AICQ SICEV S.r.l.

Rev.	Data	Motivo Revisione	Preparato da Referente Schema/Direttore/ Resp. SGQ	Verificato da Presidente CSI/ Resp SGQ / Direttore/ Resp. Tecnico	Approvato da Direttore/ Presidente
01	13/02/2024	Aggiornamento a seguito della pubblicazione della 42001 (*eliminato DIS*) e inseriti riferimenti normativi nel paragrafo 2.3	S.Gorla	C. D'Aquaro	D. Gilormo
00	01/06/2023	Prima stesura ed emissione	V. Mazza	C. D'Aquaro	D. Gilormo

INDICE

1. SCOPO E CAMPO DI APPLICAZIONE

2. DOCUMENTI

2.1 Documenti di base
2.2 Documenti applicabili
2.3 Documenti di riferimento

3. DEFINIZIONI E ACRONIMI

4. REQUISITI SPECIFICI PER LA CERTIFICAZIONE DEI VALUTATORI (VSAI) E DEI RESPONSABILI DEI GRUPPI DI VERIFICA (VSAI RGVI) DI SISTEMI INTELLIGENZA ARTIFICIALE.

4.1 Requisiti minimi
4.2 Requisiti addizionali per il riconoscimento delle competenze in ambiti specifici
4.3 Situazioni particolari e trasferimento da altro OdC
4.4 Sorveglianza, mantenimento e rinnovo della Certificazione

5. PROCESSO DI CERTIFICAZIONE

5.1. Modalità d'esame per la certificazione

5.2 Criteri di valutazione

6. MATERIE DI ESAME

6.1 Modalità di esame
6.2 Conoscenze oggetto di esame

AICQ SICEV S.r.l.

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente Regolamento ha lo scopo di definire i requisiti minimi per la concessione della certificazione delle competenze delle figure professionali di Valutatore e di Responsabile del Gruppo di Valutazione dei Sistemi di Gestione per l'Intelligenza Artificiale, per la sorveglianza, il mantenimento e il rinnovo della certificazione delle competenze.

Il presente Regolamento si applica sia ai Candidati che abbiano presentato domande di Certificazione sia ai Valutatori/Responsabili dei Gruppi di Verifica dei Sistemi di Gestione per l'Intelligenza Artificiale già iscritti ai Registri.

2. DOCUMENTI

2.1 Documenti di base:

- RG 01 – Regolamento per le Certificazione delle competenze dei Valutatori e dei Responsabili dei Gruppi di Valutazione di Sistemi di Gestione e di Prodotto
- ISO/IEC 42001: Information technology — Artificial intelligence — Management system.

2.2 Documenti applicabili

- Politica, Vision, Mission
- Manuale del Sistema di Gestione per la Qualità di AICQ SICEV e relative Procedure
- Codice deontologico
- ISO 9001:2015 Quality management systems - Requirements
- ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection – Information management systems – Requirements
- Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale)

2.3 Documenti di riferimento

- UNI CEI EN ISO/IEC 17021-1:2015 Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione – parte 1: Requisiti
- UNI CEI EN ISO/IEC 17024:2012 "Requisiti generali per gli organismi che operano nella certificazione del Personale"
- ISO/IEC 42006 Information technology -- Artificial intelligence -- Requirements for bodies providing audit and certification of artificial intelligence management systems.
- ISO/IEC 23053:2022 Framework for Artificial intelligence (AI) Systems using Machine Learning
- UNI EN ISO 19011:2018 Linee guida per gli audit dei sistemi di gestione
- ISO/IEC Guide 73:2002 – Risk management – Vocabulary – Guidelines for use in standards
- IAF 7/03 Guidelines for the accreditation of bodies operating certification/registration of Information Security Management Systems
- ISO/IEC 13335 Information technology -- Security techniques -- Management of information and communications technology security
- ISO 31000 Risk management system

AICQ SICEV S.r.l.

- ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection- Guidance on managing information security risk

- *Regolamento Accredia RG-01*
- *Regolamento Accredia RG-01-02*

- Guida CEN 14:2010

- CobiT - Control Objectives for Information and related Technology (ISACA)
- Auditing Artificial Intelligence (ISACA)

- Introduction to the self-assessment guide for AI systems (CNIL)

- A Guide to ICO Audit Artificial Intelligence (AI) Audits (ICO)
- Guidance on AI audit framework (ICO)

- Towards Auditable AI Systems (Federal Office for Information Security)

- Standard and/or project under the direct responsibility of ISO/IEC JTC 1/SC 42 Artificial Intelligence:
  - ISO/IEC TS 4213:2022 Information technology — Artificial intelligence — Assessment of machine learning classification performance
  - ISO/IEC 20546:2019 Information technology — Big data — Overview and vocabulary
  - ISO/IEC TR 20547-1:2020 Information technology — Big data reference architecture — Part 1: Framework and application process
  - ISO/IEC TR 20547-2:2018 Information technology — Big data reference architecture — Part 2: Use cases and derived requirements
  - ISO/IEC 20547-3:2020 Information technology — Big data reference architecture — Part 3: Reference architecture
  - ISO/IEC TR 20547-5:2018 Information technology — Big data reference architecture — Part 5: Standards roadmap
  - ISO/IEC 22989:2022 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology
  - ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
  - ISO/IEC TR 24027:2021 Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making.
  - ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence
  - ISO/IEC TR 24029-1:2021 Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview
  - ISO/IEC TR 24030:2021 Information technology — Artificial intelligence (AI) — Use cases.
  - ISO/IEC TR 24368:2022 Information technology — Artificial intelligence — Overview of ethical and societal concerns
  - ISO/IEC TR 24372:2021 Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems
  - ISO/IEC 24668:2022 Information technology — Artificial intelligence — Process management framework for big data analytics
  - ISO/IEC 38507:2022 Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations
  - ISO/IEC NP 23894: Tecnologia dell'informazione — Intelligenza artificiale — Gestione del rischio
  - ISO/IEC TS 25058:2024
  - ISO/IEC TR 5459:2024
  - ISO/IEC DIS 42005
  - ISO/IEC 8183:2023

Nota: a causa del continuo aggiornamento normativo, anche se esplicitamente citata una determinata revisione, si intende che l'edizione valida dei sopra citati documenti è comunque l'ultima emessa.

AICQ SICEV S.r.l.

3 DEFINIZIONI E ACRONIMI

Per le definizioni valgono quelle riportate nelle norme UNI EN ISO 19011, ISO/IEC 42001 e tutte quelle eventualmente indicate nei Documenti di riferimento.
In particolare, i termini audit e verifica ispettiva ed i termini derivati auditor e valutatore sono da considerare completamente equivalenti nel presente Regolamento, anche se nella letteratura e nelle norme alle volte si preferisce utilizzare il primo od il secondo di essi.

Sono inoltre utilizzati i seguenti acronimi:

CSI – Comitato di Sorveglianza dell'Imparzialità
RGVI – Responsabile del Gruppo di Verifica Ispettiva
V.I. – Verifica Ispettiva (Audit)
VSAI – Valutatore del Sistema di Gestione Intelligenza Artificiale

Nota: nei seguenti paragrafi del presente Regolamento quando viene usato il termine "Valutatore" il medesimo include le seguenti figure professionali:

- VSAI – Valutatore di Sistemi di Gestione Intelligenza Artificiale
- VSAI - RGVI – Responsabile Gruppo di Valutazione di Sistemi di Gestione Intelligenza Artificiale

4. REQUISITI SPECIFICI PER LA CERTIFICAZIONE DEI VALUTATORI (VSGSI) E DEI RESPONSABILI DEI GRUPPI DI VERIFICA (VSGSI RGVI) DI SISTEMI DI GESTIONE INTELLIGENZA ARTIFICIALE (SGIA)

4.1 Requisiti minimi

Con riferimento a quanto indicato nel paragrafo 5.1 del Regolamento Generale RG 01, vengono di seguito riportati, in forma tabellare, i requisiti minimi per ciascun percorso di certificazione.

REQUISITI MINIMI	**VSAI** (da VSG di altro Schema a VSAI - Nota 3)	**VSAI RGVI** (da RGVI di altro Schema a VSAI RGVI – Nota 4)
Grado di istruzione	Grado minimo: istruzione secondaria di secondo grado	
Esperienza di lavoro specifica in ambito Governance AI	Almeno 2 anni	Almeno 3 anni
Formazione ed addestramento come auditor	Corso di 40 o 32 ore, riconosciuto da AICQ SICEV di formazione e addestramento su audit ISO/IEC 42001 (in conformità a UNI EN ISO 19011 e ISO/IEC 17021-1) con superamento dell'esame finale (corso di 24 ore per chi è già certificato per un altro Schema). Vedere paragrafo 6.2.2 di RG 01	
Esperienza di audit (Note 1 e 2)	4 audit completi (di cui almeno 1 di 2ª o di 3ª parte) per almeno 8 giornate; 2 devono essere condotti sotto la direzione di un RGVI certificato o qualificato; oppure 7 audit completi (di cui 2 di 2° o 3° parte) per almeno 14 giornate se gli audit non sono stati svolti con un RGVI certificato/qualificato (il che	In aggiunta a quanto previsto per VSAI: 3 audit completi per almeno 6 giornate (1°, 2° o 3° parte) come RGVI in addestramento/ facente funzione sotto la direzione e guida di un RGVI certificato o qualificato; oppure 5 audit come RGVI, di cui almeno 1 di 3° parte per almeno 10 giornate se gli audit non sono stati svolti con un RGVI certificato/qualificato (il che implica la discussione all'orale di un rapporto completo e corredato delle evidenze raccolte).

AICQ SICEV S.r.l.

	implica la discussione all'orale di un rapporto completo e corredato delle evidenze raccolte). Almeno 2 audit devono essere stati completati negli ultimi 2 anni.	Almeno 2 audit devono essere stati completati negli ultimi 2 anni.
Lingue Straniere (su richiesta)	Capacità di colloquio e di redazione di elaborati in lingua. Tale conoscenza può essere dimostrata da dichiarazioni rese da Istituti di formazione linguistica pubblici, privati o dalla Società di appartenenza del Candidato. AICQ SICEV si riserva di verificare durante la prova orale le reali conoscenze del candidato.	

Nota 1: Per audit completo si intende un audit che copra tutte le fasi descritte dal paragrafo 6 della UNI EN ISO 19011 o al paragrafo 9 della ISO/IEC 17021-1 e che copra l'intera norma del Sistema di Gestione Intelligenza Artificiale
Nota 2: Nel conteggio delle giornate-uomo, per i soli RGVI, possono essere conteggiati anche i tempi di preparazione e di reporting (pari a 1,5 giornate aggiuntive per ogni audit eseguito).

Nota 3: Un Auditor già certificato per gli Schemi Qualità e/o Ambiente e/o Salute e Sicurezza e/o Sicurezza delle Informazioni può essere certificato VSAI alle seguenti condizioni:
- Grado di Istruzione: Nessun Requisito Addizionale (NRA) rispetto alla Tabella di para 4.1
- Esperienza di lavoro specifica: NRA rispetto alla Tabella di para 4.1
- Formazione e addestramento: NRA rispetto alla Tabella di para 4.1
- Esperienza di audit: 3 audit di SGAI completi (di cui almeno 1 di 2ª o 3ª parte) per almeno 6 giorni nel ruolo di VSIA condotti sotto la direzione di un RGVI certificato o qualificato, oppure 5 audit di SGAI completi (di cui almeno 1 di 2° o 3° parte) per almeno 10 giorni se gli audit non sono stati svolti con un RGVI certificato/qualificato; gli audit devono essere stati effettuati negli ultimi 2 anni.

Nota 4: Un RGVI già certificato per gli Schemi Qualità e/o Ambiente e/o Salute e Sicurezza e/o Sicurezza delle Informazioni può essere certificato VSAI RGVI alle seguenti condizioni:
- Grado di Istruzione: Nessun Requisito Addizionale (NRA) rispetto alla Tabella di para 4.1
- Esperienza di lavoro specifica: NRA rispetto alla Tabella di para 4.1
- Formazione e addestramento: NRA rispetto alla Tabella di para 4.1
- Esperienza di audit: 3 audit di SGAI completi (di cui almeno 1 di 3ª parte) per almeno 6 giorni come RGVI in addestramento/ facente funzione sotto la direzione e guida di un RGVI certificato o qualificato; oppure 5 audit di SGAI completi (di cui almeno 1 di 2° o 3° parte) per almeno 10 giorni come RGVI se gli audit non sono stati svolti con un RGVI certificato/qualificato (il che implica la discussione all'orale di un rapporto completo e corredato delle evidenze raccolte). Gli audit devono essere stati effettuati negli ultimi 2 anni.

Nota 5: Per un periodo di tempo limitato dall'entrata in vigore del presente regolamento e fino ad un massimo di 36 mesi dalla data di pubblicazione della ISO/IEC 42001 potranno essere ammessi all'esame orale e riconosciuti VSAI o VSAI RGVI, in deroga ai requisiti di ingressi minimi succitati, coloro che:
· hanno maturato esperienza di almeno 5 anni come auditor ISO/IEC 27001 e/o ISO 9001 (IAF 33 e/o 34 e/o 35)
· dimostrino conoscenze sui temi: Intelligenza Artificiale, Big Data, Data Science, Business Analytics, Machine Learning, Metaverso … tramite partecipazione a Master e/o corsi di almeno di 16 ore o in alternativa dimostrino attività di almeno un anno sui temi succitati tramite dichiarazione dell'azienda di appartenenza.

AICQ SICEV S.r.l.

4.2 Requisiti addizionali per il riconoscimento delle competenze in ambiti specifici

In materia di Intelligenza Artificiale, ISO e IEC hanno sviluppato parecchie linee guida per Organizzazioni che operano in ambiti specifici (alcune sono indicate anche al cap. 2.3 di questo documento) e altre sono ancora in via di pubblicazione.

Per poter ottenere il riconoscimento di competenza in un determinato ambito specifico, il Candidato, in aggiunta ai requisiti minimi indicati al capitolo 4.1, dovrà dimostrare la conoscenza degli standard emessi da ISO/IEC JTC 1/SC 42 con le seguenti modalità:

1. Richiesta contestuale all'esame di prima certificazione. Requisiti richiesti:
    - Partecipazione a corsi di almeno 8 ore (eventuali deroghe in termini di durata potranno essere valutate per singolo caso), con attestato di superamento di un esame finale, sullo standard / linea guida specifica, OPPURE formulazione da parte della commissione esaminatrice, di un numero adeguato di domande correlate all'ambito specifico, in aggiunta all'esame di certificazione per VSAI / VSAI-RGVI
    - Esperienza lavorativa o consulenziale nello specifico ambito (relativo standard/ linee emanate da ISO/IEC JTC 1/SC 42) per un periodo di almeno 3 anni con un impegno temporale di almeno 15 giorni/anno (oppure 2 anni con un impegno temporale di almeno 25 giorni/anno) OPPURE esecuzione di almeno il 50% degli audit indicati come minimo nella tabella del cap. 4.1 nell'ambito specifico

2. Richiesta in fase di rinnovo della certificazione o di estensione della stessa. Requisiti richiesti:
    - Partecipazione a corsi di almeno 8 ore (eventuali deroghe in termini di durata potranno essere valutate per singolo caso), con attestato di superamento di un esame finale, sullo standard / linea guida specifica emanata da ISO/IEC JTC 1/SC 42, oppure superamento di un esame scritto predisposto da AICQ SICEV composto da un numero adeguato di domande correlate all'ambito specifico. L'esame può essere eseguito anche da remoto secondo le procedure in vigore presso AICQ SICEV
    - Esperienza lavorativa o consulenziale nello specifico ambito (relativo allo standard / linea guida emanate da ISO/IEC JTC 1/SC 42) per un periodo di almeno 3 anni con un impegno temporale di almeno 15 giorni/anno (oppure 2 anni con un impegno temporale di almeno 25 giorni/anno) OPPURE esecuzione di un almeno 4 audit completi (di cui almeno 1 di 2ª o di 3ª parte) per almeno 8 giornate nell'ambito specifico.

4.3 Situazioni particolari e trasferimento da altro OdC

AICQ SICEV intende riconoscere le grandi professionalità presenti nel mondo della industria e dei servizi, semplificando il processo di certificazione delle competenze, che tuttavia non può prescindere da una valutazione oggettiva.
Per queste tipologie di candidati viene, in prima istanza, riconosciuta l'esistenza delle conoscenze necessarie al ruolo di auditor; i candidati sono quindi esonerati dalla prova scritta (come da Reg. 01). Deve comunque essere sostenuta la prova orale, nel corso della quale la commissione d'esame dovrà valutare e confermare non solo la capacità di sostenere il ruolo di auditor, ma anche la consistenza delle conoscenze, e delle esperienze lavorative.

Le situazioni particolari attualmente riconosciute da AICQ SICEV includono:

- Le certificazioni CISA e CISM [ISACA (Information Systems Audit and Control Association & Foundation)], CISSP (ISC)[2], o Attestato di superamento di Master post-universitari con percorsi formativi almeno equivalenti.

- Valutatori e/o RGVI già certificati secondo altri schemi di certificazione di AICQ SICEV (es: Qualità, Ambiente, Salute e Sicurezza, Sicurezza delle Informazioni …). In questi casi, ma solo per un periodo di tempo limitato dall'entrata in vigore del presente regolamento, (fino ad un massimo di 36 mesi dalla data di pubblicazione della ISO/IEC 42001"), sarà possibile ammettere agli esami di certificazione AICQ SICEV Candidati Valutatori che:

- Rispettino i requisiti previsti dal presente Regolamento per quanto concerne:
  - Grado di Istruzione
  - Esperienza di Lavoro specifica (salvo nota 5)
  - Formazione e addestramento (salvo nota 5)

- Presentino come "Esperienza di Audit" le evidenze oggettive di audit eseguiti anche per altri Schemi di Certificazione (es: Qualità, Ambiente, Salute e Sicurezza, Sicurezza delle Informazioni …)

- VSAI di grande esperienza professionale così definita:
  - almeno 5 anni di esperienza lavorativa in Sistemi di Gestione Intelligenza Artificiale;
  - almeno 15 audit (comprensivi di quelli in addestramento) per un minimo di 30 giornate di impegno, di cui almeno 5 condotti come Responsabile del Gruppo di Verifica.

A fronte di tali requisiti minimi, è prevista una serie di compensazioni ed equivalenze per quanto riguarda le esperienze professionali e specifiche, come di seguito indicato:

- Ogni gruppo di 10 V.I. complete in più delle 15 viene riconosciuto come sostitutivo di 1 anno di esperienza lavorativa specifica, con un massimo di quattro anni;

- Ogni gruppo di 80 ore di corsi di formazione frequentati relativi a discipline inerenti i Sistemi di Gestione Intelligenza Artificiale viene riconosciuto come sostitutivo di 0,5 anni di esperienza lavorativa specifica, con un massimo di 1 anno;

- Lo stato di Docente Universitario Ordinario, Associato o a Contratto in discipline attinenti i Sistemi di Gestione per la Sicurezza delle Informazioni viene riconosciuto come sostitutivo di un anno di esperienza lavorativa specifica;

- Lo stato di docente in corsi per l'Intelligenza Artificiale riconosciuti da AICQ SICEV viene riconosciuto come sostitutivo di un anno di esperienza lavorativa specifica;

- La qualifica di assessor in relazione a modelli di Sistemi di Gestione Intelligenza Artificiale viene riconosciuta come sostitutiva di un anno di esperienza lavorativa specifica;

- La partecipazione a convegni come relatore con temi specifici sull' Intelligenza Artificiale viene riconosciuta come sostitutiva di 6 mesi di esperienza lavorativa specifica;

- La pubblicazione su riviste nazionali/internazionali (anche on line) di articoli con temi specifici sull' Intelligenza Artificiale viene riconosciuta per ogni articolo come sostitutiva di 3 mesi di esperienza lavorativa specifica.

Complessivamente non possono essere sostituiti più di quattro anni di esperienza lavorativa specifica.

Per il trasferimento da altro OdC si veda il Regolamento generale RG01.

4.4 Sorveglianza, mantenimento e rinnovo della Certificazione

La certificazione ha una validità triennale.

Durante il periodo di validità della certificazione, la sorveglianza e il mantenimento annuale è da ritenersi automaticamente confermato secondo quanto previsto al paragrafo 11.1 di RG 01

Per il rinnovo della certificazione si applica quanto previsto nel paragrafo 11.2 di RG 01 con le seguenti variazioni per quanto concerne il numero di audit eseguiti:

AICQ SICEV S.r.l.

A) affinché venga rinnovata la certificazione della competenza il VSAI deve avere effettuato nel triennio almeno 2 V.I. per un totale di almeno 4 giorni;

B) affinché venga rinnovata la certificazione della competenza il VSAI RGVI deve avere effettuato nel triennio almeno 3 V.I. di cui almeno 2 svolgendo le funzioni di RGVI per un totale di almeno 6 giorni.

5. PROCESSO DI CERTIFICAZIONE

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 e il massimo valore dei risultati della valutazione dei requisiti, 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 qualità documentato, in grado di garantire l'adozione di processi di certificazione conformi ai requisiti di questo documento e di garantire, altresì, la produzione e conservazione delle relative evidenze oggettive;
- assicura la verifica dell'aggiornamento professionale;
- definisce, adotta e rispetta il proprio codice deontologico.
- rende pubblico lo schema di certificazione, garantendo che questo sia coerente con i requisiti previsti dalla prassi di riferimento.

Gli esami vengono condotti secondo quanto definito dal Regolamento RG 01 per le figure di auditor/Lead auditor.
AICQ SICEV, tramite la propria struttura tecnica, anche per il tramite del Referente (collaboratore esterno), effettua l'analisi documentale dei richiedenti l'accesso all'esame di certificazione per verificare la congruità delle informazioni riportate a fronte dei requisiti indicati nella domanda d'esame (informazioni inerenti al percorso professionale, formazione, ecc.) e verifica i documenti comprovanti le attività e i titoli richiesti, come allegati, dalla domanda di certificazione.
All'esito positivo dell'analisi del "curriculum vitae" integrato da documentazioni comprovanti le attività lavorative e formative dichiarate dal candidato, AICQ SICEV comunica al richiedente il suo status di candidato all'esame e la data della prima sessione disponibile.

5.1. Modalità d'esame per la certificazione

L'esame di certificazione consiste in una prova scritta ed una prova orale.

La prova scritta, finalizzata ad accertare le conoscenze in ambito AI e alla relativa all'applicazione e implementazione nonché alle definizioni e al soddisfacimento dei requisiti di un sistema di gestione per l'AI, consiste nel rispondere a 30 domande a risposta chiusa.

Modalità assegnazione punteggio: 1 punto a domanda corretta
Il tempo totale a disposizione: è di quarantacinque (45) minuti

All'esito positivo della prova scritta, il candidato può essere ammesso alla prova orale.

La prova orale finalizzata a accertare le conoscenze relative al processo di audit e quindi alla verifica del sistema di gestione, applicando anche quanto descritto dalla ISO 19011 in merito alle metodologie di audit in ambito AI consiste in un colloquio con la Commissione d'esame della durata di circa 45 minuti incrementato di circa 15 minuti per analizzare le risposte errate e/o non date nella prova scritta.

Il candidato che non supera l'esame può ripeterlo in tutto o in parte, come appropriato, nelle sessioni successive. Nel caso la singola prova orale se positiva ha validità per un periodo di 12 mesi.

AICQ SICEV S.r.l.

I membri del CSI di AICQ SICEV hanno diritto ad assistere come osservatori, senza alcun preavviso, a tutte le prove di esame relazionando circa l'esito della loro sorveglianza al Presidente del CSI.

Alle sessioni di esami AICQ SICEV possono inoltre presenziare osservatori dell'Ente di Accreditamento o di eventuali Autorità competenti, comunicandolo al/ai Candidato/i. Detti osservatori hanno la facoltà di intervistare direttamente i candidati.

Durante lo svolgimento delle prove d'esame, i Candidati non possono consultare alcuna documentazione, né usare cellulari, né scambiare informazioni con altri candidati. Il mancato rispetto di tali precazioni è causa di interruzione dell'esame stesso

5.2 Criteri di valutazione

- Per accedere alla prova orale, le figure professionali in oggetto dovranno ottenere un punteggio maggiore o uguale a 60/100 nella prova scritta. Tale prova concorre per il 40% alla votazione finale. Si precisa che nessuna delle risposte non data o errata può inficiare l'esito dell'esame, se si ottiene il punteggio minimo richiesto: non sono previste domande critiche, tutte le domande errate verranno discusse nella successiva fase orale.
- La votazione della prova orale è costituita dalla media delle votazioni dei singoli Commissari (se più di uno) che deve essere uguale o superiore a 67/100. Tale prova concorre per il 60% alla votazione finale;
- La votazione finale, quale media pesata della prova scritta e di quella orale, deve essere uguale o superiore a 67/100.

6. MATERIE DI ESAME

6.1 Modalità di esame

Le modalità di esame sono definite nel paragrafo 8 di RG 01.

6.2 Conoscenze oggetto di esame

Oltre alle materie di esame comuni a tutti gli Schemi di Certificazione riportate nel paragrafo 8.11 (argomento: AUDIT) del Regolamento RG 01, i seguenti argomenti sono specifici per lo Schema Sicurezza delle Informazioni:

1 Gestione della AI

1.1 Principi fondamentali di gestione (Basic Management)

- Processo Decisionale
- Pianificazione
- Organizzazione
- Risorse umane
- Revisione

1.2 Principi di Gestione dei Sistemi per AI:

- L'importanza ed efficacia di un Sistema di Gestione in ambito AI nelle Organizzazioni, tenendo conto anche degli aspetti economici e di efficienza, della missione e delle strategie aziendali;
- Uso dei principi di gestione della AI;
- I principi AI e loro applicazione;
- Il ruolo degli AI Manager, requisiti funzionali e posizione nell'organizzazione.
- Compatibilità con altri Sistemi di Gestione.

AICQ SICEV S.r.l.

Ed in particolare:

- Sistemi di gestione basati sul Quality Management.
- Sistemi di gestione basati sull' AI Management (vedi ISO/IEC 42001)
- Criteri di Auditing Interno per AI.
- Gestione e valutazione dei Principi AI
- Gestione della configurazione.
- Gestione delle risorse umane per la AI.
- Organizzazione: ruoli, responsabilità, possibili incompatibilità e segregazione.
- Gestione delle modifiche ai Sistemi Informativi.
- Risk Analysis e Risk Assessment.
- Rischi relativi all'analisi dei dati
- Rischi connessi alla gestione della documentazione di sistema.
- Sistemi di controllo interno ed elementi di Corporate Governance.
- Rischi nella gestione della catena di fornitura.

1.3 Concetti:

Fondamenti di AI, gestione e miglioramento dei processi di AI, e le verifiche (auditing).
In particolare:

- Elementi base di AI, dei concetti di sistema dei Principi.
- Fondamentali di Algoritmi.
- Fondamenti di Data science e analisys
- Fondamenti di ML e DL
- Criteri di classificazione dei dati trattati.
- Fondamenti di sicurezza
- Business Continuity, Disaster Recovery e Crisis Management.
- Principi AI e loro impatti
- Rischi per AI e loro impatti.

1.4 Politica della AI:

Governance dell'AI come professione e come compito della gestione, gestione attraverso gli obiettivi della Intelligenza Artificiale, standardizzazione, reporting e rendiconto e formulazione della politica dell'Intelligenza Artificiale

1.5 Concetti organizzativi:

- Principi organizzativi e procedure e regole rilevanti;
- Strutture organizzative delle responsabilità, mansioni e competenze.

1.6 Definizione della politica:

- Visione e missione;
- Strategia e politica, obiettivi strategici ed operativi;
- Approccio - sistematico delle organizzazioni di gestione;
- Modelli di gestione, efficacia ed efficienza, gestione dei progetti.

1.7 Impegno del Management:

- Integrazione di: metodologie e strumenti;
- Gestione tramite i processi;
- Impegno verso i clienti ed ai requisiti cogenti;
- Politica Intelligenza Artificiale, obiettivi Intelligenza Artificiale;
- Riesame della gestione, disponibilità delle risorse.

1.8 Standard e linee guida:

Standard ISO ed EN e linee guida relative ai fondamenti e terminologia, e le verifiche dei sistemi di certificazione e accreditamento nonché le prescrizioni ACCREDIA applicabili:

- Vedi elenco ai cap. 2.2 e cap. 2.3 di questo documento

2. Organizzazione della AI:

2.1 Organizzazione

AICQ SICEV S.r.l.

Organizzazione delle deleghe delle responsabilità e coordinamento dei compiti. Compiti, posizione e ruolo del personale impegnato nell'Intelligenza Artificiale.

2.2 Meccanismo di coordinamento:
Obiettivi, struttura, procedure e comitati, documentazione del sistema di gestione Intelligenza Artificiale.

2.3 Verifica (auditing):
Verifiche e revisione dell'organizzazione della gestione del Sistema di Intelligenza Artificiale, verifica dei processi e dei sistemi, principi per le tecniche d'intervista.

3. Principi di gestione dei processi

- Identificazione dei processi
- Pianificazione dei processi
- Gestione dei processi
- Misura e di miglioramento dei processi

4. Tecniche di miglioramento della Gestione della Intelligenza Artificiale

4.1 Organizzazione di un'indagine:
Programmazione, previsione e controllo dell'avanzamento.

4.2 Motivazione:
Teorie della motivazione in relazione alla Intelligenza Artificiale.

4.3 Tecniche:
Pianificazione delle indagini, specifica/descrizione degli obiettivi, sviluppo ed uso dei modelli, scelta del modello, pensare in modo induttivo e deduttivo, ciclo plan- do-check-act, tecniche di indagine e valutazione.

4.4 Progetti e programmi del miglioramento della Gestione della Intelligenza Artificiale:
Principi e metodi, messa a punto dei gruppi o team per la Gestione della Intelligenza Artificiale, coinvolgimento del personale

4.5 Benchmarking:
Regole e tecniche del Benchmarking

5. Gestione delle risorse, delle infrastrutture e degli ambienti

5.1 Analisi dell'esigenza di competenza, di formazione e di addestramento:
Integrazione dei programmi di formazione interna dall'alto al basso, identificazione del bisogno della formazione a breve ed a lungo termine e definizione ed organizzazione dei programmi di formazione.

5.2 Valutazione dell'efficacia dell'addestramento:
Accertare la consapevolezza, della rilevanza e dell'importanza delle loro attività; mantenere la registrazione di istruzione, di esperienza, dell'addestramento e della qualificazione.

5.3 Infrastrutture
Caratteristiche strutturali dell'edificio e/o locali (certificati di abitabilità, conformità degli impianti tecnologici, rispondenza della progettazione sia dei locali che degli impianti).
Valutazione della protezione degli ambienti da attacchi esterni.
Analisi dei rischi e relative coperture per le minacce dovute ad eventi naturali.
Protezioni contro il fuoco e gli allagamenti.
Sicurezza dei Cablaggi (energia elettrica e rete T.D.), infrastrutture di supporto o impianti ausiliari (UPS).
I cablaggi debbono essere protetti con canaline incassate.
Modalità di controllo accesso ai locali, sistemi di allarme e videosorveglianza
Manutenzione delle infrastrutture, impianti e apparecchiature … e un'organizzazione in grado di riparare i guasti in tempi definiti.

AICQ SICEV S.r.l.

5.4 Ambienti del lavoro
Messa in sicurezza dei locali (muri adeguati e porte antincendio, porte blindate, porte controllate da apertura con badge o chiave, vetri antiproiettile/ antisfondamento).
Uso di armadi chiusi e/o blindati, casseforti.
Sicurezza in rispetto alla normativa (D.Lgs. 81/2008 e succ. …)

6. Acquisto e subappalto

6.1 Selezione e riesame:
Selezioni e riesami dei fornitori e dei subappaltatori per mezzo di verifiche e/o classificazione del fornitore.

6.2 Accordi:
Accordi (contratti o non) circa la Intelligenza Artificiale.

6.3 Partnership:
Nell'acquisto, nel subappalto in situazioni normali/usuali o non-normali / non usuali e/o nel controllo e nella consegna "just-in-time".

7. Analisi e raccolta dei dati, metodi statistici

7.1 Obiettivo
Selezione dell'Intelligenza Artificiale, informazione per diversi livelli, codificazione, processo statistico, presentazione dei dati, procedure e sistemi, selezione e tecniche.

7.2 Reporting
Tipi di presentazione e valutazione, tecniche di presentazione, requisiti della presentazione per l'alto, medio e basso management e per tutto il personale.

7.3 Metodi statistici
- Teoria della probabilità
- Teorema di Bayes
- Stima
- Campione
- Uso/utilità dei metodi statistici, nelle verifiche per la Intelligenza Artificiale, nell'analisi dei difetti e negli studi dei processi
- Metodi statistici basilari come istogramma, torte, diagrammi, e tendenze per la gestione ed il funzionamento dei servizi
- Tecniche e analisi statistica (media, devianza, moda, curve di regressione, curve di distribuzione, probabilità, Gauss, etc.)
- Controllo del processo
- Controllo dei lotti
- Progetto degli esperimenti (DOE)
- Affidabilità

8 Controllo della non conformità

8.1 Controllo di non conformità
Individuazione, identificazione delle non conformità. Autorità per la risposta sulla non conformità.

8.2 Registrazioni della non conformità
Registrazioni della natura delle non conformità e commenti.
Dati per analisi e attività di miglioramento

8.3 Riesame e trattamento della non conformità
Riesame del non conformità, tendenze e modello di accreditamento, accettazione della disposizione di non conformità, competenze di valutazione delle conseguenze.

AICQ SICEV S.r.l.

9 Aspetti Sociali

9.1 Soddisfazione del personale

Motivazione, premi, e misura della soddisfazione del personale.

9.2 Comunicazione

Comunicazione, posizione e ruolo degli specialisti della Intelligenza Artificiale gestione del cambiamento, partecipazione ai livelli gestionali ed operativi, aspetti motivazionali nella gestione e nell'organizzazione, stile e cultura del management ed identificazione nell'organizzazione.

10 Aspetti legali e normative

10.1 Legislazione

Legislazioni nazionali ed internazionali, leggi, sicurezza, ambiente, analisi dei rischi, responsabilità contrattuale.
Ed in particolare:

- L. 300/1970 Statuto dei Lavoratori
- Data Protection: Regolamento (UE) 2016/679 del parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- Conoscenze degli aspetti normativi sulla tutela del Segreto di Stato (L. 124/2007)
- Responsabilità Civili, Penali e Amministrative
- Aspetti relativi alla Proprietà Intellettuale e copyright (L. 633/41 – D.lgs. 518/92 – L. 248/00 – Reg. 338/01)
- Aspetti contrattuali relativi all'Outsourcing ed agli approvvigionamenti connessi alla Security
- Aspetti connessi alla Sicurezza delle Informazioni e all'Intelligenza Artificiale per quel che concerne le responsabilità amministrativa delle Società D.lgs. 231/2000, normative di settore, normativa nordamericana (Sarbanes Oxley Act)
- Il rischio operativo (Basilea II)
- Crimini Informatici (Lg. 547/1993)
- Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica (legge 15 febbraio 2012, n. 12
- Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (legge 48/22008)
- Aspetti relativi al commercio elettronico (d.lgs. 70/2003 art. 14 e segg.)
- Aspetti legali relativi all'antiterrorismo (L.155/2005 cosiddetto Decreto Pisanu)
- Aspetti legali legati alla proprietà industriale (d.lgs. 30/2005)

10.2 Aspetti normativi

Norme nazionali ed internazionali, accreditamento e certificazione.

Per quanto non espressamente previsto nel presente Regolamento di Schema si rimanda al Regolamento Generale Reg 01 e al Regolamento Uso Marchio.

AICQ SICEV S.r.l.