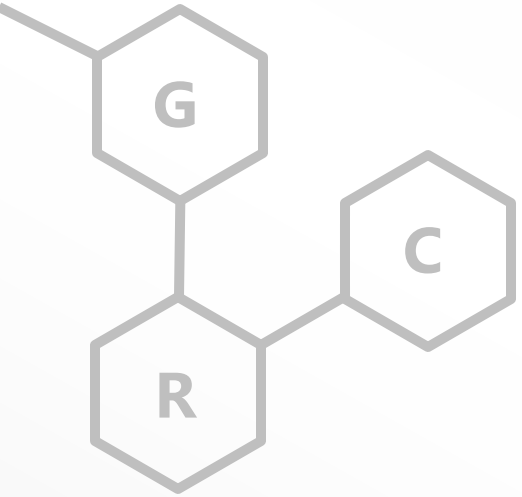
ISO 27001 vs. North American Privacy



ISO 27001 vs. SOX

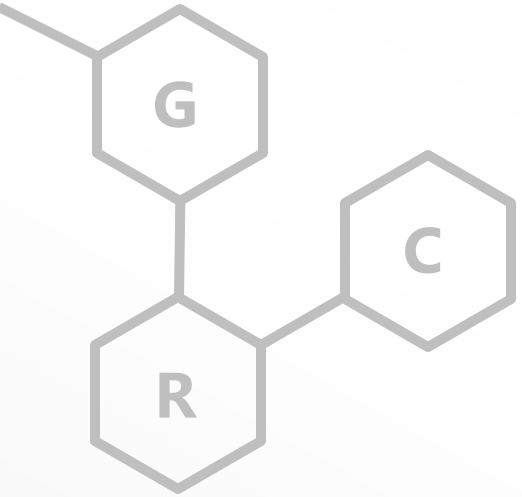
91 Controls unique to ISO 27001

612 Controls not covered by ISO 27001



Solution:

Leverage a Common Control Framework

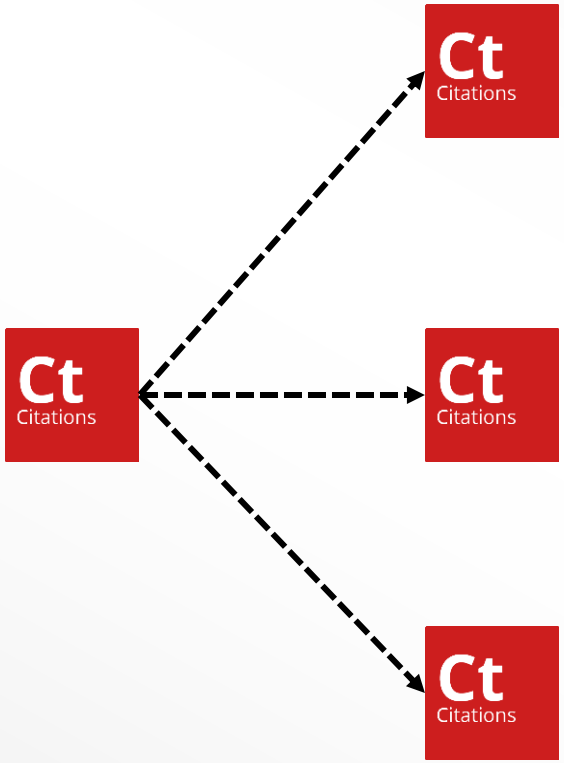


What is a Common Control?

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

Everyone Crosswalks Citations

Physical access to assets is managed and protected. **(PR.AC-2, Framework for Improving Critical Infrastructure Cybersecurity)**

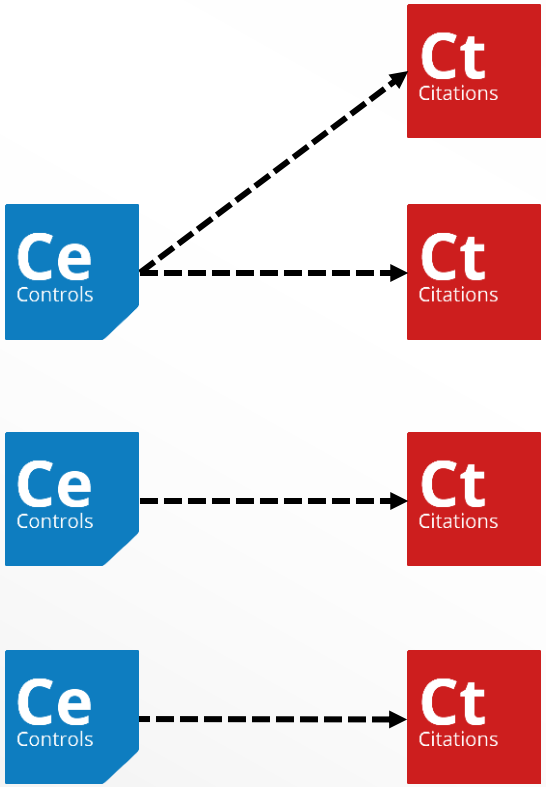


The organization provides {organizationally documented security safeguards} to control access to areas within the facility officially designated as publicly accessible. **(PE-3c., Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53, Revision 4)**

The organization issues authorization credentials for facility access. **(PE-2b., Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53, Revision 4)**

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. **(A.11.1.6 Control, ISO 27001:2013, Information Technology - Security Techniques - Information Security Management Systems - Requirements, 2013)**

UCF Mapper Harmonizes Controls to a Single Set of Common Controls



Physical access to assets is managed and protected. **(PR.AC-2, Framework for Improving Critical Infrastructure Cybersecurity)**

Establish and maintain a facility physical security program. **(CC ID 00711)**

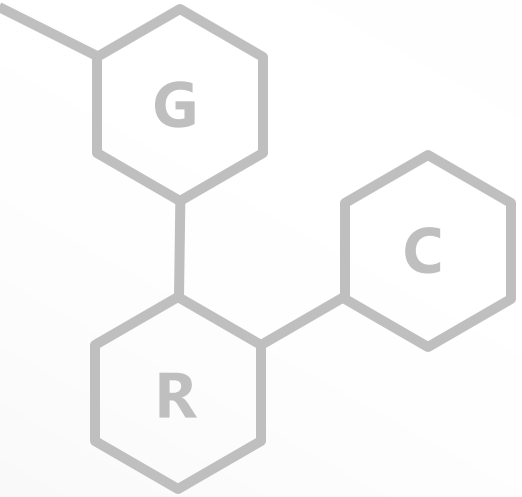
The organization provides {organizationally documented security safeguards} to control access to areas within the facility officially designated as publicly accessible. **(PE-3c., Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53, Revision 4)**

Establish and maintain identification issuance procedures for identification cards or badges. **(CC ID 06598)**

The organization issues authorization credentials for facility access. **(PE-2b., Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53, Revision 4)**

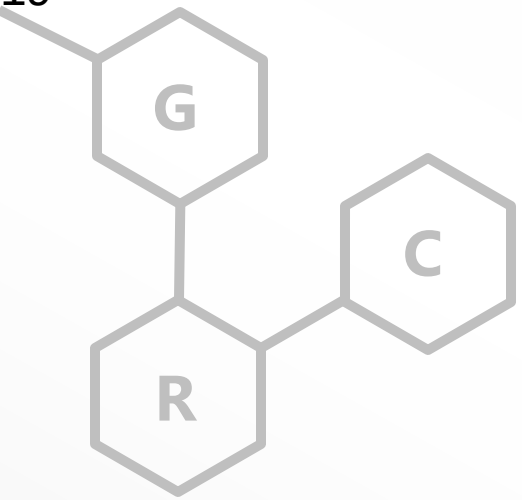
Isolate loading areas from information processing facilities, if possible. **(CC ID 12028)**

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. **(A.11.1.6 Control, ISO 27001:2013, Information Technology - Security Techniques - Information Security Management Systems - Requirements, 2013)**



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.



Benefits of a Common Control Framework

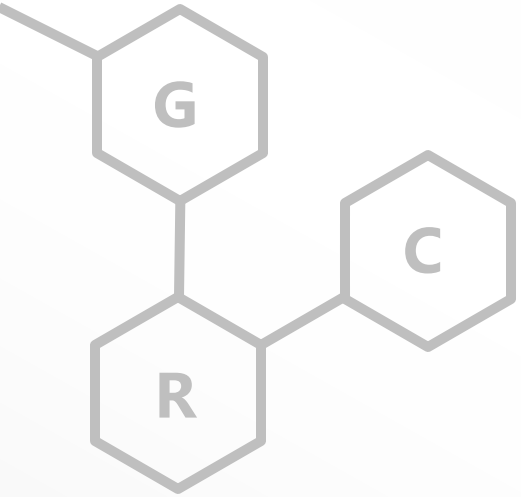
- Integrate All Types of Authority Documents
- Single, Harmonized Set of Controls
- Implementation Controls Provide Details
- Keep Up with Regulatory Changes
- Common Control Audit

Allows Integration of Different Solutions with Different Data Types.

Three Key Components

UCF Mapper

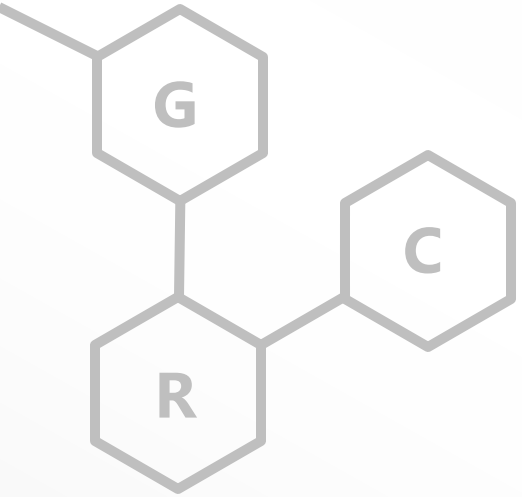
UCF Common Controls Hub



Unified Compliance Framework®

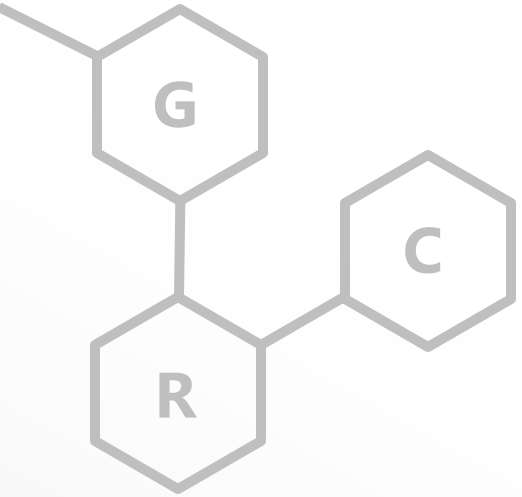
- Content
- Structure
- Methodology

The UCF is the world's largest and most researched Common Control framework.



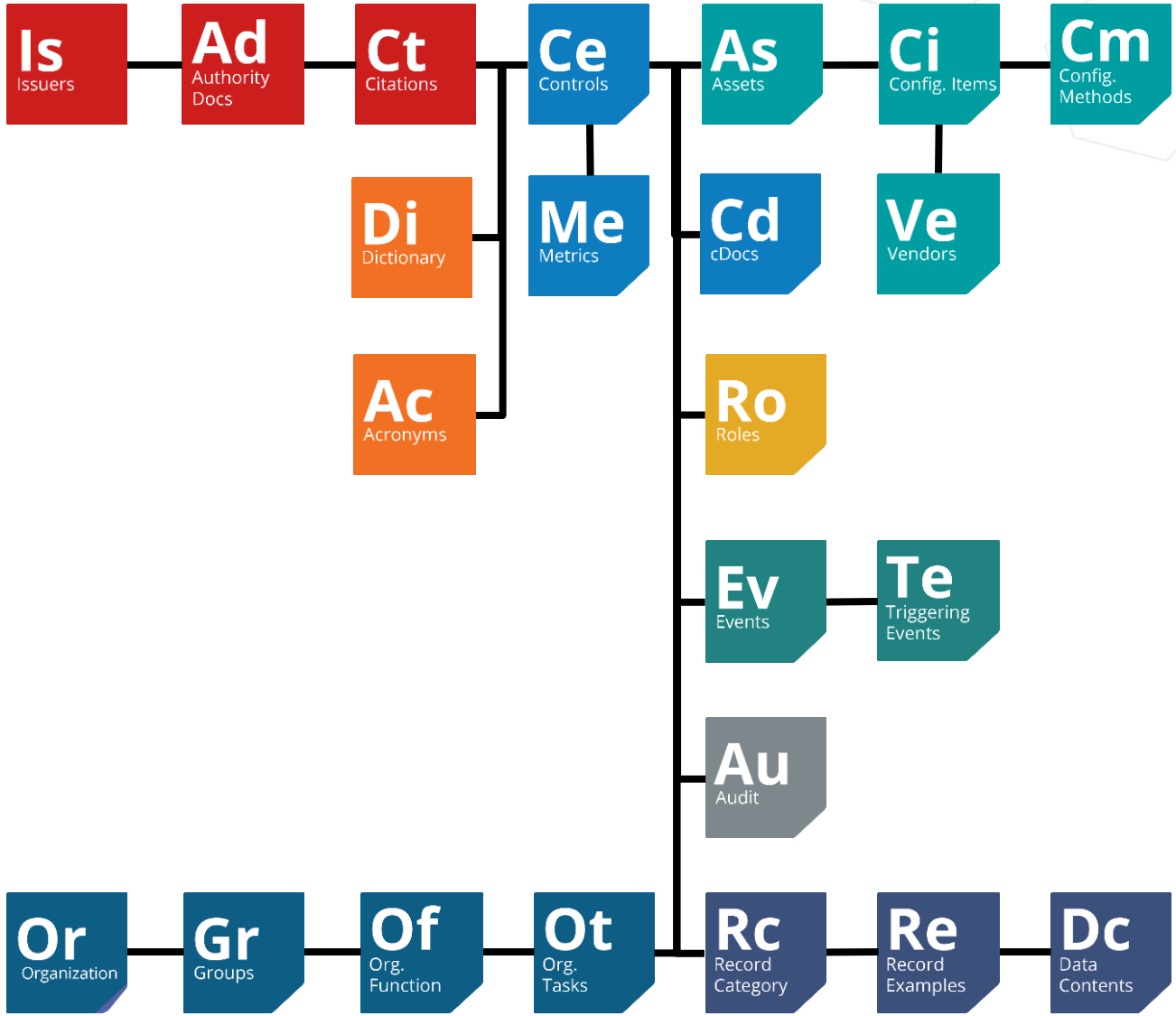
UCF Content

- eGRC/Operational Management
- Information Security/Information Technology
- Physical and Environmental Protection
- Systems Continuity
- Records Management
- Privacy
- Risk Management
- Ethics
- Third Party and Supply Chain Management



UCF Structure

The Structure of Governance & Compliance



Three Key Components

Patented Proc  eating the UCF

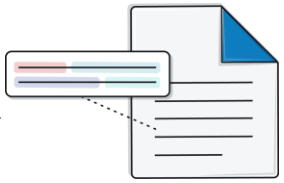
UCF Mapper

- Training Program Administered through (ISC)^2
- Allows Any Certified UCF Mapper to Add Content to the UCF
  - Self-Service Customers
  - Individual Contributors
  - Consultants/Mapping Providers
  - Authority Document Issuers
- Content Mapped to the UCF Available through Common Controls Hub and API

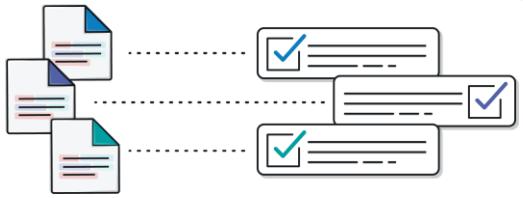
Patented UCF Mapper Process

Authority Document Research

Citation Extraction

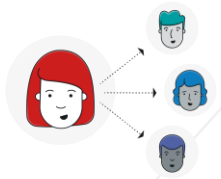


Tagging Mandates for Verbs and Nouns

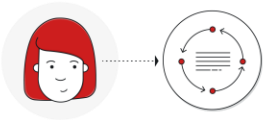


Matching Mandates to Controls

Test Tools and Configurations



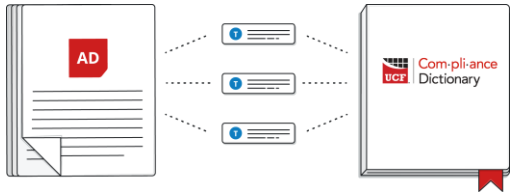
Interview People



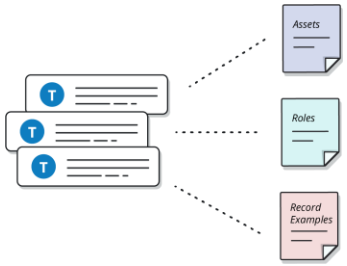
Observe Processes

Examine Records or Assets

Audit Question Creation



Term Mapping

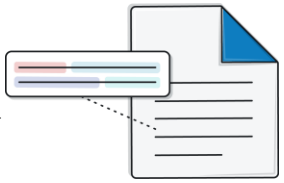


Mapping Terms to Named Entities

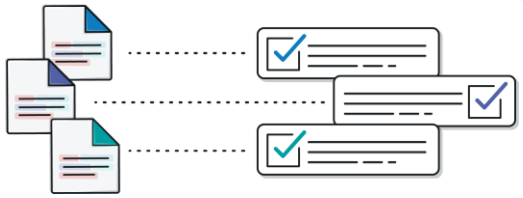
Patented UCF Mapper Process

Authority Document Research

Citation Extraction

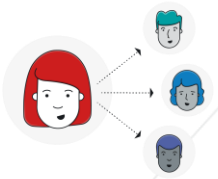


Tagging Mandates for Verbs and Nouns

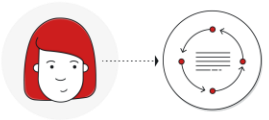


Matching Mandates to Controls

Test Tools and Configurations



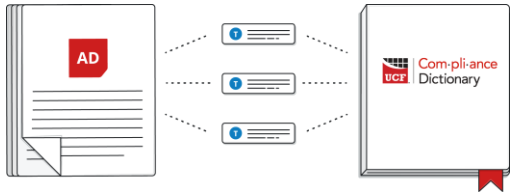
Interview People



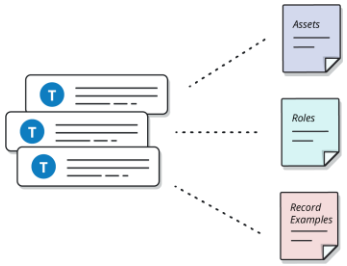
Observe Processes

Examine Records or Assets

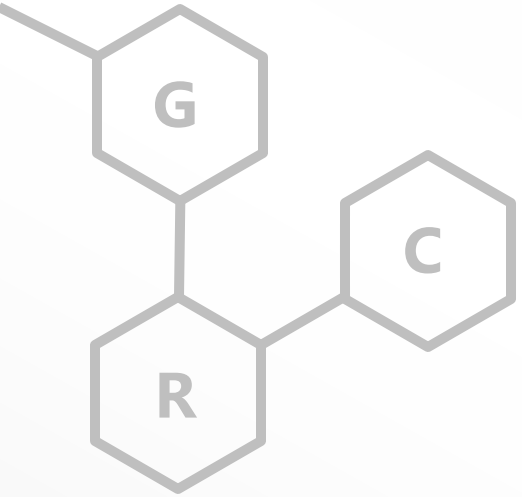
Audit Question Creation



Term Mapping



Mapping Terms to Named Entities



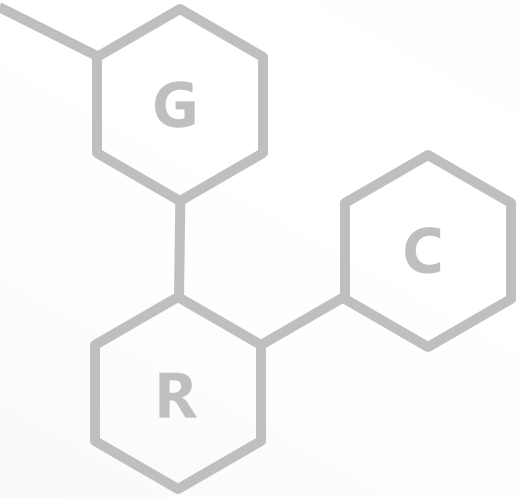
UCF Mapper

Original Citation

Different Words; Same Requirement

CITATION REFERENCE	NIST 800-171 CITATION GUIDANCE	CC ID	CONTROL TITLE
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	01411	Establish access rights based on least privilege.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	01411	Establish access rights based on least privilege.

permitted to execute.



UCF | Com·pli·ance Dictionary

Patented Structured Dictionary: Key to Compliance Mapping

…and a great many other things!

UCF Mapper is Revolutionary

- Any organization can add Authority Documents to the Unified Compliance Framework
- First truly professional mapping tool
- No wasted effort
- Incremental Authority Document update support
- All Common Controls Hub and Unified Compliance Framework features supported

First Professional Mapping Tool

- Patented scientific and linguistic processes for highest quality mapping
- Leverages several Natural Language Processing (NLP) engines
- ComplianceDictionary
- Eliminate redundancy within and between Authority Documents
- Auditable and fully documented
- Mapper, Reviewer, Approver, Lexicographer, and Lawyer

No Wasted Effort

- No more one-off spreadsheets
- No more having to start over when one standard or law changes
- All effort into Unified Compliance Framework immediately available through Common Controls Hub
- Authority Document updates can take a fraction of the time
- Over time, the value increases rather than decreases

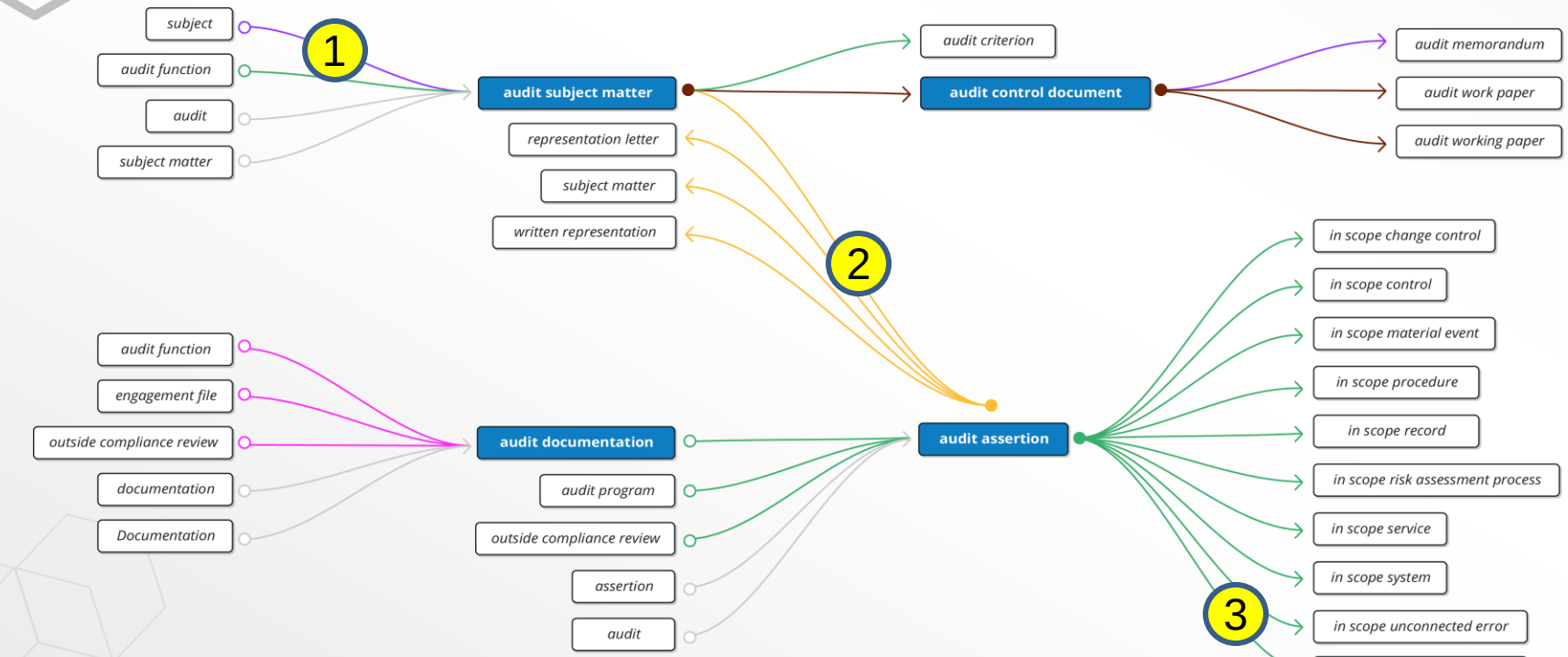
All Common Controls Hub Features Available

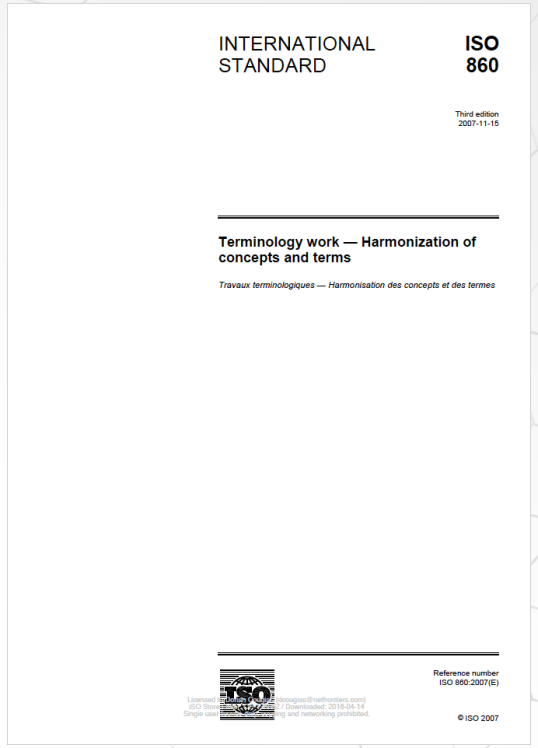
- UCF API to GRC automation
- Spreadsheet and Custom Compliance Templates
- Compare and perform Gap/Overlap analysis

Benefits of Leveraging UCF Mapper

- Highest quality mapping tools
  - Built-in AI for tagging mandates and matching Common Controls
  - ComplianceDictionary eliminates language ambiguities
  - Eliminate redundancy in your controls
- Any work done today can be leveraged tomorrow and beyond so your investment of time and $$ is protected
- Authority Document updates can take a fraction of the time
- All Common Controls Hub features are available
  - Authority Document Lists, Compare, Builds, and connection to GRC automation via the UCF API

UCF Mapper Uses Semantic Crosswalking to Accurately Map Citations to Controls




INTERNATIONAL STANDARD **ISO 860**

Third edition
2007-11-15

Terminology work — Harmonization of concepts and terms

Travaux terminologiques — Harmonisation des concepts et des termes

Reference number
ISO 860:2007(E)

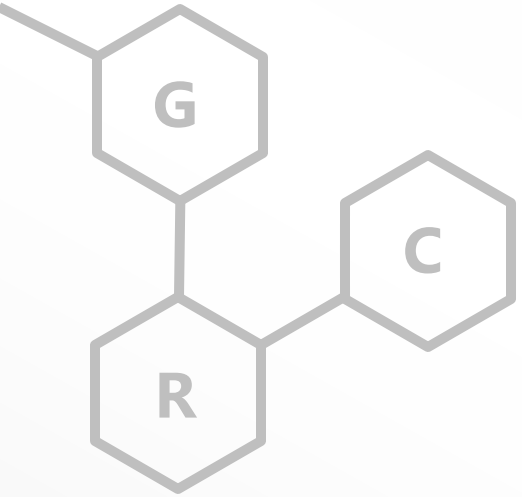
© ISO 2007

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.

Three Key Components



Access UCF via A 

mon Controls Hub