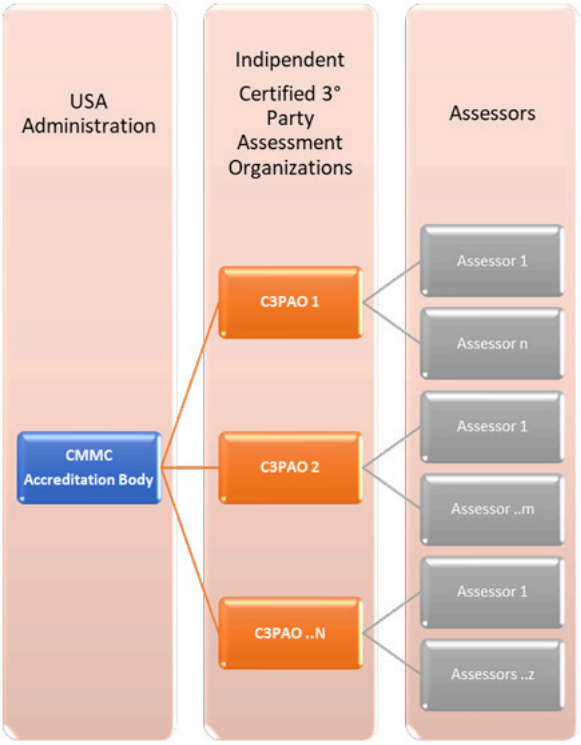
Una nuova frontiera nelle certificazioni di sicurezza cyber: Il CMMC

A cura di: Giustino Fumagalli e Paolo Sferlazza 30 Marzo 2020

Da fine gennaio 2020, il *Department of Defence americano* (DoD) ha rilasciato la versione 1.0 di un nuovo standard di certificazione, il *CyberSecurity Maturity Model Certification* **(CMMC)**, certificazione obbligatoria per tutti coloro che risponderanno a una RFQ dal prossimo autunno. E con oltre 300.000 (sì, trecentomila) fornitori, la platea interessata è impressionante.

Le modalità di certificazione non sono ancora note; infatti in questo momento il CMMC *Accreditation Body* è al lavoro per definire le modalità più idonee a garantire le necessità del DoD e adeguati livelli di imparzialità. Inoltre, l'amministrazione ha tenuto a precisare che i **costi di certificazione** terranno conto delle possibilità dell'intera filiera, che vede in prima fila i colossi delle forniture militari ma anche piccole e piccolissime imprese al termine della catena di fornitura.



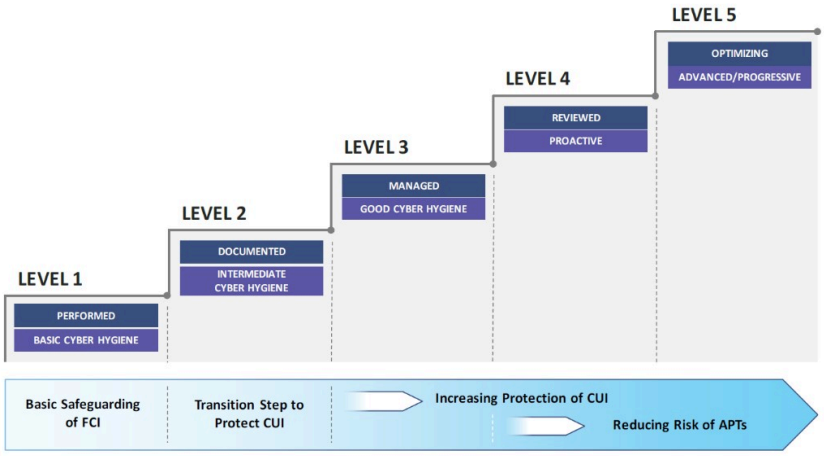
Lo schema gerarchico di **responsabilità** per la certificazione è comunque chiaro: al primo livello troviamo il CMMC *Accreditation Body*, che ha il compito di definire tutte le regole per la certificazione e di accreditare le C3PAO (*Certified 3rd Party Assessment Organization*), ovvero gli enti di certificazione che poi rilasceranno i certificati.
Le C3PAO si avvalleranno degli *Assessors* (ovvero *Auditors*) per effettuare le attività di verifica di conformità allo standard.

Nulla di nuovo sotto il sole, ma al momento – a parte il CMMI Institute che ha supportato il DoD nella realizzazione della norma -, non si hanno notizie (bensì soltanto voci) su altri enti che abbiano chiesto l'accreditamento.

A giugno dovrebbe essere tutto più chiaro, visto che è prevista la prima tornata di training e corsi per gli *Assessors*. Tuttavia, si deve considerare che per le verifiche più complesse (relative al Livello 5) è previsto che gli *Assessors* possano essere nominati dal DoD o, comunque, di sua fiducia.

Ma **perché una nuova certificazione?** A chi non doveva operare su informazioni classificate, ove insistono altre norme e regole, per lavorare con il DoD bastava effettuare un *self-assessment* e autocertificare la propria "cyber-posture"; il DoD ha scoperto (tutto mondo è Paese!) che oltre il 90% delle dichiarazioni non erano esattamente vere!

Il CMMC prevede **cinque livelli** di certificazione.



Il Livello 1 stabilisce le misure minime atte a garantire che non vengano esposte all'esterno le FCI -Federal Contract Information, ovvero le informazioni non destinate al pubblico dominio che definiremmo in termini aziendali "ad uso interno" o riservate a chi le

deve conoscere in base al principio del *Need to Know*. Dal Livello 2 in poi si tratta di proteggere le CUI – *Controlled Unclassified Information*, ovvero tutte quelle informazioni che definiremmo in termini aziendali "Confidenziali" ma non classificate secondo l'Executive Order 13526 o l'Atomic Energy Act; tra queste abbiamo le "NATO restricted" e "NATO Unclassified" e, per la Difesa, tutte le "Controlled Technical Information"[1][2].

Il Level 1 di certificazione è obbligatorio per tutti i fornitori; poi, in base al tipo di commessa o di dato scambiato e gestito con l'Amministrazione, si sale di Livello sino al Level 5.

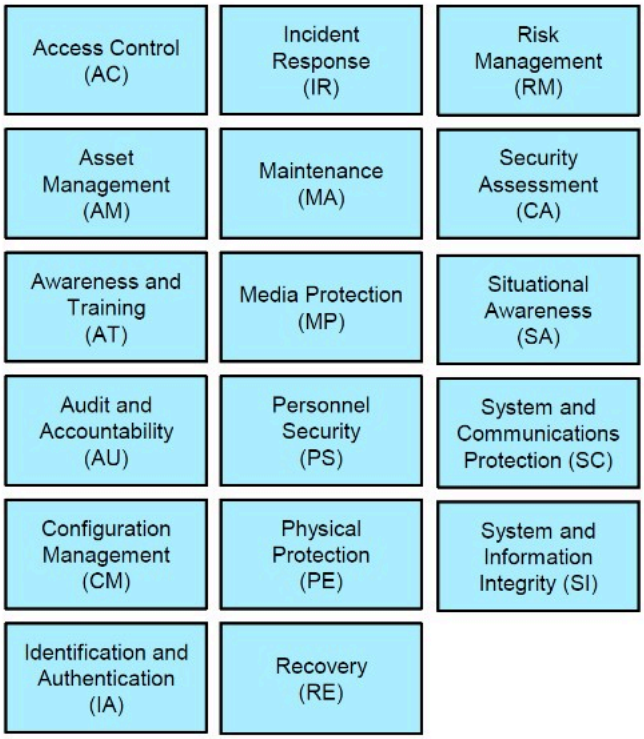
Dalle spiegazioni fornite dal DoD si può dedurre che in realtà il Level 2 sia solo un passo transitorio al Level 3, mentre i Level 4 e 5 riguardano prevalentemente i *Prime contractors*. Probabilmente avremo quindi requisiti di Gara che prevedono i Livelli 1 (come standard minimo), poi Level 3 e per i *Prime* Level 4 o Level 5 in base alla criticità del progetto/programma. Questo vuol dire che a parte i "Big" della Difesa a cui toccheranno i Level 4 e 5, i fornitori di parti "pregiate", dovranno presumibilmente certificarsi per il Level 3.

Come per la ISO27001 è presumibile che non necessariamente tutta la società dovrà essere certificata: basterà invece il perimetro ove si svolgono le attività relative alla Gara, i relativi processi e infrastrutture, quello che nella ISO sono nel "Campo di Applicazione". Per le **aziende più grandi**, questo potrebbe significare il dover avere più certificati per ambiti produttivi diversi.

Dato il numero di aziende coinvolte – non solo negli USA ma nel mondo intero – questo processo avverrà per gradi, partendo proprio dai "Big" per poi coinvolgere, a scendere, tutti gli altri.

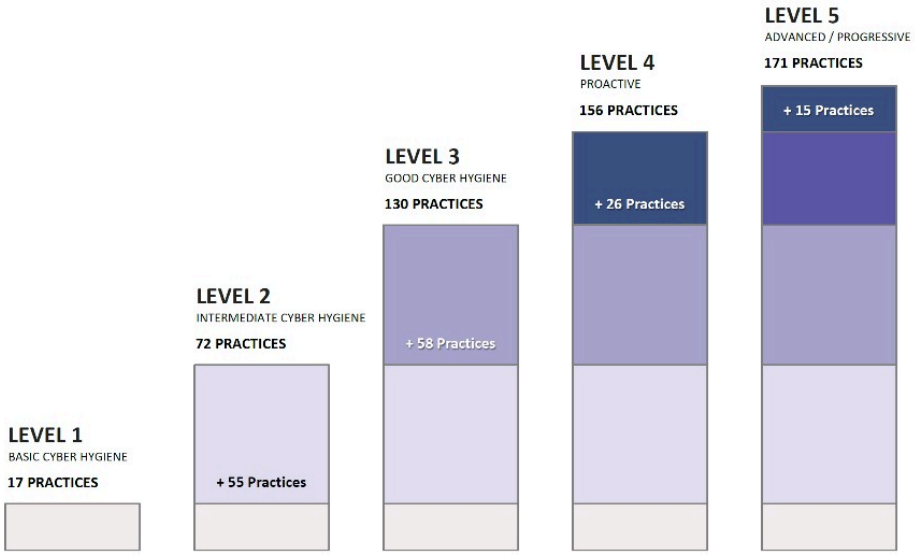
CMMC: Il nuovo Standard basato sul Maturity Model

Volendo avere diversi livelli di requisiti di sicurezza in base alle informazioni da trattare, il Cybersecurity Maturity Model Certification è disegnato a livelli crescenti di misure di sicurezza, appunto dal Level 1 al Level 5; ogni livello si appoggia e migliora quello sottostante.



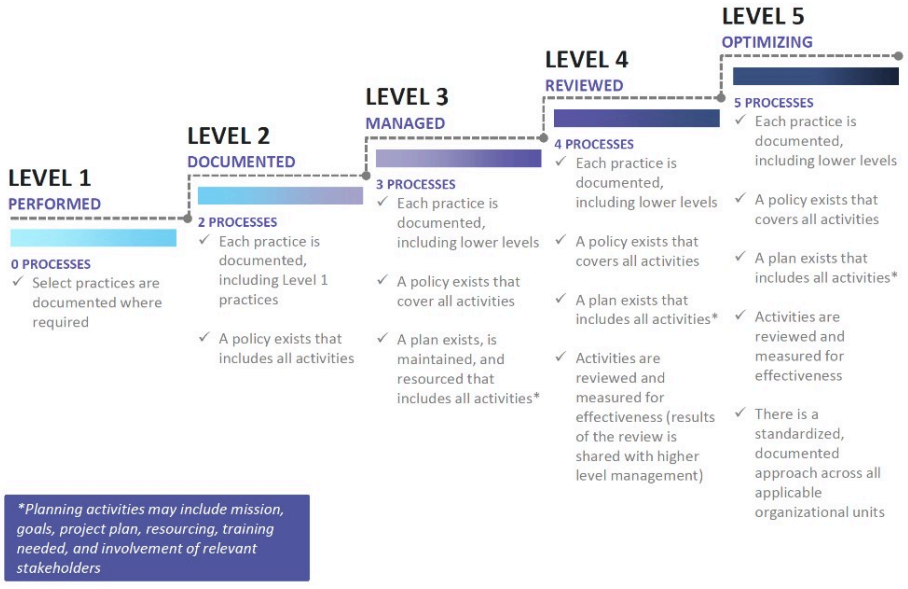
Vengono identificati 17 *Capability Domains*, ognuno delle quali prevede **un insieme di *Practices*** (misure di sicurezza), che si accrescono per ogni Livello di certificazione. Il CMMC, come la ISO27001, è orientato sia agli aspetti tecnologici sia alla gestione delle persone e di come sono implementati i processi; possiamo quindi vedere i *Capability Domains* come i *Controls Objective* della ISO27001 e le *Practices* come i Controls ISO27001, anche se rispetto alla ISO le norme americane entrano maggiormente nel dettaglio delle misure da implementare, facendo sostanzialmente riferimento a tutto il *framework* normativo NIST e FIPS pertinente.

Le misure di sicurezza sono state definite avendo a riferimento le principali norme già utilizzate in ambito Federale: in particolare chi approccerà il Level 3 avrà come riferimento tutti i controlli della NIST SP800-171r1 più un altro set di 20 controlli per un totale di 130 *Practices*, mentre per i Level 4 e 5 vi sono, tra le altre cose, ulteriori controlli ereditati dalla NIST SP800-171B arrivando a 171 *Practices*.



Il CMMC richiede inoltre di garantire adeguati **livelli di maturità dei processi** che guidano tali *Practices*. Valutare i processi per mezzo di un *Maturity Model* lo abbiamo già visto, ad esempio con il Cobit 5; il CMMC richiede di valutare contestualmente la maturità dei *Capability Domains* applicabili. Si raggiunge un determinato Level di certificazione se **contemporaneamente** si garantiscono, oltre alle *Practices* richieste, l'opportuno livello di maturità del processo afferente quelle *Practices*. Ad esempio, se si deve raggiungere il Level 3, dovranno essere implementate le 130 *Practices* caratteristiche di quel livello e i processi a loro afferenti dovranno essere **tutti** a livello *"Managed"*; la mancanza di uno dei requisiti porta a certificarsi al livello inferiore.

Anche se non si fa mai riferimento a un sistema di gestione, le misure nel loro complesso portano a un risultato equivalente. Infatti, se si vanno a leggere con attenzione le *Practices*, già al Level 2 abbiamo da "Sviluppare, documentare e periodicamente aggiornare i System Security plans" e periodicamente "Verificare i *Security Controls* nel sistema organizzativo al fine di verificare se siano efficaci nella loro applicazione nel tempo" e al Level 3 si devono definire **misure per il monitoraggio** continuo che faciliti la consapevolezza di minacce e vulnerabilità emergenti avendo sotto controllo lo stato complessivo della Sicurezza delle Informazioni nel perimetro in certificazione.



Il CMMC sembra destinato a diventare il nuovo standard per tutta l'amministrazione federale e statale statunitense, e probabilmente anche per il B2B americano. Potrà avere l'onda lunga in Europa e soppiantare la ISO27001? Diciamo che anche le future certificazioni ENISA, inevitabilmente, strizzeranno l'occhio al CMMC.

**Le figure presenti nel testo, ad eccezione della prima, sono tratte dalla documentazione ufficiale del CMMC V1.0.*

Note

[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 – Noncommercial 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.*

Articolo a cura di **Giustino Fumagalli** e **Paolo Sferlazza**

Profilo Autore

Giustino Fumagalli

Socio fondatore di Gerico Security Srl (www.gerico-sec.it) opera come Chief Information Security Officer e garantisce consulenze direzionali nel campo della sicurezza delle informazioni e continuità operativa.
Con un importante passato nella progettazione di software real-time e project management per sistemi spaziali e telecomunicazioni, ha partecipato a progetti civili e militari internazionali, anche di protezione civile e protezione delle infrastrutture critiche. Supporta le aziende nella gestione dei rischi, nella realizzazione di programmi di information security e continuità operativa, eventualmente accompagnandole nell'ottenimento della certificazione ISO/IEC 27001, ISO 22301 e della nuova certificazione americana CMMC. Inoltre, segue direttamente le tematiche legate all'Industrial Security, e alle evoluzioni in materia di "Security for Safety" nel mondo Navale ed in quello Aeronautico, quali le norme ED202A e ED203A.
È certificato Senior Security Manager UNI10459:2017, in accordo al Decreto del Ministero dell'Interno n.269/2010 e al disciplinare del 24 febbraio 2015 del Capo della Polizia. È inoltre certificato PMP per il Project Management, CISM, CRISC di ISACA per l'information security, CBCP in materia di Business Continuity, Lead Risk manager ISO31000, è infine qualificato Lead Auditor ISO27001 e Lead Auditor ISO22301.

Profilo Autore

Paolo Sferlazza

Socio fondatore di Gerico Security Srl lavora come advisor, auditor e trainer nel campo della sicurezza delle informazioni, continuità operativa, gestione dei servizi IT e sicurezza delle carte di pagamento.
Ha accompagnato primarie aziende e infrastrutture critiche italiane nell'ottenimento della certificazione ISO/IEC 27001, ISO 22301 e ISO/IEC 20000.
È un Qualified Security Assessor riconosciuto dal PCI Council per la certificazione dei sistemi di pagamento PCI DSS.
Ha conseguito la certificazione CISA, CISM, CRISC di ISACA, ed è auditor qualificato e tiene docenze sugli schemi ISO/IEC 27001, ISO 22301, ISO/IEC 27001 e ISO 9001 ed è iscritto ai registri AICQ SICEV quale auditor sulla sicurezza delle informazioni e continuità operativa. Ha inoltre ottenuto altre certificazioni nel campo della sicurezza delle informazioni e dell'IT governance tra cui OPST, COBIT e ITIL. Ha progettato ed erogato docenze, anche in ambito militare, su tematiche di Information Risk Management, ITIL. Ha effettuato audit interno, assessment e consulenza in merito all'accreditamento dei laboratori VA rispetto alla 17025. Si occupa si sicurezza delle informazioni nel mondo specifico dell'automotive in conformità con lo standard di settore TISAX.
Collabora con primari enti di certificazione come auditor di terza parte.