

Does DFARS Clause 252.204-7012 apply to you?

Use CDI COMPLY™, TransR's Compliance Solution for DFARS Clause 252.204-7012!

SAFEGUARDING COVERED DEFENSE INFORMATION(CDI) AND CYBER INCIDENT REPORTING

The deadline for compliance to DFARS Clause 252.204-7012 was December 31, 2017 for all companies doing business with the DoD. This applies to all DoD contractors regardless of company size, contract value, or whether your company is a Prime Contractor or Subcontractor. It's time for corrective action!

Potential consequences of non-compliance include:

- Penalties
- Termination for Convenience
- Termination for Default
- Obligation to fulfill the contract terms with payment withheld until compliance with DFARS Clause 252.204-7012

Among the most onerous of the subject DFARS clause elements is the assertion that the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information(CUI) in Nonfederal Information Systems and Organizations". This publication has 14 distinct security families, totaling 110 requirements, some basic and some derived.

DFARS Clause 252.204-7012 requirements can be summarized as follows:

1. Safeguard covered defense information (NIST.SP.800-171 compliance)
2. Report cyber incidents
3. Submit malicious software
4. Preserve affected media
5. Support forensic analysis
6. Support damage assessment
7. Flow down the clause to subcontractors as applicable

In our experience, there are four company maturity levels with respect to DFARS Clause 252.204-7012 compliance:

- Unaware
- Aware, but unsure of the full scope and applicability to their company
- Aware, but requiring supplemental resources to augment existing staff to meet the deadline
- Fully compliant

TransR provides custom solutions from Total Project Responsibility to on-going Preventative Maintenance!

Learn more at [TransR Compliance Solutions: DFARS 252.204-7012.html](https://www.transrcorp.com/TransR-Compliance-Solutions-DFARS-252.204-7012.html) regarding the actual requirements of DFARS Clause 252.204-7012 as well as NIST.SP.800-171. Buyer beware – DFARS Clause 252.204-7012 is a superset of NIST.SP.800-171.

TransR Corporation's core team of specialists plus our teaming partners -- Astute Back-Office and Axis Technologies – leverage **CDI COMPLY™**, our proprietary methodology and toolset, to help you attain compliance to safeguarding CDI and cyber incident reporting. This team has decades of experience in information management in complex engineering, manufacturing and logistic support environments, and our experts are cognizant of the considerations for safe and secure information management, enterprise system integration and collaboration.

www.TransRcorp.com

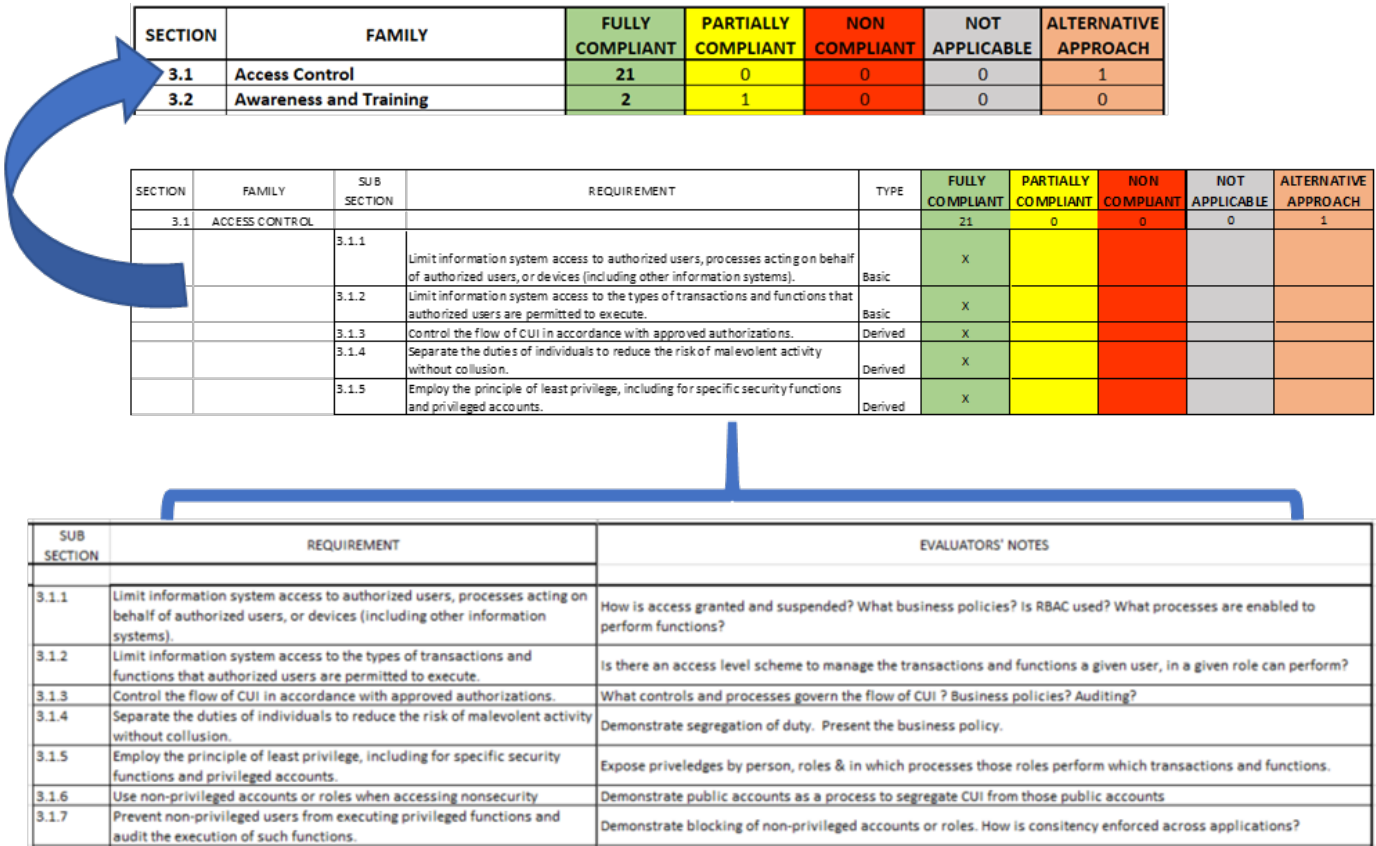
Sample TransR CDI COMPLY™ Audit Dashboard for NIST.SP.800-171 Portion of the DFARS Clause

MANAGEMENT SUMMARY REPORT						
CLIENT: Company XYZ Proprietary Assessment Content						
SECTION	FAMILY	FULLY COMPLIANT	PARTIALLY COMPLIANT	NON COMPLIANT	NOT APPLICABLE	ALTERNATIVE APPROACH
3.1	Access Control	21	0	0	0	1
3.2	Awareness and Training	2	1	0	0	0
3.3	Audit and Accountability	9	0	0	0	0
3.4	Configuration Management	9	0	0	0	0
3.5	Identification and Authentication	10	0	0	0	1
3.6	Incident Response	2	0	1	0	0
3.7	Maintenance	6	0	0	0	0
3.8	Media Protection	8	0	0	1	0
3.9	Personnel Security	2	0	0	0	0
3.10	Physical Protection	5	0	0	1	0
3.11	Risk Assessment	3	0	0	0	0
3.12	Security Assessment	4	0	0	0	0
3.13	System and Communications Protection	12	1	2	1	0
3.14	System and Information Integrity	5	1	1	0	0
		98	3	4	3	2

Audit Complete

TransR Corporation© 2017-2018	CDI COMPLY™ Proprietary NIST 800-171 Assessment Workbook
-------------------------------	--

The individual requirements, evaluated by specific TransR team questions, roll up into the 14 dashboard families.



Time for action! Contact us at CustomerRelations@TransRcorp.com or call 844-eTransR (387-2677)

Use TransR's CDI COMPLY™ To Become DFARS Clause 252.204-7012 Compliant!