SCHEDA REQUISITI PER LA CERTIFICAZIONE DEGLI ISMS (Information Security Management Systems) AUDITOR / RESPONSABILI GRUPPO DI AUDIT

5	30.08.2017	Pag. 5	*Presidente* *Comitato di Schema*	*Amministratore Delegato*
4	28.09.2016	Pag.1	*Presidente* *Comitato di Certificazione*	*Amministratore Unico*
Rev.	**Data**	**Motivazioni**	**Convalida**	**Approvazione**

REQUISITI MINIMI

PROFILO	Persona che conduce audit sui Sistemi di Gestione della Sicurezza delle Informazioni (rif. Norme UNI EN ISO 19011:2012 e UNI CEI EN ISO/IEC 17021:2011).
TITOLO DI STUDIO	Il candidato deve essere in possesso almeno del Diploma di Istruzione Secondaria Superiore. N.B. *Sono accettati tutti i titoli, corsi e diplomi riconosciuti equipollenti a quelli italiani, ai sensi delle vigenti disposizioni di legge.*
FORMAZIONE E ADDESTRAMENTO SPECIFICO	E' necessario aver frequentato un corso per ISMS Auditor della durata di 40 ore secondo la Normativa vigente: UNI EN ISO 19011, ISO/IEC 27000, UNI CEI ISO/IEC 27001, UNI CEI ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27006 ed eventuali Prescrizioni ACCREDIA applicabili e riferimenti legislativi in essere (p.es. D.lgs. 196/2003).
ESPERIENZA DI LAVORO	E' necessaria una documentata ed appropriata **esperienza lavorativa continuativa di base** in attività tecniche presso aziende, Enti o nella consulenza, per un periodo non inferiore a: - 5 anni E' necessaria inoltre una documentata ed appropriata **esperienza lavorativa continuativa specifica** di almeno 2 anni nel campo dei Sistemi di gestione della sicurezza delle informazioni (tale esperienza può essere compresa in quella lavorativa di base).
ESPERIENZA DI AUDIT	Ai fini della certificazione come **ISMS Auditor** è necessario documentare la seguente esperienza di audit maturata come Auditor negli ultimi 3 anni: - 5 Audit completi, non tutti interni, eseguiti su almeno 4 distinti sistemi di cui almeno 2 nell'ultimo anno **Almeno 4** dei suddetti Audit dovranno essere effettuati come Auditor in addestramento sotto la direzione e guida di un Responsabile Gruppo di Audit (RGA) certificato da un Organismo di Certificazione del Personale o qualificato da Organismo di Certificazione di Sistema, per un totale di almeno 20 giorni di esperienza di audit. Ai fini della certificazione come **ISMS Responsabile Gruppo di Audit** è necessario documentare, in aggiunta ai requisiti previsti per l'ISMS Auditor, la seguente esperienza di audit maturata, negli ultimi 2 anni come Responsabile di almeno: - 5 Audit completi, non tutti interni, eseguiti su almeno 4 distinti sistemi **Almeno 3** dei suddetti audit dovranno essere effettuati ricoprendo il ruolo di Responsabile Gruppo di Audit sotto la direzione e guida di un Responsabile Gruppo di Audit (RGA) certificato da un Organismo di Certificazione del Personale o qualificato da Organismo di Certificazione di Sistema, per un totale di almeno 15 giorni di esperienza di audit. **AUDIT VALIDI AI FINI DELLA CERTIFICAZIONE:** Vengono considerati validi, ai fini della certificazione, esclusivamente gli audit effettuati in accordo alla Norma UNI CEI ISO/IEC 27001 e che coprano tutte le fasi descritte da 6.2 a 6.6 della UNI EN ISO 19011, anche se eseguiti in tempi diversi, purché la durata complessiva dell'audit in campo non sia inferiore ad 8 ore (1 giorno lavorativo). Per ogni audit valido viene riconosciuta 1 giornata lavorativa aggiuntiva, per l'esame della documentazione e la preparazione del rapporto, compresa nel totale delle giornate richieste. Non sono pertanto validi, ai fini della certificazione, gli audit: - che riguardano solo il monitoraggio dell'attuazione di azioni correttive e gli audit effettuati secondo norme che non siano equivalenti alla norma UNI CEI ISO/IEC 27001. - eseguiti nel solo ruolo di esperto tecnico.

AMMISSIONE ESAME DI CERTIFICAZIONE	Per l'ammissione all'esame di certificazione CEPAS, il Candidato deve dimostrare di possedere le conoscenze e gli aspetti comportamentali richiesti dalle Norme UNI EN ISO 19011 e UNI CEI EN ISO/IEC 17021 per la conduzione di audit sui Sistemi di gestione della Sicurezza delle Informazioni; in particolare tecniche e metodologie di audit, esperienza specifica nelle aree tecniche dei processi dell'organizzazione sottoposta ad audit. --- **1)** Il Candidato in possesso dei requisiti di formazione specifica, esperienza lavorativa complessiva, esperienza specifica di audit sopra descritti potrà essere ammesso all'esame di certificazione come da procedura vigente (PG30). --- **2)** Il Candidato in possesso di certificazione valida come ISMS Auditor/ Responsabile Gruppo di Audit, rilasciata da un Organismo di certificazione del personale accreditato, che fornisca tutta la documentazione attestante la conformità dei requisiti per la certificazione, ivi compresi eventuali rinnovi e mantenimenti, potrà essere ammesso alla prova tecnica specifica orale dell'esame CEPAS come da procedura vigente (PG30). --- **3)** Il Candidato in possesso di certificazione valida come ISMS Auditor, rilasciata da Organismo di certificazione del personale riconosciuto da CEPAS, che documenta un'attività lavorativa specifica di almeno 6 anni nei Sistemi di Gestione della Sicurezza delle informazioni ed è in possesso i seguenti requisiti: - superamento esame finale di un corso per ISMS Auditor di 40 ore - 7 Audit completi, condotti nel ruolo di Auditor, effettuati negli ultimi 3 anni a fronte della Norma UNI CEI ISO/IEC 27001, per un totale di almeno 35 giornate lavorative, di cui 4 sotto la direzione e guida di un Responsabile Gruppo di Audit (RGA) per un totale di almeno 20 giorni di esperienza di audit, - aggiornamento professionale di almeno 24 ore nei precedenti 3 anni, su temi della ISMS potrà essere ammesso alla prova tecnica specifica orale dell'esame CEPAS come da procedura vigente (PG30). Il candidato in possesso di certificazione valida come ISMS Responsabile Gruppo di Audit rilasciata da Organismo di certificazione del Personale riconosciuto da CEPAS che documenta, in aggiunta ai requisiti per Auditor (p.to 3), anche il possesso dei seguenti requisiti: - 3 Audit completi effettuati negli ultimi 2 anni a fronte della Norma UNI CEI ISO/IEC 27001, per un totale di almeno 15 giornate lavorative condotti nel ruolo di Responsabile Gruppo di Audit, sotto la direzione e guida di un Responsabile Gruppo di Audit (RGA) per un totale di almeno 15 giorni di esperienza di audit. può essere ammesso alla prova tecnica specifica orale dell'esame CEPAS come da procedura vigente (PG30). --- **4)** Il Candidato che documenta i seguenti requisiti: - esperienza lavorativa continuativa complessiva di 10 anni di cui 6 specifici nel campo dei Sistemi di gestione della sicurezza delle informazioni - superamento esame finale di un corso per ISMS Auditor di 40 ore - 7 Audit completi effettuati negli ultimi 3 anni a fronte della Norma UNI CEI ISO/IEC 27001, per un totale di almeno 35 giornate lavorative - aver superato positivamente un percorso di training come ISMS Auditor in accordo ai principi delle Norme UNI EN ISO 19011 e UNI CEI EN ISO/IEC 17021 (parti applicabili) da parte di un Organismo di certificazione di Sistema nel caso di audit di III parte oppure, nel caso di audit di I o II parte, sotto la direzione e guida di un ISMS Responsabile Gruppo di Audit certificato da Organismo di certificazione del Personale accreditato - aggiornamento professionale di almeno 24 ore nei precedenti 3 anni, su temi della ISMS potrà essere ammesso alla parte scritta specifica (caso di audit) e alla prova tecnica specifica orale dell'esame CEPAS come **ISMS Auditor** come da procedura vigente (PG30). Il Candidato che documenta, in aggiunta ai requisiti per Auditor (p.to 4), anche il possesso dei seguenti requisiti: - 3 Audit completi effettuati negli ultimi 2 anni a fronte della Norma UNI CEI ISO/IEC 27001, per un totale di almeno 15 giornate lavorative condotti nel ruolo di Responsabile Gruppo di Audit

	- aver superato positivamente un percorso di training come ISMS Responsabile Gruppo di Audit in accordo ai principi delle Norme UNI EN ISO 19011 e UNI CEI EN ISO/IEC 17021 (parti applicabili) da parte di un Organismo di certificazione di Sistema nel caso di audit di III parte oppure, nel caso di audit di I o II parte, sotto la direzione e guida di un ISMS Responsabile Gruppo di Audit certificato da Organismo di certificazione del Personale accreditato potrà essere ammesso alla parte scritta specifica (caso di audit) e alla prova tecnica specifica orale dell'esame CEPAS come ISMS Responsabile Gruppo di Audit come da procedura vigente (PG30). --- **5)** Il Candidato in possesso di certificazione come Auditor di S.G.Q./S.G.A. e/o S.G.Safety rilasciata da un Organismo di Certificazione del Personale accreditato e/o riconosciuto, che documenta i seguenti requisiti per la certificazione: - esperienza lavorativa continuativa specifica di almeno 2 anni nel campo dei Sistemi di gestione della Sicurezza delle Informazioni - frequenza di un corso per ISMS Auditor di almeno 24 ore - aver effettuato 3 Audit completi come Auditor sotto la direzione e guida di un Responsabile Gruppo di Audit (RGA) qualificato negli ultimi 2 anni a fronte della Norma UNI CEI ISO/IEC 27001 per un totale di almeno 15 giorni di esperienza di audit potrà essere ammesso alla parte scritta specifica (caso di audit) e alla prova orale dell'esame CEPAS per ISMS Auditor come da procedura vigente (PG30). --- **6)** Il Candidato che ha superato positivamente la valutazione in campo, in occasione di un audit completo esterno (di II o III parte), in accordo alla procedura vigente, ed in possesso di tutti i requisiti di formazione specifica, esperienza lavorativa complessiva, esperienza specifica di audit descritti al punto 1, potrà essere ammesso alla prova tecnica specifica orale dell'esame CEPAS come da procedura vigente (PG30).
ISCRIZIONE AL REGISTRO	Il candidato che supera l'esame di certificazione viene iscritto nel registro CEPAS degli ISMS Auditor o dei Responsabili Gruppo di Audit e riceve il certificato CEPAS attestante il possesso della certificazione.
PASSAGGIO DI REGISTRO da ISMS Auditor a ISMS Responsabile Gruppo di Audit	E' possibile richiedere il passaggio di registro, trascorsi almeno 6 mesi dalla prima certificazione, integrando gli Audit ISO/IEC 27001 prodotti per la prima certificazione, al fine di soddisfare quanto richiesto dalla presente scheda per la certificazione come ISMS Responsabile Gruppo di Audit. In particolare, è necessario documentare la seguente esperienza di audit maturata, negli ultimi 2 anni consecutivi, come Responsabile di almeno: - **5** Audit completi, non tutti interni, eseguiti su almeno 4 distinti sistemi **Almeno 3** dei suddetti audit dovranno essere effettuati ricoprendo il ruolo di Responsabile Gruppo di Audit sotto la direzione e guida di un Responsabile Gruppo di Audit (RGA) certificato da un Organismo di Certificazione del Personale o qualificato da Organismo di Certificazione di Sistema, per un totale di almeno 15 giorni di esperienza di audit.
RISPETTO DEL CODICE DEONTOLOGICO (estratto)	L' ISMS Auditor / Responsabile Gruppo di Audit certificato e/o in iter di certificazione firma il Codice Deontologico CEPAS con il quale si impegna, inoltre, a: ▪ rendere noti ai propri Clienti (interni ed esterni) i contenuti del codice deontologico; ▪ soddisfare tutti gli impegni presi con lettera di incarico; ▪ tenere una registrazione di tutti i reclami presentati contro di loro per attività svolte nell'ambito della validità della Certificazione CEPAS e permettere a CEPAS l'accesso a dette registrazioni; entro 10 giorni dal ricevimento del reclamo, inviare comunicazione scritta e copia del reclamo stesso a CEPAS; ▪ non effettuare attività promozionali (pubblicità, materiale informativo, ed altro) che possano indurre i Clienti ad una non corretta interpretazione del significato delle certificazioni o delle qualificazioni CEPAS ed, inoltre, indurre aspettative, nel cliente, non rispondenti alle reali situazioni in atto; ▪ non effettuare attività concorrenziale nei confronti di CEPAS.

DURATA **MANTENIMENTO**	La durata della certificazione CEPAS è quinquennale e si rinnova, in assenza di revoca e/o rinuncia alla certificazione, al termine dei cinque anni di validità, come da procedura vigente (PG13). Annualmente, l'ISMS Auditor / Responsabile Gruppo di Audit certificato produrrà a CEPAS la dichiarazione di assenza reclami ed il pagamento della quota di mantenimento prevista dal tariffario CEPAS in vigore.
AGGIORNAMENTO PROFESSIONALE E MIGLIORAMENTO CONTINUO	L'aggiornamento professionale, rivolto specialmente all'identificazione delle aree di miglioramento personale e tecnico/normativo, dovrà essere documentato tramite evidenze attestanti la formazione specifica effettuata per almeno 40h / 5 anni.
RINNOVO DELLA CERTIFICAZIONE	Al termine dei cinque anni di validità, in conformità allo schema di certificazione, CEPAS considera, per il rinnovo della certificazione stessa, che venga soddisfatto e documentato almeno quanto segue, come da procedura vigente (PG13): - attività professionale in corso di svolgimento; - esperienza lavorativa specifica maturata nel settore ISMS: - per ISMS Auditor: 6 ISMS audit completi (su almeno 3 sistemi diversi), di cui almeno 2 nell'ultimo anno - per ISMS Responsabili Gruppo di Audit: 8 ISMS audit completi (su almeno 2 sistemi diversi) di cui almeno 2 nell'ultimo anno e di cui almeno 5 condotti in qualità di Responsabile - aggiornamento professionale per almeno 40 ore nei precedenti 5 anni; - richiesta rinnovo certificazione (MD63rin), contenente accettazione documenti CEPAS, dichiarazione Assenza reclami e accettazione clausole contrattuali - test di verifica dell'aggiornamento delle conoscenze.