

CEPAS

Viale di Val Fiorita, 90 - 00144 Roma
Tel. 065915373 - Fax: 065915374
E-mail: esami@cepas.it
Sito internet: www.cepas.it

PROCEDURA GESTIONALE**sigla: PG30****Pag. 1 di 8****MODALITÀ DI VALUTAZIONE DEGLI
ISMS AUDITOR / RESPONSABILI GRUPPO DI AUDIT**

4	19.09.2008	Pag. 8	<i>R.A. Favorito</i>	<i>G. Colferai</i>
3	16.05.2008	Pagg. 4, 6	<i>R.A. Favorito</i>	<i>G. Colferai</i>
Rev.	Data	Motivazioni	Convalida	Approvazione

INDICE**1.0 SCOPO E CAMPO DI APPLICAZIONE****2.0 RIFERIMENTI****3.0 PROCESSO DI VALUTAZIONE****4.0 ESAME**

- 4.1 Requisiti di ammissione esame di certificazione**
- 4.2 Finalità esame**
- 4.3 Argomenti e modalità svolgimento esame**
- 4.4 Criteri di valutazione**

5.0 CERTIFICAZIONE

- 5.1 Rilascio del certificato**
- 5.2 Passaggio di Registro (da ISMS Auditor a Responsabile Gruppo di Audit)**

1.0 SCOPO E CAMPO DI APPLICAZIONE

La presente procedura descrive le modalità operative adottate da CEPAS per l'attività di valutazione e certificazione degli Auditor (AUD) e dei Responsabili Gruppo di Audit (RGA) di Sistemi di Gestione per la Sicurezza delle Informazioni (ISMS). La procedura si applica nei processi di certificazione delle figure professionali specificate che operano nell'ambito dei Sistemi di Gestione per l'ISMS ed evidenzia le responsabilità delle diverse funzioni CEPAS coinvolte.

2.0 RIFERIMENTI

- Riferimenti CEPAS per la certificazione degli Auditor e dei Responsabili Gruppo di Audit:
 - Norma UNI CEI EN ISO/IEC 17024:2004
 - IAF GD 24:2004 Guidance on the Application of ISO/IEC 17024:2003
 - Manuale del Sistema di Gestione per la Qualità CEPAS, sez. 5 (MQ01)
 - Schema di Certificazione CEPAS: Regolamento Generale CEPAS (RG01), Codice Deontologico (CD01), Prescrizioni per l'Uso del Marchio (MC01), Modulo richiesta ammissione esame/certificazione (MD08accr), Scheda Requisiti CEPAS SH142 e la presente procedura PG30
 - RT 15 Sincert "Prescrizioni integrative per l'accreditamento degli Organismi di Certificazione del Personale (per la figura di Auditor di sistemi di gestione), in accordo alla norme ISO/IEC 17024:2003 e ISO 19011:2002"
- Riferimenti normativi per la valutazione degli Audit:
 - UNI EN ISO 19011:2003
 - UNI CEI ISO/IEC 27001:2006
 - UNI CEI EN ISO/IEC 17021:2006
 - ISO/IEC 17799:2005

3.0 PROCESSO DI VALUTAZIONE

La valutazione di idoneità del Candidato, ai fini del rilascio della certificazione CEPAS, avviene attraverso la sequenza, temporale e vincolante, di ciascuna delle seguenti fasi:

- valutazione preliminare della documentazione prodotta dal Candidato eseguita da CEPAS, che accerta il possesso o meno, da parte dello stesso, dei requisiti di cui alla Scheda SH142; successivamente, il R.Q. effettua una ulteriore analisi documentale; nei casi dubbi, il Direttore può inoltre procedere a:
 - richiesta di informazioni/documenti supplementari al candidato;
 - accertamento, tramite invio di un Commissario appositamente incaricato, dell'attività svolta presso le aziende citate nella documentazione presentata.

CEPAS invia ai candidati che hanno presentato domanda di certificazione la seguente modulistica, realizzata in accordo con quanto definito dalla Linea Guida IAF GD 24:2004 sull'applicazione della norma ISO/IEC 17024:2003, contenente tutte le informazioni necessarie a CEPAS per verificare il possesso dei requisiti richiesti per la certificazione:

- MD71: Modulo di registrazione audit UNI CEI ISO/IEC 27001:2006
- MD71dich: Modulo fac simile lettera di referenze (per documentare esperienza lavorativa)
- MD71dich_training: Moduli di registrazione audit condotti sotto la direzione e guida di Responsabili Gruppo di Audit certificati da OdC del Personale o qualificati da OdC di Sistema

La suddetta modulistica è considerata completa solo se corredata dai documenti indicati nei moduli stessi (es. rapporti di audit, curriculum e certificato valido del supervisore, ecc.).

ad esito positivo segue:

- esame di certificazione CEPAS, eseguito dalla Commissione di Esame a fronte di parametri e sulla base di strumenti prefissati, specificati nel paragrafo successivo;

ad esito positivo segue:

- valutazione tecnica dei risultati, di cui ai punti sopra indicati, eseguita dal Gruppo di Approvazione Settoriale CEPAS;

ad esito positivo segue:

- approvazione da parte del Direttore CEPAS;

ad esito positivo segue:

- ratifica da parte del Comitato di Certificazione / Comitato di Schema.

Qualora l'esito di una qualsiasi delle suddette fasi sia negativo, CEPAS interrompe il processo di valutazione e informa il Candidato che decide quindi se proseguire o meno nell'iter di certificazione. Per procedere nell'iter sarà necessario prima risolvere le carenze riscontrate nella singola fase, nei tempi indicati da CEPAS.

4.0 ESAME

4.1 Requisiti di ammissione esame di certificazione

Il Candidato che ha frequentato il corso di 40 ore sulla Sicurezza delle Informazioni CEPAS è ammesso direttamente all'esame di certificazione.

Sono ammessi a sostenere l'esame CEPAS per ISMS Auditor/Responsabili Gruppo di Audit tutti coloro che, avendo presentato formale richiesta attraverso il modulo MD08, documentano il possesso dei seguenti requisiti minimi, allegandoli al modulo e di cui alla Scheda SH142:

- diploma di istruzione secondaria superiore o titolo superiore,
- copia documento d'identità valido,
- attestato di frequenza di un corso per ISMS Auditor
- evidenze oggettive in merito alle conoscenze richieste dalla Norma UNI EN ISO 19011/2003
- evidenze oggettive in merito agli anni di esperienza lavorativa continuativa complessiva e agli anni di esperienza lavorativa specifica nel campo dell'ISMS,
- evidenze oggettive in merito agli audit completi UNI CEI ISO/IEC 27001:2006 validi a fini della certificazione,
- evidenze oggettive in merito agli audit completi effettuati sotto la direzione e guida di un Responsabile Gruppo di Audit,
- copia di: "Codice Deontologico" (CD01) e "Prescrizioni per l'uso del Marchio" (MC01), già in possesso del Candidato, firmati per accettazione delle procedure dell'intero iter di certificazione,
- regolare pagamento delle quote previste per l'ammissione agli esami come da tariffario CEPAS.

La documentazione completa per la richiesta di certificazione deve essere trasmessa a CEPAS entro 10 giorni lavorativi prima della data d'esame.

4.2 Finalità esame

L'esame ha lo scopo di:

- approfondire le informazioni presentate dal Candidato, nell'ambito della sua esperienza professionale, valutando l'adeguatezza della documentazione presentata e la sua congruenza con il/i settore/i di interesse indicato/i dal Candidato;
- accertare il possesso da parte del Candidato delle conoscenze tecniche e metodologiche necessarie a svolgere il ruolo di ISMS Auditor o di Responsabile Gruppo di Audit. ai fini del rilascio della relativa Certificazione;

Rientrano tra tali conoscenze e abilità:

Area Auditing:

- norme UNI EN ISO 19011/2003, UNI CEI ISO/IEC 27001:2006, ISO/IEC 27002:2005 e serie collegata, e Prescrizioni SINCERT applicabili
- tipologie di audit
- pianificazione dell'audit che deve prevedere:
 - comunicazione con l'organizzazione sottoposta ad audit
 - documentazione dell'esame preliminare
 - esame della documentazione

- selezione del team di audit
- preparazione dell'audit e riunione del team
- cenni sulle finalità degli 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
- elementi di metrologia industriale, tecniche statistiche, tecniche affidabilistiche ("failure analysis") applicabili al settore
- differenze di ruolo fra Auditor e Responsabile Gruppo di Audit, nella gestione dell'audit e dei membri del team
- codice deontologico dell'Auditor certificato.

Area Legale:

- L. 300/1970
- riferimenti legislativi in essere (D.Lgs 518/92, L. 547/93, DPR 513/97) e modificazioni successive
- misure minime di sicurezza (All. B del Disciplinare Tecnico al D.Lgs 196/03 e modificazioni successive)
- conoscenze degli aspetti normativi sulla tutela del segreto di Stato
- Responsabilità Civili, Penali e Amministrative
- iniziative di tipo giuridico e assicurativo a protezione del patrimonio informativo aziendale
- aspetti relativi alla Proprietà Intellettuale e copyright
- 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

Area Tecnologica:

- elementi base dell'ISMS, dei concetti di sistema e delle reti
- fondamentali della Security
- criteri e strumenti di classificazione dei dati trattati
- tecniche di controllo accesso fisico e logico
- sistemi e credenziali per l'autenticazione informatica
- principali protocolli per il trasferimento dei dati
- modalità di protezione delle informazioni ed elementi di crittografia
- firma elettronica, digitale
- sicurezza soluzioni Wireless
- Intranet, VPN, LAN
- Virus, I-Worms, Programmi maligni, Prodotti e tecniche di prevenzione e di contrasto
- Business Continuity, Disaster Recovery e Crisis Management
- applicazione delle soluzioni individuate delle vulnerabilità e delle minacce
- tecniche e metodologie di audit nell'ISMS
- applicativi, standard dei prodotti (ISO, UNI)
- principali tools di selezione accessi logici utilizzati nei main frame
- standard di riferimento nazionali e internazionali:
 - criteri di valenza europea ITSEC
 - ISO 15408 Parte 1 - 2 e 3 (cenni) (ex Common Criteria)
 - UNI CEI ISO/IEC 27001:2006, per ISMS (Information Security Management System)

Area Management:

- Aspetti organizzativi dell'Information Technology
- Aspetti organizzativi dell'Information Security
- Gestione delle problematiche complesse
- D.Lgs. 231/2001, sistemi di controllo ed elementi di Corporate Governance
- D. Lgs 196/2003, D.Lgs 196 del 30 giugno 2003 - Codice in materia di protezione dei dati personali
- Norma UNI CEI ISO/IEC 27001:2006 Tecnologie delle informazioni. Tecniche di sicurezza. Sistemi di gestione delle sicurezza delle informazioni – Requisiti
- Norma ISO/IEC 27002: 2005 Information Technology - Security techniques - Code of Practice for information security management
- Definizione della politica dell'ISMS
- Definizione delle strategie dell'ISMS
- Organizzazione della struttura di ISMS
- Risk Assessment: Risk Analysis e Risk Evaluation
- Risk Management
- BS 25999-1: 2006 Business Continuity Management, Part 1: Code of practice
- BS 25999-2: 2007 Business Continuity Management, Part 2: Specification
- 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

L'esame è condotto dai Commissari d'esame CEPAS, nominati dal Presidente, i quali si accertano, attraverso opportune tecniche, che il Candidato possieda i requisiti e le caratteristiche personali utili allo svolgimento delle attività professionali per le quali richiede la certificazione. La Commissione definirà inoltre, in sede d'esame, l'idoneità allo svolgimento del ruolo richiesto, sulla base della documentazione prodotta e lo comunicherà al candidato al termine dell'esame (ISMS Auditor oppure ISMS Responsabile Gruppo di Audit).

I Commissari sono responsabili della valutazione delle prove d'esame del Candidato e per questo ne rispondono a CEPAS; per tutte le attività di valutazione i Commissari garantiscono indipendenza di giudizio, assenza di conflitto di interessi e riservatezza dei dati.

4.3 Argomenti e modalità svolgimento esame

Modalità svolgimento esame

L'esame CEPAS per ISMS Auditor/Responsabili Gruppo di Audit si svolge nelle località e date stabilite, di volta in volta, dal Direttore il quale, con l'ausilio del personale dipendente, provvede a comunicarle a ciascun Candidato. Alla sessione d'esame CEPAS sono presenti i candidati, la Commissione d'esame e il personale CEPAS

Prima dell'inizio delle prove d'esame, i candidati sono tenuti a:

- esibire un documento di identità valido,
- firmare il foglio presenze,
- presentare la ricevuta degli avvenuti pagamenti delle quote previste per la partecipazione all'esame.

Argomenti

L'esame CEPAS consiste in:

- una prova scritta di carattere specifico (capacità di applicare correttamente le norme);
- una prova scritta di carattere generale (conoscenza ed interpretazione delle norme);
- una prova orale (colloquio).

La prova scritta di carattere specifico, caso di studio, riferito ad un audit, è volta ad accertare la conoscenza, da parte del Candidato, delle metodologie di esecuzione delle attività per le quali si è richiesta la Certificazione (ISMS Auditor/Responsabile Gruppo di Audit). Per tale prova è previsto un tempo massimo di 70 minuti.

La prova scritta di carattere generale è volta ad accertare il possesso, da parte del Candidato, delle conoscenze tecniche necessarie a svolgere le attività relative alla domanda di Certificazione presentata. E' composta da:

- un numero minimo di 20 domande, per le quali vengono fornite cinque risposte di cui una sola è sicuramente esatta. Per tale prova è previsto un tempo massimo di 45 minuti.

Durante l'intero svolgimento delle prove d'esame, il Candidato può consultare esclusivamente le Norme, in versione ufficiale o autorizzata, sempre in maniera individuale. La consultazione di documentazione differente (es. materiale didattico di corsi, interpretazioni della Norma, ecc.) e/o lo scambio di informazioni con altri candidati è causa di interruzione dell'esame stesso.

La prova orale (colloquio) è volta a:

- approfondire il livello di conoscenza degli elementi culturali di base di cui alle prove scritte,
- approfondire nell'ambito della esperienza professionale le informazioni presentate dal Candidato,
- valutare l'adeguatezza, l'estensione ed il grado di aggiornamento delle esperienze specifiche operative,
- verificare il modo di gestire i rapporti interpersonali del Candidato,
- valutare le caratteristiche personali previste dalla Norma di riferimento (UNI EN ISO 19011:2003 – par.7) in funzione del ruolo di Auditor o di Responsabile Gruppo di Audit,
- valutare la congruenza tra la richiesta di certificazione da parte del Candidato (nel ruolo di AUD o RGA) e lo Schema di Certificazione CEPAS,

Le due prove, nel loro insieme, sono finalizzate a verificare le conoscenze, le capacità applicative delle Norme UNI CEI ISO/IEC 27001:2006, e UNI EN ISO 19011:2003, ed i requisiti personali dei candidati richiesti dalla norma UNI EN ISO 19011:2003 (par.7). La valutazione delle caratteristiche personali (rif. UNI EN ISO 19011 par.7) è condotta anche con l'ausilio di opportuni strumenti dedicati (colloquio, questionario ecc.).

I Commissari, al termine delle prove, comunicano a ciascun candidato l'esito della valutazione delle prove da essi effettuata. Il Personale CEPAS presente comunica, quindi, l'esito finale dell'esame al candidato, ricordandogli le fasi successive previste dallo schema di certificazione già in suo possesso.

4.4 Criteri di valutazione

La Commissione di Esame procede alla valutazione di idoneità del Candidato a fronte dei criteri e dei parametri di seguito specificati:

- la votazione massima ottenibile è di 80 punti, ed è data dalla sommatoria delle votazioni conseguite dal candidato nelle tre prove d'esame.
- la valutazione complessiva è positiva se la somma delle votazioni ottenute nelle tre prove (scritto e orale) raggiunge almeno 56 punti, tenendo comunque presente che deve essere anche superata la soglia minima fissata per le prove scritte, pari a 36 punti.
- la valutazione di idoneità al ruolo di Responsabile Gruppo di Audit è data dalle evidenze emerse durante la prova orale, in riferimento alla UNI EN ISO 19011:2003 (par.7.3.2).
- * alla prova scritta di carattere specifico, viene attribuita una votazione massima di 10 punti.
- * alla prova scritta di carattere generale, viene attribuita una votazione massima di 50 punti.
- * alla prova orale, viene attribuita una votazione massima di 20 punti.

Se il candidato non supera la soglia di 36 punti nelle prove scritte, non viene ammesso alla prova orale e dovrà ripetere l'intero esame (scritto e orale) trascorsi almeno 6 mesi dalla data dello stesso. Sono ammesse ulteriori ripetizioni dell'esame, anche prima dei 6 mesi, previo parere favorevole del Comitato di Certificazione. Ogni ripetizione comporta il pagamento della quota prevista dal tariffario vigente.

Il Candidato in possesso di tutti i requisiti richiesti viene proposto al Gruppo di Approvazione Settoriale e, ad esito positivo, da questo presentato al Direttore CEPAS per l'approvazione. Il Direttore, per i candidati ritenuti idonei,

rilascia il Certificato, provvede all'iscrizione nell'apposito Registro e propone la ratifica al Comitato di Certificazione CEPAS.

5.0 CERTIFICAZIONE

5.1 Rilascio del certificato

Il Direttore, sulla base di tutta la documentazione relativa al Candidato e su eventuali indicazioni fornite dai Gruppi di Approvazione Settoriali, valuta l'eventuale necessità di chiedere ulteriori informazioni ai Responsabili delle Aziende presso cui, o per conto delle quali, il Candidato ha eseguito gli Audit. In tal caso, il Direttore stabilisce anche quali tempi e modalità siano necessari.

Ad esito positivo della valutazione e all'avvenuto pagamento della tariffa di iscrizione, il Direttore approva l'emissione del certificato e comunica il nominativo del Candidato ritenuto idoneo al Comitato di Certificazione / Comitato di Schema che ratifica la certificazione.

La notifica dell'ottenimento della certificazione, unitamente alle modalità per la consegna di certificato e timbro, vengono comunicate al Candidato dal Direttore CEPAS.

5.2 Passaggio di Registro (da ISMS Auditor a ISMS Responsabile Gruppo di Audit)

Il personale certificato CEPAS, in qualità di ISMS Auditor può richiedere il rilascio del certificato come Responsabile Gruppo di Audit e l'iscrizione nel relativo registro, trascorsi almeno 6 mesi dalla prima iscrizione nel Registro.

La richiesta di passaggio richiede l'integrazione della documentazione prodotta per la prima certificazione, sulla base di quanto richiesto dalla Scheda requisiti CEPAS di riferimento, ed il pagamento della quota secondo tariffario.

La valutazione di idoneità del Candidato avviene attraverso la sequenza, temporale e vincolante, di ciascuna delle seguenti fasi:

- valutazione preliminare della documentazione prodotta dal Candidato eseguita da CEPAS, che accerta il possesso o meno, da parte dello stesso, dei requisiti per il passaggio di Registro, di cui alla Scheda SH142; successivamente, il R.Q. effettua una ulteriore analisi documentale; nei casi dubbi, il Direttore può inoltre procedere a:
 - richiesta di informazioni/documenti supplementari al candidato;
 - accertamento, tramite invio di un Commissario appositamente incaricato, dell'attività svolta presso le aziende citate nella documentazione presentata,
 - invitare il Candidato per un colloquio di approfondimento.

ad esito positivo segue:

- valutazione di idoneità della documentazione, di cui ai punti sopra indicati, eseguita dal Gruppo di Approvazione Settoriale CEPAS; il Gruppo di Approvazione Settoriale si riserva inoltre di valutare la congruenza tra la documentazione presentata dal Candidato e la proposta di passaggio di registro;

ad esito positivo segue:

- approvazione da parte del Direttore CEPAS

ad esito positivo segue:

- ratifica da parte del Comitato di Certificazione / Comitato di Schema CEPAS

Qualora l'esito di una qualsiasi delle suddette fasi sia negativo e/o il Candidato non corrisponda la quota prevista dal tariffario, CEPAS interrompe il processo di valutazione e informa il Candidato che decide quindi se proseguire o meno nell'iter di passaggio di registro. Per procedere nell'iter sarà necessario prima risolvere le carenze riscontrate nella singola fase, nei tempi indicati da CEPAS.

CEPAS infine provvederà all'aggiornamento dei relativi registri e all'emissione del nuovo certificato e timbro, chiedendo la restituzione di quelli superati. Il passaggio di Registro non comporta la variazione della data di scadenza triennale.