A new frontier in Cybersecurity certifications: the CMMC

By Gerico Security Srl (www.gerico-sec.it)

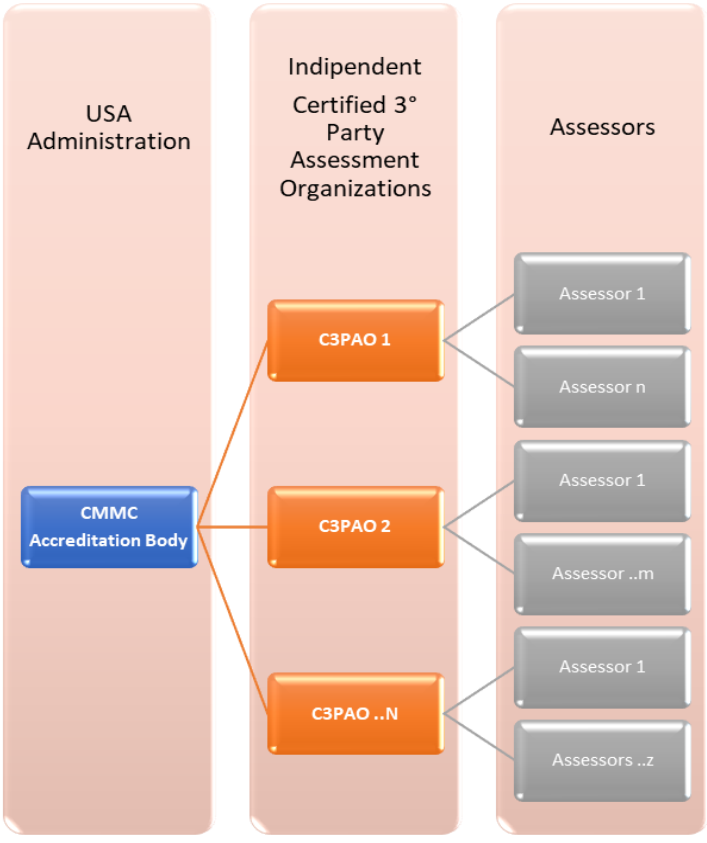
The US Department of Defense (*DoD*) has released the version 1.0 of a new certification standard since the end of January 2020**. It is the Cybersecurity Maturity Model Certification (CMMC) which is a mandatory certification for all those who will respond to an RFQ from next autumn. Therefore, considering over 300.000 suppliers (yes three hundred thousand), I would say that the audience involved is impressive.

The certification procedures are unknown at this stage indeed, at the present time, the CMMC Accreditation Body is working with the aim of defining the most appropriate modalities to meet the DoD needs and adequate levels of impartiality. Furthermore, the administration has made it clear that certification costs will be based on of the entire supply, not only the giants of military supplies that are in the front line but also small and very small business, included at the end of the supply chain. Nevertheless, the certification hierarchical scheme of responsibility is clear:

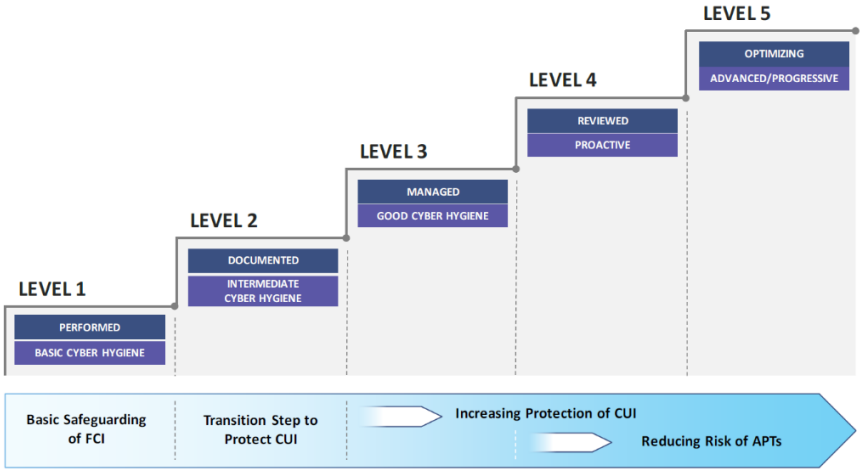
First level CMMC Accreditation Body is tasked with setting all the certification rules and accrediting C3PAO (Certified 3rd Party Assessment Organization) which are the certification bodies entitled to grant the certificates. C3PAO will avail themselves of Assessors (Auditors) in pursuit of compliance verification with the standard.

There is nothing new under the sun, but at the moment, apart from the CMMI Institute , which has supported the DoD in setting the standard, there is no news (there are only rumors) about other bodies that have applied for accreditation.

Everything should be more specific in June as the first round of Trainers and courses for Assessors is expected. On the other hand, as far as the most complex audits are concerned (related to the Level 5), the Assessors can be appointed by the DoD or at least by trusted bodies.



So how come that a new certification is required? Self-assessments of and self-certifications about the "cyber-posture" were enough to meet the requirements for working with the DoD for those that did not have to handle classified information and in the case in which other laws and regulations were issued. Needless to say that the DoD found out (all the world is the same) that over 90% of the statements were not so truthful!



The CMMC provides for 5 certification levels.

The Level 1 sets forth minimum measures to prevent disclosure of FCI -Federal Contract Information, or of information not intended for the public domain, which would be defined as "for internal use" in business terms, or covered information to which users can have limited access based on the *Need- to- Know* principle. From Level 2 onwards, it is about protecting the CUI - Controlled Unclassified Information, that includes all the information which would be defined as "Confidential" in business terms but which is not classified according to the Executive Order 13526 or the Atomic Energy Act; it is included the "NATO restricted" information and the "NATO Unclassified" information and all the "Controlled Technical Information"[1][2] for the Defense

The certification Level 1 is mandatory for all suppliers then, it levels up to Level 5 according to the types of supply or data that are treated or shared with the Administration.

According to the explanations provided by the DoD, we can assume that Level 2 is just a transitional step to Level 3, while Levels 4 and 5 are mainly for Prime contractors. Therefore, the tendering procedure will probably be set for Levels 1 (as minimum standard) and for Level 3 as a next step then, for prime Level 4 or Level 5 on the basis of the project/plan criticality accordingly. This means that, apart from the "Bigs" of the Defense that will have to deal with Levels 4 and 5, the suppliers of "significant" supply activities are likely to be certified according to Level 3.

Likely, the whole organization is not to be certified likewise it is not required for ISO27001, while the activities, processes and infrastructures within the perimeter related to the tendering procedure are to be certificated wherever, according to the ISO, they are within the "Area of application". For the main corporations, this might mean more certifications for different sectors of activity.

Taking into consideration not only the USA but also worldwide, this process will take place gradually from the "Bigs" to the others following a descending order accordingly.

---

[1] Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents."

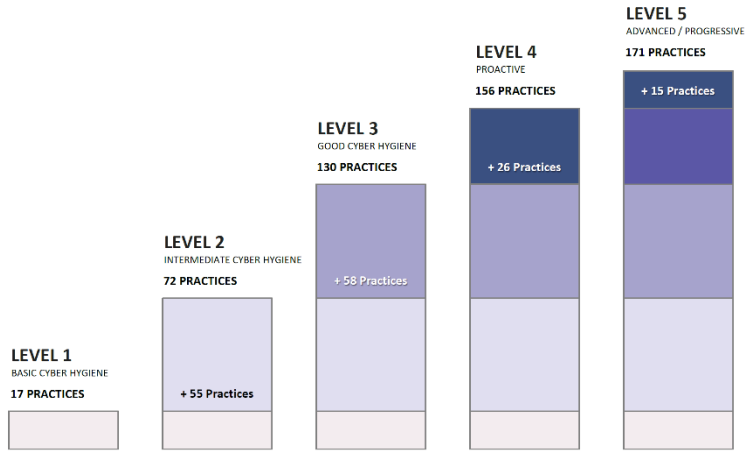
[2] "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data – Non-commercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

CMMC: the new Standard based on Maturity Model

In pursuit of different security level requirements and according to the information to be treated, the Cybersecurity Maturity Model Certification is based on increasing security measures from Level 1 to Level 5; each lever is built on and improves the level below. 17 Capability Domains are identified, each of them provides a set of Practices (security measures), that are increased for each certification Level. The CMMC, which is similar to the ISO27001, contemplates technological issues, people management and process implementation; Capability Domains can be considered as the Controls Objective of ISO27001 and Practices as the Controls of ISO27001. However, as far as implementing measures are concerned, US regulations are more detailed than ISO standards referring to the whole relevant NIST e FIPS regulatory framework.

Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	

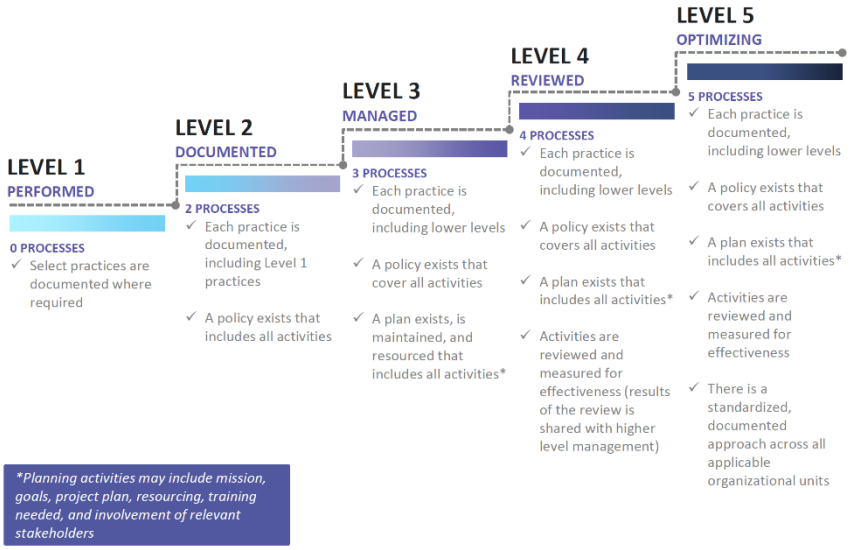
The security measures have been defined by referring to the main regulations used within the Federal area. In particular, who is to deal with Level 3 will have to consider all NIST SP800-171r1 controls together with a set of 20 controls for a total of 130 Practices, while, as far as Level 4 and 5 are concerned, there are also additional control inherited from NIST SP800-171B coming to 171 Practices.



In addition, the CMMC requires appropriate levels of process Maturity that lead the Practices. We have already seen process evaluations by using Maturity Models e.g. using Cobit 5; the CMMC requires the simultaneous maturity assessment of the applicable Capability Domains. A specific certification Level will be achieved if both the maturity level of the Practice and its process is ensured simultaneously. For instance, in order to achieve the Level 3, the 130 Practices, which pertain to the specific Level 3, are to be implemented and their related processes need to be at the “Managed” level; the lack of one of the requirements leads to a lower level of certification.

No reference is made to a management System. Nevertheless, the measures as a whole lead to an equivalent result. Indeed, reading the Practices at the Level 2 carefully “ System Security Plans are to be developed, documented and periodically updated” and “Security Controls are to be checked periodically to verify if they are effective within their implementation over time ” and at Level 3, continuous monitoring measures are to

be defined to facilitate awareness of threats and vulnerabilities, maintaining under control the whole information security posture within the certification perimeter.



The CMMC seems poised to be the new standard for the entire United States Federal and State Administration and probably also for the U.S B2B. Will it have effects on Europe like a long wave replacing ISO27001? It can be said that the ensuing ENISA certifications will give a wink to the CMMC.

**The figures in the text, apart from the first one, are taken from CMMC V1.0 official documentation*

*** CMMC V1.02 was released at the end of march. It includes only few adjustment and corrections.*

Gerico Security Srl (www.gerico-sec.it)

It is a consulting and business-integrated services company on risk management Information & Cyber Security and Business Continuity. It has been set up by specialists of the sector to satisfy the demand for security. The expertise has been acquired by and based on the activity of design and development of real-time systems, carried out over the years (Space and Telecommunications) together with a supporting activity to major critical infrastructures (Telecommunication and gas transportation and storage) in the sector of Information Security and business Continuity and to large and small-sized enterprises within financial, insurance and value-added fields.

The company is ISO27001 certified (Certification n. 57112, issued by CSQA, expire date 26/11/2022), it provides specialist consulting services, assessment, internal and third-party audit activities, personnel training, support for business process certifications and key-in- hand project services of Governance Risk & Compliance.

GeRiCO Security Srl
Sede legale Via Passerini, 2 20900 Monza (MB)