SCHEDA REQUISITI PER LA QUALIFICAZIONE DEL CORSO PER ISMS AUDITOR / RESPONSABILI GRUPPO DI AUDIT

1	18.03.2019	Rev. Generale	*Presidente CSI / Schema*	*Amministratore Delegato*
0	21.11.2013	CEPAS srl	*Presidente Comitato di Certificazione*	*Amministratore Unico*
Rev.	**Data**	**Motivazioni**	**Convalida**	**Approvazione**

REQUISITI ORGANIZZATIVI DELL'ENTE EROGANTE IL CORSO	
Organizzazione	L'organizzazione deve designare un proprio rappresentante legale e un responsabile "tecnico" per la didattica (quest'ultimo sarà l'interfaccia CEPAS, per tutti gli aspetti concernenti il processo di qualificazione e di mantenimento).
Risorse umane	L'organizzazione dovrà utilizzare almeno 2 docenti che si alternano durante il corso; per un numero di partecipanti inferiore a 10 è consentito un solo docente. **REQUISITI PER I DOCENTI** Ciascun docente, individualmente, deve documentare: • 5 anni di attività professionale nell'ISMS • almeno 100 ore di docenza sui temi oggetto del corso • aggiornamento professionale, svolto negli ultimi tre anni, sui temi specifici della formazione in oggetto non inferiore a 24 ore • certificazione come ISMS Auditor rilasciata da Organismo di Certificazione del Personale accreditato e riconosciuto da CEPAS
Infrastruttura	L'organizzazione dovrà garantire in ogni edizione del corso l'idoneità dei locali destinati alla formazione, in accordo alla Normativa cogente in vigore, relativamente agli strumenti di supporto didattici (strumenti informatici, audiovisivi ecc.). Per i corsi erogati in modalità FAD dovrà essere garantita la disponibilità di idonea piattaforma dimensionata per l'utenza.
Comunicazione	Il corso deve essere presentato ai partecipanti mediante adeguato documento (*brochure o altro simile*) contenente almeno le seguenti informazioni: • organizzazione titolare del corso, identificata dal proprio logo (eventuali partner commerciali di supporto devono essere indicati come tali) • numero di iscrizione nel Registro CEPAS (a qualificazione ottenuta) • luogo e periodo di svolgimento • programma didattico dettagliato, struttura e durata in ore del corso (non inferiore ai requisiti minimi CEPAS) • scopo e finalità • nome del coordinatore tecnico e altri riferimenti della segreteria dell'Organizzazione titolare • requisiti di accesso per i partecipanti • rilascio dell'attestato di Corso qualificato ai soli partecipanti in possesso dei requisiti di accesso • validità del corso come uno dei requisiti per la certificazione CEPAS • il percorso di certificazione dell'ISMS Auditor • il numero massimo dei partecipanti (in ogni caso non superiore a 20 persone) (*) • assenza consentita (in ogni caso non superiore al 5% sul totale di 40 ore) Su tale documento, il riferimento al possesso della qualificazione CEPAS sarà autorizzato solo a qualificazione ottenuta. In iter di qualificazione può essere apposto solo il riferimento "corso in fase di qualificazione da parte del CEPAS", previa approvazione CEPAS. *(*) Il numero di partecipanti può essere aumentato fino ad un massimo di 35 persone, qualora il corso inserito all'interno di un percorso formativo della durata di almeno 600 ore sui Sistemi di Gestione per la Qualità e/o Ambiente e/o Safety e/o Sicurezza delle Informazioni, del quale i partecipanti abbiano già seguito almeno 250 ore. Per le esercitazioni occorre prevedere almeno 2 tutor / assistenti. Restano invariati i requisiti di accesso dei partecipanti, come di seguito riportati*

REQUISITI MINIMI PER IL CORSO	
Durata	40 ore totali di lezioni, esercitazioni ed esami. Ogni giornata non può contribuire per più di 8 ore al computo delle 40 ore totali.
Obiettivi	• conoscenza e comprensione delle norme a fronte delle quali devono essere eseguiti gli Audit interni ed esterni; • conoscenza delle metodologie per preparare, condurre e chiudere l'audit, per preparare e distribuire il rapporto di audit; • capacità attitudinali richieste per pianificare e dirigere l'audit, capacità di organizzazione, comunicazione e gestione; • acquisizione delle conoscenze specifiche degli aspetti tecnici e organizzativi dei processi per la tutela delle informazioni e la sicurezza dei sistemi informatici aziendali.
Requisiti di accesso dei partecipanti al corso	• diploma di istruzione secondaria superiore o titolo superiore • appropriata e documentata esperienza di lavoro di 1 anno in attività nel settore ISMS • Superamento del questionario tecnico di ingresso con almeno 15 domande a risposta chiusa (sono esclusi i quesiti con risposte Vero/Falso), relative alle conoscenze di information security
STRUTTURA	
ARGOMENTI	***Le norme/linee guida citate si intendono nella loro versione vigente/applicabile*** ***<u>Area Auditing</u>*** • norma UNI EN ISO 19011, ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27006 e Prescrizioni ACCREDIA applicabili • Norma UNI EN ISO 19011: - nuova terminologia adeguata alla logica del processo di audit - principi dell'attività di audit - approccio basato sul rischio (risk-based approach) - contesto dell'organizzazione - la leadership e l'impegno per l'implementazione e mantenimento del sistema di gestione - nuovi strumenti a disposizione per la conduzione degli audit (audit in campo ed audit virtuali) - la conformità legislativa e la catena di fornitura - gestione di un programma di audit comprensiva della gestione dei rischi ed opportunità del programma di audit - pianificazione operativa e coordinamento degli audit - attività di audit - competenza e valutazione degli auditor secondo i nuovi requisiti • Norma UNI CEI EN ISO/IEC 17021, in particolare cap. 9 e Appendici A, D, E, F • Tipologie di audit • Pianificazione dell'audit che deve prevedere: o comunicazione con l'organizzazione sottoposta ad audit; o documentazione dell'esame preliminare; o esame della documentazione; o selezione del team di audit; o preparazione dell'audit e riunione del team. • Cenni sulle finalità di audit preliminari • Preparazione ed uso (con esempi di modulistica) di checklist durante le fasi di audit • Preparazioni delle riunioni di audit, con esempi • Contenuto, programma e conduzione delle riunioni di apertura e chiusura • Comportamento dell'auditor nello svolgimento dell'audit, incluse le relazioni con l'azienda, l'importanza delle evidenze oggettive; rilevazione, redazione e comunicazione delle anomalie • Criteri per la formulazione e metodologie per l'identificazione dei rilievi e loro classificazione

- Attività di follow-up
- Cenni sulla gestione del rischio come applicabile nel settore ISMS
- Cenni sul rispetto dei requisiti di legge su salute e sicurezza da parte del Gruppo di Audit
- Elementi di metrologia industriale, tecniche statistiche, tecniche affidabilistiche ("failure analysis") applicabili al settore
- Differenze di ruolo fra Auditor e Responsabili Gruppo di Audit, nella gestione dell'audit e dei membri del team
- Schema di certificazione CEPAS per ISMS auditor
- Codice deontologico CEPAS dell'Auditor

Area Legale

- L. 300/1970
- Aspetti legali relativi ai Decreti legislativi e modificazioni successive:
  - Normativa Privacy (GDPR)
  - Diritto d' Autore: L. 633/41 - D. Lgs 518/92 - L. 248/00 - Regol. 338/01 (SIAE)
  - Responsabilità penali delle Persone Giuridiche (pirateria informatica, pedoporno, truffe informatiche ai danni dello stato) D. Lgs. 231/01
  - Commercio elettronico, D. Lgs 70/03
  - Proprietà Industriale, D. Lgs. 30/05
  - Amministrazione Digitale (firme elettroniche etc.) D. Lgs. 82/05
  - Antiterrorismo (pacchetto Pisanu) L. 155/05
  - Violazione reti informatiche,
- Conoscenze degli aspetti normativi sulla tutela del segreto di Stato
- Responsabilità Civili, Penali e Amministrative
- Aspetti contrattuali relativi all'Outsourcing connessi alla Security
- Aspetti contrattuali (security audit) Fornitori, Clienti, Terze Parti
- Aspetti di diritto e procedura penali connessi alla Security
- Iniziative di tipo giuridico e assicurativo a protezione del patrimonio informativo aziendale

Area Tecnologica

- Elementi base dell'ISMS, dei concetti di sistema e delle reti
- Fondamentali dell'Information Security
- Criteri e strumenti di classificazione dei dati trattati
- Tecniche di controllo accesso fisico e logico
- Modalità di protezione delle informazioni ed elementi di crittografia
- Firma elettronica, digitale
- Virus, I-Worms, Programmi maligni, Prodotti e tecniche di prevenzione e di contrasto
- Business Continuity, Disaster Recovery e Crisis Management
- Penetration tests (cenni) e relativi aspetti legali
- Applicazione delle soluzioni individuate delle vulnerabilità e delle minacce
- ITSEC (cenni)
- ISO 15408 Parte 1 - 2 e 3 (cenni) (ex Common Criteria)
- Elementi base dei principali rischi per l'ICT Security nei: commercio elettronico, EDI (Elettronic Data Interchange), posta elettronica, operazioni bancarie o di trading remote, sistemi di gestione integrati ERP, sistemi di supporto a e decisioni (DSS), sviluppo e/o acquisto di Sistemi Informativi e di Telecomunicazione, re-ingegnerizzazione dei processi o del relativo sw, gestione della documentazione di sistema.

Area Management

La formazione manageriale di base dovrebbe includere aspetti che vanno dalla comunicazione efficace alla gestione del budget, dal problem solving ad aspetti strategici.
In particolare per la formazione dell'ISMS Auditor si dovranno includere:

	• Aspetti organizzativi dell'Information Technology • Aspetti organizzativi dell'Information Security • Gestione delle problematiche complesse • Normativa Privacy (GDPR) • D.Lgs 231/01, sistemi di controllo ed elementi di Corporate Governance • Norma ISO 31000 Risk Management – Principles and guidelines. • Norma ISO/IEC 27000, Information technology -- Security techniques -- Information security management systems - Fundamentals and vocabulary • Norma ISO/IEC 27001 Tecnologie delle informazioni. Tecniche di sicurezza. Sistemi di gestione delle sicurezza delle informazioni – Requisiti • Norma ISO/IEC 27002, Information Technology - Security techniques - Code of Practice for information security management • Norma ISO/IEC 27005, Information technology — Security techniques — Information security risk management • Norma ISO/IEC 27006, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems • ISO/IEC 27007 Information technology — Security techniques • ISO/IEC 27013 Information technology — Security techniques • Definizione della Information Security Policy • Definizione delle strategie dell'ISMS • Organizzazione della struttura di ISMS • BS 25999-1: 2006 Business Continuity Management, Part 1: Code of practice • ISO 22301 Societal security - Business continuity management systems - Requirements • Sistemi di misurazione per analisi Costi/Benefici • Modalità di supporto alle attività delle istituzioni deputate • Rischi di ICT Security connessi allo sviluppo e/o acquisto di Sistemi Informativi e di Telecomunicazione. • Rischi ICT Security connessi con la re-ingegnerizzazione dei processi o del relativo sw • Rischi connessi alla gestione della documentazione di sistema
Esercitazioni	Devono costituire il 50% del tempo totale del corso e devono essere ripartite su**:** • conoscenza delle Norme applicabili; • normativa nazionale ed europea del sistema di accreditamento e certificazione • conoscenza area tecnologica, legale e di management, • uso degli strumenti di audit; • programma di audit; • metodologie per la formulazione dei rilievi emersi nell'audit. **Casi su:** • Preparazione delle attività di audit sul campo: - pianificazione delle attività di audit sul campo - assegnazioni delle attività al gruppo di audit - preparazione dei documenti di lavoro - simulazione di riunione chiusura di audit Tutte le esercitazioni devono essere raccolte, registrate e documentate in modo appropriato dall'Organizzazione e devono essere finalizzate alla verifica della conformità ai requisiti fissati per gli argomenti del corso.

Documentazione	Il corso di formazione deve essere definito da un "pacchetto formativo" scritto, documentale e/o multimediale, composto almeno da: • Questionario tecnico di ingresso • Guida per il docente che deve contenere: - descrizione dettagliata dei contenuti - descrizione delle esercitazioni da effettuare e utilizzo dei relativi strumenti - descrizione delle metodologie didattiche da applicare in ciascuna attività - tempi da dedicare a ciascuna attività - criteri per la raccolta ed archiviazione delle registrazioni - obiettivi di ogni singolo modulo/intervento formativo • Materiale per il partecipante che deve contenere: - materiale didattico completo utilizzato in aula - una sintesi, in forma descrittiva oppure schematica, di tutti gli argomenti trattati - curricula dei singoli docenti - una bibliografia selettiva - modulo per la valutazione del corso e dei docenti - regolamento del corso comprendente i reclami - criteri di valutazione delle esercitazioni e dell'esame • Guida per la conduzione degli esami finali che deve contenere: - descrizione per titoli delle prove (scritte e orali) con tempi relativi - almeno un esempio (non svolto) di ciascuna delle prove scritte - almeno 10 esempi di domande per esami orali Il pacchetto formativo deve essere firmato da un Progettista di formazione e da un Esperto di argomento. Le due persone possono coincidere, se la persona possiede i requisiti minimi di entrambe le funzioni.
Valutazione	La valutazione complessiva di ogni partecipante deve essere formalizzata e registrata e deve consentire di determinare se gli obiettivi del corso sono stati conseguiti. La valutazione finale deve essere superata con una soglia minima, secondo criteri prestabiliti dall'Organizzazione ed approvati da CEPAS. Devono almeno essere previste: ▪ 1 prova scritta, individuale, volta ad accertare le conoscenze acquisite dai candidati della durata di 1,5 ore ▪ 1 prova orale di approfondimento dei temi citati e valutazione delle abilità e dei comportamenti personali del candidato (rif. Norma UNI EN ISO 19011 p.to 7.2 e Norma UNI CEI EN ISO/IEC 17021, Appendici A, D) della durata di 15 minuti. COMMISSIONE D'ESAME La Commissione d'esame deve essere composta da almeno 2 Commissari (anche nel caso di un numero di partecipanti inferiore a 10) di cui uno deve essere il docente del corso certificato come ISMS Responsabile Gruppo di Audit; il secondo Commissario può essere, invece, altro docente oppure un esperto nominato dall'ente organizzatore del corso. Tutte le singole prove devono essere raccolte e documentate in modo appropriato dall'Organizzazione.

CONDIZIONI PER IL MANTENIMENTO DELLA QUALIFICAZIONE CEPAS	
Durata della Qualificazione	La qualificazione del corso ha una durata annuale e si rinnova tacitamente di anno in anno, in assenza di revoca e/o rinuncia.
Sorveglianza	Il corso qualificato sarà oggetto di sorveglianza annuale, attraverso verifica diretta (in fase di erogazione del corso) e indiretta (di tipo documentale), nelle sessioni scelte a discrezione da CEPAS.
Prescrizioni	Tutte le seguenti prescrizioni dovranno essere rispettate dall'Ente erogante il corso: • rispettare i requisiti di cui alla "Scheda/e di riferimento per il corso • non cedere, modificare e/o trasferire ad alcun titolo, la qualificazione del corso, senza la preventiva autorizzazione di CEPAS, che se ne riserva l'accettazione previa opportuna verifica e valutazione insindacabili. • comunicare entro il 15 gennaio di ogni anno il programma annuale delle edizioni del corso e confermare, 5 giorni prima dell'inizio, ciascuna edizione del corso e i nominativi dei docenti; • consentire ai Commissari incaricati da CEPAS la valutazione periodica (visita di sorveglianza annualmente prevista) sia sul campo sia presso la sede dove vengono conservate le registrazioni inerenti la gestione del corso qualificato (es. registrazioni dei reclami o dei requisiti dei partecipanti, monitoraggio dei docenti, risoluzione di non conformità riscontrate); • consentire ai Commissari o al Personale CEPAS debitamente autorizzato, la valutazione documentale relativa a tutte le edizioni del corso successive all'ottenimento della qualificazione; • notificare e inviare a CEPAS ogni variazione nei contenuti del programma didattico del corso e/o dei docenti e ogni comunicazione relativa al Corso qualificato (locandina, articoli, pubblicità a mezzo stampa, web) al fine di verificare la coerenza e correttezza delle informazioni rispetto al significato della qualificazione CEPAS; • inviare a CEPAS, in formato elettronico, entro 15 giorni dal termine del corso, l'elenco dei candidati che hanno superato le singole edizioni, completo di indirizzi, recapiti telefonici/fax, e-mail, autorizzati dai candidati stessi; • mantenere un registro dei reclami e dei moduli di valutazione del corso e dei docenti (compilati dai partecipanti al corso stesso) e renderli disponibili, su richiesta, a CEPAS; entro 10 giorni dalla ricezione del reclamo, inviare comunicazione scritta e copia del reclamo stesso a CEPAS; • versare, alle scadenze previste, le quote annuali relative al mantenimento della qualificazione del corso, indicate nel tariffario CEPAS in vigore • non utilizzare la qualificazione del corso come sinonimo di certificazione professionale dei partecipanti • non effettuare attività concorrenziale nei confronti di CEPAS • .