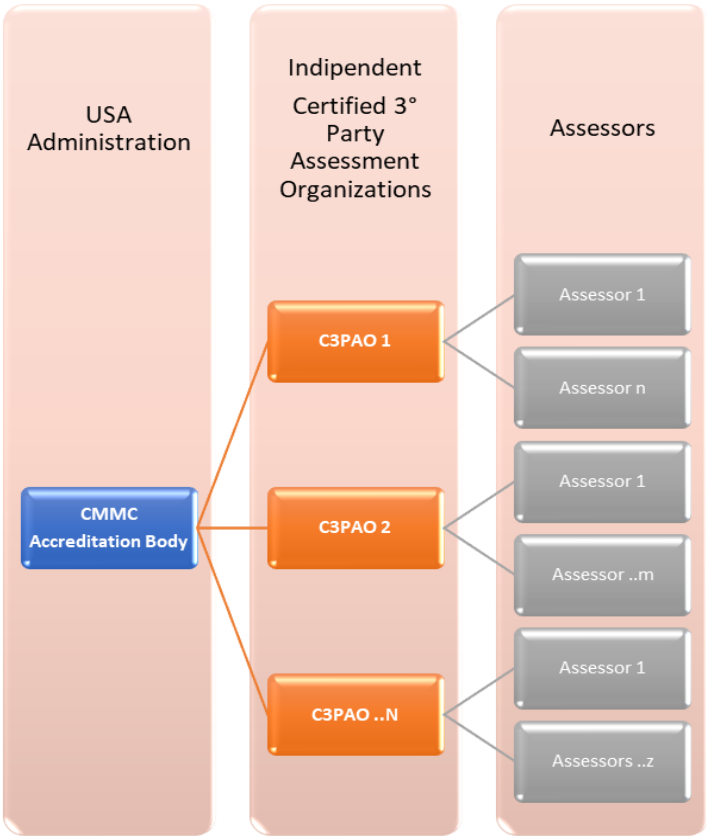
Una nuova frontiera nelle certificazioni di Cyber Sicurezza: Il CMMC

A cura di Gerico Security Srl

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 ad una RFQ dal prossimo autunno. E con oltre 300.000 (si trecentomila) fornitori, direi che 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:

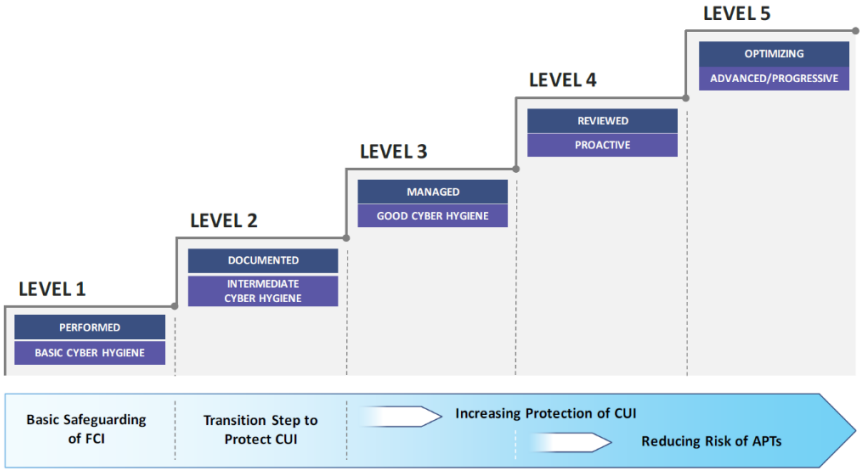


al primo livello troviamo il CMMC Accreditation Body, che ha il compito di definire tutte le regole per la certificazione, e di accreditare le C3PAO (Certified 3rd Party Assessment Organization) ovvero gli enti di certificazione che poi rilasceranno i certificati. Le C3PAO si avvalleranno degli Assessors (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 (ma solo voci) su altri enti che abbiano chiesto l'accreditamento.

A giugno dovrebbe essere tutto più chiaro, visto che è prevista la prima tornata di Trainers 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 auto certificare 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 5 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 or l'Atomic Energy Act; tra queste abbiamo le "NATO restricted" e "NATO Unclassified", e per la Difesa tutte le "Controlled Technical Information"[12].

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, invece basterà il perimetro ove si svolgono le attività relative alla Gara, i relativi processi ed infrastrutture, quello che nella ISO sono nel "Campo di Applicazione". Per le più grandi aziende 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, questo processo avverrà per gradi, partendo proprio dai "Big" e a scendere tutti gli altri.

---

[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."

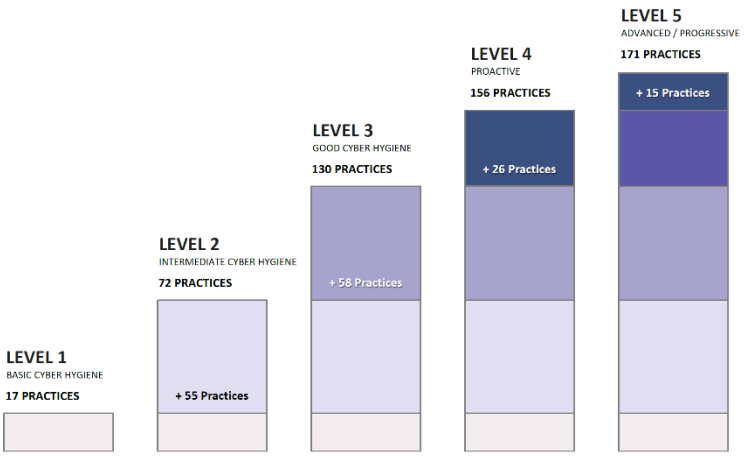
[2] "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering 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.

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 Practice (misure di sicurezza), che si accrescono per ogni Livello di certificazione. Il CMMC, come la ISO27001 è orientata 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 Practice 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.

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)	

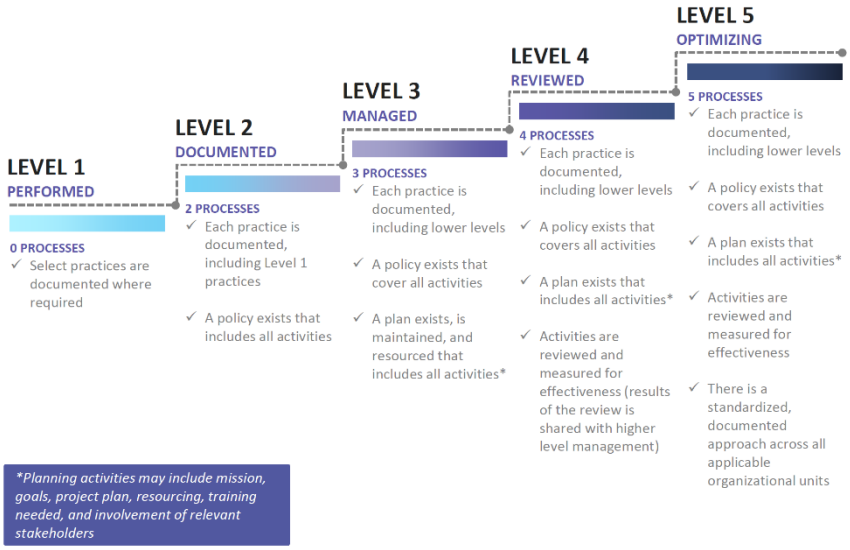
Le misure di sicurezza sono state definite avendo a riferimento le principali norme già utilizzate in ambito Federale, in particolare chi approccerà il Level 3 avrà come riferimento tutti i controlli della NIST SP800-171r1 più un altro set di 20 controlli per un totale di 130 Practice, mentre per i Level 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 Practice. 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 Practice richieste l'opportuno livello di maturità del processo afferente quelle Practice. Ad esempio, se si deve raggiungere il Level 3, dovranno essere implementate le 130 Practice 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 ad un Sistema di gestione le misure nel loro complesso portano ad un risultato equivalente. Infatti, se si vanno a leggere con attenzione le Practice 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 americana, 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*

*** A marzo 2020 il DoD ha rilasciato la versione 1.02 del CMMC con lievi correzioni ed aggiustamenti*

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

Azienda di consulenza specialistica e supporto integrato in tema di Gestione dei rischi, Information & Cyber Security e Business Continuity. Nasce da specialisti del settore per dare concretezza alla domanda di Security basandosi sulla esperienza maturata negli anni nella progettazione e sviluppo di sistemi real-time (Spazio e Telecomunicazioni), nel supporto in tema di Information Security e Continuità Operativa a grandi Infrastrutture critiche (Trasporto e stoccaggio Gas e Telecomunicazioni) e a diverse realtà grandi e piccole di società nel settore finanziario, assicurativo e di servizi a valore aggiunto.

L'azienda, certificata ISO27001 (Certificato n.57112 rilasciato da CSQA, Scadenza 26/11/2022), eroga servizi di consulenza specialistica, attività di assessment e audit interni e su terze parti, formazione, supporto alla certificazione di processi aziendali e realizzazione di progetti di Governance Risk & Compliance chiavi in mano.