Agenzia per la
Cybersicurezza Nazionale

# Linee guida per l'applicazione dei criteri di premialità

## di cui all'articolo 14 della legge n. 90/2024

sentita l'Autorità nazionale anticorruzione

Ottobre 2025

# INDICE

**1. Premessa** ..... **1**

1.1. Quadro normativo di riferimento ..... 1

**2. Ambito di applicazione** ..... **4**

2.1. Ambito di applicazione soggettivo ..... 4

2.2. Ambito di applicazione oggettivo ..... 4

2.2.1. Tecnologie di cybersicurezza ..... 4

**3. *Bill of materials*: finalità ed elementi necessari** ..... **6**

3.1. Elementi necessari: ampiezza e profondità della BOM ..... 6

**4. Nazionalità della tecnologia di cybersicurezza** ..... **8**

4.1. Criteri valutativi ..... 8

**5. Criteri di premialità** ..... **9**

5.1. Natura obbligatoria del criterio di premialità ..... 9

5.2. Modalità di calcolo e ponderazione del criterio di premialità ..... 9

5.3. Clausole tipo ..... 10

**6. Controlli e attività di verifica** ..... **11**

**7. Gare e lotti dedicati** ..... **12**

**APPENDICE TECNICA BOM** ..... **14**

**1. Struttura della BOM** ..... **15**

1.1. Profondità della BOM ..... 15

1.2. Ampiezza della BOM ..... 15

1.3. Formato di presentazione della BOM ..... 17

1.3.1. BOM applicata ai prodotti ..... 17

1.3.2. BOM applicata ai servizi ..... 17

1.4. Campi minimi della BOM rilevanti ai fini della premialità ..... 18

1.5. Campi ulteriori della BOM non rilevanti ai fini della premialità ..... 19

1.6. Schema riassuntivo delle caratteristiche per la corretta formattazione della BOM ..... 19

**2. Dettaglio dei campi minimi e dei campi ulteriori ..... 21**

2.1. Campi minimi per componenti/servizi ..... 21

2.2. Campi ulteriori per componenti/servizi ..... 22

3. Strumenti utilizzabili al fine di creare, validare, analizzare, firmare e convertire una BOM ..... 24

4. Esempio di BOM ..... 25

**APPENDICE TECNICA TELCO - APPLICAZIONE DEL CRITERIO DI PREMIALITÀ AI SISTEMI E AI SERVIZI 4G E 5G (SA E NSA) ..... 30**

**1. Applicazione del criterio di premialità ai sistemi e servizi di telefonia mobile 4G e 5G (SA e NSA) .... 31**

# 1. Premessa

L'Agenzia per la cybersicurezza nazionale (ACN), quale Autorità nazionale di cybersicurezza ai sensi del decreto-legge 14 giugno 2021, n. 82, cura e promuove un quadro normativo aggiornato e coerente nel dominio della cybersicurezza, al fine di assicurare – anche tramite lo sviluppo e la diffusione di standard, linee guida e raccomandazioni – precipuamente la tutela della sicurezza nazionale nello spazio cibernetico.

In un contesto caratterizzato da un'evoluzione tecnologica rapida e continua, un elemento essenziale di tutela della cybersicurezza è la gestione del rischio intrinseco alla catena di approvvigionamento, che rappresenta uno dei principali vettori di attacco. I fornitori di software, hardware o servizi IT sono spesso le iniziali vittime di un più ampio attacco cyber, i cui sistemi sono utilizzati per introdurre elementi malevoli prima della distribuzione o durante gli aggiornamenti, in modo da compromettere le infrastrutture digitali su vasta scala.

In questo quadro di sviluppo tecnologico e di progressiva sofisticazione della minaccia cibernetica, è dunque essenziale, ai fini della tutela della sicurezza nazionale nel cyberspazio, assicurare che gli approvvigionamenti di prodotti e servizi tecnologici tengano in debita considerazione, anche in relazione al contesto d'uso, i profili di cybersicurezza.

In tal senso si dirige l'intervento del legislatore con l'articolo 14 della legge 28 giugno 2024, n. 90 (d'ora in poi "articolo 14"), a cui ha fatto seguito il DPCM 30 aprile 2025, pubblicato nella G.U. n. 102 del 5 maggio 2025 – da ultimo aggiornato dal DPCM 2 ottobre 2025, pubblicato nella G.U. n. 243 del 18 ottobre 2025 – che ne rappresenta il primo e principale strumento di attuazione (d'ora in poi "DPCM").

La lettura sistematica dei predetti provvedimenti, nella parte in cui essi esplicitano l'esigenza di promuovere l'autonomia tecnologica e strategica del Paese in un contesto di sicurezza nazionale, rafforza il concetto di sovranità digitale, intesa innanzitutto come sovranità sul dato.

Ciò premesso, si è ritenuto di dover adottare le presenti Linee guida sentita l'Autorità nazionale anticorruzione (ANAC), in considerazione delle relative funzioni di vigilanza sull'affidamento e l'esecuzione dei contratti pubblici, anche di interesse regionale, di lavori, servizi e forniture nei settori ordinari e nei settori speciali e sui contratti secretati o che esigono particolari misure di sicurezza, nonché sui contratti esclusi dall'ambito di applicazione del Codice dei contratti pubblici. Alla stessa Autorità fa capo, inoltre, la promozione dell'efficienza, della qualità dell'attività delle stazioni appaltanti attraverso bandi-tipo, capitolati-tipo, contratti-tipo e altri atti amministrativi generali, favorendo lo sviluppo delle migliori pratiche e facilitando, a supporto delle amministrazioni aggiudicatrici, lo scambio di informazioni e l'omogeneità dei procedimenti amministrativi.

Il presente documento, pertanto, ha anche lo scopo di fornire, ai soggetti pubblici e privati destinatari, un'illustrazione delle migliori pratiche e chiarimenti operativi, in considerazione della complessità e novità della materia.

## 1.1. Quadro normativo di riferimento

Tra gli interventi più rilevanti, insieme all'adozione della Direttiva (UE) 2022/2555 (direttiva NIS2), il cui recepimento nell'ordinamento italiano è avvenuto con il decreto legislativo 4 settembre 2024, n. 138, e che

prevede un significativo ampliamento delle misure a protezione della superficie digitale dell'Unione, si colloca la già citata legge n. 90/2024.

Il contesto normativo in cui si colloca questa legge è caratterizzato da una crescente attenzione alla sicurezza cibernetica, riflessa anche in precedenti provvedimenti legislativi, come il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, che ha posto le basi per la creazione del Perimetro di sicurezza nazionale cibernetica, con l'obiettivo di identificare i soggetti strategici per la sicurezza nazionale e stabilire procedure specifiche per la protezione delle loro infrastrutture digitali.

Come anticipato in premessa, la legge n. 90/2024 è intervenuta anche nell'ambito del *procurement*, data la richiamata rilevanza dei processi di approvvigionamento di beni e servizi informatici.

Tale intervento si inserisce in un quadro normativo nel quale il Codice dei contratti pubblici (di cui al decreto legislativo 31 marzo 2023, n. 36) già contempla, all'art. 108, comma 4, disposizioni specifiche in materia di approvvigionamento di beni e servizi digitali, prevedendo che, in tali attività, le stazioni appaltanti – incluse le centrali di committenza – ai fini dell'individuazione del miglior rapporto qualità-prezzo per l'aggiudicazione, tengano sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego sia connesso alla tutela degli interessi nazionali strategici. Nei suddetti casi, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 10 per cento.

Ulteriori corollari del citato art. 108 del Codice dei contratti pubblici, onde meglio definirne e circoscriverne l'ambito applicativo, vengono poi declinati dall'articolo 14, comma 2, lettere da *a)* a *d)*, della legge n. 90/2024, rappresentando così, per le amministrazioni appaltanti, un sicuro parametro di riferimento allorché vengano in evidenza, per le relative attività di *procurement*, esigenze di tutela della cybersicurezza.

La lettera *e)* del soprarichiamato comma 2 stabilisce, inoltre, che siano previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso "*di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti alla NATO o di Paesi che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle infrastrutture classificate, ricerca e innovazione".* Gli stessi sono stati individuati con il DPCM nell'Allegato 3[1].

È importante sottolineare come il DPCM, in attuazione dello stesso articolo 14, preveda che le disposizioni sulla premialità riguardino una platea che contempla i soggetti che, inclusi nel Perimetro, abbiano la veste di amministrazioni pubbliche o di ente pubblico, ovvero siano entità private, pure nei casi in cui queste ultime non siano tenute al rispetto del Codice dei contratti pubblici, come meglio si dirà appresso. Con particolare riferimento, infine, ai servizi e ai sistemi di telefonia mobile 4G e 5G (in versione sia *stand-alone* che *non stand-alone*), e alle loro successive evoluzioni tecnologiche, è sempre prevista l'applicazione dei criteri di premialità da parte delle amministrazioni rappresentate nel Comitato interministeriale per la sicurezza della Repubblica di cui all'articolo 5 della legge 3 agosto 2007, n. 124 (amministrazioni CISR), in ragione della connessione di queste ultime con le funzioni di tutela della sicurezza nazionale.

[1] Per pronto riferimento, si rammenta che i Paesi individuati sono: Australia, Corea del Sud, Giappone, Israele, Nuova Zelanda e Svizzera.

Detto ciò riguardo all'elemento soggettivo, va altresì precisato, quanto all'elemento oggettivo, che i presupposti per l'applicazione delle disposizioni in tema di premialità vengono a sussistere nei casi in cui i soggetti tenuti al loro rispetto debbano acquisire "tecnologie di cybersicurezza", per la cui identificazione si assume a criterio guida quanto specificato dal DPCM. È infatti questo il provvedimento da cui enucleare, nell'ambito delle più vaste categorie tecnologiche individuate nell'Allegato 2 dello stesso decreto, quelle a cui collegare l'applicazione delle disposizioni sulla premialità. Riguardo a tale profilo, si rinvia al paragrafo 2.2.1.

# 2. Ambito di applicazione

## 2.1. Ambito di applicazione soggettivo

Come anticipato in Premessa, i soggetti tenuti all'applicazione della disciplina in parola sono i soggetti pubblici e privati inclusi nel Perimetro di sicurezza nazionale cibernetica, anche nella loro veste di stazioni appaltanti, individuati conformemente alla procedura di cui all'art. 1, comma 2-*bis*, del decreto-legge n. 105/2019. Con specifico riferimento ai servizi e ai sistemi di telefonia mobile sopra richiamati, l'ambito soggettivo di applicazione della suddetta disciplina riguarda parimenti – in ragione della loro connessione con le funzioni di tutela della sicurezza nazionale – le amministrazioni CISR.

Quanto, in particolare, ai soggetti privati, gli stessi, pure nelle ipotesi in cui non siano tenuti, nella scelta del contraente, al rispetto del decreto legislativo n. 36/2023, sono chiamati a tenere in considerazione, ai sensi dell'articolo 14, il criterio di premialità, nelle modalità di cui al paragrafo 5.

Inoltre, seppur non inserite nel Perimetro di sicurezza nazionale cibernetica, rientrano nell'ambito di applicazione anche le centrali di committenza, come definite all'art. 1, lett. *i)*, dell'Allegato I.1 al decreto legislativo n. 36/2023, che vengono in rilievo in virtù del loro ruolo di supporto alle pubbliche amministrazioni nell'ambito delle procedure di approvvigionamento di beni e servizi ICT e che indicono le procedure per l'acquisizione dei beni e servizi di cui al paragrafo 2.2.

Tutti i soggetti individuati nel presente paragrafo, laddove il riferimento ad essi sia complessivo e unitario, verranno nel prosieguo indicati come "*soggetti acquirenti*".

## 2.2. Ambito di applicazione oggettivo

Le procedure di approvvigionamento alle quali si applicano i criteri di premialità sono quelle volte ad acquisire tecnologie di cybersicurezza, come definite al successivo paragrafo 2.2.1 (ivi inclusi i servizi e i sistemi di telefonia mobile 4G e 5G, in versione sia *stand-alone* che *non stand-alone*, e loro successive evoluzioni tecnologiche), destinate ad essere utilizzate dai soggetti Perimetro sulle reti, sui sistemi informativi e sui servizi informatici di loro pertinenza inseriti nell'elenco dei c.d. "beni ICT" di cui all'art. 1, comma 2, lett. *b)*, del decreto-legge n. 105/2019, nonché quelle funzionali alla protezione fisica e logica dei predetti beni ICT. I criteri di premialità trovano, parimenti, applicazione, come anticipato, ai predetti servizi e sistemi di telefonia mobile comunque acquisiti dalle amministrazioni CISR.

### 2.2.1. Tecnologie di cybersicurezza

Nel contesto del DPCM, al fine di individuare le tecnologie di cybersicurezza a cui collegare l'applicazione delle disposizioni sulla premialità, occorre fare riferimento al più ampio ambito delle "categorie tecnologiche" già individuate dal DPCM all'Allegato 2, selezionando quelle che, secondo un principio generale di cybersicurezza, svolgono, sia prioritariamente, sia in via eventuale, funzioni di sicurezza e cioè funzioni in grado di impattare sulla sicurezza dei dati e delle informazioni, in termini di riservatezza, integrità e disponibilità.

Nell'ambito dell'Allegato 2 del DPCM, sono state individuate, pertanto, le seguenti tecnologie, distinte in due classi, separate al solo scopo di specificare che quelle di cui al punto *b)* comporteranno l'applicazione del criterio di premialità solo nei casi in cui esse siano preposte a funzioni di sicurezza informatica attinenti alla tutela del dato e delle informazioni:

a) tecnologie di cui ai numeri 1, 2, 3, 5, 6, 8, 9, 10, 11, 12, 13, 14, 16, 17, 20, 23;
b) tecnologie di cui ai numeri 4, 7, 15, 18, 19, 21, 22. Possono rientrare in tale ambito, a titolo esemplificativo, dispositivi di rete che abbiano anche funzioni di filtraggio dei flussi di dati (*screening router*), ovvero di controllo accessi logici (*switch* con *port security*); relativamente ai servizi cloud, rientrano in tale ambito le tecnologie erogate in modalità SaaS (*Software as a Service*) afferenti alle categorie di cui alla lett. *a)* (ad esempio, Sistemi di gestione delle informazioni e degli eventi di sicurezza "SIEM" erogati in modalità SaaS).

Considerato il particolare ambito di applicazione costituito dai servizi e dai sistemi di telefonia mobile 4G e 5G, in versione sia *stand-alone* (SA) che *non stand-alone* (NSA), e successive evoluzioni tecnologiche, l'applicazione del criterio di premialità è adattata allo specifico contesto riferito alle infrastrutture funzionali a tali sistemi e servizi e che ne costituiscono la dorsale tecnologica (e cioè le reti di telecomunicazione mobile 4G e 5G). Tale contesto applicativo viene dettagliato nella dedicata "Appendice Tecnica TELCO - Applicazione del criterio di premialità ai sistemi e ai servizi di telefonia mobile 4G e 5G (SA e NSA)".

# 3. *Bill of materials*: finalità ed elementi necessari

Il motivo per cui l'art. 4 del DPCM ha previsto che i soggetti interessati all'applicazione del criterio di premialità facciano riferimento alla "*Bill of Materials*" (d'ora in avanti, BOM) sta nel far sì che vengano esattamente individuati i luoghi di provenienza dei singoli componenti/servizi appartenenti alle tecnologie di cybersicurezza di cui al paragrafo 2.2.1. Va da sé, infatti, che la componentistica venga valutata con la più opportuna ampiezza e profondità, in maniera che l'applicazione del citato criterio risulti compiutamente aderente alla *ratio legis.* Fatto salvo quanto previsto dalla dedicata "Appendice Tecnica TELCO" in relazione ai sistemi e ai servizi di telefonia mobile 4G e 5G, in versione sia *stand-alone* (SA) che *non stand-alone* (NSA), e successive evoluzioni tecnologiche, alla quale si rinvia, appaiono adeguate a soddisfare tali esigenze le modalità di seguito illustrate, che tengono conto della struttura gerarchica ad albero della BOM[2]. Resta inteso che, al fine di poter valutare l'aderenza ai criteri di premialità, la compilazione della BOM dovrà essere eseguita dagli offerenti e acclusa alla proposta secondo un formato processabile digitalmente e di uso comune.

All'uopo, il formato più indicato (per l'illustrazione del quale si rinvia alla "Appendice Tecnica BOM") è il formato CycloneDX, versione 1.6[3], data la flessibilità nel rappresentare, con lo stesso *framework*, sia prodotti (definiti come *components* nel formato) che servizi (definiti come *services* nel formato). Tale strumento appare, allo stato dell'arte, sotto un profilo tecnico, quello più completo, adeguato e conferente rispetto alle informazioni funzionali alla predisposizione e alla valutazione della BOM ai fini della presente disciplina. Il ricorso a tale formato risponde, altresì, ad un'esigenza di semplificazione, nonché di aderenza ai principi di economicità, efficienza ed efficacia dell'azione amministrativa, derivanti dalla possibilità di adottare o sviluppare un unico *tool* volto alla predisposizione e all'analisi automatizzata della BOM. Si osserva, inoltre, che il formato CycloneDX è supportato da un ampio insieme di produttori di tecnologie ICT[4]. L'eventuale uso da parte dell'offerente di un formato diverso – di sostanziale equivalenza rispetto all'indicato standard – potrà comunque essere valutato dai soggetti acquirenti, nell'ambito delle loro procedure acquisitive.

## 3.1. Elementi necessari: ampiezza e profondità della BOM

Quale linea di indirizzo generale, come meglio dettagliato nell'Appendice Tecnica BOM, la struttura della "*Bill of Materials*" deve essere improntata al modello che prevede:

- a "livello 0" (livello radice), l'indicazione del bene o del servizio oggetto di descrizione;
- a "livello 1", un elenco di componenti/servizi di cui l'oggetto della fornitura è costituito. Per ogni componente/servizio appartenente al livello 1 non è richiesta, ai fini della premialità, l'indicazione del rapporto con componenti/servizi appartenenti ai sottostanti livelli. Tuttavia, pur non incidendo

[2] Al riguardo, si è tenuto conto, tra gli altri, del documento recentemente realizzato dal *Bundesamt für Sicherheit in der Informationstechnik* ("BSI") – "*Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products – Part 2*".

[3] La versione 1.6 del formato è stata standardizzata a livello industriale dall'*European Computer Manufacturers Association* ("ECMA") nel giugno 2024 (*https://ecma-international.org/publications-and-standards/standards/ecma-424/*).

[4] https://cyclonedx.org/about/supporters/.

sull'applicazione della premialità, è opportuno, in un'ottica di cyber resilienza, che vengano dichiarati eventuali riferimenti ad altri componenti/servizi (*externalReferences*), quale che sia il loro livello, con cui sussiste un rapporto funzionale di dipendenza rispetto a quelli di livello 1.

Si ritiene di dover chiarire l'assorbente ragione per la quale si è ritenuto opportuno che i soggetti acquirenti richiedano la dichiarazione di eventuali riferimenti ad altri componenti/servizi (*externalReferences*), quale che sia il loro livello nell'ambito della BOM, con cui sussiste il suddetto rapporto funzionale di dipendenza. Tale ragione sta nel garantire un più alto livello di cybersicurezza dei beni oggetto delle attività di *procurement*, anche dopo la fase acquisitiva. Ciò in quanto i soggetti acquirenti, in virtù di tale ulteriore livello di dettaglio della componentistica, laddove dovesse successivamente essere segnalata da ACN[5] una causa di vulnerabilità ad essa riferibile, potranno disporre di un'utile mappatura per riscontrarne l'eventuale sussistenza sui dispositivi acquistati e per le conseguenti attività di *remediation*.

[5] Tale circostanza è riferita alle attività di allertamento e segnalazione delle vulnerabilità rilevate da ACN nell'ambito delle proprie attività di monitoraggio della minaccia, ovvero segnalate alla stessa ACN in sede di *Coordinated vulnerability disclosure*, nonché, infine, riscontrate in sede di scrutinio tecnologico da parte del Centro di valutazione e certificazione nazionale dell'ACN (CVCN).

# 4. Nazionalità della tecnologia di cybersicurezza

## 4.1. Criteri valutativi

Ai fini dell'attribuzione del criterio di premialità, ciascuno dei componenti elencati al livello 1 della BOM deve essere riconducibile a uno dei Paesi di cui all'articolo 14, comma 1, indicati nell'Allegato 3 del DPCM.

Al fine di individuare il predetto requisito, occorre che sia esattamente indicato il Paese in cui è localizzato il sito produttivo dei componenti di riferimento, secondo quanto verrà meglio dettagliato nell'Appendice Tecnica BOM, ovvero, per quanto riguarda i servizi, il loro luogo di erogazione. In entrambi i casi, il requisito della provenienza andrà riportato nel sottocampo "*address.country*" all'interno dei campi, rispettivamente, "*Manufacturer*" e "*Provider",* entrambi obbligatori. Radicare nel Paese di produzione o di erogazione il requisito di cui trattasi offre, infatti, le maggiori garanzie riguardo al perseguimento delle esigenze di effettiva tutela sottese alla normativa in questione.

# 5. Criteri di premialità

## 5.1. Natura obbligatoria del criterio di premialità

Nelle procedure relative agli affidamenti di cui al Libro II, Parte I e Parte IV, del decreto legislativo n. 36/2023, le centrali di committenza e le stazioni appaltanti devono espressamente inserire nei documenti di gara, nel bando, nell'avviso o nell'invito, il riferimento alla premialità di cui all'articolo 14, anche facendo ricorso alla clausola tipo di cui al paragrafo 5.3.

Quanto affermato al punto precedente si intende vincolante, *mutatis mutandis*, anche per i soggetti privati tenuti all'osservanza della normativa in questione e non vincolati al rispetto del codice dei contratti pubblici; sicché quanto sopra previsto andrà trasfuso, dai soggetti in questione, nelle loro procedure contrattuali di approvvigionamento.

Per quanto riguarda i sistemi e i servizi di telefonia mobile 4G e 5G, in versione sia *stand-alone* (SA) che *non stand-alone* (NSA), e successive evoluzioni tecnologiche, si rimanda all'Appendice Tecnica TELCO.

## 5.2. Modalità di calcolo e ponderazione del criterio di premialità

Venendo in rilievo, con riferimento all'impiego dei componenti/servizi di cui si è detto al paragrafo 3, la tutela della sicurezza nazionale del Paese, appare opportuno che i soggetti tenuti all'applicazione dell'articolo 14 dispongano, con le presenti Linee guida, di una stregua unitaria ai fini della determinazione del peso da attribuire alla premialità (impregiudicata la concorrenza degli altri criteri obbligatori di premialità di cui all'art. 108 del Codice dei contratti pubblici).
Diversamente dagli altri casi di premialità, nella fattispecie in questione la particolare rilevanza dell'interesse pubblico primario indirizza il meccanismo applicativo di tale specifica premialità nei sensi più oggettivi e rigidi sopra illustrati.

Si ritiene che un equilibrato rapporto con la concorrente istanza di *par condicio* degli operatori economici possa raggiungersi fissando in un punteggio pari a 8 punti il valore dello specifico "premio" da attribuire nelle procedure di *procurement* ai sensi dell'articolo 14.

Per la modalità di attribuzione del punteggio per gli approvvigionamenti di sistemi e servizi telefonia mobile 4G e 5G, in versione sia *stand-alone* che *non stand-alone*, e successive evoluzioni tecnologiche si rinvia alle specificità trattate nell'Appendice Tecnica TELCO.

Per quanto riguarda gli approvvigionamenti di beni e servizi ICT diversi dai sistemi e servizi telefonia mobile 4G e 5G, il punteggio pari a 8 punti, sopra indicato, non è suscettibile di alcun frazionamento, nel senso che esso o è applicabile integralmente, laddove ciascun componente/servizio appartenente al livello 1 rispetti i requisiti o, in caso contrario, non lo è affatto. (meccanismo di natura "on/off").

## 5.3. Clausole tipo

Le stazioni appaltanti, comprese le centrali di committenza, includono nella documentazione di gara una clausola *ad hoc* per l'attribuzione della premialità. A titolo esemplificativo, qui di seguito vengono proposte due ipotesi di clausola tipo:

**Ipotesi 1 (generale, ad esclusione di approvvigionamenti di sistemi e servizi telefonia mobile 4G e 5G, in versione sia *stand-alone* che *non stand-alone*, e successive evoluzioni tecnologiche)**

"*Ai sensi dell'articolo 4, primo periodo, del DPCM del 30 aprile 2025, come modificato dal DPCM 2 ottobre 2025, gli operatori economici producono, in sede di offerta, l'elenco di tutti gli elementi (componenti o servizi) per il livello 1 della BOM (Bill of Materials) conforme ai requisiti di cui alle Linee guida adottate dall'Agenzia per la cybersicurezza nazionale, sentita l'Autorità nazionale anticorruzione, comprensiva almeno dei campi minimi indicati nelle medesime Linee guida, nonché una autodichiarazione che attesti che la propria offerta contempla, al livello di dettaglio riportato nella BOM, di cui si attesta la correttezza e la completezza, l'uso di tecnologie di cybersicurezza italiane, o di Paesi appartenenti all'Unione europea, o di Paesi aderenti all'Alleanza atlantica (NATO), o di Paesi terzi di cui all'Allegato 3 del citato DPCM. La BOM dovrà essere fornita, ai sensi dell'Allegato 1, parte II, n. 1), lett. a), del DPCM 30 aprile 2025, in formato CycloneDX versione 1.6 o altro formato equivalente, previa autorizzazione della stazione appaltante*"[6].

**Ipotesi 2 (approvvigionamenti di sistemi e servizi telefonia mobile 4G e 5G, in versione sia *stand-alone* che *non stand-alone*, e successive evoluzioni tecnologiche)**

"*Ai sensi dell'articolo 4, secondo e terzo periodo, del DPCM del 30 aprile 2025, come modificato dal DPCM 2 ottobre 2025, gli operatori economici producono, in sede di offerta, l'elenco di tutti i componenti di fabbricazione delle infrastrutture impiegate per erogare i servizi e sistemi di telefonia mobile 4G e 5G, in versione sia stand-alone che non stand-alone, e successive evoluzioni tecnologiche, conforme ai requisiti di cui alle Linee guida adottate dall'Agenzia per la cybersicurezza nazionale, sentita l'Autorità nazionale anticorruzione, comprensiva dei campi del prospetto indicati nelle medesime Linee guida, nonché una autodichiarazione che attesti che la propria offerta contempla, al livello del prospetto indicato nelle medesime Linee guida, di cui si attesta la correttezza e la completezza, l'uso di tecnologie di cybersicurezza italiane, o di Paesi appartenenti all'Unione europea, o di Paesi aderenti all'Alleanza atlantica (NATO), o di Paesi terzi di cui all'Allegato 3 del citato DPCM. Il prospetto di tutti i componenti di fabbricazione delle infrastrutture impiegate per erogare i servizi e sistemi di telefonia mobile 4G e 5G, in versione sia stand-alone che non stand-alone, e successive evoluzioni tecnologiche, dovrà essere fornito come previsto nel prospetto di cui all'Appendice tecnica TELCO delle medesime Linee guida*".

[6] In merito alla previsione, a discrezione della stazione appaltante, di formati differenti, si rimanda a quanto indicato nel paragrafo 3 circa la sostanziale equivalenza dei rispettivi contenuti informativi, per le finalità del DPCM.

# 6. Controlli e attività di verifica

Eventuali difformità rispetto a quanto autodichiarato dall'offerente che dovessero successivamente emergere, come ad esempio in sede di scrutinio tecnologico effettuato da ACN ai sensi dell'art. 1, comma 6, lett. *a)*, del decreto-legge n. 105/2019, potranno costituire causa di risoluzione contrattuale - previa introduzione di specifiche clausole di risoluzione espressa - comportando una violazione del principio di fiducia di cui all'art. 2 del decreto legislativo n. 36/2023, ferma restando ogni altra conseguenza stabilita dallo stesso codice ai sensi dell'art. 98, comma 2, e dell'art. 96, comma 15, anche relativamente all'obbligo di segnalazione all'ANAC.

# 7. Gare e lotti dedicati

È il caso di precisare che i contenuti del DPCM del 30 aprile 2025 e le raccomandazioni delle presenti Linee Guida attengono a procedure di approvvigionamento strettamente inerenti alla protezione di interessi nazionali strategici e ai contesti di tutela della sicurezza nazionale.

In relazione a tali esigenze, le stazioni appaltanti, ivi incluse le centrali di committenza, procederanno con apposite gare, o lotti dedicati, al fine di soddisfare il relativo quadro esigenziale e di rispettare le finalità di tutela della sicurezza nazionale della disposizione di cui all'articolo 14.

# APPENDICE TECNICA BOM

# 1. Struttura della BOM

## 1.1. Profondità della BOM

Come anticipato, in termini più generali, nel paragrafo 3.1 e conformemente ad un approccio seguito a livello internazionale[7], per la BOM è richiesto un solo livello di profondità, da intendersi come la descrizione degli elementi primari che compongono l'oggetto della fornitura.

In altri termini, la struttura della BOM segue il modello "*Multi-Module Product*" definito nella "*Authoritative Guide to SBOM, Second Edition*" di OWASP[8]. Essa deve contenere, pertanto:

- un singolo *bom.metadata.component*, riferito al bene o al servizio oggetto di descrizione (Livello 0);
- un elenco di elementi, indicati in *bom.components* (per prodotti) *o bom.services* (per servizi), per ciascun bene o servizio costituente l'oggetto della fornitura (Livello 1).

*La BOM è costituita da un solo livello di profondità.*
*Da un punto di vista strutturale, riferito al formato di elezione CycloneDX versione 1.6, la BOM contiene un solo elemento radice (**livello 0**) **bom.metadata.component, riferito all'oggetto della fornitura**, e l'elenco di componenti/servizi di cui esso è costituito, indicati in **bom.components** e/o **bom.services (livello 1)**.*

## 1.2. Ampiezza della BOM

Al predetto livello 1 di profondità, la BOM deve estendersi in ampiezza, includendo componenti software, firmware e servizi.
Tra le componenti software, per quanto riguarda il sistema operativo, si distinguono i seguenti scenari:

- **scenario 1**: le funzioni di cybersicurezza sono parte integrante del sistema operativo. In questo caso, il sistema operativo è indicato quale componente di livello 1 della BOM (è incluso in *bom.components*) e contribuisce all'attribuzione del punteggio di premialità;
- **scenario 2**: le funzioni di cybersicurezza sono erogate tramite componenti applicativi che impiegano il sistema operativo, posto al livello 2, in rapporto di dipendenza esterna. In questo caso, il sistema operativo, quindi, è indicato tra le *externalReferences* e non contribuisce all'attribuzione del punteggio premiale.

Con riferimento agli scenari sopracitati, si riporta di seguito un esempio di una categoria significativa di prodotto ("*appliance*"), e cioè di una piattaforma software eseguita su hardware dedicato.

---

[7] *Cfr.* il documento "*The Minimum Elements For a Software Bill of Materials (SBOM) pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity*", realizzato nel 2021 dal Dipartimento del Commercio americano in cooperazione con l'ufficio preposto alla gestione delle telecomunicazioni (*NTIA – National Telecommunications and Information Administration*).
[8] *Open web application security project*, una fondazione no profit, di rilevanza mondiale, che ha l'obiettivo di migliorare la sicurezza del software.

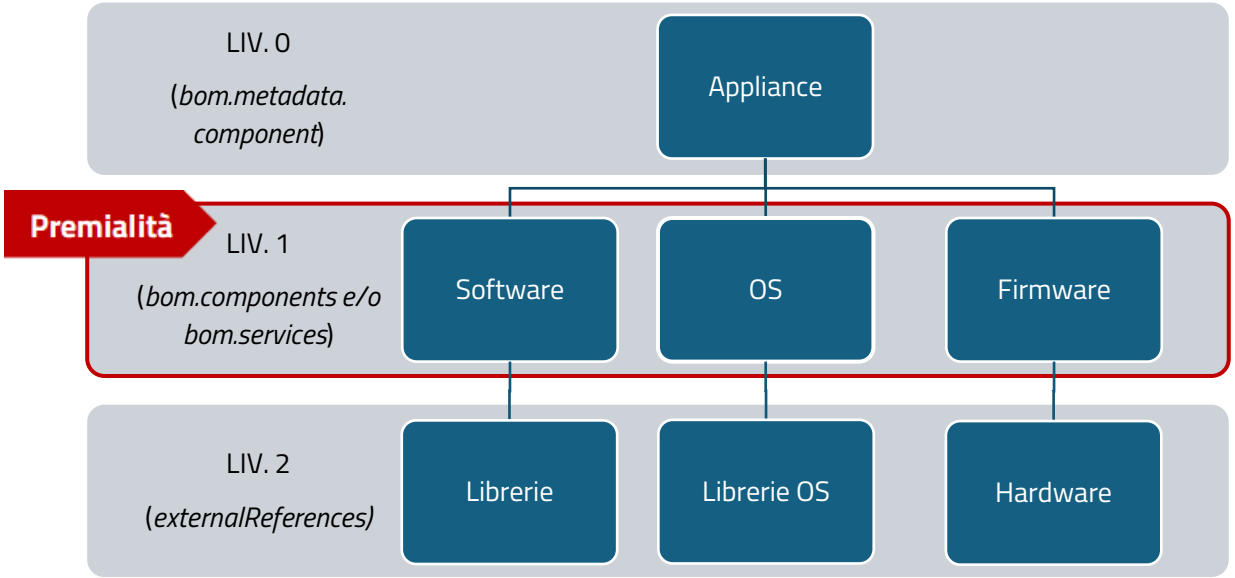


*Figura 1: Schema esemplificativo della copertura in ampiezza e profondità di una BOM per un prodotto complesso il cui sistema operativo implementa direttamente funzioni di cybersicurezza. Si evidenzia che, coerentemente con il requisito di profondità ed ampiezza, gli elementi per la valutazione dell'eventuale premialità sono quelli presenti al livello 1 (cerchiati in rosso) e, segnatamente, componenti Software, OS e Firmware afferenti a tecnologie di cybersicurezza. Il sistema operativo è elencato a livello 1 perché implementa direttamente funzioni di cybersicurezza.*

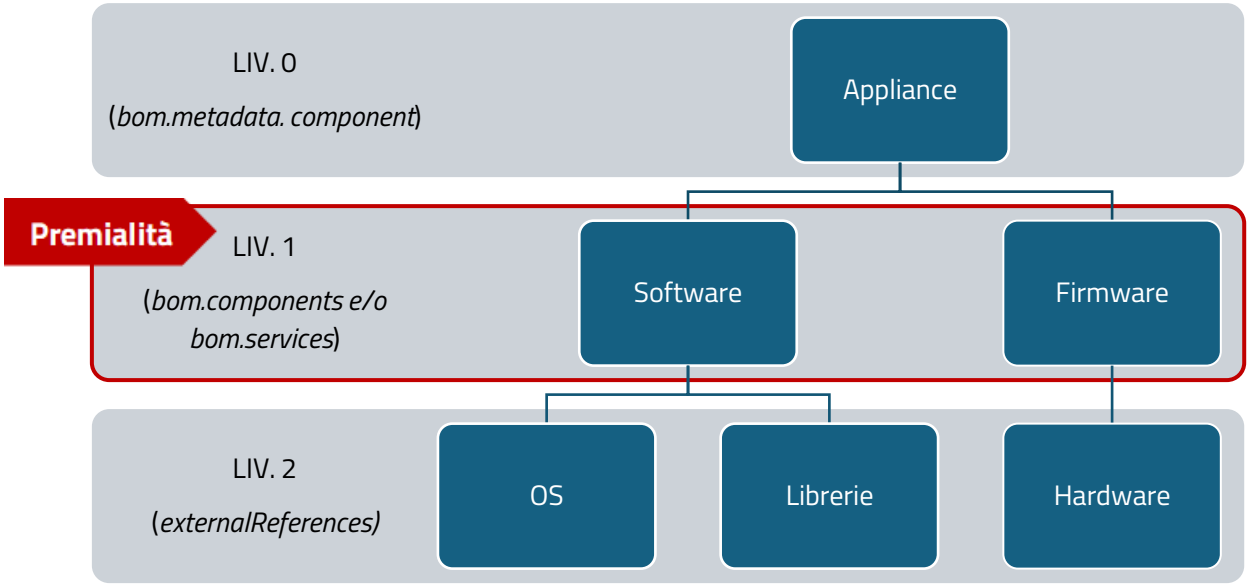


*Figura 2: Schema esemplificativo della copertura in ampiezza e profondità di una BOM per un prodotto complesso il cui sistema operativo non implementa direttamente funzioni di cybersicurezza. Si evidenzia che, coerentemente con il requisito di profondità ed ampiezza, gli elementi per la valutazione dell'eventuale premialità sono quelli presenti al livello 1 (cerchiati in rosso) e, segnatamente, componenti Software, e Firmware afferenti a tecnologie di cybersicurezza. Il sistema operativo è elencato a livello 2 perché non implementa direttamente funzioni di cybersicurezza.*

*La BOM deve contenere, a livello 1, i componenti software/firmware ed i servizi costituenti le tecnologie di cybersicurezza. Il sistema operativo è indicato, alternativamente, a livello 1, se implementa direttamente le funzioni di cybersicurezza, o quale riferimento esterno (livello 2), in caso contrario.*
*La BOM deve contenere almeno i componenti riferiti alle seguenti tipologie dello standard CycloneDX versione 1.6: "**Application**", "**Firmware**", "**Service**", "**Operating System**" (quest'ultimo se indicato a livello 1).*

## 1.3. Formato di presentazione della BOM

### 1.3.1. BOM applicata ai prodotti

**Per i prodotti di tipo software**, è richiesto all'operatore economico di fornire una cosiddetta SBOM ('*Software Bill of Materials*'). In questo ambito, ciò che abitualmente è considerato un componente consiste, a titolo esemplificativo, in:

- un insieme di file eseguibili (compilati o interpretati);
- librerie dinamicamente collegate agli eseguibili;
- framework e piattaforme software;
- servizi esterni con cui gli eseguibili interagiscono.

Queste macrocategorie sono valide a prescindere dalla specifica classe di software, che sia un applicativo, una macchina virtuale oppure il firmware di un dispositivo.

**Per i prodotti di tipo *appliance***, all'operatore economico è richiesto di fornire una SBOM che indichi i componenti di livello 1, come illustrato nelle figure 1 e 2. Per i prodotti hardware non assimilabili alle più complesse *appliance*[9], all'operatore economico è richiesto di fornire una SBOM comunque indicando, a livello 1, il firmware installato sullo specifico elemento hardware.

### 1.3.2. BOM applicata ai servizi

Allo stesso modo dei prodotti, l'ambito di applicazione è focalizzato sui servizi indicati nel paragrafo 2.2.1.

Quale principio di carattere generale, il criterio di premialità tiene conto del luogo di erogazione del servizio stesso.
In tal senso, la BOM deve contenere, tra i servizi elencati al livello 1, un riferimento a:

- informazioni sul servizio impiegato e sulla sua versione;
- informazioni sul *provider*, con specifico riguardo alla localizzazione delle infrastrutture da esso impiegate per l'erogazione del servizio.

[9] Ad esempio, le categorie 8, 9, 10, 12 e 14 indicate nell'Allegato 2 del DPCM.

Per quanto riguarda i servizi erogati tramite tecnologia cloud, per poter applicare in modo sostenibile e, allo stesso tempo, efficace il criterio di premialità, occorre adottare un approccio che tenga conto delle peculiarità di tale tecnologia. È noto, infatti, che i servizi cloud:

- si basano su un'architettura stratificata, che comprende infrastrutture, piattaforme e applicativi[10];
- prevedono un modello di gestione a "responsabilità condivisa", in cui i diversi strati dell'architettura possono essere amministrati da soggetti differenti, che ne conoscono i rispettivi dettagli tecnologici;
- sono caratterizzati da un'alta dinamicità, che consente di variare rapidamente le infrastrutture e le piattaforme sottostanti a un servizio. Ciò mal si concilia con una descrizione statica come quella contenuta in una BOM.

Tenuto conto di tali peculiarità dei servizi cloud, considerato quanto indicato nell'art. 4 del DPCM, che fa esplicito riferimento alle "*infrastrutture impiegate per erogare un servizio*", nonché in linea con i requisiti di cui al Regolamento Cloud per la PA[11], ai fini dell'attribuzione del punteggio premiale rileva l'indicazione del Paese ove risiede l'infrastruttura, ossia il *datacenter* o la *region*, impiegata dal *cloud service provider* che eroga il servizio in questione.

Quale informazione aggiuntiva, non valutabile per l'attribuzione del punteggio premiale, ma comunque a supporto di quanto dichiarato nei campi minimi, l'operatore economico può includere, come referenza esterna, un'indicazione relativa alla qualifica eventualmente rilasciata da ACN per quel servizio, mediante la struttura di seguito riportata, a titolo esemplificativo:

- *bom.services[].externalReferences[].type* = attestation;
- *bom.services[].externalReferences[].url* = https://www.acn.gov.it/portale/w/<id-scheda> (URL della scheda afferente al servizio incluso nel "Catalogo delle infrastrutture digitali e dei Servizi Cloud").

## 1.4. Campi minimi della BOM rilevanti ai fini della premialità

Considerato quanto espresso sopra riguardo alle informazioni che l'operatore economico deve fornire per vedersi attribuito il punteggio premiale, queste vengono codificate in specifici campi inclusi all'interno della BOM, la cui corretta compilazione è obbligatoria. Si evidenzia che l'operatore economico, al fine di meglio comprendere ed interpretare il dato da inserire nella BOM, può far riferimento ai chiarimenti indicati nella colonna '**Interpretazione del Campo**' riportata nelle liste tabellari che seguono e allo schema[12] del formato CycloneDX versione 1.6 utilizzati per la validazione della BOM.

---

[10] I modelli di servizio noti, rispettivamente, come IaaS ("*Infrastructure as a Service*"), PaaS ("*Platform as a Service*") e SaaS ("*Software as a Service*").

[11] Si consideri, ad esempio, il requisito PR.DS-01 previsto nel Regolamento Cloud per la PA di cui al Decreto del Direttore Generale di ACN n. 21007 del 27 giugno 2024, che specifica che, ai fini della qualificazione ACN dei servizi Cloud per la Pubblica Amministrazione, i dati devono essere trattati e conservati presso un'infrastruttura localizzata nel territorio dell'Unione Europea.

[12] Lo schema CycloneDX versione 1.6 è reperibile liberamente al seguente link: *https://github.com/CycloneDX/specification/blob/master/schema/bom-1.6.schema.json*.

*Per poter ottenere il punteggio premiale, l'operatore economico deve fornire una BOM compilata con i campi minimi riportati nella lista tabellare 1 all'interno dell'Appendice Tecnica, potendo far riferimento alla colonna 'Interpretazione del campo' al fine di fornire un dato coerente con le specificità dei vari elementi.*

## 1.5. Campi ulteriori della BOM non rilevanti ai fini della premialità

La BOM rappresenta un patrimonio informativo utile, tra l'altro, per la gestione delle vulnerabilità, come già evidenziato nel paragrafo 3.1 in relazione alle *externalReferences*.

Pertanto, le stazioni appaltanti, ivi incluse le centrali di committenza - in ragione dell'esercizio della discrezionalità spettante alla commissione giudicatrice - possono prevedere nella documentazione di gara, ai fini della valutazione dell'offerta tecnica, criteri o sub-criteri che valorizzino la presenza nella BOM di uno o più tra i campi ulteriori, indicati nella presente Appendice Tecnica. Inoltre, come già precisato al paragrafo 5.1, la valorizzazione dei campi ulteriori potrà essere richiesta anche dai soggetti non vincolati all'applicazione del Codice dei contratti pubblici, restando inteso, in ogni caso, che detta valorizzazione non concorre all'attribuzione del punteggio premiale.

## 1.6. Schema riassuntivo delle caratteristiche per la corretta formattazione della BOM

| Caratteristiche | Descrizione |
|---|---|
| *Profondità* | *La BOM, nel caso di specie, è costituita da un solo livello di profondità.*<br>*Da un punto di vista strutturale, riferito al formato di elezione CycloneDX versione 1.6, la BOM contiene un solo elemento radice (livello 0) bom.metadata.component, riferito all'oggetto della fornitura, e l'elenco di componenti/servizi di cui esso è costituito, indicati in bom.components e/o bom.services (livello 1).* |
| *Ampiezza* | *La BOM deve contenere, a livello 1, i componenti software/firmware ed i servizi costituenti le tecnologie di* |

| | |
|---|---|
| | *cybersicurezza. Il sistema operativo è indicato, alternativamente, a livello 1, se implementa direttamente le funzioni di cybersicurezza o quale riferimento esterno (livello 2) in caso contrario.*<br><br>*La BOM deve contenere almeno i componenti riferiti alle seguenti tipologie dello standard CycloneDX versione 1.6: "Application", "Firmware", "Service", "Operating System" (quest'ultimo se indicato a livello 1).* |
| *Formato* | *La BOM deve essere presentata in un formato processabile digitalmente e di uso comune. Il formato più idoneo allo scopo è lo standard open source e pubblicamente accessibile CycloneDX in versione 1.6.*<br><br>*Ulteriori formati potranno essere ritenuti ammissibili solo nei casi in cui la stazione appaltante possa valutarne la sostanziale equivalenza rispetto a CycloneDX versione 1.6, per le finalità delle presenti Linee guida.* |
| *Campi minimi* | *Per poter ottenere il punteggio premiale, l'operatore economico deve fornire una BOM compilata con i campi minimi riportati nella lista tabellare 1 all'interno dell'Appendice Tecnica, potendo far riferimento alla colonna 'Interpretazione del Campo' al fine di fornire un dato coerente con le specificità dei vari elementi.* |
| *Campi ulteriori* | *Le stazioni appaltanti, ivi incluse le centrali di committenza - in ragione dell'esercizio della discrezionalità spettante alla commissione giudicatrice - possono prevedere nella documentazione di gara, ai fini della valutazione dell'offerta tecnica, criteri o sub-criteri che valorizzino la presenza nella BOM di uno o più tra i campi ulteriori, indicati nella presente Appendice Tecnica. Resta inteso che i suddetti criteri e sub-criteri non concorrono all'attribuzione del punteggio premiale.* |

# 2. Dettaglio dei campi minimi e dei campi ulteriori

Di seguito la lista tabellare dei campi minimi della BOM (lista 1) e le liste dei campi ulteriori (liste 2 e 3).

## 2.1. Campi minimi per componenti/servizi

*Lista 1 riportante i campi minimi e l'interpretazione di ogni campo.*

| CAMPO MINIMO | INTERPRETAZIONE DEL CAMPO |
|---|---|
| bom.metadata.component | Indicazione del prodotto oggetto di fornitura, sia esso un prodotto software/hardware che un servizio. |
| bom.components[].manufacturer | **Per ogni componente presente all'interno della BOM**, l'operatore economico deve compilare il campo '*bom.components[].manufacturer*', comprensivo almeno dei seguenti sottocampi:<br>○ *bom.components[].manufacturer.name;*<br>○ *bom.components[].manufacturer.address.country*, nel quale è esplicitato il country code dello Stato, in formato ISO 3166-1, **in cui è localizzato il sito produttivo dello specifico componente di riferimento**;<br>○ *bom.components[].manufacturer.url.*<br><br>Si evidenzia che, nel caso in cui il componente sia un *software open-source*, l'operatore economico dovrà compilare il campo sopracitato solamente nell'ipotesi in cui lo stesso software sia distribuito da una singola entità organizzativa riconosciuta (ad esempio, distribuzioni specifiche di sistemi operativi o di librerie open source). In caso contrario, l'operatore economico potrà specificare la provenienza del componente *open source* nel relativo campo "*externalReferences*", coerentemente con quanto previsto nella successiva lista tabellare dei campi ulteriori per i componenti. |
| bom.components[].type | L'operatore economico deve fornire, **per ogni componente presente all'interno della BOM,** la tipologia di componente ('*application, library, etc...*'), con riferimento alle tipologie presenti nel formato CycloneDX (versione 1.6). |

| | |
|---|---|
| bom.components[].name | L'operatore economico deve fornire, **per ogni componente presente all'interno della BOM,** l'informazione associata al nome dello specifico componente. |
| bom.components[].version | L'operatore economico deve fornire, **per ogni componente presente all'interno della BOM**, l'informazione associata alla versione dello specifico componente. |
| bom.services[].provider | L'operatore economico deve fornire, **per ogni servizio presente all'interno della BOM,** le informazioni legate all'effettivo erogatore del servizio. In dettaglio, dovrà compilare obbligatoriamente almeno i seguenti campi:<br>• *bom.services[].provider.name*;<br>• *bom.services[].provider.address.country,* nel quale è esplicitato il country code della nazione, in formato ISO 3166-1, **in cui risiede l'infrastruttura attraverso la quale viene erogato il servizio**;<br>• *bom.services[].provider.url.* |
| bom.services[].name | L'operatore economico deve fornire, **per ogni servizio presente all'interno della BOM,** l'informazione associata al nome dello specifico servizio. |
| bom.services[].version | L'operatore economico deve fornire, **per ogni servizio presente all'interno della BOM,** l'informazione associata alla versione del servizio considerato. |

## 2.2. Campi ulteriori per componenti/servizi

*Lista 2 dei campi ulteriori nell'ambito di prodotti (componenti).*

| CAMPO ULTERIORE | INTERPRETAZIONE DEL CAMPO |
|---|---|
| bom.components[].purl | L'operatore economico può fornire il **package URL** associato al componente software, al fine di permetterne l'identificazione univoca.<br>Le specifiche minime sono liberamente accedibili al seguente link ('*https://github.com/package-url/purl-spec*'). |

| | |
|---|---|
| bom.components[].swid | L'operatore economico può fornire lo **swid**, un tag identificativo del software secondo lo standard ISO/IEC 19770-2:2015. |
| bom.components[].swhid | L'operatore economico può fornire lo **swhid**, un tag identificativo del software che ne garantisce l'integrità, definito dallo standard ISO/IEC 18670. |
| bom.components[].properties | L'operatore economico può fornire **ulteriori informazioni** che ritenga utili alla valutazione dell'eventuale aderenza ai criteri di premialità (e.g. localizzazione di un impianto produttivo).<br>Il campo consente di documentare proprietà specifiche del componente in formato dizionario "*nome:valore*". |
| bom.components[].hashes | L'operatore economico può fornire, per ogni componente presente all'interno della BOM, le informazioni legate agli **hash del componente**, quindi l'hash effettivo e tutte le informazioni legate alle procedure per poterlo usare come attestazione di integrità del componente stesso (e.g. algoritmo, etc...). |
| bom.components[].cpe | L'operatore economico può fornire, per ogni componente presente all'interno della BOM, il codice univoco **CPE**, al fine di identificare il componente stesso. |
| bom.components[].externalReferences | L'operatore economico utilizza questo campo per fornire informazioni riguardanti le **dipendenze** dello specifico servizio da elementi non presenti all'interno della BOM. In dettaglio, l'operatore economico compila, per ciascun servizio della BOM, i seguenti campi come riportato di seguito:<br>• *bom.components[].externalReferences[].type* = tipo di riferimento;<br>• *bom.components[].externalReferences[].url* = URL del riferimento. |

*Lista 3 campi ulteriori nell'ambito di servizi (services).*

| CAMPO ULTERIORE | INTERPRETAZIONE DEL CAMPO |
|---|---|
| bom.services[].properties | L'operatore economico utilizza questo campo per documentare proprietà specifiche del componente in formato dizionario "*nome:valore*". |
| bom.services[].description | L'operatore economico utilizza questo campo per fornire, per ogni servizio presente all'interno della BOM, le informazioni associate all'accessibilità dello stesso (URL/API). |
| bom.services[].externalReferences | L'operatore economico utilizza questo campo per fornire informazioni riguardanti le **dipendenze** dello specifico servizio da elementi non presenti all'interno della BOM. In dettaglio, l'operatore economico compila, per ciascun servizio della BOM, i seguenti campi come riportato di seguito:<br>• *bom.services[].externalReferences[].type* = tipo di riferimento;<br>• *bom.services[].externalReferences[].url* = URL del riferimento.<br><br>Nel caso di un **servizio qualificato ai sensi del Regolamento Cloud di ACN**, l'operatore economico può usare il campo per specificare il link alla specifica scheda all'interno del catalogo pubblico[13], inserendo i campi come di seguito indicato:<br>• *bom.services[].externalReferences[].type* = attestation;<br>• *bom.services[].externalReferences[].url* = https://www.acn.gov.it/portale/w/<id-scheda> URL al link della scheda relativa al servizio cloud qualificato presente sul catalogo pubblico di ACN. |

# 3. Strumenti utilizzabili al fine di creare, validare, analizzare, firmare e convertire una BOM

[13] Catalogo pubblico ACN*: https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud.*

Di seguito un elenco di tool pubblicamente accessibili che gli operatori economici possono utilizzare, tra l'altro, per la creazione, validazione (rispetto alla sola conformità sintattica della BOM allo schema CycloneDX versione 1.6 e non rispetto ai criteri di premialità delle Linee guida), analisi, firma e conversione delle BOM.

| STRUMENTO | DESCRIZIONE | FUNZIONALITÀ |
|---|---|---|
| **Cyclonedx-python** *https://github.com/CycloneDX/cyclonedx-python* | Strumento realizzato in linguaggio python che supporta la generazione di SBOM in formato CycloneDX. | Generazione ed Analisi della BOM. |
| **CycloneDX CLI** *https://github.com/CycloneDX/cyclonedx-cli* | Strumento impiegabile da riga di comando, disponibile per vari sistemi operativi, che supporta l'analisi, la validazione, la firma e la conversione della BOM. | Analisi, Validazione, Firma e Conversione del formato della BOM. |

Si rimanda, inoltre, alla pagina dedicata del portale OWASP per un elenco degli strumenti liberamente accessibili per la gestione di BOM in formato CycloneDX: https://cyclonedx.org/tool-center/

Fermo restando quanto sopra riportato riguardo all'utilizzo di CycloneDX o di altro formato (si veda paragrafo 3) ai fini del riscontro degli elementi utili per l'attribuzione del punteggio premiale, si informa che uno strumento in forma prototipale di validazione automatizzata delle BOM, predisposte utilizzando il formato CycloneDX, versione 1.6, di cui viene anche fornito il codice sorgente, è messo a disposizione a titolo collaborativo da parte di ACN sul proprio sito istituzionale.

Tale strumento, sotto l'esclusiva responsabilità dell'utilizzatore, sarà liberamente utilizzabile e modificabile, nel rispetto delle condizioni fissate in sede di rilascio, da parte degli utenti interessati all'applicazione delle presenti Linee guida.

# 4. Esempio di BOM

Di seguito si riporta un esempio di BOM illustrativo.

**SBOM di un'applicazione esempio ('*Example Application*') in formato json CycloneDX 1.6**

Nota: nell'esempio sono stati evidenziati in grassetto i campi minimi e in colore rosso le indicazioni dei Paesi di provenienza da valutare ai fini dell'attribuzione della premialità.

```
1. {
 2.  "bomFormat": "CycloneDX",
 3.  "specVersion": "1.6",
 4.  "version": 1,
 5.  "metadata": {
 6.   "timestamp": "2025-06-25T12:00:00Z",
 7.   "tools": [
 8.    {
 9.     "vendor": "ACME Corp.",
10.     "name": "ACME BOM Generator",
11.     "version": "1.0"
12.    }
13.   ],
14.   "authors": [
15.    {
16.     "name": "ACME Corp. Embedded Team",
17.     "email": "security@acmecorp.com"
18.    }
19.   ],
20.   "manufacturer": {
21.    "name": "ACME Corp.",
22.    "url": [
23.      "https://www.ACME_Corp.com"
24.      ]
25.   },
26.   "component": {
27.    "name": "ACMEGate",
28.            "type": "application",
29.            "description": "ACMEgate product target of the BOM",
30.            "version": "rev3"
31.   }
32.  },
33.
34.  "services": [
35.   {
36.    "bom-ref": "ACMEGate-cloud-service",
37.    "name": "ACMEGateAuthService",
38.    "version": "rev1.1",
39.    "description": "https://example.com/api/v1/ticker",
40.    "provider": {
41.     "name": "ACME Corp.",
42.     "address": {
43.       "country": "XX"
44.     },
45.     "url": [
46.       "https://www.searchenginename.com"
47.       ]
48.    },
49.
50.    "externalReferences": [
51.     {
52.      "type": "attestation",
53.      "url": "https://www.acn.gov.it/portale/w/sa-xxxx",
54.      "comment": "ACN qualification"
55.     }
```

```
56.     ]
57.   }
58.  ],
59.
60.
61.  "components": [
62.   {
63.    "type": "application",
64.    "bom-ref": "ACMEGate-appliance",
65.    "name": "ACMEGate",
66.    "version": "rev3",
67.    "description": "Enterprise Firewall Appliance",
68.    "cpe": "cpe:2.3:h:acme:ACMEGate:rev3:*:*:*:*:*:*:*",
69.    "hashes": [
70.      {
71.        "alg": "SHA-256",
72.        "content": "121a7c7a462a954e5c3d2cfe217045f79c3ab5d0ba83dfc439acddc93d603df3"
73.      },
74.      {
75.        "alg": "SHA-512",
76.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                "content": "d92e739bd0da5d62ab04507229d80e35bd5219925bdae07ecc4fac878464d28a6af8e22b910be34fa752cf456bbeaf514d062f1430ac3cacd00c512d4549b83c"
77.      }
78.    ],
79.    "manufacturer": {
80.      "name": "ACME Corp.",
81.      "address": {
82.        "country": "XX"
83.      },
84.      "url": [
85.        "https://www.searchenginename.com"
86.        ]
87.    },
88.    "externalReferences": [
89.      {
90.        "type": "support",
91.        "url": "https://www.libssh.org",
92.        "comment": "ssh library"
93.      }
94.    ]
95.  },
96.  {
97.    "type": "firmware",
98.    "bom-ref": "acmeos-7.4.1",
99.    "name": "ACMEOS",
100.    "version": "1.1.2",
101.    "description": "ACME Security Operating System",
102.    "hashes": [
103.      {
104.        "alg": "SHA-256",
105.        "content": "121a7c7a462a954e5c3d2cfe217045f79c3ab5d0ba83dfc439acddc93d603df3"
106.      },
107.      {
108.        "alg": "SHA-512",
```

```
109.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                "content": "d92e739bd0da5d62ab04507229d80e35bd5219925bdae07ecc4fac878464d28a6af8e22b910be34fa752cf456bbeaf514d062f1430ac3cacd00c512d4549b83c"
110.       }
111.      ],
112.     "cpe": "cpe:2.3:o:ACME:acmeos:7.4.1:*:*:*:*:*:*:*",
113.     "manufacturer": {
114.       "name": "ACME Inc. XXXX",
115.       "address": {
116.         "country": "XX"
117.       },
118.       "url": [
119.         "https://www.searchenginename.com"
120.         ]
121.     },
122.
123.     "purl": "pkg:generic/acme/acmeos@7.4.1",
124.     "externalReferences": [
125.       {
126.         "type": "distribution",
127.         "url": "https://www.support.ACME_Corp.com/firmware/acmeos/7.4.1",
128.         "comment": "Firmware download"
129.       },
130.       {
131.         "type": "documentation",
132.         "url": "https://www.docs.ACME_Corp.com/acmeos/7-4-1/release-notes",
133.         "comment": "Release notes"
134.       }
135.     ]
136.   },
137.   {
138.     "type": "operating-system",
139.     "bom-ref": "Ubuntu 24.04.2 LTS",
140.     "name": "Ubuntu Desktop",
141.     "version": "24.04.2 LTS",
142.       "hashes": [
143.       {
144.         "alg": "SHA-256",
145.         "content": "d7fe3d6a0419667d2f8eff12796996328daa2d4f90cd9f87aa9371b362f987bf"
146.       }
147.     ],
148.     "cpe": " cpe:2.3:o:acmelinux:acuntu_linux:22.04:*:*:*:lts:*:*:* ",
149.     "manufacturer": {
150.       "name": "ACMELINUX",
151.       "address": {
152.         "country": "XX"
153.       },
154.       "url": [
155.         "https://ubuntu.com/download/desktop/thank-you?version=24.04.2&architecture=amd64&lts=true"
156.         ]
157.     },
158.     "externalReferences": [
159.       {
160.         "type": "support",
161.         "url": "https://www.kernel.org/pub/",
```

```
162.        "comment": "external library module"
163.      }
164.    ]
165.  },
166.  {
167.    "type": "application",
168.    "bom-ref": "cli-shell",
169.    "name": "ACME CLI Shell",
170.    "version": "1.0.0",
171.    "hashes": [
172.      {
173.        "alg": "SHA-256",
174.        "content": "e887f2b14fda03b9fdd53debbf568b2a3ba6f2ad8331236e768fd6cf4f38e397"
175.      }
176.    ],
177.    "cpe": "cpe:2.3:a:acme:cli_shell:1.0.0:*:*:*:*:*:*:*",
178.    "manufacturer": {
179.      "name": "ACME Inc.",
180.      "address": {
181.        "country": "XX"
182.      },
183.      "url": [
184.        "https://www.searchenginename.com"
185.        ]
186.    },
187.
188.    "purl": "pkg:generic/acmecorp/cli-shell@1.0.0",
189.    "externalReferences": [
190.      {
191.        "type": "documentation",
192.        "url": "https://www.ACME_Corp/ACMEGate_specs",
193.        "comment": "Specs and manuals"
194.      }
195.    ]
196.  }
197. ]
198. }
```


199.

# APPENDICE TECNICA TELCO – APPLICAZIONE DEL CRITERIO DI PREMIALITÀ AI SISTEMI E AI SERVIZI 4G E 5G (SA E NSA)

# 1. Applicazione del criterio di premialità ai sistemi e servizi di telefonia mobile 4G e 5G (SA e NSA)

Il criterio di premialità si applica, per lo speciale settore delle telecomunicazioni, all'approvvigionamento, anche da parte delle Centrali di committenza, di servizi e sistemi di telefonia mobile 4G e 5G, in versione sia *stand-alone* che *non stand-alone*, e successive evoluzioni tecnologiche, nei casi previsti dal DPCM.

Conformemente a quanto previsto dall'art. 4, comma 2, del DPCM, il criterio di premialità riferito ai predetti sistemi e servizi si applica previa analisi dell'elenco di tutti i componenti di fabbricazione delle infrastrutture impiegate per erogarli (le reti di telecomunicazione).

In questo contesto, tuttavia, l'analisi dettagliata della BOM di ogni singolo componente infrastrutturale appare poco percorribile. Si adotta, pertanto, un approccio sistemico, volto a valutare, più che i singoli componenti, gli elementi architetturali che compongono una rete 4G/5G.

Traendo ispirazione dal citato "*Report on EU coordinated risk assessment of 5G*", nonché dal documento "*Threat landscape for 5G networks*" di ENISA, il criterio di premialità tiene conto dei seguenti macro-componenti architetturali, applicabili anche al contesto delle reti 4G nonché, indifferentemente, alle reti 5G di tipo SA e NSA.

| Macro-componente | Rischio associato (da Rapporto UE) |
|---|---|
| Rete di accesso radio (RAN) | ALTO |
| Rete di trasporto (Backhaul) | MODERATO/ALTO |
| Rete core (CN) | CRITICO |

In occasione della presentazione dell'offerta, ciascun operatore economico dovrà compilare un prospetto come segue, il cui contenuto informativo è paragonabile, seppur a un diverso livello di dettaglio, a quello della BOM, limitatamente alle finalità di attribuzione del punteggio premiale. Nello specifico, l'operatore economico dovrà compilare, nell'offerta tecnica, la colonna "Valore", conformemente alla descrizione.

Nei prospetti seguenti e nel prosieguo si indica con la locuzione "Paesi elencati" i Paesi di cui all'articolo 4, comma 2, del DPCM.

Il fattore di moltiplicazione *k* è proporzionale al grado di rischiosità delle diverse componenti:

| Parametro | Descrizione | Valore (%) | Coefficiente (*k*) |
|---|---|---|---|
| RAN | Numero di stazioni radio base composte da apparati prodotti esclusivamente presso Paesi elencati rispetto al totale delle stazioni radio base installate. | <da compilare> | 3 |
| BKL | Percentuale di traffico trasportato sui collegamenti di backhaul ed elaborato attraverso apparati di rete (router, switch) e di sicurezza (firewall, IDS, IPS, security gateway) prodotti da Paesi elencati rispetto al totale. | <da compilare> | 1 |
| CN | Numero di funzioni core realizzate tramite apparati prodotti da Paesi elencati rispetto al totale. | <da compilare> | 4 |

Nota metodologica:

Non essendo immediatamente applicabile, nel caso delle reti 4G e 5G, il livello di dettaglio garantito dalla BOM così come definita dalle presenti Linee Guida per gli altri casi, la provenienza delle componenti tecnologiche nelle diverse macro-componenti (RAN, rete di trasporto, rete core) è individuata tenendo conto della nazionalità del produttore, definita con criteri derivati da quelli di cui all'articolo 2, comma 5-*bis*, del decreto-legge 15 marzo 2012, n. 21. È dunque definita tecnologia non riconducibile ai Paesi elencati quella prodotta da:

a) qualsiasi persona giuridica che non abbia la sede legale o dell'amministrazione ovvero il centro di attività principale in un Paese elencato o che non sia comunque ivi stabilita;
b) qualsiasi persona giuridica che, pur avendo stabilito la sede legale o dell'amministrazione o il centro di attività principale in un Paese elencato, o che sia comunque ivi stabilita, risulti controllata, direttamente o indirettamente, da una persona giuridica di cui alla lettera a).

Per il calcolo dei parametri RAN, BKL e CN valgono le seguenti indicazioni:

- RAN: nel caso di reti 5G in modalità NSA (*non stand-alone*), vanno considerate sia le stazioni radio base di tipo eNodeB, sia quelle di tipo gNodeB;
- BKL: il valore può essere stimato con un margine di errore/incertezza di 10 punti (ad es., a fronte di un valore dichiarato pari al 50%, si ritiene conforme alla dichiarazione un valore di traffico effettivo ricompreso tra il 40% e il 60%);
- CN: il calcolo del parametro è limitato alle sole funzioni core indicate nell'allegato 1 del DPCM 15 giugno 2021, afferenti al *control plane* di una rete core 5G aderente al modello SBA (Service Based Architecture) e alle corrispondenti funzioni delle reti core 4G (EPC - Evolved Packet Core), per quanto applicabile, come da prospetto seguente:

| Funzione core 5G (SBA) | Funzione core 4G (EPC) |
|---|---|
| AUSF | HSS |
| UDM | |
| NSSF | (non presente) |
| PCF | PCRF |
| SMF | MME |
| | PGW-C |

La stazione appaltante, per ciascun offerente, calcolerà il coefficiente risultante moltiplicando il valore indicato nell'offerta tecnica con il fattore *k* e calcolerà il punteggio complessivo sommando i valori ottenuti.

In pratica, indicando con Pa il punteggio dell'operatore economico "a", si otterrà:

Pa = RAN x 3 + BKL + CN x 4

Il punteggio premiale massimo (pari ad 8 punti) sarà attribuito all'operatore che otterrà il punteggio massimo.

Agli altri operatori verrà attribuito un punteggio proporzionale decrescente, arrotondato al centesimo.

Esempio:

**Operatore A**

| Parametro | Descrizione | Valore (%) | Coefficiente (*k*) |
|---|---|---|---|
| RAN | Numero di stazioni radio base composte da apparati prodotti esclusivamente presso Paesi elencati rispetto al totale delle stazioni radio base installate. | 60% | 3 |
| BKL | Percentuale di traffico trasportato sui collegamenti di backhaul ed elaborato attraverso apparati di rete (router, switch) e di sicurezza (firewall, IDS, IPS, security gateway) prodotti da Paesi elencati rispetto al totale. | 40% | 1 |
| CN | Numero di funzioni core realizzate tramite apparati prodotti da Paesi elencati rispetto al totale. | 3/5 = 60% | 4 |

**Operatore B**

| Parametro | Descrizione | Valore (%) | Coefficiente (*k*) |
|---|---|---|---|
| RAN | Numero di stazioni radio base composte da apparati prodotti esclusivamente presso Paesi elencati rispetto al totale delle stazioni radio base installate. | 100% | 3 |
| BKL | Percentuale di traffico trasportato sui collegamenti di backhaul ed elaborato attraverso apparati di rete (router, switch) e di sicurezza (firewall, IDS, IPS, security gateway) prodotti da Paesi elencati rispetto al totale. | 20% | 1 |
| CN | Numero di funzioni core realizzate tramite apparati prodotti da Paesi elencati rispetto al totale. | 5/5 = 100% | 4 |

Di conseguenza:

Pa = 0,6 x 3 + 0,4 + 0,6 x 4 = 4,6

Pb = 1 x 3 + 0,2 + 1 x 4 = 7,2

In questo caso, il punteggio premiale massimo di 8 punti sarebbe attribuito all'Operatore b.

L'operatore a, invece, otterrebbe un punteggio proporzionalmente inferiore, arrotondato al centesimo, secondo la seguente proporzione:

8 : 7,2 = x : 4,6 → x = (8 x 4,6) / 7,2 = 5,11