

**REGISTRO DEI RUOLI PROFESSIONALI RELATIVI
ALL'INTELLIGENZA ARTIFICIALE
COERENTI CON IL REGOLAMENTO EUROPEO (UE) 2024/1689 (AI ACT)**

Revisioni:

00	27/07/2026	Prima stesura ed emissione	Team AI AICQ SICEV	C. D'Aquaro	D. Gilormo
Rev.	Data	Motivo Revisione	Preparato da Referente Schema/Direttor e/Resp. SGQ	Verificato da Presidente CSI/ Resp SGQ / Direttore/ Resp. Tecnico	Approvato da Presidente/ A.D.

INDICE

INDICE	2
1. Scopo e campo di applicazione.....	3
1.1 Definizione dei profili professionali relativi all'Intelligenza Artificiale coerenti con l'AI Act	3
Governance e accountability	3
Etica e impatto sociale.....	3
Rischio e conformità	4
Implementazione e sistemi di gestione	4
Utilizzo competente e AI literacy.....	4
2. Quadro documentale.....	5
2.1 Documenti di base	5
2.2 Documenti applicabili	5
2.3 Documenti di riferimento	6
3. Definizioni e acronimi	7
4. Requisiti specifici per la certificazione.....	8
4.1 Struttura del Registro	8
4.2 Requisiti minimi	8
4.3 Domanda per accedere al processo di certificazione	8
4.4 Rinnovo, sorveglianza e mantenimento della certificazione.....	9
4.5 Certificazione per più profili	9
4.6 Trasferimento da un differente Organismo di Certificazione.....	Errore. Il segnalibro non è definito.
5. Processo di certificazione ed esame per la certificazione AICQ SICEV	10
5.1 Modalità e argomenti di esame.....	10
5.2 Materie di esame.....	11
5.3 Criteri di superamento dell'esame	11
5.4 Commissione esaminatrice.....	11
5.5 Documentazione di certificazione	12
Allegato 1 - Requisiti minimi e schede profilo	13
Allegato 2 - Sintesi delle materie di esame per profilo	34
Allegato 3 – Fac-simile modello di presentazione esperienze lavorative.....	35
Allegato 4 - Bibliografia e fonti di riferimento.....	37

1. Scopo e campo di applicazione

Il presente Registro individua e disciplina nove profili di ruolo professionale relativi all'Intelligenza Artificiale, complementari a quelli previsti dalla norma UNI 11621-8 e definiti in coerenza con il Regolamento (UE) 2024/1689 sull'Intelligenza Artificiale ("AI Act"), con particolare riferimento agli obblighi di governance, sorveglianza umana (art. 14), AI literacy (art. 4), gestione del rischio, trasparenza e conformità normativa ivi previsti.

I profili descritti nel presente Registro sono riconosciuti dal mercato e non sono disciplinati dalla UNI 11621-8; essi rispondono a esigenze organizzative e di conformità emerse dall'applicazione pratica dell'AI Act, in particolare laddove la normativa attribuisce obblighi e responsabilità a ruoli e funzioni non necessariamente coincidenti con i profili tecnici di sviluppo AI. La certificazione è rilasciata da AICQ SICEV nel rispetto della UNI CEI EN ISO/IEC 17024 e dei regolamenti generali dell'ente.

Il Registro si articola in nove profili professionali distinti, ciascuno con missione, responsabilità, risultati attesi e requisiti di accesso specifici. I profili sono concepiti come complementari tra loro e rispetto ai profili UNI 11621-8: ogni figura presidia un ambito distinto della governance, dell'implementazione o dell'uso dell'Intelligenza Artificiale e può operare in raccordo con le altre nell'ambito di strutture organizzative complesse, oppure coincidere nella stessa persona nelle organizzazioni di minori dimensioni.

Il presente documento regola i rapporti intercorrenti tra AICQ SICEV, quale Organismo di Certificazione del personale, e le persone fisiche che richiedono tale certificazione volontaria

1.1 Definizione dei profili professionali relativi all'Intelligenza Artificiale coerenti con l'AI Act

I nove profili sono raggruppati per area funzionale. Il Registro non prevede una gerarchia tra i profili e più profili possono coincidere nella stessa persona, in particolare nelle PMI.

Governance e accountability

AI Human Overseer & Chief Governance Officer	Presidia la sorveglianza umana sui sistemi AI ad alto rischio ex art. 14 AI Act e la governance complessiva dell'AI dell'organizzazione.
Corporate Planner AI-Ready	Integra l'impatto dell'AI nella pianificazione strategica e operativa dell'organizzazione.

Etica e impatto sociale

AI Ethicist	Presidia le implicazioni etiche, sociali e valoriali dei sistemi AI.
AI Community Juror	Rappresenta la prospettiva civica di cittadini e utenti nei processi di governance dei sistemi AI ad elevato impatto sociale.

Rischio e conformità

AI Risk Assessor	Identifica, valuta e monitora i rischi associati ai sistemi AI lungo il ciclo di vita.
AI Compliance Auditor	Verifica la conformità di sistemi, processi e documentazione AI rispetto a requisiti normativi e standard applicabili.

Implementazione e sistemi di gestione

AI MS LEAD IMPLEMENTER AND INTERNAL AUDITOR ISO/IEC 42001	Guida l'implementazione di progetti AI e del sistema di gestione dell'AI (AIMS) conforme a ISO/IEC 42001 e ne conduce gli audit interni.
--	--

Utilizzo competente e AI literacy

Competent Ai User	Utilizza sistemi AI nell'ambito delle proprie mansioni con consapevolezza di capacità, limiti e rischi.
AI Literate	Possiede le conoscenze basilari sull'AI richieste a chiunque entri in contatto, anche indirettamente, con sistemi AI in azienda.

I nove profili sono descritti nel presente documento con struttura regolamentare omogenea, coerente con quella adottata per i profili UNI 11621-8, arricchita da dettagli operativi e criteri di valutazione specifici per l'AI Act.

2. Quadro documentale

Se non esplicitamente citata, si intende come valida l'ultima edizione emessa dei sotto citati documenti.

2.1 Documenti di base

Costituiscono documenti di base del presente Regolamento:

- Regolamento (UE) 2024/1689 sull'Intelligenza Artificiale (AI Act);
- serie UNI 11621 sui profili professionali ICT, con particolare riferimento alla UNI 11621-8 per i profili AI Governance, quale riferimento sistematico e complementare;
- UNI 11506 sulle attività professionali non regolamentate;
- UNI EN 16234 (e-CF) sul quadro europeo delle competenze ICT;
- UNI CEI EN ISO/IEC 17024 sui requisiti per gli organismi che effettuano la certificazione di persone;
- regolamenti generali di AICQ SICEV applicabili alla certificazione delle competenze professionali.

2.2 Documenti applicabili

Sono considerati applicabili ai fini del presente Regolamento:

- Politica, Vision, Mission di AICQ SICEV
- Manuale del Sistema di Gestione per la Qualità di AICQ SICEV e relative Procedure
- Codice etico e deontologico per l'integrità professionale
- Regolamento (UE) 2024/1689 sull'Intelligenza Artificiale (AI Act), con particolare riferimento agli artt. 4 (AI literacy), 14 (sorveglianza umana), 16-17 (obblighi del provider e sistema di gestione della qualità) e 26 (obblighi del deployer);
- Regolamento (UE) 2016/679 (GDPR);
- ISO/IEC 42001:2023 sui sistemi di gestione dell'AI (AIMS);
- ISO/IEC 22989:2022 sui concetti e terminologia dell'intelligenza artificiale;
- ISO/IEC 23894:2023 sulla gestione del rischio AI;
- ISO/IEC 25059 sulla qualità dei sistemi AI;
- ISO/IEC 38507:2022 sulle implicazioni di governance derivanti dall'utilizzo dell'intelligenza artificiale da parte delle organizzazioni;
- ISO 31000:2018 sulla gestione del rischio;
- ISO 19011:2018 sulle linee guida per l'audit dei sistemi di gestione;
- standard tecnici o documenti di indirizzo richiamati nei singoli profili.

2.3 Documenti di riferimento

Costituiscono riferimenti professionali rilevanti:

- NIST Artificial Intelligence Risk Management Framework 1.0 (NIST AI RMF);
- OECD AI Principles del 2019 e aggiornate nel 2024;
- UNESCO Recommendation on the Ethics of Artificial Intelligence del 2021;
- Ethics Guidelines for Trustworthy AI della Commissione europea (HLEG AI, 2019);
- serie IEEE 7000 sull'etica nei sistemi autonomi;
- rapporti tecnici ISO/IEC TR 24027 (bias);
- ISO/IEC TR 24028 (trustworthiness);
- ISO/IEC TR 24368 (implicazioni etico-sociali);
- Linee guida della Commissione europea e dell'AI Office sull'applicazione del Regolamento (UE) 2024/1689.
- Legge 14 gennaio 2013 n.4, Disposizione in materia di professioni non organizzate (Gazzetta Ufficiale della Repubblica Italiana n. 22 del 26 gennaio 2013)
- CEN Guide 14:2010 – Common policy guidance for addressing standardization on qualification of professions and personnel

3. Definizioni e acronimi

Ai fini del presente Regolamento si applicano le seguenti definizioni. I termini vanno intesi secondo il significato attribuito loro dagli standard e dai documenti normativi richiamati al capitolo 2.

AI Act	Regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'Intelligenza Artificiale nel mercato interno europeo.
AI Governance	Insieme di politiche, processi, ruoli, responsabilità, controlli e meccanismi decisionali che guidano sviluppo, acquisizione, deployment, uso e dismissione dei sistemi AI.
AIMS	Artificial Intelligence Management System: sistema di gestione dell'AI conforme alla ISO/IEC 42001.
AI Literacy	Insieme di competenze, conoscenze e comprensione che consentono a fornitori, deployer e persone interessate di utilizzare i sistemi AI in modo informato, tenendo conto delle loro capacità, opportunità e rischi, ai sensi dell'art. 4 del Regolamento (UE) 2024/1689.
Sorveglianza umana / Human Oversight	Insieme di misure tecniche e organizzative, di cui all'art. 14 del Regolamento (UE) 2024/1689, volte a consentire a persone fisiche di sorvegliare efficacemente il funzionamento di un sistema AI ad alto rischio, prevenendo o riducendo al minimo i rischi per la salute, la sicurezza o i diritti fondamentali.
Provider / Fornitore	Soggetto che sviluppa un sistema AI o lo fa sviluppare e lo immette sul mercato o lo mette in servizio, ai sensi del Regolamento (UE) 2024/1689.
Deployer / Utilizzatore	Soggetto che utilizza un sistema AI sotto la propria autorità nell'ambito di un'attività professionale, ai sensi del Regolamento (UE) 2024/1689.
AIA	Algorithmic Impact Assessment: valutazione strutturata degli impatti generati da un sistema algoritmico su persone, processi e diritti.
DPIA	Data Protection Impact Assessment: valutazione d'impatto sulla protezione dei dati personali ai sensi dell'art. 35 GDPR.
AI Registry	Registro organizzativo dei sistemi AI, contenente informazioni su finalità, responsabili, classificazione di rischio, documentazione tecnica e monitoraggio.
Trustworthy AI	AI affidabile, fondata su legalità, eticità, robustezza tecnica, supervisione umana, trasparenza e accountability, secondo le linee guida HLEG.
XAI	Explainable Artificial Intelligence: insieme di metodi e pratiche volti a rendere interpretabili e spiegabili le decisioni dei sistemi AI.
HITL / HOTL / HIC	Human In The Loop / Human On The Loop / Human In Command: modalità di sorveglianza o intervento umano nel funzionamento di un sistema AI, finalizzate a garantire il controllo e la responsabilità decisionale.
e-CF	European e-Competence Framework (UNI EN 16234): quadro di riferimento europeo per le competenze ICT, strutturato su cinque aree e quattro livelli EQF.
EQF	European Qualifications Framework: quadro europeo delle qualifiche, strutturato su otto livelli, utilizzato per classificare le qualificazioni professionali.

4. Requisiti specifici per la certificazione

4.1 Struttura del Registro

AICQ SICEV intende gestire la certificazione dei 9 Profili Professionali complementari relativi all'AI Governance e all'applicazione del Regolamento (UE) 2024/1689, coerentemente con la legge 4/2013 e con i documenti richiamati al capitolo 2.

4.2 Requisiti minimi

Con riferimento a quanto indicato nel Regolamento Generale RG 03, i requisiti minimi per il percorso di certificazione risultano strettamente legati al profilo selezionato.

L'accesso alla certificazione si fonda sulla valutazione complessiva dell'esperienza, della competenza e della conoscenza della materia dimostrate dal candidato.

I requisiti formali di seguito elencati costituiscono riferimenti orientativi; la commissione d'esame valuta con autonomia professionale la sostanza delle competenze acquisite.

Per tutti i profili sono considerati:

- titolo di studio coerente con il profilo; in alternativa, esperienza professionale documentata e comprovata competenza nella materia costituiscono percorso equivalente a pieno titolo (fatta eccezione per il profilo AI Literate, per il quale non è richiesto alcun titolo di studio);
- esperienza complessiva nel settore ICT, AI o in ambiti affini, ove pertinente al profilo;
- esperienza specifica nelle attività caratterizzanti il profilo richiesto;
- formazione specialistica pertinente;
- produzione di evidenze professionali verificabili, ove applicabile.

La compensazione tra titolo di studio ed esperienza professionale è sempre ammessa e incoraggiata: il Registro intende valorizzare professionisti motivati, esperti e competenti nella materia, indipendentemente dal percorso formativo formale seguito.

Per i dettagli dei singoli profili si rimanda alle schede di Allegato 1.

Per i profili di Governance, Etica, Rischio, Conformità e Implementazione è richiesta conoscenza trasversale dei seguenti ambiti: AI Act e principi fondamentali di governance AI; gestione del rischio AI; protezione dei dati personali e GDPR; principi di etica e AI affidabile; documentazione tecnica e audit readiness; miglioramento continuo e sorveglianza umana. Il livello di profondità e le competenze specifiche variano in funzione del profilo e del livello EQF associato.

Per i profili Competent AI User e AI Literate la conoscenza richiesta è limitata agli elementi essenziali dell'AI Act in materia di AI literacy e ai comportamenti di uso corretto e sicuro.

4.3 Domanda per accedere al processo di certificazione

Il candidato che vuole accedere al processo di certificazione dovrà presentare idonea documentazione, ovvero la Domanda di esame di certificazione comprensiva della documentazione indicata dal regolamento RG03, e dichiarare di non avere in corso altre richieste di certificazione per il medesimo profilo.

Oltre alla documentazione richiesta, per la certificazione nel/i profilo/i professionale/i di cui al presente Registro (con esclusione del profilo AI Literate, per il quale si applica una procedura semplificata di cui al par. 4.2), il candidato dovrà produrre:

- una dichiarazione ai sensi del DPR 445/2000 di affidabilità giuridica e onorabilità professionale;
- un elaborato di presentazione dell'esperienza lavorativa più significativa a fronte della specifica figura professionale per la quale si richiede la certificazione (vedi Allegato 3).

4.4 Rinnovo, sorveglianza e mantenimento della certificazione

La certificazione ha validità quinquennale e il suo mantenimento è subordinato all'esito positivo della sorveglianza effettuata dall'OdC con cadenza annuale.

Per la sorveglianza e il mantenimento annuale, il candidato dovrà produrre:

- la dimostrazione di continuità dell'attività caratterizzanti il profilo di cui al presente Registro;
- la dimostrazione tramite idonea documentazione di aver continuato il proprio percorso di aggiornamento permanente in materia di AI Act, AI Governance, etica AI, risk management o conformità normativa di almeno 8 ore annue.
- la presenza di eventuali reclami e/o contenziosi relativi all'attività certificata;
- il pagamento regolare delle quote annuali dovute all'Organismo di certificazione.

Per il profilo AI Literate, in ragione della sua natura di livello base e trasversale, la sorveglianza annuale è limitata alla partecipazione a un aggiornamento periodico di AI literacy almeno di 4 ore annue.

Il candidato in sostituzione delle esperienze e delle altre evidenze può presentare una dichiarazione ai sensi del DPR 445/2000 dove vengono elencate esperienze specifiche, partecipazione a corsi o effettuazione di docenza specifica in ambito AI Governance. In caso di presentazione dell'autodichiarazione è richiesto, in aggiunta, l'indicazione di uno o più nominativi/reference che AICQ SICEV si riserva di contattare per verificare la veridicità di quanto dichiarato.

Per il rinnovo quinquennale deve essere presentata la domanda di rinnovo corredata dalla documentazione richiesta per la sorveglianza annuale (continuità lavorativa e formazione) e dal curriculum aggiornato (facoltativo una nuova foto per aggiornare il tesserino digitale)

4.5 Certificazione per più profili

Il candidato, già certificato per almeno un profilo, che richieda la certificazione per altri profili in una sessione successiva dovrà sostenere prove ridotte, secondo le modalità previste dal Regolamento Generale RG 03 e riepilogate nella tabella seguente:

Situazione	Prove ridotte (per ogni profilo aggiuntivo)	Note
Sessione successiva – stesso profilo o profilo affine	20 domande a risposta chiusa + 1 caso studio/prova pratica + orale min. 20 min	Profilo già certificato

Stessa sessione – più profili	10 domande a risposta chiusa + 1 caso studio/prova pratica + orale min. 15 min per ogni profilo aggiuntivo	Esame completo per il profilo più complesso
-------------------------------	--	---

5. Processo di certificazione ed esame per la certificazione AICQ SICEV

Il processo di certificazione come definito dalla UNI CEI EN ISO/IEC 17024 comprende l'insieme delle attività che AICQ SICEV mette in atto per verificare se il candidato soddisfa i requisiti di competenza, abilità e conoscenza richiesti.

Per garantire l'efficacia ed efficienza del processo di certificazione AICQ SICEV: garantisce i necessari requisiti di imparzialità, indipendenza, trasparenza, competenza e assenza di conflitti di interesse; assicura l'omogeneità delle valutazioni; definisce, adotta e rispetta il proprio sistema di gestione per la qualità documentato; assicura la verifica dell'aggiornamento professionale; definisce, adotta e rispetta il proprio codice deontologico; rende pubblico lo schema di certificazione.

5.1 Modalità e argomenti di esame

L'esame di certificazione è strutturato sulla base di tre prove: due prove scritte e un esame orale, ad eccezione del profilo AI Literate per il quale è prevista una prova unica semplificata, come indicato al termine del presente paragrafo.

Prova	Modalità e finalità	Tempo massimo
Prova scritta	Test a risposta chiusa con 40 domande con 4 risposte, di cui una sola esatta (sono escluse le risposte vero/falso).	60 minuti
Caso di studio (per i profili di Governance, Etica, Rischio, Conformità e Implementazione) / Prova pratica (per Competent AI User)	Prova finalizzata a verificare la capacità effettiva del candidato di applicare le competenze richieste in contesti operativi coerenti con le attività professionali di riferimento.	30 minuti
Prova orale	Prova finalizzata ad approfondire eventuali incertezze emerse nelle prove precedenti e a verificare il livello di padronanza delle conoscenze e delle abilità richieste dal profilo, attraverso la formulazione di 4 quesiti.	30-40 minuti

È possibile accedere alla prova orale previo superamento delle prove precedenti. Le prove scritte vengono somministrate ai candidati separatamente. La correzione della prima prova scritta avviene durante lo svolgimento della seconda prova. Non è possibile invertire l'ordine delle prove di esame.

Per il profilo AI Literate l'esame è costituito da un'unica prova a risposta chiusa di 20 domande, della durata massima di 30 minuti, senza caso di studio né prova orale, in ragione della natura di base e trasversale del profilo.

5.2 Materie di esame

In considerazione della specificità dei diversi profili professionali, le materie di esame risultano strettamente legate al profilo selezionato. Le materie comuni ai profili di Governance, Etica, Rischio, Conformità e Implementazione sono indicate nella tabella seguente; per le materie specifiche di ciascun profilo, incluse quelle di Competent AI User e AI Literate.

Si rimanda alle schede di Allegato 1.

1. AI Act (struttura, classificazione del rischio, obblighi, governance, enforcement) 2. ISO/IEC 42001 e sistemi di gestione AI (AIMS) 3. ISO/IEC 23894 e gestione del rischio AI 4. NIST AI Risk Management Framework (AI RMF 1.0) 5. GDPR applicato ai sistemi AI e alle decisioni automatizzate 6. Principi di AI affidabile (trasparenza, spiegabilità, equità, robustezza, sorveglianza umana, accountability) 7. Governance dei dati applicata all'AI 8. European e-Competence Framework (e-CF) e quadro EQF 9. Ruoli e responsabilità nella governance AI 10. Documentazione tecnica e tracciabilità delle decisioni AI 11. Gestione degli incidenti AI 12. Audit readiness e conformità normativa 13. Miglioramento continuo e sorveglianza umana (HITL/HOTL/HIC)

5.3 Criteri di superamento dell'esame

Per superare l'esame, il candidato deve ottenere almeno un punteggio del 70% nelle singole prove. Il voto finale è costituito dalla media delle votazioni delle singole prove.

Per il superamento della prova "caso di studio" o "prova pratica", il valore del punteggio complessivo attribuito è quello della media dei punteggi ottenuti, con il vincolo di aver ottenuto almeno 5/10 per la peggiore delle risposte.

Qualora il candidato non abbia concluso l'esame con esito positivo, le eventuali singole prove superate rimangono valide per 12 mesi e l'esame può essere nuovamente sostenuto.

5.4 Commissione esaminatrice

La commissione esaminatrice deve soddisfare nel suo insieme i seguenti requisiti: conoscenza delle regole e criteri definiti dall'Organismo di Certificazione per l'esame di certificazione in coerenza con quanto richiamato dalla UNI CEI EN ISO/IEC 17024; possesso della certificazione del profilo pertinente o qualificazione equivalente in base a una procedura interna dell'OdC; competenza maturata, a seguito di esperienze lavorative di almeno 5 anni, in ambito AI Governance, con comprovata esperienza nell'ambito di almeno uno dei domini pertinenti al profilo (AI Act e conformità normativa, ISO/IEC 42001, risk management AI, etica AI, audit dei sistemi AI, pianificazione strategica AI o AI literacy).

Si intende che la commissione d'esame, nel suo insieme, abbia competenze superiori a quelle previste per i candidati che sostengono l'esame.

La Commissione è costituita da uno o più esaminatori che coprano le pertinenti competenze richieste dallo schema

I membri delle commissioni non possono essere stati docenti nei corsi di formazione dei candidati, salvo adottare specifiche misure di mitigazione dello specifico rischio di imparzialità.

Sono altresì tenuti a mantenere la riservatezza sulle prove di esame e a cooperare per la loro gestione in sicurezza.

5.5 Documentazione di certificazione

AICQ SICEV rilascia un documento alle persone certificate che attesta la conformità ai requisiti richiesti. Il documento deve almeno riportare: il nominativo della persona certificata con relativo codice fiscale; l'identificazione del profilo professionale e il relativo codice registro; le date di rilascio, di emissione corrente e di scadenza della certificazione; il nome e la firma del responsabile di AICQ SICEV (o suo delegato).

5.6 Aspetti di Sicurezza per i Candidati e i Visitatori

Le sessioni di esame, svolte in presenza, si svolgono solitamente in uffici dove i rischi e le misure adottate sono quelle tipiche di questa attività; non sono di norma richiesti DPI, ma è richiesto di prendere visione dell'informativa presente in sede in merito alle regole comportamentali.

In determinati casi, può essere previsto l'uso di sedi atte ad ospitare esami pratici e che potrebbero pertanto richiedere l'uso dei DPI applicabili; tale uso è disciplinato nelle "Schede di qualificazione sede di esame" che possono essere predisposte da AICQ SICEV stessa o dai suoi Organismi di Valutazione, secondo quanto indicato nella procedura P09.

I Candidati potranno accedere agli uffici solo se accompagnati da personale AICQ SICEV o da essa abilitato.

I Candidati devono qualificarsi/identificarsi, sia in presenza sia da remoto, mostrando un documento valido di riconoscimento, dando così la possibilità al personale responsabile AICQ SICEV di effettuare il riconoscimento e la relativa registrazione nell'apposito spazio previsto nel modulo Verbale - Verbale di Esame.

Per quanto non espressamente previsto nel presente Regolamento di Schema si rimanda al Regolamento Generale Reg 03 e al Regolamento Uso Marchio.

Allegato 1 -Requisiti minimi e schede profilo – Allegato 1.2 Clausola semplificata

Le schede seguenti costituiscono parte integrante del Registro. Ogni profilo è descritto con struttura omogenea per consentire valutazioni coerenti da parte della commissione d'esame, dei candidati e di tutti i soggetti coinvolti nel processo di certificazione.

La struttura comprende: identificazione del profilo; missione e collocazione organizzativa; requisiti minimi di accesso; risultati attesi; compiti principali; conoscenze e abilità; materie di esame specifiche; criteri di valutazione del caso studio/prova pratica; nota di delimitazione professionale.

AICQ SICEV

1. AI Human Overseer & Chief Governance Officer

Codice: AIHOCG EQF: EQF 7 Natura: Profilo complementare riconosciuto dal mercato

Sezione	Intelligenza Artificiale – Governance
Natura del profilo	Profilo complementare riconosciuto dal mercato, non disciplinato dalla UNI 11621-8, definito in coerenza con l'art. 14 del Regolamento (UE) 2024/1689 (obbligo di sorveglianza umana) e con le funzioni di accountability apicale della AI Governance.
Definizione sintetica	Presidia la sorveglianza umana sui sistemi di Intelligenza Artificiale ad alto rischio ai sensi dell'art. 14 del Regolamento (UE) 2024/1689 e assume la responsabilità di governo complessivo del sistema di gestione dell'AI, fungendo da punto apicale di accountability per le decisioni assunte o supportate da sistemi AI.
Missione	Garantisce che i sistemi di IA ad alto rischio siano utilizzati con un livello di sorveglianza umana effettiva, tale da prevenire o minimizzare i rischi per la salute, la sicurezza e i diritti fondamentali delle persone, e assicura che il sistema di governance dell'AI dell'organizzazione sia coerente, documentato, proporzionato e sostenibile nel tempo.

Collocazione organizzativa e responsabilità

Opera a livello direzionale o di funzione delegata dal vertice aziendale, con potere effettivo di intervento sui sistemi AI (sospensione, disattivazione, non applicazione dell'output). Riporta al vertice aziendale o al comitato AI, ove costituito. Coordina i profili di AI Risk Assessor, AI Compliance Auditor e Data Protection Officer e si raccorda con gli operatori di prima linea incaricati della sorveglianza operativa. Nelle organizzazioni prive di un Chief AI Officer distinto, può cumulare le funzioni apicali di indirizzo e controllo dell'AI Governance.

Requisiti minimi di accesso alla certificazione

Grado di istruzione	Laurea, preferibilmente in discipline ICT, ingegneristiche, giuridiche o organizzative. In alternativa, diploma con esperienza professionale significativa e adeguatamente documentata.
Esperienza complessiva	Esperienza in governance, gestione operativa, compliance o gestione di processi con impatto su persone, sicurezza o diritti fondamentali.
Esperienza specifica	Almeno 2 anni in ruoli con responsabilità di controllo, supervisione o potere di intervento su processi automatizzati o sistemi AI ad alto rischio; la qualità e la responsabilità effettiva dell'esperienza prevalgono sulla sola durata.
Formazione specialistica	Formazione su AI Act (in particolare art. 14 e obblighi del deployer), ISO/IEC 42001, progettazione della sorveglianza umana (HITL, HOTL, HIC), gestione degli incidenti AI.
Evidenze professionali	Procedure di sorveglianza umana, log e verbali di intervento, policy di escalation, report di governance al vertice, registro dei sistemi AI ad alto rischio presidiati.
Certificazioni rilevanti	ISO/IEC 42001 Foundation/Implementer; AIGP; percorsi certificati su AI Act e sorveglianza umana; CRISC; qualifiche equivalenti valutate dalla commissione.
Lingue straniere	Su richiesta: livello minimo B2 QCER/CEFR, verificabile in sede di prova orale.

Risultati attesi

Responsabile finale	Procedura di sorveglianza umana; policy di intervento e sospensione dei sistemi AI; relazione di governance al vertice; registro degli interventi di sorveglianza umana.
Esecutore	Monitoraggio operativo dei sistemi AI ad alto rischio; gestione degli alert; attivazione delle procedure di escalation; verbalizzazione degli interventi effettuati.
Contributore	AI Registry, risk assessment, piani di formazione degli operatori di prima linea, documentazione tecnica per l'audit readiness.

Compiti principali

- Definisce e implementa modalità di sorveglianza umana proporzionate al livello di rischio dei sistemi AI (oversight by design, human-in-the-loop, human-on-the-loop, human-in-command).
- Esercita, o delega con criteri definiti e verificabili, il potere di interrompere, ignorare o annullare l'output di un sistema AI ad alto rischio.
- Assicura che gli operatori incaricati della sorveglianza dispongano di competenza, autorità e tempo sufficienti per esercitare un controllo effettivo.
- Coordina il sistema complessivo di governance AI, raccordando policy, ruoli, responsabilità e meccanismi decisionali.
- Gestisce l'escalation di incidenti e non conformità rilevati nell'esercizio della sorveglianza umana.
- Riferisce periodicamente al vertice aziendale sull'efficacia della sorveglianza umana e sull'adeguatezza del sistema di governance.

Conoscenze e abilità

AI Act (art. 14 e obblighi correlati del deployer), tecniche di progettazione della sorveglianza umana (HITL/HOTL/HIC), ISO/IEC 42001, gestione del rischio operativo, gestione degli incidenti, capacità decisionale in condizioni di incertezza, comunicazione con il vertice aziendale.

Materie di esame specifiche

Sorveglianza umana ex art. 14 AI Act; obblighi del deployer secondo il Regolamento (UE) 2024/1689; progettazione dell'oversight (HITL/HOTL/HIC); governance AI e accountability; gestione degli incidenti e delle non conformità; ISO/IEC 42001; comunicazione e reportistica direzionale; casi di intervento su sistemi AI ad alto rischio.

Criteri di valutazione del caso studio / prova pratica

Il caso studio valuta la capacità del candidato di progettare un modello di sorveglianza umana proporzionato al livello di rischio di un sistema AI, definire i meccanismi di intervento, escalation e reportistica, e collegarli al sistema complessivo di governance dell'organizzazione.

Nota di delimitazione professionale

L'AI Human Overseer & Chief Governance Officer non sostituisce il DPO, il CISO o l'auditor indipendente, ma presidia in modo unitario la funzione di sorveglianza umana e di governance complessiva dei sistemi AI, in raccordo con tali figure specialistiche.

2. Corporate Planner AI-Ready

Codice: CPAIR Natura: Profilo complementare riconosciuto dal mercato

Sezione	Intelligenza Artificiale – Governance
Natura del profilo	Profilo complementare riconosciuto dal mercato. Non è disciplinato dalla UNI 11621-8.
Definizione sintetica	Integra la dimensione dell'Intelligenza Artificiale nella pianificazione strategica e operativa dell'organizzazione, valutando opportunità, rischi, investimenti, scenari e trasformazioni abilitate dall'AI.
Missione	Assicura che la pianificazione aziendale incorpori l'impatto dell'AI su processi, mercati, competenze, investimenti, modelli organizzativi, sostenibilità e risk appetite. Fornisce metodo, analisi e strumenti decisionali per rendere la strategia AI-Ready senza sostituire le responsabilità direzionali.

Collocazione organizzativa e responsabilità

Opera nella pianificazione strategica, nel controllo di gestione, nelle funzioni di innovazione, digital transformation o direzione generale. Collabora con CAIO, CFO, CIO, responsabili di funzione, risk manager e compliance per tradurre le opportunità tecnologiche AI in piani aziendali realistici, misurabili e sostenibili.

Requisiti minimi di accesso alla certificazione

Grado di istruzione	Laurea in economia, ingegneria gestionale, ICT, statistica, data science, organizzazione aziendale o discipline affini. In alternativa, diploma con esperienza significativa in pianificazione, controllo o trasformazione digitale.
Esperienza complessiva	Esperienza in pianificazione aziendale, controllo di gestione, strategia, consulenza direzionale, trasformazione digitale o ICT; esperienze più brevi con elevata qualità e profondità tematica sono valutabili su istanza motivata.
Esperienza specifica	Almeno 1 anno in attività di corporate planning, portfolio planning, business transformation o AI readiness, con evidenze documentate di analisi di scenario, piani di investimento o roadmap digitali.
Formazione specialistica	Formazione documentata in AI Governance, AI Act, ISO/IEC 42001, digital transformation, business planning, risk management e data-driven decision making.
Evidenze professionali	Piani strategici AI-Ready, AI readiness assessment, gap analysis, roadmap di trasformazione, business case AI, analisi make/buy, portafoglio iniziative, KPI strategici e report direzionali.
Certificazioni rilevanti	ISO/IEC 42001 Foundation/Implementer; AIGP; AAIA; AAISM; AAIR; COBIT; ITIL; project management; certificazioni in business analysis, risk management o data analytics.
Lingue straniere	Su richiesta: livello minimo B2 QCER/CEFR, verificabile in sede di prova orale.

Risultati attesi

Responsabile finale	AI Readiness Assessment; piano strategico AI-Ready; roadmap di trasformazione documentata; modello di prioritizzazione delle iniziative AI.
Esecutore	Analisi di scenario; gap analysis organizzativa; business case AI; piano di investimento; indicatori di maturità e performance AI.
Contributore	Strategia AI organizzativa, programma di AI literacy, piano di change management, piano di procurement AI, registro opportunità e rischi AI.

Compiti principali

- Integra le variabili AI nei processi ordinari di pianificazione strategica e budget.
- Conduce assessment di maturità e identifica gap di dati, competenze, processi, tecnologia e governance.
- Supporta la direzione nella definizione di obiettivi AI-enabled coerenti con missione, vincoli e capacità aziendali.
- Costruisce scenari di investimento, analisi costi-benefici e criteri di priorità delle iniziative AI.
- Monitora trend normativi, tecnologici e di mercato rilevanti.
- Coordina il raccordo tra piano industriale, piano digitale, risk appetite, compliance e formazione.

Conoscenze e abilità

Strategic planning, scenario analysis, business model innovation, AI readiness, AI Act, ISO/IEC 42001, principi di AI risk management, KPI/OKR, controllo di gestione, governance ICT, data governance e change management.

Materie di esame specifiche

Pianificazione strategica AI; analisi di scenario e foresight; AI readiness assessment; AI Act (implicazioni per la pianificazione); ISO/IEC 42001; costruzione di business case AI; portfolio management; definizione e monitoraggio di KPI; change management; valutazione economico-organizzativa degli investimenti AI.

Criteri di valutazione del caso studio / prova pratica

Il caso studio valuta la capacità di costruire una roadmap AI-Ready sostenibile, che colleghi obiettivi di business, gestione dei rischi, investimenti, sviluppo delle competenze e requisiti di governance in un piano coerente e misurabile.

Nota di delimitazione professionale

Il Corporate Planner AI-Ready non è un profilo tecnico di sviluppo AI né un revisore di conformità. Il suo presidio è la pianificazione informata, documentata e misurabile dell'adozione AI nell'organizzazione.

3. AI Ethicist

Codice: AIE EQF: EQF 7 Natura: Profilo complementare riconosciuto dal mercato

Sezione	Intelligenza Artificiale – Governance
Natura del profilo	Profilo complementare riconosciuto dal mercato. Non è disciplinato dalla UNI 11621-8.
Definizione sintetica	Analizza, valuta e presidia le implicazioni etiche, sociali e valoriali associate allo sviluppo, all'acquisizione, al deployment e all'uso dei sistemi di Intelligenza Artificiale.
Missione	Garantisce che le decisioni relative all'AI siano valutate anche rispetto a diritti fondamentali, equità, non discriminazione, trasparenza, dignità umana, impatto sociale, inclusione e sostenibilità. Contribuisce a rendere operativo il principio di AI affidabile, responsabile e centrata sulla persona.

Collocazione organizzativa e responsabilità

Opera in comitati etici, funzioni compliance, innovation office, organismi consultivi, team di governance o gruppi interdisciplinari. Collabora con CAIO, DPO, legale, risk assessor, product manager, HR, rappresentanze degli utenti e stakeholder esterni, portando una valutazione professionale degli aspetti etici che non emergono da sole analisi tecniche o giuridiche.

Requisiti minimi di accesso alla certificazione

Grado di istruzione	Laurea magistrale o titolo equivalente preferibilmente in filosofia, etica applicata, giurisprudenza, scienze sociali, psicologia, ICT, data science o discipline interdisciplinari. L'esperienza professionale documentata e la produzione intellettuale (pubblicazioni, ricerche, docenza) costituiscono percorso equivalente alla laurea magistrale a pieno titolo.
Esperienza complessiva	Esperienza in ambiti professionali connessi a etica, compliance, governance, ricerca, diritti fondamentali, tecnologie digitali o AI; percorsi accademici o di ricerca con pubblicazioni documentate costituiscono esperienza equivalente.
Esperienza specifica	Almeno 1 anno in attività di ethics assessment, Responsible AI, valutazione degli impatti sociali, bias e fairness, governance tecnologica o comitati etici; attività di ricerca, pubblicazione o docenza in etica AI sono riconosciute come esperienza specifica rilevante.
Formazione specialistica	Formazione specialistica su AI ethics, AI Act, diritti fondamentali, UNESCO AI Ethics, OECD AI Principles, ISO/IEC TR 24368, bias e fairness, valutazione d'impatto e stakeholder engagement.
Evidenze professionali	Framework etici AI, pareri etici, ethical impact assessment, linee guida Responsible AI, valutazioni di bias e fairness, verbali di comitati, raccomandazioni e piani di mitigazione etica.
Certificazioni rilevanti	AIGP; AI Ethics certification; ISO/IEC 42001; AAIA; AAISM; AAIR; formazione in etica applicata, human rights, privacy o responsabilità algoritmica; qualifiche equivalenti valutate dalla commissione.
Lingue straniere	Su richiesta: livello minimo B2 QCER/CEFR, verificabile in sede di prova orale.

Risultati attesi

Responsabile finale	Framework etico AI; AI Ethics Policy; relazione di valutazione etica; pareri motivati su sistemi AI ad impatto significativo.
Esecutore	Ethical Impact Assessment; analisi bias e fairness; raccomandazioni di mitigazione; verbali di ethical review; materiali di formazione su Responsible AI.
Contributore	Risk assessment AI, DPIA, Algorithmic Impact Assessment, product requirements, requisiti di supervisione umana, comunicazione trasparente agli stakeholder.

Compiti principali

- Definisce principi, criteri e procedure per la valutazione etica dei sistemi AI.
- Analizza rischi di discriminazione, esclusione, opacità, manipolazione, perdita di autonomia e impatti sui diritti fondamentali.
- Supporta la progettazione e la revisione dei requisiti di trasparenza, supervisione umana e responsabilità.
- Conduce o contribuisce a ethical impact assessment e stakeholder review.
- Formula raccomandazioni proporzionate e verificabili per ridurre gli impatti negativi.
- Forma team e management sui principi di Responsible AI e AI affidabile.

Conoscenze e abilità

Etica applicata, diritti fondamentali, AI Act, UNESCO Recommendation on AI Ethics, OECD AI Principles, Trustworthy AI (HLEG), ISO/IEC TR 24368, ISO/IEC TR 24027, bias e fairness, explainability, accountability, stakeholder engagement e tecniche di valutazione d'impatto etico-sociale.

Materie di esame specifiche

Etica AI e Responsible AI; diritti fondamentali applicati all'AI; bias, fairness e discriminazione algoritmica; AI Act (requisiti di trasparenza, supervisione umana, diritti fondamentali); UNESCO Recommendation on AI Ethics; OECD AI Principles; ISO/IEC TR 24368; Trustworthy AI (HLEG); ethical impact assessment; stakeholder engagement; casi pratici di valutazione etica.

Criteri di valutazione del caso studio / prova pratica

Il caso studio valuta la capacità di riconoscere dilemmi etici complessi, motivare una posizione argomentata, proporre misure di mitigazione proporzionate e documentare le decisioni in modo verificabile e comprensibile per interlocutori non specialisti.

Nota di delimitazione professionale

L'AI Ethicist non sostituisce il legale, il DPO o l'auditor. Fornisce valutazione etica professionale e contribuisce al sistema di decisione responsabile dell'organizzazione, operando in modo complementare alle figure giuridiche e tecniche.

4. AI Community Juror

Codice: AICJ EQF: EQF 5 Natura: Profilo complementare riconosciuto dal mercato

Sezione	Intelligenza Artificiale – Governance
Natura del profilo	Profilo complementare riconosciuto dal mercato. Non è disciplinato dalla UNI 11621-8.
Definizione sintetica	Rappresenta la prospettiva di cittadini, utenti e stakeholder non tecnici nei processi di consultazione, valutazione e governance dei sistemi AI ad elevato impatto sociale.
Missione	Favorisce una partecipazione informata e documentata nei processi decisionali sull'AI, contribuendo a rendere visibili bisogni, timori, aspettative e impatti percepiti dalla comunità. Il profilo porta nel processo di governance una valutazione civica strutturata, non sostitutiva delle responsabilità tecniche o giuridiche.

Collocazione organizzativa e responsabilità

Opera in giurie civiche, comitati consultivi, tavoli pubblici, advisory board, organismi etici o processi deliberativi. È particolarmente rilevante in ambiti come la sanità, la pubblica amministrazione, l'istruzione, il lavoro, il welfare, la sicurezza urbana e i servizi essenziali, dove i sistemi AI interagiscono direttamente con i diritti e il benessere dei cittadini.

Requisiti minimi di accesso alla certificazione

Grado di istruzione	Diploma o laurea, con adeguata AI literacy e capacità di comprendere documentazione semplificata su rischi, benefici, limiti e impatti dei sistemi AI. Per contesti complessi è preferibile laurea in scienze sociali, comunicazione, giurisprudenza, ICT o discipline affini.
Esperienza complessiva	Esperienza in ambiti di partecipazione pubblica, rappresentanza stakeholder, advocacy, servizi pubblici, comunicazione sociale, valutazione degli impatti o governance partecipativa; la motivazione e la capacità di rappresentanza civica informata prevalgono sulla sola anzianità.
Esperienza specifica	Almeno 1 anno in processi deliberativi, consultazioni pubbliche, comitati etici, valutazioni di impatto sociale, user research o stakeholder engagement su tecnologie digitali o sistemi AI, con evidenze documentate della partecipazione attiva e del contributo apportato.
Formazione specialistica	Formazione su AI literacy avanzata, AI Act (elementi essenziali), diritti fondamentali, democrazia deliberativa, gestione dei conflitti, tecniche di consultazione, valutazione di impatto sociale e comunicazione del rischio.
Evidenze professionali	Partecipazione documentata a consultazioni, verbali, report stakeholder, raccomandazioni civiche, analisi di impatto sociale, contributi a linee guida e pareri consultivi.
Certificazioni rilevanti	Percorsi certificati di AI literacy, public engagement, policy evaluation, facilitation, privacy o etica pubblica. Non sono richieste certificazioni tecniche avanzate.
Lingue straniere	Su richiesta: livello minimo B2 QCER/CEFR, verificabile in sede di prova orale.

Risultati attesi

Responsabile finale	Parere civico motivato; report di consultazione stakeholder; raccomandazioni di interesse pubblico; sintesi documentata delle aspettative della comunità.
Esecutore	Sessioni di ascolto strutturate; analisi delle osservazioni raccolte; contributi a questionari e consultazioni; verbalizzazione delle posizioni emerse.
Contributore	Ethical impact assessment, Algorithmic Impact Assessment, linee guida di comunicazione verso gli utenti, requisiti di trasparenza e supervisione umana.

Compiti principali

- Partecipa a processi deliberativi su sistemi AI ad elevato impatto.
- Rappresenta in modo documentato interessi, timori e aspettative della comunità.
- Contribuisce alla valutazione degli impatti sociali, inclusivi e distributivi.
- Verifica la comprensibilità delle informazioni fornite agli utenti e ai cittadini.
- Formula raccomandazioni non tecniche ma motivate, chiare e tracciabili.
- Supporta la costruzione di fiducia, accettabilità e accountability nei progetti AI di interesse pubblico.

Conoscenze e abilità

AI literacy, elementi essenziali di AI Act, diritti fondamentali, partecipazione civica, public policy, comunicazione del rischio, stakeholder engagement, valutazione di impatto sociale, accessibilità, inclusione e principi di trasparenza e accountability.

Materie di esame specifiche

AI literacy (livello avanzato); AI Act (elementi essenziali per stakeholder non tecnici); partecipazione civica e processi deliberativi; stakeholder engagement; valutazione degli impatti sociali dell'AI; diritti fondamentali; comunicazione del rischio; analisi di casi ad alto impatto sociale.

Criteri di valutazione del caso studio / prova pratica

Il caso studio valuta la capacità di leggere un progetto AI, individuare gli impatti sociali rilevanti, formulare osservazioni motivate e distinguere chiaramente tra fatti osservati, percezioni della comunità e raccomandazioni argomentate.

Nota di delimitazione professionale

L'AI Community Juror non è un auditor, un risk assessor o un esperto tecnico. Il valore del profilo sta nella rappresentanza competente, strutturata e documentata della prospettiva civica all'interno dei processi di governance AI.

5. AI Risk Assessor

Codice: AIRA Natura: Profilo complementare riconosciuto dal mercato

Sezione	Intelligenza Artificiale – Governance
Natura del profilo	Profilo complementare riconosciuto dal mercato. Non è disciplinato dalla UNI 11621-8.
Definizione sintetica	Identifica, analizza, valuta, classifica e monitora i rischi associati ai sistemi di Intelligenza Artificiale lungo il ciclo di vita, definendo misure di mitigazione e controlli coerenti con il contesto.
Missione	Rende governabile il rischio AI attraverso un metodo strutturato, evidenze documentate e criteri ripetibili, collegando gli impatti potenziali su persone, organizzazione, sicurezza, continuità operativa, dati, conformità e qualità del sistema ai controlli e alle misure di trattamento adottate.

Collocazione organizzativa e responsabilità

Opera in funzioni di risk management, compliance, sicurezza, qualità, AI governance, product management o audit interno. Collabora con CAIO, CISO, DPO, AI Product Manager, data scientist, legale e responsabili di processo, fornendo valutazioni professionali e supportando le decisioni di accettazione, trattamento o escalation del rischio.

Requisiti minimi di accesso alla certificazione

Grado di istruzione	Laurea in ICT, ingegneria, sicurezza, matematica, statistica, risk management, economia, giurisprudenza o discipline affini. In alternativa, diploma con esperienza significativa e documentata.
Esperienza complessiva	Esperienza in ICT, sicurezza, risk management, compliance, data governance, qualità o AI; la padronanza metodologica e la capacità di applicazione degli standard di risk management sono elementi determinanti nella valutazione.
Esperienza specifica	Almeno 1 anno in valutazione dei rischi, definizione di controlli, sicurezza, audit, business continuity, privacy risk assessment o AI risk management, con evidenze di risk register o assessment documentati.
Formazione specialistica	Formazione su AI Act, ISO/IEC 23894, NIST AI RMF, ISO 31000, ISO/IEC 42001, cybersecurity applicata all'AI, DPIA/AIA, continuità operativa e gestione degli incidenti.
Evidenze professionali	AI risk assessment, risk register, classificazione AI Act, piani di trattamento del rischio, controlli implementati, report di monitoraggio, evidenze di mitigazione, valutazioni del rischio residuo e reporting alla direzione.
Certificazioni rilevanti	ISO 31000 Risk Manager; ISO/IEC 42001; CRISC; CISM; ISO/IEC 27001; business continuity; AAIA; AAISM; AAIR; privacy; cybersecurity; certificazioni equivalenti valutate dalla commissione.
Lingue straniere	Su richiesta: livello minimo B2 QCER/CEFR, verificabile in sede di prova orale.

Risultati attesi

Responsabile finale	AI Risk Assessment Report; AI Risk Register; classificazione del rischio AI secondo AI Act; piano di trattamento del rischio; valutazione del rischio residuo.
Esecutore	Analisi di minacce e vulnerabilità; Algorithmic Impact Assessment; mappatura dei controlli; monitoraggio di drift e incidenti; report periodici al management.
Contributore	DPIA, audit readiness, Model Cards, technical documentation, business continuity, incident response e policy AI.

Compiti principali

- Identifica asset, finalità, stakeholder, contesto d'uso e possibili impatti del sistema AI.
- Classifica il sistema secondo AI Act, criticità operativa, dati trattati e impatti su diritti e sicurezza.
- Analizza rischi tecnici, organizzativi, etici, privacy, cybersecurity, continuità e supply chain.
- Definisce controlli, misure di mitigazione, livelli di rischio residuo e responsabilità.
- Monitora metriche, drift, incidenti, near miss e cambiamenti del contesto.
- Produce report utilizzabili da direzione, compliance, audit e product management.

Conoscenze e abilità

AI Act, ISO/IEC 23894, NIST AI RMF, ISO 31000, ISO/IEC 42001, cybersecurity, privacy risk, data governance, threat modeling AI, FMEA, risk matrix, gestione degli incidenti AI, business continuity, model monitoring e progettazione di controlli di mitigazione.

Materie di esame specifiche

AI risk management; AI Act (classificazione del rischio, obblighi di documentazione, supervisione umana); ISO/IEC 23894; NIST AI RMF; ISO 31000; threat modeling applicato all'AI; definizione di controlli; gestione del risk register; risk treatment; monitoraggio e incident response AI; casi pratici di valutazione del rischio.

Criteri di valutazione del caso studio / prova pratica

Il caso studio valuta la capacità di identificare rischi concreti e specifici, classificarli in modo coerente con AI Act e standard applicabili, stimarne la priorità, proporre controlli proporzionati al contesto e documentare chiaramente il rischio residuo.

Nota di delimitazione professionale

L'AI Risk Assessor non sostituisce il titolare del rischio aziendale né l'auditor indipendente. Fornisce valutazioni professionali strutturate e supporta le decisioni di accettazione, trattamento o escalation del rischio.

6. AI Compliance Auditor

Codice: AICA Natura: Profilo complementare riconosciuto dal mercato

Sezione	Intelligenza Artificiale – Governance
Natura del profilo	Profilo complementare riconosciuto dal mercato. Non è disciplinato dalla UNI 11621-8.
Definizione sintetica	Valuta e verifica la conformità di sistemi, processi, documentazione e controlli AI rispetto a requisiti normativi, standard tecnici, policy interne, obblighi contrattuali e criteri di audit applicabili.
Missione	Fornisce assurance professionale sulla conformità e sull'efficacia dei controlli di AI Governance, raccogliendo evidenze oggettive, formulando rilievi chiari e supportati da prove, e monitorando l'attuazione delle azioni correttive.

Collocazione organizzativa e responsabilità

Opera come auditor interno, auditor di seconda parte, consulente di audit readiness o componente di team di verifica su sistemi di gestione e processi AI. Collabora con CAIO, compliance, legal, DPO, risk assessor, IT, security, product manager e fornitori, mantenendo l'indipendenza di giudizio necessaria al ruolo.

Requisiti minimi di accesso alla certificazione

Grado di istruzione	Laurea in ICT, giurisprudenza, economia, ingegneria, sistemi di gestione, sicurezza o discipline affini. In alternativa, diploma con esperienza significativa in audit, compliance o sistemi di gestione.
Esperienza complessiva	Esperienza in ICT, audit, compliance, sistemi di gestione, sicurezza, qualità, privacy o AI; la conoscenza degli standard di audit e la capacità di raccolta e valutazione critica delle evidenze sono elementi centrali nella valutazione.
Esperienza specifica	Almeno 1 anno in audit, verifiche di conformità, sistemi di gestione, controlli ICT, privacy, sicurezza o valutazioni AI, con dimostrata competenza nella raccolta, valutazione critica e classificazione delle evidenze; l'esperienza di audit in ambiti affini è riconosciuta come equivalente.
Formazione specialistica	Formazione su tecniche di audit (ISO 19011), AI Act, ISO/IEC 42001, ISO/IEC 23894, GDPR, documentazione tecnica AI, gestione delle non conformità e azioni correttive.
Evidenze professionali	Piani di audit, check-list di verifica, rapporti di audit, rilievi classificati, gap analysis, follow-up, verifiche documentali, campionamenti, evidenze raccolte e piani di remediation.
Certificazioni rilevanti	ISO 19011; ISO/IEC 42001 Lead Auditor; ISO/IEC 27001 Lead Auditor; AIGP; CISA; CISM; AAIA; AAISM; AAIR; DPO; qualifiche equivalenti valutate dalla commissione.
Lingue straniere	Su richiesta: livello minimo B2 QCER/CEFR, verificabile in sede di prova orale.

Risultati attesi

Responsabile finale	Piano di audit AI; rapporto di audit AI; dichiarazione di conformità interna; elenco rilievi classificati; raccomandazioni e piano di follow-up.
Esecutore	Check-list di audit; conduzione interviste; verifica delle evidenze; campionamenti; gap analysis; monitoraggio dell'attuazione delle azioni correttive.
Contributore	Audit readiness, technical documentation AI, AI Registry, risk assessment, DPIA, vendor assessment e riesame direzionale.

Compiti principali

- Pianifica l'audit AI definendo campo, criteri, obiettivi, campionamento e programma.
- Verifica la conformità a AI Act, GDPR, ISO/IEC 42001, ISO/IEC 23894, policy interne e requisiti contrattuali.
- Raccoglie evidenze oggettive mediante documenti, interviste, osservazioni e verifiche campionarie.
- Formula rilievi chiari, classificati e supportati da prove.
- Valuta l'adeguatezza delle azioni correttive proposte e ne monitora l'attuazione.
- Contribuisce alla preparazione di verifiche di terza parte e valutazioni di conformità esterne.

Conoscenze e abilità

AI Act, ISO/IEC 42001, ISO/IEC 23894, ISO 19011, GDPR, sistemi di gestione AI, raccolta e valutazione di audit evidence, campionamento, classificazione delle non conformità, azioni correttive, documentazione tecnica AI, AI Registry, vendor audit e audit di controlli ICT.

Materie di esame specifiche

AI Act (obblighi di documentazione, requisiti per sistemi ad alto rischio, supervisione); ISO/IEC 42001 (verifica del sistema di gestione AI); ISO/IEC 23894; ISO 19011 (pianificazione e conduzione dell'audit); raccolta di audit evidence; classificazione delle non conformità; sistemi di gestione AI; GDPR; documentazione tecnica AI; verifica dei fornitori; casi di audit AI.

Criteri di valutazione del caso studio / prova pratica

Il caso studio valuta la capacità di pianificare una verifica strutturata, individuare le evidenze pertinenti, formulare rilievi corretti e proporzionati e proporre azioni di follow-up, mantenendo la necessaria distinzione tra ruolo di audit e ruolo di consulenza.

Nota di delimitazione professionale

L'AI Compliance Auditor non sostituisce l'organismo notificato o l'ente di certificazione quando richiesti dalla legge. Opera come auditor professionale interno, di seconda parte o come supporto alla preparazione per la conformità, mantenendo l'indipendenza di giudizio che caratterizza il ruolo.

7. AI MS LEAD IMPLEMENTER AND INTERNAL AUDITOR ISO/IEC 42001

Codice: AIMSLIIA EQF: EQF 6 Natura: Profilo complementare riconosciuto dal mercato

Sezione	Intelligenza Artificiale – Implementazione e Sistemi di Gestione
Natura del profilo	Profilo complementare riconosciuto dal mercato, non disciplinato dalla UNI 11621-8, riferito alla figura che guida l'implementazione di progetti AI e del relativo sistema di gestione (AIMS) conforme a ISO/IEC 42001 e ne conduce gli audit interni, in coerenza con i requisiti organizzativi del Regolamento (UE) 2024/1689 e con i principi della ISO 19011 per l'audit dei sistemi di gestione.
Definizione sintetica	Pianifica, coordina e conduce l'implementazione di progetti di adozione dell'Intelligenza Artificiale e del sistema di gestione dell'AI (AIMS) dell'organizzazione, traducendo i requisiti normativi e di governance in processi, ruoli, documentazione e controlli operativi, e ne pianifica e conduce gli audit interni per verificarne l'efficacia e la conformità a ISO/IEC 42001.
Missione	Garantisce che l'adozione dell'AI in azienda avvenga attraverso un sistema di gestione strutturato, documentato e certificabile, integrando i requisiti di ISO/IEC 42001, del Regolamento (UE) 2024/1689 e degli standard collegati (ISO/IEC 23894, ISO/IEC 27001) nei processi organizzativi, con un approccio orientato all'implementazione concreta e misurabile, e ne assicura il controllo interno attraverso la pianificazione e conduzione di audit interni periodici, secondo i principi della ISO 19011.

Collocazione organizzativa e responsabilità

Opera in progetti di trasformazione, PMO AI, funzioni di qualità/sistemi di gestione o consulenza di implementazione. Collabora con l'AI Human Overseer & Chief Governance Officer, l'AI Risk Assessor, l'AI Compliance Auditor, l'IT, le funzioni di business e i fornitori, coordinando il progetto di implementazione dall'assessment iniziale alla messa a regime del sistema di gestione, oltre a pianificare e condurre il programma di audit interno dell'AIMS.

Requisiti minimi di accesso alla certificazione

Grado di istruzione	Laurea in ICT, ingegneria gestionale, sistemi di gestione qualità o discipline affini. In alternativa, diploma con esperienza documentata in project management o implementazione di sistemi di gestione.
Esperienza complessiva	Esperienza in project management, sistemi di gestione (qualità, sicurezza, IT), implementazione di standard ISO o trasformazione digitale.
Esperienza specifica	Almeno 2 anni nella conduzione di progetti di implementazione di sistemi di gestione o di soluzioni AI, con evidenze di pianificazione, gap analysis e messa a regime dei processi.
Formazione specialistica	Formazione su ISO/IEC 42001 Lead Implementer e Internal Auditor, AI Act, project management (PMI/PRINCE2/Agile), ISO/IEC 23894, ISO 19011, gestione del cambiamento.

Evidenze professionali	Piani di progetto, gap analysis, matrice di conformità, procedure e policy implementate, piani di formazione, programma e rapporti di audit interno, report di stato avanzamento lavori.
Certificazioni rilevanti	ISO/IEC 42001 Lead Implementer e/o Internal Auditor; PMP; PRINCE2; certificazioni Agile/Scrum; qualifiche equivalenti valutate dalla commissione.
Lingue straniere	Su richiesta: livello minimo B2 QCER/CEFR, verificabile in sede di prova orale.

Risultati attesi

Responsabile finale	Piano di implementazione del sistema di gestione AI; documentazione del AIMS conforme a ISO/IEC 42001; matrice di conformità AI Act; piano di messa a regime dei controlli; programma di audit interno dell'AIMS e relativi rapporti di audit.
Esecutore	Procedure operative, policy interne, registro dei processi, piani di formazione e comunicazione al personale, conduzione degli audit interni dell'AIMS, gestione del cronoprogramma di progetto.
Contributore	Risk assessment, audit readiness, documentazione tecnica, coordinamento con fornitori e change management.

Compiti principali

- Pianifica il progetto di implementazione del sistema di gestione dell'AI, definendo obiettivi, perimetro, risorse e tempistiche.
- Conduce la gap analysis rispetto a ISO/IEC 42001 e ai requisiti dell'AI Act applicabili all'organizzazione.
- Definisce processi, ruoli, responsabilità, policy e documentazione necessari al sistema di gestione.
- Coordina i workstream tecnici, organizzativi e di compliance coinvolti nel progetto.
- Gestisce il cambiamento organizzativo e la formazione del personale coinvolto.
- Monitora l'avanzamento del progetto e riferisce agli sponsor e al vertice aziendale.
- Pianifica e conduce gli audit interni del sistema di gestione dell'AI (AIMS), secondo i principi della ISO 19011, verificandone l'efficacia e la conformità a ISO/IEC 42001.
- Prepara l'organizzazione alle verifiche di audit di certificazione, coordinandosi con l'organismo di certificazione.

Conoscenze e abilità

ISO/IEC 42001 e struttura degli AIMS, ISO 19011 e tecniche di audit dei sistemi di gestione, project management (metodologie waterfall e Agile), AI Act (requisiti organizzativi per provider e deployer), gestione del cambiamento, ISO/IEC 23894, tecniche di gap analysis, comunicazione e stakeholder management.

Materie di esame specifiche

ISO/IEC 42001 (struttura e implementazione dell'AIMS); ISO 19011 (pianificazione e conduzione degli audit interni); AI Act (obblighi organizzativi di provider e deployer); project management applicato a progetti AI; gap analysis e piani di remediation; change management; ISO/IEC 23894; documentazione e controllo dei processi; audit readiness.

Criteri di valutazione del caso studio / prova pratica

Il caso studio valuta la capacità di pianificare un progetto di implementazione di un sistema di gestione dell'AI conforme a ISO/IEC 42001, identificare i gap organizzativi, definire un piano d'azione realistico e proporzionato, collegarlo ai requisiti dell'AI Act e pianificare un audit interno dell'AIMS secondo i principi della ISO 19011.

Nota di delimitazione professionale

L'AI MS LEAD IMPLEMENTER AND INTERNAL AUDITOR ISO/IEC 42001 non sostituisce l'AI Compliance Auditor né l'organismo di certificazione: presidia la costruzione, l'implementazione operativa e l'audit interno (prima parte) del sistema di gestione dell'AI, propedeutica alle successive verifiche indipendenti di conformità e certificazione.

8. Competent AI User

Codice: AICU EQF: EQF 4 Natura: Profilo complementare riconosciuto dal mercato

Sezione	Intelligenza Artificiale – Utilizzo Competente e AI Literacy
Natura del profilo	Profilo complementare riconosciuto dal mercato, riferito ai requisiti di AI literacy avanzata di cui all'art. 4 del Regolamento (UE) 2024/1689, rivolto al personale che utilizza sistemi AI nell'ambito delle proprie mansioni operative.
Definizione sintetica	Utilizza sistemi di Intelligenza Artificiale nell'ambito delle proprie mansioni professionali con consapevolezza delle capacità, dei limiti, dei rischi e degli obblighi normativi applicabili, adottando un uso corretto, sicuro e responsabile degli strumenti AI messi a disposizione dall'organizzazione.
Missione	Contribuisce all'uso corretto e responsabile dell'AI nei processi operativi in cui è coinvolto, riconoscendo i limiti degli output generati dai sistemi AI, applicando le procedure di verifica e segnalazione previste dall'organizzazione e contribuendo al rispetto degli obblighi di AI literacy previsti dall'AI Act.

Collocazione organizzativa e responsabilità

Opera in qualunque funzione aziendale che utilizzi sistemi AI nei processi operativi (customer service, marketing, HR, produzione, back office, ecc.). Riporta al proprio responsabile di funzione e si raccorda con l'AI Human Overseer & Chief Governance Officer o con i referenti di governance AI per la segnalazione di anomalie o dubbi sull'utilizzo degli strumenti.

Requisiti minimi di accesso alla certificazione

Grado di istruzione	Diploma. Non è richiesto un titolo specifico, mentre è richiesta una comprensione operativa degli strumenti AI utilizzati.
Esperienza complessiva	Esperienza professionale nella funzione operativa di riferimento; non è richiesta esperienza specifica in ambito AI.
Esperienza specifica	Utilizzo documentato di almeno uno strumento o sistema AI nell'ambito delle proprie mansioni per un periodo minimo di 6 mesi.
Formazione specialistica	Percorso di formazione su AI literacy di base, elementi essenziali dell'AI Act, uso responsabile degli strumenti AI, riconoscimento di bias e allucinazioni, procedure aziendali di verifica e segnalazione.

Evidenze professionali	Attestati di formazione, checklist di utilizzo corretto, esempi di verifica critica degli output, segnalazioni di anomalie effettuate.
Certificazioni rilevanti	Percorsi certificati di AI literacy aziendale o di settore; non sono richieste certificazioni tecniche avanzate.
Lingue straniere	Non richieste, salvo specifiche esigenze di ruolo.

Risultati attesi

Responsabile finale	Utilizzo corretto e documentato degli strumenti AI nell'ambito delle proprie mansioni.
Esecutore	Verifica critica degli output generati dai sistemi AI prima del loro utilizzo operativo; segnalazione di anomalie, errori o comportamenti anomali dei sistemi.
Contributore	Feedback per il miglioramento delle procedure d'uso, contributi a sessioni di formazione tra pari, osservazioni per l'aggiornamento delle policy d'uso.

Compiti principali

- Utilizza gli strumenti e i sistemi AI messi a disposizione secondo le procedure e le finalità previste dall'organizzazione.
- Riconosce i limiti e i possibili errori degli output generati dall'AI (allucinazioni, bias, risposte non aggiornate).
- Applica le procedure di verifica critica prima di utilizzare o comunicare a terzi un output generato dall'AI.
- Segnala tempestivamente anomalie, comportamenti anomali o dubbi di conformità ai referenti aziendali.
- Partecipa ai percorsi di aggiornamento sull'AI literacy previsti dall'organizzazione.
- Contribuisce, nel proprio ambito operativo, al rispetto degli obblighi di trasparenza verso gli utenti finali quando previsto.

Conoscenze e abilità

Elementi essenziali dell'AI Act (in particolare art. 4, obblighi di AI literacy), riconoscimento dei limiti e dei rischi dei sistemi AI generativi e predittivi, verifica critica degli output, procedure aziendali di utilizzo sicuro, principi di protezione dei dati personali nell'uso di strumenti AI.

Materie di esame specifiche

Elementi essenziali dell'AI Act e obblighi di AI literacy; capacità e limiti dei sistemi AI generativi e predittivi; riconoscimento di bias e allucinazioni; procedure aziendali di uso corretto e sicuro; protezione dei dati personali nell'uso di strumenti AI; casi pratici di utilizzo corretto e scorretto degli strumenti AI.

Criteri di valutazione del caso studio / prova pratica

La prova pratica valuta la capacità del candidato di individuare correttamente i limiti e i possibili errori di un output generato da un sistema AI in un caso operativo tipico della propria funzione, e di applicare correttamente la procedura di verifica e segnalazione prevista.

Nota di delimitazione professionale

Il Competent AI User non ha responsabilità di governance, di sviluppo tecnico o di conformità normativa, ma applica correttamente, nel proprio ambito operativo, le regole di utilizzo sicuro e responsabile degli strumenti AI messi a disposizione dall'organizzazione.

9. AI Literate

Codice: AIL EQF: EQF 3 Natura: Profilo complementare riconosciuto dal mercato

Sezione	Intelligenza Artificiale – Utilizzo Competente e AI Literacy
Natura del profilo	Profilo complementare riconosciuto dal mercato, riferito al livello base di alfabetizzazione sull'Intelligenza Artificiale richiesto a qualunque persona che, nell'ambito della propria organizzazione, entri in contatto con sistemi AI, ai sensi dell'art. 4 del Regolamento (UE) 2024/1689.
Definizione sintetica	Possiede le conoscenze essenziali sul funzionamento, sulle opportunità e sui rischi dell'Intelligenza Artificiale necessarie per comprendere, nell'ambito del proprio ruolo, il contesto in cui operano i sistemi AI con cui entra in contatto, anche indirettamente.
Missione	Contribuisce a diffondere nell'organizzazione una cultura di base sull'AI, sufficiente a comprendere cosa sia un sistema di Intelligenza Artificiale, quali siano le principali opportunità e i principali rischi, e quali comportamenti adottare in via generale, in coerenza con l'obbligo di AI literacy previsto dall'AI Act per tutto il personale, indipendentemente dal ruolo specifico.

Collocazione organizzativa e responsabilità

Profilo trasversale, non legato a una funzione specifica. Riguarda potenzialmente l'intero personale dell'organizzazione, inclusi i ruoli che non utilizzano direttamente sistemi AI ma che operano in un contesto organizzativo in cui l'AI è presente.

Requisiti minimi di accesso alla certificazione

Grado di istruzione	Nessun titolo di studio specifico richiesto.
Esperienza complessiva	Nessuna esperienza specifica richiesta.
Esperienza specifica	Nessuna esperienza specifica richiesta; è sufficiente l'appartenenza all'organizzazione o il coinvolgimento, anche occasionale, in contesti in cui sono presenti sistemi AI.
Formazione specialistica	Percorso di formazione base sull'AI literacy (durata minima raccomandata: 2 ore), comprendente nozioni essenziali su cos'è l'AI, principali applicazioni, rischi generali (bias, disinformazione, uso improprio dei dati) e riferimenti normativi essenziali.
Evidenze professionali	Attestato di partecipazione al percorso formativo di base; superamento di un test di verifica dell'apprendimento.
Certificazioni rilevanti	Attestato interno o di terze parti di AI literacy di base; non è richiesta alcuna certificazione tecnica.
Lingue straniere	Non richieste.

Risultati attesi

Responsabile finale	Comprensione di base dimostrata attraverso il superamento del test di verifica dell'apprendimento.
Esecutore	Partecipazione attiva al percorso formativo; applicazione dei comportamenti di base indicati (ad esempio, non condividere dati sensibili con strumenti AI non autorizzati).
Contributore	Segnalazione, ove necessario, di situazioni percepite come rischiose o non chiare legate all'uso dell'AI nel proprio contesto di lavoro.

Compiti principali

- Acquisisce e mantiene una comprensione di base del funzionamento generale dei sistemi di Intelligenza Artificiale.
- Riconosce, in linea generale, la presenza di sistemi AI nei processi o negli strumenti con cui entra in contatto.
- Comprende i principali rischi generali connessi all'uso dell'AI (errori, bias, uso improprio dei dati personali, disinformazione).
- Adotta comportamenti prudenti di base nell'interazione con strumenti AI, in coerenza con le policy aziendali.
- Partecipa ai percorsi di aggiornamento periodico previsti dall'organizzazione in materia di AI literacy.

Conoscenze e abilità

Nozioni essenziali su cosa sia un sistema di Intelligenza Artificiale e su come funzioni in linea generale; consapevolezza delle principali opportunità e dei principali rischi dell'AI; elementi essenziali dell'obbligo di AI literacy previsto dall'AI Act; comportamenti di base per un uso prudente degli strumenti AI.

Materie di esame specifiche

Nozioni introduttive sull'Intelligenza Artificiale; principali applicazioni e limiti dell'AI; rischi generali (bias, errori, disinformazione, uso dei dati); elementi essenziali dell'AI Act in materia di AI literacy; comportamenti di base per un uso prudente degli strumenti AI.

Criteri di valutazione del caso studio / prova pratica

Non è prevista una prova di caso studio per questo profilo; la verifica avviene tramite un test di apprendimento a risposta chiusa, focalizzato sulla comprensione dei concetti essenziali trattati nel percorso formativo.

Nota di delimitazione professionale

L'AI Literate non è un profilo professionale operativo o specialistico, ma rappresenta il livello minimo di alfabetizzazione sull'AI atteso da qualunque persona nell'ambito di un'organizzazione che utilizza sistemi di Intelligenza Artificiale, in attuazione dell'obbligo generale di AI literacy previsto dall'AI Act.

ALLEGATO 1.2 - Clausola di accesso semplificato alla certificazione per tutte le qualifiche eccetto il profilo AI Literate (per un periodo di transizione)

Per un periodo transitorio di **12 mesi dalla data di pubblicazione del presente schema** di certificazione, è ammessa l'iscrizione al registro dei profili professionali AI secondo una procedura di accesso semplificato (di seguito Procedura Semplificata), che riduce alcune delle modalità di valutazione previste dal percorso di certificazione ordinario, riservata ai candidati in possesso dei seguenti requisiti:

L'attivazione della Procedura Semplificata non costituisce un diritto automatico del candidato: essa è avviata su specifica decisione della Commissione di esame/certificazione, che valuta preliminarmente il possesso dei requisiti minimi di ammissibilità di cui al successivo punto a) e delibera in merito all'ammissione del candidato al percorso semplificato. In assenza di tale decisione, ovvero in caso di valutazione negativa dei requisiti minimi, resta comunque salvo il diritto del candidato di accedere alla procedura di certificazione ordinaria.

a) Requisiti di ammissibilità

1. Titolo di studio: Diploma di scuola secondaria di secondo grado, ovvero Laurea Triennale o Magistrale, in materie tecnico-scientifiche ad indirizzo ICT e/o in materie giuridiche o economiche-sociali con un piano di studi che abbia incluso esami ICT a indirizzo ICT;
2. Esperienza professionale pregressa: esperienza lavorativa comprovata di almeno 2 (due) anni maturata nel ruolo specifico corrispondente alla figura professionale per la quale si richiede la certificazione;
3. Predisposizione di un elaborato dell'esperienze lavorativa più significativa, redatta in coerenza con la specifica figura professionale (o le specifiche figure professionali) per la quale si richiede la certificazione, secondo il modello e le indicazioni di cui all'Allegato 3.

b) Modalità di valutazione

L'ammissione al registro secondo la Procedura Semplificata è subordinata a un processo di valutazione ridotto rispetto al percorso di certificazione ordinario – in luogo delle prove scritte, sono previsti l'esame del curriculum vitae e un colloquio individuale – che prevede:

1. l'esame del curriculum vitae presentato dal candidato, volto a verificarne la coerenza con i requisiti di cui al punto a);
2. un colloquio individuale, finalizzato a verificare:
 - la conoscenza e la padronanza dei temi propri del profilo professionale per cui è richiesta la certificazione;
 - l'effettiva rispondenza e approfondimento dell'esperienza lavorativa dichiarata negli elaborati di cui al punto a), comma 3.

L'esito positivo di entrambe le fasi valutative (esame documentale e colloquio) costituisce condizione necessaria per l'iscrizione del candidato al registro secondo la Procedura Semplificata.

c) Criteri di soglia e punteggio

1. La valutazione del colloquio è espressa in centesimi (0-100 punti), attribuiti secondo la seguente ripartizione indicativa:
 - fino a 60 punti per la verifica della conoscenza e padronanza dei temi propri del profilo professionale;
 - fino a 40 punti per la verifica di coerenza, pertinenza e approfondimento dell'esperienza lavorativa presentata negli elaborati di cui all'Allegato 3.
2. Il punteggio minimo per il superamento del colloquio è fissato in 70 punti, con l'ulteriore condizione che il punteggio conseguito in ciascuna delle due sotto-aree di cui al comma 1 non sia inferiore al 60% del massimo attribuibile per l'area medesima.
3. Il mancato raggiungimento della soglia minima complessiva, ovvero della soglia minima in una delle sotto-aree, comporta l'esito negativo della valutazione e la non ammissione al registro secondo la Procedura Semplificata, fermo restando il diritto del candidato di accedere alla procedura di certificazione ordinaria.
4. L'esito della valutazione, con indicazione del punteggio conseguito, è comunicato al candidato in forma scritta a cura dell'organismo di certificazione.

Allegato 2 - Sintesi delle materie di esame per profilo

Profilo	Focus prevalente	Output professionale atteso nel caso studio/prova pratica
AI Human Overseer & Chief Governance Officer	Sorveglianza umana e governance AI	Modello di sorveglianza umana e governance con meccanismi di intervento ed escalation
Corporate Planner AI-Ready	Pianificazione strategica e AI readiness	Roadmap AI-Ready con business case e KPI
AI Ethicist	Etica, diritti fondamentali e impatto sociale	Parere etico motivato e misure di mitigazione
AI Community Juror	Partecipazione civica e prospettiva stakeholder	Report di consultazione e raccomandazioni civiche
AI Risk Assessor	Rischio AI e controlli di mitigazione	Risk register, classificazione e piano di trattamento
AI Compliance Auditor	Audit e conformità normativa	Piano di audit, rilievi classificati e follow-up
AI MS LEAD IMPLEMENTER AND INTERNAL AUDITOR ISO/IEC 42001	Implementazione e audit interno di progetti AI e sistemi di gestione	Piano di implementazione dell'AIMS con matrice di conformità e rapporto di audit interno
Competent Ai User	Uso corretto e sicuro degli strumenti AI	Individuazione dei limiti di un output AI e corretta applicazione della procedura di verifica
AI Literate	AI literacy di base	Test di verifica dell'apprendimento sui concetti essenziali

Allegato 3 – Fac-simile modello di presentazione esperienze lavorative

Il presente Allegato propone un fac-simile dal quale il candidato, in fase di presentazione della domanda di certificazione per uno dei profili considerati nel presente Regolamento, predisporrà un documento dove evidenzierà un'esperienza lavorativa che ritiene più significativa a fronte della specifica figura professionale.

Il presente Allegato non si applica al profilo AI Literate.

La discussione dell'esperienza riportata è necessaria per il superamento dell'esame orale, in considerazione del fatto che lo scopo generale è quello di mettere in grado la commissione esaminatrice di apprezzare le competenze sviluppate dal candidato nel progetto descritto.

PROFILO:

.....
.....
.....

PERIODO DI RIFERIMENTO: data di avvio (___/___/___) – data di termine (___/___/___)

.....
.....
.....

SETTORE DI ATTIVITÀ:

.....
.....
.....

OGGETTO DELLA ATTIVITÀ GESTITA DAL CANDIDATO:

.....
.....
.....

DENOMINAZIONE / BREVE DESCRIZIONE / OBIETTIVO/I DEL PROGETTO O DELL'INCARICO:

.....
.....
.....

RUOLO DEL CANDIDATO E RESPONSABILITÀ NELL'AMBITO DEL PROGETTO/ATTIVITÀ:

.....

.....

.....

MODALITÀ ADOTTATE DAL CANDIDATO PER LA GESTIONE DELL'ATTIVITÀ SOPRA DESCRITTA:

.....

.....

.....

DESCRIZIONE DI MAGGIOR DETTAGLIO: attività svolte, metodi e strumenti utilizzati, documenti e deliverable prodotti, stakeholder coinvolti, criticità riscontrate, soluzioni adottate, risultati conseguiti:

.....

.....

.....

EVENTUALI STANDARD, FRAMEWORK O NORMATIVE APPLICATE (AI Act, ISO/IEC 42001, ISO/IEC 23894, GDPR, NIST AI RMF, ecc.):

.....

.....

.....

RISULTATI E IMPATTO DELL'ATTIVITÀ:

.....

.....

.....

Allegato 4 - Bibliografia e fonti di riferimento

Normativa e regolamenti

- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 (Artificial Intelligence Act), Gazzetta ufficiale dell'Unione europea, EUR-Lex.
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR), Gazzetta ufficiale dell'Unione europea.

Standard internazionali

- ISO/IEC 42001:2023 – Information technology – Artificial intelligence – Management system.
- ISO/IEC 23894:2023 – Information technology – Artificial intelligence – Guidance on risk management.
- ISO/IEC 25059:2023 – Software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Quality model for AI systems.
- ISO 31000:2018 – Risk management – Guidelines.
- ISO 19011:2018 – Guidelines for auditing management systems.
- ISO/IEC TR 24027:2021 – Bias in AI systems and AI aided decision making.
- ISO/IEC TR 24028:2020 – Overview of trustworthiness in artificial intelligence.
- ISO/IEC TR 24368:2022 – Overview of ethical and societal concerns.

Standard per la certificazione delle persone

- UNI 11621-8 – Attività professionali non regolamentate – Profili professionali ICT – Parte 8: AI Governance.
- UNI 11506 – Attività professionali non regolamentate – Figure professionali operanti nel settore ICT.
- UNI EN 16234 (e-CF) – European e-Competence Framework, edizione vigente.
- UNI CEI EN ISO/IEC 17024:2012 – Valutazione della conformità – Requisiti generali per gli organismi che effettuano la certificazione di persone.

Documenti di indirizzo e riferimenti professionali

- NIST – Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, National Institute of Standards and Technology, 2023.
- OECD – AI Principles, Organisation for Economic Co-operation and Development, adottati nel 2019 e aggiornati nel 2024.
- UNESCO – Recommendation on the Ethics of Artificial Intelligence, General Conference, 2021.
- European Commission, High-Level Expert Group on AI – Ethics Guidelines for Trustworthy AI, 2019.
- IEEE – Serie IEEE 7000 su etica nei sistemi autonomi e intelligenti.

Le edizioni e le versioni aggiornate degli standard e dei documenti elencati sono quelle vigenti alla data di applicazione del presente Regolamento. In caso di revisione o sostituzione di uno standard, l'ente valuterà l'adeguamento del Regolamento secondo le procedure applicabili.