## § 2.1 Schemas harmonized in the Federated Compliance Mapping model

As of this writing there are several framework schemas that are in active use:

* + NIST’s Control Correlation Identifier (CCI) – The CCI provides a standard identifier and description for each of the singular, actionable statements that comprise an IA control or IA best practice. CCI bridges the gap between high-level policy expressions and low-level technical implementations. CCI allows a security requirement that is expressed in a high-level policy framework to be decomposed and explicitly associated with the low-level security setting(s) that must be assessed to determine compliance with the objectives of that specific security control. This ability to trace security requirements from their origin (e.g., regulations, IA frameworks) to their low-level implementation allows organizations to readily demonstrate compliance to multiple IA compliance frameworks. CCI also provides a means to objectively rollup and compare related compliance assessment results across disparate technologies.
  + NIST Derived Relationship Mapping – The Derived Relationship Mapping (DRMs) Analysis Tool provides Users the ability to generate DRMs for Reference Documents with the Cybersecurity Framework as the Focal Document. The DRMs are non-authoritative and represent a starting point when attempting to compare Reference Documents. Refer to Sections 3.3 – 3.5 of NIST Interagency Report (IR) 8278, National Cybersecurity OLIR Program: Guidelines for OLIR Users and Developers for additional guidance around understanding and utilizing Derived Relationship Maps.
  + NIST National Checklist Program for IT Products – Guidelines for Checklist Users and Developers, 800-70, R4 (and greater) - to facilitate development of checklists and to make checklists more organized and usable, NIST established the National Checklist Program (NCP). This publication explains how to use the NCP to find and retrieve checklists, and it also describes the policies, procedures, and general requirements for participation in the NCP.
  + NIST Open Security Controls Assessment Language (OSCAL) – NIST, in collaboration with industry, is developing the Open Security Controls Assessment Language (OSCAL). OSCAL is a set of formats expressed in XML, JSON, and YAML. These formats provide machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results.
  + TagVault Software Identification (SWID) Tagging – NIST has developed a SWID Tag validation methodology and schema that can be used to verify that a produced SWID has properly implemented the requirements defined in NISTIR 8060. TagVault has turned it into a queryable API and reference framework.
  + Unified Compliance Framework – the UCF has been at the forefront of compliance frameworks before the term GRC was coined by Michael Rasmussen. The Unified Compliance team have multiple patents regarding compliance frameworks, dictionary structures, etc. Their structure and framework standard will be presented throughout. The patents covered in this section include the following:

| **Country** | **Application|Patent No.** | **Filing Date|Issue Date** | **Title** |
| --- | --- | --- | --- |
| US | 13/723,018|9,009,197 | 2012-12-20|2015-04-14 | METHODS AND SYSTEMS FOR A COMPLIANCE FRAMEWORK DATABASE SCHEMA |
| US | 13/952,212|8,661,059 | 2013-07-26|2014-02-25 | COMPLIANCE FRAMEWORK DATABASE SCHEMA |
| US | 14/685,466|9,996,608 | 2015-04-13|2018-06-12 | METHODS AND SYSTEMS FOR A COMPLIANCE FRAMEWORK DATABASE SCHEMA |
| US | 15/794,405|10,353,933 | 2017-10-26|2019-07-16 | METHODS AND SYSTEMS FOR A COMPLIANCE FRAMEWORK DATABASE SCHEMA |
| US | 16/026,524 | 2018-07-03 | METHODS AND SYSTEMS FOR A COMPLIANCE FRAMEWORK DATABASE SCHEMA |
| US | 16/432,634 | 2019-06-05 | METHODS AND SYSTEMS FOR A COMPLIANCE FRAMEWORK DATABASE SCHEMA |
| US | 16/432,737 | 2019-06-05 | METHODS AND SYSTEMS FOR A COMPLIANCE FRAMEWORK DATABASE SCHEMA |
| US | 14/963,063|9,575,954 | 2015-12-08|2017-02-21 | STRUCTURED DICTIONARY |
| US | 15/404,916|9,977,775 | 2017-01-12|2018-05-22 | STRUCTURED DICTIONARY |
| US | 15/957,764|10,606,945 | 2018-04-19|2020-03-31 | STRUCTURED DICTIONARY |

In addition to these schemas, there are guidelines for *doing* the mapping that can be found in the following which we will reference throughout:

* + ISO 19770-8 (2020) Information technology – IT asset management – Part 8: Guidelines for mapping of industry practices to/from the ISO/IEC 19770 family of standards
  + NISTIR 8278 National Cybersecurity Online Informative References (OLIR) Program: Guidance for OLIR Users and Developers
  + Unified Compliance Framework – Unified Compliance Schema and Mapping Standard