Schema di Certificazione CISO

LISTA REVISIONI

Rev.	Data	Descrizione	Redazione e Verifica	Approvazione (DIR)
0	12.01.2024	1^ emissione	Francesco D'Arcadia (RSG) Vincenzo Alonge (RES)	Antonio Capobianco
1	10.05.2024	Aggiornamento a ISO 11621-4:2024. Modificato Par 1.3 e 2.1	Francesco D'Arcadia (RSG) Vincenzo Alonge (RES)	Antonio Capobianco
2	13.06.2024	Modificato par. 2.5, 2.10 e inserito par. 2.6 con sottoparagrafi. Specificata ovunque la versione 2024 per la ISO 11621	Francesco D'Arcadia (RSG) Vincenzo Alonge (RES)	Antonio Capobianco
3	15.10.2024	Modiicato par. 2.4, 2.5 e 2.6 aggiunti 2.3.1 e 2.3.2	Francesco D'Arcadia (RSG) Vincenzo Alonge (RES)	Antonio Capobianco

Indice

1 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento definisce le attività, responsabilità, controlli e verifiche previste per lo Schema di Certificazione CISO (Certified Information Security Officer).

Il presente documento definisce i requisiti e le modalità per la certificazione dei profili di seconda generazione in ambito ICT di cui alla norma UNI 11506:2021 correlata al dettaglio dei profili professionali codificati nella UNI 11621:2021.
Il prospetto contenente il profilo di ruolo professionale per l'ICT disponibile al punto 2 è stato elaborato, allineando le e-Competence rispetto al Prospetto B.15 della UNI EN 16234-1— Relazione tra CWA 16458: 2018 ed EN 16234-1". Con tale attività, i profili di ruolo professionale per l'ICT di seguito pubblicati risultano essere allineati con le e-Competence della UNI EN 16234-1:2020.

Di seguito si riporta la tabella di corrispondenza tra il profilo di riferimento codificato e il nome dell'esame di certificazione offerto da Fata Informatica.

Profilo professionale di riferimento UNI 11621-4:2024	**Denominazione Schema di Certificazione Fata Informatica**
Responsabile della sicurezza delle informazioni (CISO), Prospetto 6	Certified Information Security Officer

1.1 TERMINOLOGIA

I profili professionali nell'ambito delle professioni ICT sono declinati secondo il sistema e-CF e non secondo il sistema EQF, ma a tale riferimento si riconducono. Si ricorda che il livello di istruzione viene qui usato per paragone e non può essere considerato prescrittivo in funzione del fatto che si può raggiungere la competenza anche massima senza nessun titolo curricolare, ma solo con l'esperienza professionale (e.g. Enzo Ferrari non era ingegnere).
Ai fini di una corretta interpretazione si riporta la tabella di correlazione a seguire:

Livello e-CF	Livello EQF	Cicli EU	Livello istruzione
e-5	**8**	**III ciclo**	Dottorato PHD (higher Education)
e-4	**7**		Laurea Magistrale/Master Universitario (higher Education)
e-3	**6**		Laurea/Bachelor (higher Education)
e-2	**5**	**II ciclo**	Istruzione Tecnica Superiore (Further Education)
	4		Istruzione Secondaria (Secondary School)
e-1	**3**	**I ciclo**	Istruzione Secondaria Primo Grado (Italy)

Nella definizione dei compiti viene usata la terminologia delle tabelle RACI i cui elementi sono qui sotto dettagliati.

Responsabile finale – Garantisce (R)
Essere Responsabile vuol dire essere l'unico "owner" del lavoro. L'owner deve terminare o approvare un task, un obiettivo o una decisione quando questi sono completati. L'owner si deve assicurare che le responsabilità siano assegnate per tutte le attività collegate. C'è solo un owner responsabile per ciascun deliverable. Il termine "Responsabilità" è anche usato come termine generico, senza che ci sia una relazione con la matrice RACI.

Esecutore – Assicura
Le "Persone che fanno" un lavoro sono responsabili per quel lavoro. Essi devono realizzare il task o l'obiettivo o prendere le relative decisioni. Più persone possono essere insieme responsabili di un deliverable. I termini "responsabile" e "responsabilità" sono anche usati come termini generici, senza relazione con la Matrice RACI.

Contributore – Contribuisce
I contributori forniscono contributi prima che il lavoro sia completato o terminato. Sono partecipanti attivi e "in the loop". Più persone possono essere contributori di un deliverable.

Informed – Informato
Sono coloro che vengono informati sull'attività o sul processo in questione.

1.2 DESCRIZIONE SINTETICA DEL PROFILO

Seguendo le indicazioni del sistema e-CF e delle norme e documento da esso scaturite, il profilo professionale è descritto attingendo direttamente a quanto indicato nella norma di riferimento 11621-4:2024 che a sua volta si riferisce alla CWA 16458 e successive; pertanto l'organizzazione del profilo viene proposta in linea con le norme citate.

1.3 DOCUMENTAZIONE DI RIFERIMENTO

UNI CEI EN ISO/IEC 17024:2012	Requisiti Generali per gli organismi che operano nella certificazione del personale
UNI 11506 :2021	Attività professionali non regolamentate – Figure professionali operanti nel settore ICT – Requisiti per la valutazione della conformità delle conoscenze, abilità, autonomia e responsabilità per i profili professionali ICT basati sul modello e-CF
UNI 11621-4 :2024	Attività professionali non regolamentate - Profili di ruolo professionale per l'ICT - Parte 4: Profili di ruolo professionale relativi alla sicurezza delle informazioni
UNI EN 16234-1:2020	e-Competenze Framework (e-CF) – Framework comune europeo per i professionisti ICT in tutti i settori – Parte 1: Framework (modello di riferimento)

2 SCHEMA DI CERTIFICAZIONE Certified Information Security Officer

2.1 PROFILO DI RUOLO PROFESSIONALE

Di seguito si riporta il profilo di ruolo professionale per il presente schema di certificazione che corrisponde a **"Responsabile della sicurezza delle informazioni (CISO)", Prospetto 6 della UNI 11621-4:2024**.

Definizione sintetica

Ha responsabilità di massimo livello nell'ambito della gestione della sicurezza delle informazioni all'interno dell'organizzazione.

Missione

Definisce la strategia per la gestione della sicurezza delle informazioni, coordinando i security manager, i fornitori o il personale specialistico per garantirne la continua e corretta attuazione nel tempo all'interno di un budget definito. Si interfaccia con tutte le figure di responsabilità aziendali.

Risultati attesi

Responsabile finale (R)

- Politica per la sicurezza delle informazioni
- Altre politiche per la sicurezza delle informazioni
- Programma di analisi per la sicurezza delle informazioni
- Programma delle verifiche tecniche di sicurezza
- Incidenti relativi alla sicurezza delle informazioni risolti
- Relazioni sullo stato complessivo della sicurezza (e.g. riesame)
- Indicatori sulla sicurezza delle informazioni
- Requisiti per la sicurezza delle informazioni
- Piano di trattamento del rischio / Piano di sicurezza

Esecutore (A)

- Budget per la sicurezza delle informazioni
- Accordi di riservatezza e clausole contrattuali di sicurezza
- Programma di formazione e consapevolezza

Compiti principali

- Informare periodicamente la Direzione sullo stato della sicurezza delle informazioni
- Gestire il budget per la sicurezza delle informazioni
- Controllare e garantire continuamente il livello complessivo di sicurezza delle informazioni aziendale
- Organizzare le responsabilità relative alla sicurezza delle informazioni
- Presiedere la redazione e l'aggiornamento delle policy per la sicurezza delle informazioni

Competenze e_CF	Livello
D.1. Sviluppo della Strategia della Sicurezza Informatica	5
E.2. Gestione del Progetto e del Portfolio	4
E.3. Gestione del Rischio	4
E.5. Miglioramento del Processo	4
E.8. Gestione della Sicurezza dell'Informazione	4

Abilità

- S001 - affrontare le esigenze della formazione continua (CPD) del personale per soddisfare le esigenze dell'organizzazione
- S007 - analizzare i dati di feedback e usarli per attuare un continuo miglioramento nella delivery dell'istruzione e della formazione
- S008 - analizzare i dati relativi all'erogazione di un servizio
- S014 - analizzare la fattibilità in termini di costi e benefici
- S017 - analizzare le offerte ricevute
- S018 - anticipare e mitigare potenziali guasti / interruzioni nel servizio

- S019 - anticipare i cambiamenti richiesti alla strategia aziendale dell'information security e formulare nuovi piani
- S021 - applicare azioni di contenimento del rischio e dell'emergenza
- S023 - applicare gli standard, le best practice e i requisiti legali più rilevanti all'information security
- S026 - applicare la capacità di giudizio e la flessibilità nelle negoziazioni contrattuali in modo conforme alle regole e politiche interne.
- S033 - applicare tecniche di monitoraggio e collaudo
- S045 - comporre, documentare e classificare i processi fondamentali e le procedure
- S052 - comunicare e pubblicizzare sia i risultati dell'analisi del rischio che i processi di gestione del rischio
- S056 - comunicare lo stato d'avanzamento del progetto a tutte le parti interessate evidenziando argomenti come il controllo dei costi, la calendarizzazione dei risultati, il controllo qualità, l'annullamento dei rischi ed i cambiamenti alle specifiche di progetto
- S061 - contribuire allo sviluppo della strategia e delle politiche dell'ICT, incluse la qualità e la sicurezza ICT
- S066 - costruire un piano di gestione del rischio per fornire e produrre piani di azione preventivi
- S075 - definire un piano di progetto suddividendolo in singoli task di progetto
- S077 - definire, presentare e promuovere una politica dell'information security presso il senior management dell'organizzazione
- S078 - delegare i task e gestire in modo appropriato i contributi dei membri del team
- S081 - documentare la politica di gestione della sicurezza collegandola alla strategia di business
- S083 - effettuare auditing di sicurezza
- S099 - gestire il budget degli acquisti
- S103 - gestire le risorse contrattualizzate esternamente per raggiungere gli obiettivi di progetto
- S108 - identificare e massimizzare l'uso delle risorse richieste per finalizzare un piano efficace dal punto di vista dei costi
- S115 - identificare le principali milestone di un piano
- S121 - attuare il cambiamento dei processi
- S122 - attuare il piano di ripristino in caso di crisi
- S123 - incoraggiare positive relazioni con fornitori e clienti
- S125 - indirizzare e identificare gli elementi essenziali del valore offerto da un prodotto o da una soluzione
- S129 - interpretare le specifiche del prodotto / servizio
- S139 - negoziare obiettivi realistici per i livelli di servizio
- S140 - negoziare termini e condizioni del contratto
- S141 - negoziare termini, condizioni e politiche di prezzo
- S148 - ottimizzare tempi e obiettivi di consegna del portfolio progetti ottenendo il consenso sulle priorità degli stakeholder
- S156 - progettare e documentare i processi dell'analisi e della gestione del rischio
- S164 - proporre cambiamenti di processo per facilitare e razionalizzare i miglioramenti
- S165 - proporre misure efficaci di contingenza
- S174 - rivedere e analizzare gli impatti delle implementazioni
- S176 - seguire e controllare l'uso effettivo degli standard documentativi aziendali
- S181 - stabilire un piano di ripristino
- S183 - sviluppare ed analizzare criticamente la strategia aziendale sull'information security
- S187 - sviluppare piani di gestione del rischio per identificare le necessarie azioni preventive
- S197 - valutare l'erogazione di un servizio rispetto al relativo service level agreement
- S201 - verificare che i processi d'acquisto rispettino le norme legali inclusa la proprietà intellettuale (IPR)
- S202 - verificare la soluzione progettata (proof of concept)
- S234 - Elaborare e comunicare la strategia per la sicurezza delle informazioni

Conoscenze

- K023 - gli standard per la sicurezza ICT
- K030 - gli sviluppi rilevanti dell'ICT ed il loro potenziale impatto sui processi
- K036 - i differenti documenti tecnici richiesti per la progettazione, lo sviluppo e il deploying dei prodotti, delle applicazioni e dei servizi
- K037 - i differenti modelli di servizio (SaaS, PaaS, IaaS) e operativi (per esempio Cloud Computing)
- K048 - i metodi di ricerca, benchmark e metodi di misurazione
- K058 - i problemi e le implicazioni dei servizi di outsourcing
- K067 - i rischi critici per la gestione della sicurezza

- K068 - i service level agreement (SLA) applicabili
- K070 - i tipici “Termini e condizioni” dei contratti di acquisto
- K075 - i valori ed interessi dell’azienda cui applicare l’analisi del rischio
- K080 - il mercato corrente dei prodotti e servizi rilevanti
- K085 - il ritorno dell’investimento comparato all’annullamento del rischio
- K090 - l’approccio all’auditing interno del sistema informativo
- K098 - l’impatto dei requisiti legali sulla sicurezza dell’informazione
- K112 - la documentazione dello SLA
- K115 - la politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, i fornitori e i sub-contraenti
- K130 - le best practice (metodologie) e gli standard nell’analisi del rischio
- K132 - le best practice e gli standard nella gestione della sicurezza delle informazioni
- K158 - le possibili minacce alla sicurezza
- K175 - le tecniche dei processi di innovazione
- K188 - le tecniche di valutazione dei rischi e delle opportunità
- K197 - le tecnologie emergenti e le applicazioni più importanti del mercato
- K217 - I gruppi APT
- K218 - I malware
- K220 - Indicatori chiave di sicurezza
- K222 - La continuità operativa
- K224 - La gestione degli incidenti di sicurezza
- K227 - La prioritizzazione degli indicatori di compromissione
- K228 - La threat intelligence
- K229 Le botnet
- K230 Le Kill chain
- K231 Le possibili minacce alla continuità operativa ICT
- K232 Le tecniche di attacco
- K233 Le tecniche di difesa
- K234 Le tecniche di evasione
- K235 Le tecniche di mitigazione degli attacchi ransomware
- K236 Metodi di autenticazione
- K237 Metodi e strumenti per l'accesso agli archivi digitali
- K238 Modelli di sicurezza
- K239 Protocolli di autenticazione e autorizzazione
- K240 Protocolli di sicurezza delle applicazioni web
- K241 Protocolli ed architetture di rete
- K242 Strumenti di prevenzione e rilevamento delle minacce
- K243 Tecniche di anonimizzazione delle comunicazioni
- K244 Tecniche di attacco all’anonimizzazione
- K245 Tecniche di attacco alla disponibilità dei servizi e mitigazione
- K246 Tecniche di autenticazione dei messaggi
- K247 Tecniche di crittografia
- K248 Tecniche di messa in sicurezza della posta elettronica
- K249 Tecniche di progettazione sicura
- K250 Tecniche di security assessment
- K251 Tecniche di security code review
- K252 Tecnologie di controllo degli accessi
- K253 Minacce informatiche

Area di applicazione dei KPI

- Aggiornamento delle policy per la sicurezza delle informazioni
- Aggiornamento delle clausole contrattuali per la sicurezza delle informazioni
- Incidenti relativi alla sicurezza delle informazioni di tutta l'organizzazione
- Verifiche sia interne sia esterne sulla sicurezza delle informazioni
- Ritorno d'investimento sulle spese per la sicurezza delle informazioni
- Indicatori sulla sicurezza delle informazioni
- Progresso del piano di sicurezza / di trattamento del rischio

2.2 REQUISITI DI ACCESSO AL PROCESSO DI VALUTAZIONE DELLA CONFORMITÀ (ESAME DI CERTIFICAZIONE)

Ai fini dell'accesso al processo di valutazione di conformità (esame di certificazione), si riportano di seguito i seguenti requisiti (Prospetto A.2 - Elementi per l'accesso al processo di valutazione della conformità della UNI 11506:2021)

Requisiti relativi all'apprendimento formale	Il titolo di studio minimo previsto deve corrispondere al livello 3 dell'EQF, corrispondente al livello e-1 della Dimensione 3 (livelli di capacità delle e-Competence) e della UNI EN 16234-1:2020
Requisiti relativi all'apprendimento non formale	Ove previsti nella specifica parte della serie UNI 11621, i requisiti dovrebbero essere specificati in termini di crediti formativi e ambito degli stessi (per esempio con parametro 1 ora 1 credito) conseguiti alla data della presentazione della domanda o negli ultimi 24 o 36 mesi. Nello specifico si ritiene come livello minimo di crediti conseguiti: • **Responsabile della sicurezza delle informazioni (CISO) - Prospetto 6 della UNI 11621-4:2024 -** almeno 8 ore negli ultimi 12 mesi.
Requisiti relativi all'apprendimento informale (esperienza)	• **Responsabile della sicurezza delle informazioni (CISO) - Prospetto 6 della UNI 11621-4:2024 -** almeno 4 anni di esperienza comprovata. I requisiti di cui al presente punto sono soggetti a riduzione del 50% nel caso di possesso di un titolo di studio di livello 5 dell'EQF o superiore e del 20% nel caso di possesso di un titolo di studio al livello 4 o 5 dell'EQF
NOTE	Si precisa che, come indicato nella norma UNI 11596:2021 nell'Appendice A – punto A.3 – Nota 1- Secondo capoverso, nel processo di valutazione della conformità relativa ai risultati dell'apprendimento, è possibile tener conto del possesso, da parte del singolo candidato, di attestazioni rilasciate da associazioni professionali iscritte alla Sezione 2 dell'elenco del Ministero delle Imprese e del Made in Italy (ex MISE), ai sensi dell'Art.2 comma 7 della Legge 4/2013. Rimangono comunque validi i requisiti di cui ai punti 5.2.2 e 9.2.6 della UNI CEI EN ISO/IEC 17024:2012. **ATTENZIONE tale aspetto non è un elemento esimente per l'esame o parte di esso, è considerato utile esclusivamente per dimostrare e garantire il possesso dei requisiti per accedere all'esame di certificazione.**

2.3 TIPOLOGIA DI ESAME E MODALITÀ

Nella tabella di seguito sono indicate le prove che possono essere inserite negli schemi di certificazione specifici.

Tipologia	**Dettaglio**	Valutazione	Tempo massimo di esecuzione della prova
Analisi e valutazione del CV	Analisi dei requisiti di ammissibilità all'esame sulla base di quanto richiesto dalla norma UNI 11506 e UNI 11621-4. Come indicato si richiede CV completo, datato, firmato e con liberatoria Privacy e Dlgs 445. Il Cv può anche essere firmato digitalmente. Le evidenze relative ad apprendimento non formale (corsi) e informale (esperienza) possono essere di vario genere, ad esempio: attestazione della associazione di appartenenza ai sensi della Legge 4, attestati di frequenza di corsi, altre certificazioni anche di "vendor", dichiarazione del datore di lavoro ~~o lettere di incarico o comunicazioni~~ organizzative interne all'azienda ecc. ecc	Si vedano requisiti par. 2.2	
Prova scritta con domande a risposta chiusa	Esame scritto per la valutazione delle conoscenze. Esame composto da 160 domande a risposta chiusa (4 risposte di cui 1 sola veritiera). Le domande sono formulate con riferimento alle conoscenze e abilità riportate nella norma UNI 11621-4 per profilo specifico.	Ogni domanda vale 0,5 punti per un massimo di 80. Totalizzando un punteggio di almeno 50 punti si è ammessi alla prova orale.	2 ore e 40 minuti
Prova orale	Esame orale. Se il candidato ha conseguito un totale uguale o maggiore a 70 punti tra prova scritta e di laboratorio, la prova orale si considera superata e si discute brevemente l'esito delle prove precedenti e l'esaminatore fornisce consiglio e orientamento su eventuali approfondimenti. Se il candidato ha conseguito un totale tra 50 e 69 punti deve rispondere a 4 domande basate sugli argomenti con le risposte sbagliate nella prova scritta. Ciascuna domanda porta fino a 5 punti.	≥ 70 punteggio totale con le prove precedenti	Durata minima: 10 minuti Durata massima: 20 minuti

2.3.1 Domande della prova scritta

Le domande della prova scritta sono progettate per avere lo stesso peso in termini di difficoltà e devono coprire le conoscenze previste dal profilo di ruolo professionale.
Per avere lo stesso punteggio in termini di difficoltà le domande devono avere le seguenti caratteristiche:

- Il tempo stimato per comprendere e rispondere deve essere simile
    - Formulazione della domanda chiara e sintetica

- Risposte formulate in modo sintetico da leggere
- La domanda non deve andare a trattare argomenti troppo di dettaglio.

2.3.2 Domande della prova orale

Le domande della prova orale sono progettate nello stesso modo della prova scritta ma il punteggio viene assegnato dall'esaminatore in base a una griglia di valutazione (vedi par.2.4.1). Viene valutata chiarezza nell'esposizione (appropriatezza risposta) e la padronanza dell'argomento (comprensione della domanda). L'esaminatore sceglie la domanda fra quelle o fra quelle della prova scritte in cui è risultato incerto o carente.

2.4 PROGRAMMA DELLE PROVE

La commissione garantisce la sua presenza circa 30 minuti prima dell'inizio della sessione d'esame pianificata, per effettuare la verifica delle condizioni ottimali della prova.

I candidati devono comunicare preventivamente alla segreteria eventuali necessità connesse allo svolgimento delle prove d'esame, in modo da permettere all'ente di predisporre le eventuali misure di intervento.

Le prove si svolgeranno nel seguente ordine:
1. Prova scritta di verifica delle conoscenze
2. Prova orale

Le prove vengono svolte nella stessa giornata in sessione remota. Il programma delle attività per la giornata segue indicativamente il programma dato sotto:

Orario	Attività
9.00	Identificazione candidati e presentazione dell'esame, programma delle prove, criteri di valutazione, modulistica d'esame, procedura di segnalazione ricorsi e reclami
9.30	Prova scritta
12.10	Conclusione prova scritta
14.00	Avvio prove orali
18.00	Redazione Verbale Esame e conclusione giornata

2.4.1 Descrizione e criteri di valutazione delle Prove

- **Prova scritta**

Le domande della prova scritta sono 160. La durata della prova è 2 ore e 40 minuti. Si tratta di un test "closed book", quindi non è permesso consultare documenti.

Le domande sono a risposta chiusa con 4 alternative, di cui una sola esatta. La valutazione è fatta a fronte del modello delle risposte esatte.

Il candidato deve evidenziare la risposta per lui corretta, ciascuna risposta corretta vale 0,5 punti, quelle sbagliate o non date valgono 0 punti; non si assegnano punteggi negativi.

Il risultato della prova è vincolante per l'accesso alla successiva prova orale.

I risultati verranno forniti prima dell'avvio delle prove orali.

- **Prova orale**

La prova orale ha lo scopo di approfondire eventuali incertezze riscontrate nella prova scritta. Ha una durata minima di 10 minuti e massima di 20 minuti.

Se il candidato ha totalizzato tra i 50 e 69 punti, verrà sottoposto a quattro domande, ciascuna valevole per un massimo di 5 punti. Le domande devono riguardare gli argomenti che nella prova scritta sono risultati incerti o carenti.

Se il candidato totalizza, secondo la tabella riportata sotto, almeno 70 punti rispondendo alle domande, la prova è superata.

Se il candidato ha totalizzato 70 o più punti si discute il risultato della prova precedente dando indicazioni dei punti di possibile approfondimento. La prova orale si considera quindi superata.

Tabella valutazione prova orale relativamente alla risposta a una domanda

Valore	Ambito	Giudizio
0	Comprensione domanda	Il candidato resta in silenzio e non risponde alla domanda
	Appropriatezza risposta	La risposta è assente
1	Comprensione domanda	Il candidato non ha compreso la domanda
	Appropriatezza risposta	La risposta non è pertinente all'ambito della domanda. Il candidato mostra assenza di padronanza dell'argomento
2	Comprensione domanda	Il candidato ha compreso parzialmente la domanda
	Appropriatezza risposta	La risposta è generica e non soddisfacente o non completamente pertinente. Il candidato mostra assenza di padronanza dell'argomento
3	Comprensione domanda	Il candidato ha compreso la domanda
	Appropriatezza risposta	La risposta pur essendo appropriata è incompleta o incerta. Il candidato mostra una certa padronanza dell'argomento non ancora sufficiente
4	Comprensione domanda	Il candidato ha compreso pienamente la domanda
	Appropriatezza risposta	La risposta è completa ma non dettagliata. Il candidato mostra sufficiente padronanza dell'argomento.
5	Comprensione domanda	Il candidato ha compreso la domanda dando prova di una comprensione globale negli aspetti professionali collegati
	Appropriatezza risposta	La risposta è completa e dettagliata. Il candidato mostra ottima padronanza dell'argomento.

Le prove nel loro insieme devono dare una copertura quanto più possibile completa all'insieme di abilità, conoscenze e competenze definite nei singoli profili.

Al termine della prova orale del candidato, la commissione lo informa dell'esito dell'esame, ricordando che, se l'esito è risultato positivo, la delibera di certificazione finale spetta all'organo di delibera.

2.5 REQUISITI DELLA POSTAZIONE DEL CANDIDATO

Per poter partecipare alle prove di esame il candidato deve disporre di una postazione che soddisfi i seguenti requisiti:

- Si trovi in una stanza o un ambiente privato in cui nessun'altra persona sia presente;
- Una postazione computer con prestazioni sufficienti a svolgere le attività delle prove;
- una connessione internet stabile e affidabile per potersi connettere alle piattaforme necessarie allo svolgimento delle prove;
- Assicurarsi che la postazione che si intende utilizzare non sia soggetta a controlli di rete o policy di sicurezza che impediscano di raggiungere le piattaforme necessarie allo svolgimento delle prove;
- Webcam che lo inquadri in primo piano, compreso l'ambiente circostante;
- Microfono;
- Documento di riconoscimento in corso di validità per l'identificazione;
- La scrivania della postazione usata per l'esame dovrà essere sgombra. Non sono ammessi ne fogli ne libri.

2.6 REGOLE A GARANZIA DI EQUITÀ E VALIDITÀ DELLE PROVE

Al fine di garantire equità e validità delle prove di esame, saranno applicate le seguenti regole:

- Il candidato dovrà essere munito di documento di identità in corso di validità da esibire in fase di accertamento delle presenze attraverso la propria webcam mentre compaiono in primo piano su richiesta dell'esaminatore.
- Il candidato potrà partecipare da qualsiasi luogo, ma è obbligatorio che scelga una stanza o un ambiente privato, privo di fonti di rumore che possano sovrastare le prove di esame, in cui nessun'altra persona sia presente, al fine di evitare interferenze o aiuti non autorizzati. Tale ambiente dovrà essere dotato di pareti, una porta chiusa, ed essere libero da ostacoli.
- Verrà chiesto al candidato di inquadrare di inquadrare la stanza per verificare le suddette condizioni e di inquadrare la scrivania della postazione per assicurare che sia sgombra, fatta eccezione per tastiera e mouse.

- Il candidato dovrà spegnere il proprio telefono cellulare e tenerlo spento per tutta la durata delle prove di esame.
- La webcam dovrà inquadrare il volto del candidato e l'ambiente circostante durante tutto il corso dell'esame, e dovranno mantenere una sistemazione in posizione tale da garantire il corretto e continuo monitoraggio dell'ambiente circostante e del volto.
- Il candidato dovrà tenere il microfono acceso per tutta la durata delle prove.
- Il candidato dovrà mantenere condiviso lo schermo del suo Desktop durante la prova scritta.
- Verrà compilato da un esaminatore il registro delle presenze.
- Una volta avviato l'esame, nessuno dovrà entrare nella stanza.
- Il candidato non potrà per nessun motivo alzarsi e allontanarsi dalla postazione per tutta la durata delle prove di esame.

se anche una di queste regole non venisse rispettata dal candidato, sarà allontanato dalla sessione e il suo esame annullato.

2.6.1 Prova scritta

La prova scritta viene svolta "closed book", quindi non è permesso consultare durante la prova:

- libri o appunti;
- risorse online;
- più in generale materiale di testo scritto.

Eventuali telefoni cellulari dovranno essere spenti.

2.6.2 Gestione problemi di connessione

Nell'eventualità si verificassero problemi di connessione la commissione si attiverà per risolverli immediatamente garantendo che il tempo previsto per la prova non venga ridotto a causa degli interventi necessari a ripristinare l'operatività.
Qualora non fosse possibile ripristinare l'operatività, i candidati interessati dal problema potranno ripetere l'esame alla data di esame più vicina. Se il guasto fosse relativo alla postazione del candidato questa possibilità viene garantita solo per una volta, dopodiché dovrà pagare nuovamente la quota di iscrizione per sostenere nuovamente l'esame.

2.7 VALUTAZIONE COMPLESSIVA DELLE PROVE

La piattaforma software che registra le risposte alle domande della prova scritta riporta la valutazione seguendo i parametri definiti nello schema di certificazione e fornisce un rapporto di feedback sulle aree risultate carenti.
L'esame si intende superato se il candidato totalizza un punteggio finale di 70 alla conclusione della prova orale.

2.8 DECISIONE/DELIBERA DELLA CERTIFICAZIONE

L'organo di delibera, verificati gli esiti delle prove di esame, controllata l'analisi documentale e verificate le evidenze prodotte dal candidato, delibera la certificazione se ne ricorrono gli estremi, ovvero se i requisiti di schema sono soddisfatti e il risultato dell'esame di certificazione è positivo.

2.9 REQUISITI PER IL MANTENIMENTO DELLA CERTIFICAZIONE

Frequenza mantenimento:	Annuale
Modalità di mantenimento:	Il mantenimento della certificazione si basa sui seguenti elementi di base: • assenza o corretta gestione di reclami • continuo esercizio della professione • incremento di crediti formativi o incremento della formazione professionalizzante nel caso di perdita di lavoro • aggiornamento professionale secondo i seguenti livelli minimi: ○ per professione manageriale (ovvero livello medio e-CF 4-5) almeno 8 ore di crediti conseguiti negli ultimi 12 mesi;

Il professionista certificato dovrà dare evidenza in modo appropriato di quanto sopra richiesto. Riceverà notifica e-mail con le istruzioni e gli allegati necessari alla domanda di mantenimento in ottemperanza a quanto indicato dalla normativa di riferimento come indicato sopra.

Nel caso in cui, invece, siano presenti periodi di discontinuità operativa, reclami o contenziosi legali, spetta a Fata Informatica in totale autonomia valutarne la relativa gestione.
L'attività di sorveglianza deve avere come esito documentato il mantenimento, la sospensione o la revoca della certificazione a fronte della valutazione da parte di Fata Informatica in merito alla completezza, congruità della documentazione presentata nonché gestione di eventuali reclami e/o contenziosi amministrativi o legali.
Fata Informatica può prevedere di applicare delle deroghe/tolleranze alla periodicità dei mantenimenti nel ciclo di certificazione, nel caso in cui la persona certificata sia in maternità/paternità o abbia avuto difficoltà operative dovute a problemi fisici o legati alla salute.

2.10 RINNOVO DELLA CERTIFICAZIONE

Durata della certificazione:	La certificazione ha durata di anni 5 (cinque).
Modalità di rinnovo:	Il Rinnovo della certificazione si basa sui seguenti elementi di base: • assenza o corretta gestione di reclami • continuo esercizio della professione • incremento di crediti formativi o incremento della formazione professionalizzante nel caso di perdita di lavoro • somma dei crediti acquisiti in ogni anno di mantenimento precedenti il rinnovo • esame di rinnovo certificazione • pagamento della quota di Esame di rinnovo

Il professionista certificato riceverà notifica e-mail con le istruzioni e gli allegati necessari alla domanda di rinnovo in ottemperanza a quanto indicato dalla normativa di riferimento.
I professionisti certificati potranno procedere a richiesta del rinnovo della certificazione attraverso l'apposita domanda sul sito.
La domanda viene valutata da Fata Informatica che valuta l'ammissione all'esame di certificazione ai fini del rinnovo.
La documentazione fornita viene esaminata per valutare se il professionista soddisfa le condizioni previste per confermare la competenza della figura professionale, tenendo conto anche degli eventuali aggiornamenti dei requisiti, degli sviluppi tecnologici, dell'evoluzione del settore di pertinenza dello schema. Sottoscrive, inoltre, l'autodichiarazione relativa ad assenza di reclami dalle parti interessate o alla loro corretta gestione, se ricevuti. Inoltre, devono essere forniti gli eventuali ulteriori documenti/evidenze previsti dallo schema.
In caso di esito positivo la persona certificata si iscrive all'esame e paga la prevista quota.
L'esame per il rinnovo è il medesimo di quello che si svolgerebbe per una prima certificazione.

Peraltro, nel caso di variazioni normative e/o legislative la verifica di aggiornamento può essere eseguita in qualsiasi altro momento, in funzione dell'entrata in vigore delle variazioni.

In funzione degli esiti il certificato può essere rinnovato, sospeso o revocato.

2.11 SOSPENSIONE E REVOCA

Dopo l'emissione del certificato, nel caso in cui venga accertato che si è verificata anche una sola delle seguenti situazioni:

- violazione del codice deontologico;
- mancata richiesta di rinnovo entro il periodo previsto;
- mancato versamento della quota di rinnovo;
- mancata sottoscrizione, entro i termini previsti dal Regolamento generale, della documentazione contrattuale;
- mancata integrazione della documentazione richiesta al momento del rinnovo della certificazione;
- richiesta da parte della persona certificata;

viene applicato il provvedimento di sospensione.
La sospensione del certificato ha durata massima di 4 mesi; nella comunicazione di sospensione viene richiesto alla persona certificata di provvedere per risolvere i problemi che l'hanno causata con l'indicazione della scadenza massima.
Durante il periodo di sospensione la persona certificata deve rispettare i seguenti obblighi:

- sospendere l'impiego dei marchi di Fata Informatica;
- dare comunicazione ai propri committenti dell'avvenuta sospensione;
- non qualificarsi come persona certificata da Fata Informatica.

Nel in cui caso la persona certificata non provveda, entro i termini previsti, a risolvere le problematiche per cui è stato applicato il provvedimento di sospensione, Fata Informatica procede a ridurre il campo di applicazione o a revocare la certificazione.
La revoca comporta la cancellazione dal Registro delle persone certificate.

2.12 CODICE DEONTOLOGICO

Tutte le persone che hanno conseguito la certificazione o in corso di certificazione sono tenute al rispetto delle norme di etica deontologica e condotta professionale contenute nel codice deontologico definito da Fata Informatica. Il codice deontologico è un documento pubblico disponibile sul sito di Fata Informatica.
L'accettazione ed il rispetto di tali norme è ritenuta presupposto necessario per il rilascio della certificazione da parte di Fata Informatica ed il mantenimento/rinnovo della stessa.

2.13 MARCHIO DELLO SCHEMA DI CERTIFICAZIONE

Per il presente Schema di Certificazione Fata Informatica ha previsto un Marchio la cui grafica viene riportata in figura sotto.

Figura 1 - Marchio dello Schema di Certificazione

Le regole per l'uso del Marchio sono riportate nel Regolamento Generale di Fata Informatica. Il Regolamento Generale è un documento pubblico disponibile sul sito di Fata Informatica.