Redspin
A Division of Clearwater

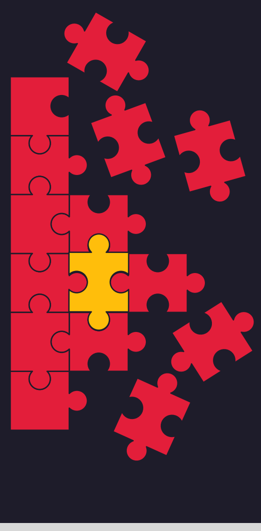
Common Cost Misconceptions of CMMC Assessments

Misconceptions about Cybersecurity Maturity Model Certification (CMMC) assessments are widespread. To help you navigate the process better, here are three common misconceptions our clients often bring to us about CMMC “fast track” solutions.

While these solutions and practices can save you time and money in coordination, they are not a fast track for CMMC and do not necessarily reduce costs for the assessment itself.

Misconception # 1

Encryption solutions will save you on assessment costs.



For CMMC Certification, you need to consider a total of 14 domains and 110 controls. While encryption is important, it's just one piece of the puzzle, mentioned in only a few controls. You must still account for the full range of requirements across all domains. Focusing solely on encryption won't significantly reduce assessment costs. Instead, try to understand when and where encryption fits into the broader CMMC puzzle to optimize your compliance strategy.

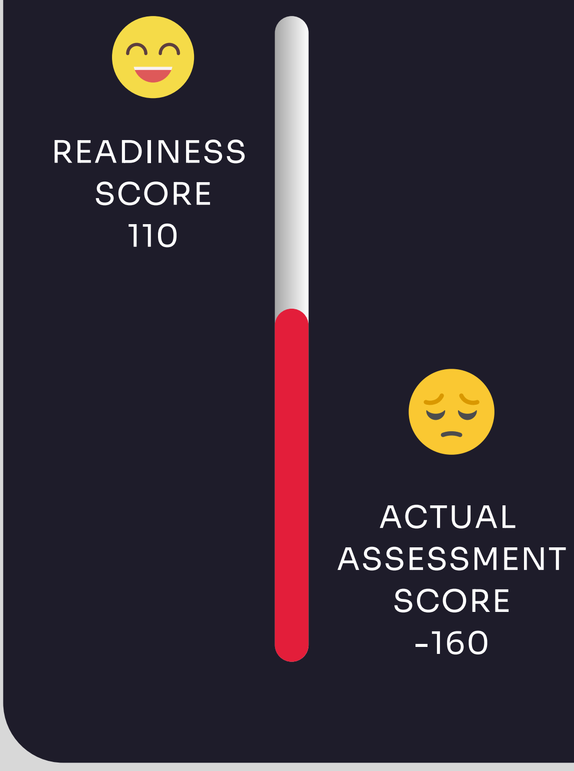
Misconception # 2

A GRC solution is a passing assessment guarantee.

There are no silver bullets for CMMC compliance. GRC solutions are great at listing information security controls but less at evaluating whether your organization truly meets the required objectives. If you're considering a GRC solution to lighten the load without the right expectations, you might be taking on more work than necessary.

Misconception # 3

A passing readiness assessment score, means you will pass a C3PAO assessment.



Ensure you select a C3PAO or RPO with the right/experienced assessors for your needs. Some OSCs fall behind during a gap assessment because their assessors 1. focus on whether a policy or procedure is documented without ensuring the documentation meets all requirements. 2. review distinct Security Requirements individually during the assessment without considering the overall compliance score based on the associated assessment objectives. Or 3. deem CMMC assessment objectives compliant or fulfilled only when all systems in scope are reviewed, not just a sample.

Redspin, a division of Clearwater, has become one of the most trusted cybersecurity companies for the Defense Industrial Base. The company's exclusive focus on tailoring our CMMC assessment, training, consulting, and managed services for each client delivers peace of mind by lowering the risk of a security incident or breach, and meeting/maintaining compliance regulations. Since our founding in 2001, we've become a thought leader in IT security, helped countless clients control their security risk, develop their security strategy, and avoid a breach headline.

Redspin
A Division of Clearwater

Talk with us:

- www.Redspin.com/contact
- email: info@redspin.com